**Antoine Chambert-Loir**

# ALGÈBRE COMMUTATIVE

*Antoine Chambert-Loir*
Centre de Mathématiques, École polytechnique, 91128 Palaiseau Cedex.
*E-mail : chambert@math.polytechnique.fr*

*Version du 29 novembre 2001, 16h51*
*Ce cours est le polycopié d'un cours enseigné par correspondance à l'université Pierre et Marie Curie (Paris 6) pendant l'année scolaire 2000-2001.*
*La version la plus à jour est disponible sur le Web à l'adresse http://www.polytechnique.fr/~chambert/teach/algcom.pdf*

# ALGÈBRE COMMUTATIVE

**Antoine Chambert-Loir**

# Table des matières

# Présentation

Le cœur de l'algèbre commutative est la notion d'anneau (commutatif unitaire) qui est la structure algébrique correspondant aux concepts collégiens d'addition, de soustraction et de multiplication. Par là, elle a deux grands champs d'application :

– l'arithmétique, via diverses notions comme la divisibilité, les idéaux, les nombres premiers, la réduction modulo un nombre premier, etc. ;

– la géométrie (algébrique) qui étudie les parties de $\mathbf{C}^n$ définies par des équations polynômiales.

Cependant, elle permet aussi de réinterpréter des structures précédemment étudiées au cours du cursus universitaire. Par exemple, la théorie des modules sur un anneau principal fournit à la fois

– un théorème de structure pour les groupes abéliens finis à savoir que pour tout groupe abélien fini G, il existe une unique suite d'entiers $(d_1, \dots, d_r)$ tels que $d_1$ divise $d_2$...qui divise $d_r$ tel que $\mathrm{G} = (\mathbf{Z}/d_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/d_r\mathbf{Z})$.

– une condition nécessaire et suffisante *calculable* pour savoir si deux matrices de $\mathrm{M}_n(\mathbf{R})$ sont semblables.

Ce cours est constitué d'une quinzaine de chapitres. Chaque chapitre sauf le premier contient

– des énoncés (propositions, théorèmes) ;

– leur démonstration ;

– des exercices dans le corps du texte dont la solution n'est pas donnée : elle se trouve d'une façon ou d'une autre dans l'énoncé ou dans la démonstration d'un résultat du cours. L'étudiant ayant appris convenablement le cours est censé être en mesure de les résoudre sans effort notable ;

– un paragraphe d'exercices (entre 5 et 10), et leur solution au paragraphe suivant. Ces exercices constituent les feuilles de TD et doivent être cherchés. D'abord sans l'aide de la correction pendant un temps raisonnable (ne pas déclarer forfait avant au moins une heure), puis avec la correction

Les énoncés et leurs démonstrations doivent être sus, les exercices assimilés.

**Plan provisoire**

1. Définitions ;
2. Anneaux, idéaux ;
3. Anneaux quotients, localisation ;
4. Idéaux premiers, maximaux. Le théorème des zéros de Hilbert ;
5. Anneaux principaux, anneaux factoriels. Le théorème de Bézout ;
6. Modules. Modules quotients, localisation ;
7. Produit tensoriel ;
8. Algèbre homologique ;
9. Modules de type fini. Anneaux noethériens ;
10. Modules de type fini sur un anneau principal ;
11. Éléments entiers, algébriques. Degré de transcendance ;
12. Modules simples, longueur. Anneaux et modules artiniens ;
13. Algèbres de type fini sur un corps.

# 1 Définitions

*Dans ce chapitre, nous regroupons la plupart des définitions importantes. Il est important de les apprendre tout de suite, même si certaines structures ne seront pas étudiées avant plusieurs chapitres. Les manier dès le début du cours fournit cependant un langage commode à l'algébriste et permet d'aborder des exemples plus intéressants.*

## 1.1. Groupe

Un *groupe* est un ensemble G muni d'une opération interne $(g, g') \mapsto g * g'$ vérifiant les propriétés suivantes :

– il existe un élément $e \in \mathrm{G}$ tel que pour tout $g \in \mathrm{G}$, $e*g = g*e = g$ (existence d'un *élément neutre*) ;

– pour tout $g \in \mathrm{G}$, il existe $g' \in \mathrm{G}$ tel que $g * g' = g' * g = e$ (existence d'un *inverse*) ;

– pour tous $g$, $g'$, $g''$ dans G, on a $g * (g' * g'') = (g * g') * g''$ (*associativité*).

De nombreuses autres notations existent pour la loi interne : outre $*$, citons $\cdot$, $\times$, $+$, $\bullet$, $*$, ., etc. Quand il ne peut pas y avoir de confusion, il est souvent courant de ne pas mettre de symbole et de noter tout simplement $gg'$ le *produit* de deux éléments $g$ et $g'$ d'un groupe G. Surtout quand la loi est noté $\cdot$, l'inverse d'un élément $g$ est noté $g^{-1}$.

L'élément neutre peut aussi être noté $e_{\mathrm{G}}$ (s'il y a plusieurs groupes), 1, ou $1_{\mathrm{G}}$, ou 0 (ou $0_{\mathrm{G}}$) si la loi est notée $+$.

Comme *exemples de groupes*, citons le groupe $\mathfrak{S}_n$ des permutations de l'ensemble $\{1, \ldots, n\}$ (la loi est la composition), le groupe $\mathbf{Z}$ des entiers relatifs (pour l'addition), l'ensemble des réels non nuls (pour la multiplication), tout espace vectoriel (pour l'addition), l'ensemble des matrices $n \times n$ inversibles (pour la multiplication), l'ensemble des matrices $n \times n$ orthogonales (encore pour la multiplication).

Si G et H sont deux groupes, un *homomorphisme de groupes* $f : \mathrm{G} \to \mathrm{H}$ est une application $f$ telle que $f(gg') = f(g)f(g')$ pour tous $g$ et $g'$ dans G. Si $f : \mathrm{G} \to \mathrm{H}$ est un homomorphisme, on a $f(e_\mathrm{G}) = e_\mathrm{H}$ et pour tout $g \in \mathrm{G}$, $f(g^{-1}) = f(g)^{-1}$.

## 1.2. Groupes abéliens

On dit qu'un groupe G est abélien si sa loi est commutative, c'est-à-dire si pour tous $g$ et $g' \in \mathrm{G}$, on a $g * g' = g' * g$. Dans ce cas, on note souvent la loi $+$, $-g$ l'inverse d'un élément $g$ et 0 ou $0_\mathrm{G}$ l'élément neutre ; on l'appelle *addition*.

## 1.3. Anneaux

Un *anneau* est un groupe abélien A noté additivement muni d'une opération de *multiplication* $(a, b) \mapsto ab$ et d'un élément 1 tel que pour tous $a$, $b$, $c$ dans A, on ait

– associativité : $a(bc) = (ab)c$ ;
– commutativité : $ab = ba$ ;
– élément neutre : $1a = a$ ;
– distributivité : $a(b + c) = ab + ac$.

Les anneaux ainsi définis sont *commutatifs* et *unitaires*. On rencontre aussi des anneaux non commutatifs dans lequel la relation de commutativité n'est pas imposée ; il faut alors renforcer la propriété de l'élément neutre en imposant à 1 d'être un élément neutre à la fois à droite et à gauche : $1a = a1 = a$, ainsi que la propriété de distributivité en rajoutant l'axiome $(a+b)c = ac+bc$. Toutefois, sauf précision supplémentaire, les anneaux seront toujours supposés commutatifs.

Comme exemples d'anneaux, citons l'anneau $\mathbf{Z}$ des entiers relatifs, mais aussi les *corps* $\mathbf{Q}$ des nombres rationnels, $\mathbf{R}$ des nombres réels, etc. Citons aussi l'anneau $\mathbf{R}[\mathrm{X}]$ des polynômes en une indéterminée à coefficients réels et les anneaux $\mathrm{C}^k(\mathrm{I}, \mathbf{R})$ des fonctions $k$-fois continûment dérivables d'un intervalle I de $\mathbf{R}$ à valeurs dans $\mathbf{R}$. Dans ce dernier cas, le fait que la loi soit bien définie revient à l'énoncé bien connu selon lequel la somme et le produit de fonctions $k$-fois continûment dérivables le sont aussi. Un exemple d'anneau non commutatif est fourni par l'ensemble des matrices $n \times n$ à coefficients dans un anneau A quelconque, par exemple $\mathrm{M}_n(\mathbf{R})$.

Soit $a$ un élément d'un anneau A. S'il existe $b \in \mathrm{A}$ tel que $ab = 1$, on dit que $a$ est *inversible*. L'ensemble des éléments inversibles de A forme un groupe pour la multiplication, d'élément neutre 1.

Si A et B sont deux anneaux, un homomorphisme d'anneaux de A dans B est une application $f : \mathrm{A} \to \mathrm{B}$ telle que l'on ait pour tous $a$ et $a' \in \mathrm{A}$,

– $f(0_\mathrm{A}) = 0_\mathrm{A}$, $f(1_\mathrm{A}) = 1_\mathrm{B}$ ;

– $f(a+a') = f(a) + f(a')$ ;
– $f(aa') = f(a)f(a')$.

### 1.4. Corps

Un *corps* est un anneau non nul dans lequel tout élément non nul est inversible.

Les corps que l'on rencontre le plus fréquemment sont les nombres rationnels **Q**, les nombres réels **R** et les nombres complexes **C**. Citons aussi les corps des fractions rationnelles à coefficients réels ou complexes, $\mathbf{R}(\mathrm{X})$ et $\mathbf{C}(\mathrm{X})$.

### 1.5. Espaces vectoriels

Un *espace vectoriel* sur un corps $k$ (dit aussi $k$-espace vectoriel) est un groupe abélien V, noté additivement, muni d'une loi $k \times \mathrm{V} \to \mathrm{V}$, produit externe, noté multiplicativement, vérifiant les propriétés suivantes : pour tous $a$ et $b$ dans $k$ et pour tous $v$ et $w$ dans V, on a
– $1v = v$ ;
– associativité : $(ab)v = a(bv)$ ;
– distributivité : $(a+b)v = av + bv$ et $a(v+w) = av + aw$.

### 1.6. Algèbres

Soit $k$ un anneau. Une *$k$-algèbre* est un anneau A muni d'un homomorphisme d'anneaux $k \to \mathrm{A}$. Cet homomorphisme n'est pas forcément injectif ; lorsqu'il l'est, on peut identifier $k$ à son image $f(k)$ par $f$, qui est un sous-anneau de A.

Donnons quelques exemples : **C** est une **R**-algèbre (le morphisme $\mathbf{R} \to \mathbf{C}$ est l'inclusion évidente) ; l'anneau des polynômes $\mathbf{R}[\mathrm{X}]$ en une variable est aussi une **R**-algèbre.

### 1.7. Polynômes

Soit $k$ un anneau et $n$ un entier naturel, $n \geq 1$. L'*anneau des polynômes* en $n$ indéterminées (ou variables) $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est défini de la façon suivante. Un monôme est une expression de la forme

$$\lambda \mathrm{X}_1^{m_1} \ldots \mathrm{X}_n^{m_n}$$

où $\lambda \in k$ et $m_1, \ldots, m_n$ sont des entiers $\geq 0$. Un polynôme est une somme d'un nombre fini de monômes. L'addition et la multiplication s'effectuent « comme on l'imagine ».

Si l'on ne veut pas se contenter de cette définition imprécise, on peut considérer l'ensemble $k^{(\mathbf{N}^n)}$ des familles presque nulles d'éléments de $k$ indexées par

l'ensemble $\mathbf{N}^n$ des $n$-uplets d'entiers positifs ou nuls. Sur cet ensemble, on définit deux lois $+$ et $\cdot$ comme suit. Soit $\lambda = (\lambda_{\mathbf{m}})_{\mathbf{m}\in\mathbf{N}^n}$ et $\lambda' = (\lambda'_{\mathbf{m}})_{\mathbf{m}\in\mathbf{N}^m}$ deux éléments de $k^{(\mathbf{N}^n)}$, on pose

$$\lambda + \lambda' = (\lambda_{\mathbf{m}} + \lambda'_{\mathbf{m}})_{\mathbf{m}\in\mathbf{N}^m}$$

et

$$\lambda \cdot \lambda' = \mu, \quad \mu_{\mathbf{m}} = \sum_{\substack{\mathbf{i},\mathbf{i}'\in\mathbf{N}^n \\ \mathbf{i}+\mathbf{i}'=\mathbf{m}}} \lambda_{\mathbf{i}}\lambda'_{\mathbf{i}'}.$$

Il faut vérifier que ces formules ont un sens, c'est-à-dire que toutes les sommes sont finies. On définit aussi 0 la famille identiquement nulle, 1 la famille telle que $1_{\mathbf{m}} = 0$ pour $\mathbf{m} \neq 0$ et $1_{\mathbf{0}} = 1$. On définit aussi, si $i \in \{1, \ldots, n\}$, $\mathrm{X}_i$ comme la famille identiquement nulle excepté pour l'indice $(0, \ldots, 1, \ldots, 0)$, le 1 étant en position $i$, où la valeur est 1. On peut vérifier que cette construction définit un anneau, noté $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, et même une *k-algèbre*, via l'homomorphisme $k \to k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ tel que $\lambda \mapsto \lambda 1$.

## 1.8. Modules

Si A est un anneau, un A-*module* est un groupe abélien M muni d'une loi externe $\mathrm{A} \times \mathrm{M} \to \mathrm{M}$ qui vérifie exactement les mêmes axiomes que ceux d'un espace vectoriel : pour tous $m$ et $m'$ dans M et pour tous $a$ et $b$ dans A, on a

- $1m = m$ ;
- associativité : $(ab)m = a(bm)$ ;
- distributivité : $(a + b)m = am + bm$ et $a(m + m') = am + am'$.

Un homomorphisme de A-modules $f : \mathrm{M} \to \mathrm{N}$ est une application telle que pour tous $m$ et $m'$ dans M et pour tous $a \in \mathrm{A}$, on ait :

- $f(m + m') = f(m) + f(m')$ ;
- $f(am) = af(m)$.

(C'est l'analogue pour les modules des applications linéaires entre espaces vectoriels.)

## 1.9. Catégories

Lorsqu'on manipule un grand nombre de structures algébriques, le langage des *catégories* est utile. Leur introduction rigoureuse nécessite des précautions importantes en théorie des ensembles que nous passons sous silence ici.

Une *catégorie* $\mathfrak{C}$ est la donnée d'une collection $\mathrm{ob}\,\mathfrak{C}$, appelée *objets* de $\mathfrak{C}$, et pour tout couple $(\mathrm{A}, \mathrm{B})$ d'objets, d'un ensemble $\mathrm{Hom}_{\mathfrak{C}}(\mathrm{A}, \mathrm{B})$ dont les éléments sont appelés morphismes de A dans B. Si A, B et C sont trois objets de $\mathfrak{C}$, on

dispose d'une application de *composition des morphismes*

$$\mathrm{Hom}_{\mathfrak{C}}(\mathrm{B},\mathrm{C}) \times \mathrm{Hom}_{\mathfrak{C}}(\mathrm{A},\mathrm{B}) \to \mathrm{Hom}_{\mathfrak{C}}(\mathrm{A},\mathrm{C}), \qquad (f,g) \mapsto f \circ g.$$

Si A est un objet de $\mathfrak{C}$, on suppose aussi donné un morphisme *identité* $\mathrm{Id}_{\mathrm{A}} \in \mathrm{Hom}_{\mathfrak{C}}(\mathrm{A},\mathrm{A})$. On demande enfin que soient vérifiés les axiomes :

– pour tout $f \in \mathrm{Hom}_{\mathfrak{C}}(\mathrm{A},\mathrm{B})$, $f \circ \mathrm{Id}_{\mathrm{A}} = \mathrm{Id}_{\mathrm{B}} \circ f = f$ ;

– pour tous $f \in \mathrm{Hom}_{\mathfrak{C}}(\mathrm{C},\mathrm{D})$, $g \in \mathrm{Hom}_{\mathfrak{C}}(\mathrm{B},\mathrm{C})$, $h \in \mathrm{Hom}_{\mathfrak{C}}(\mathrm{A},\mathrm{B})$, on a $f \circ (g \circ h) = (f \circ g) \circ h$ (associativité de la composition).

On note aussi $f : \mathrm{A} \to \mathrm{B}$ au lieu de $f \in \mathrm{Hom}_{\mathfrak{C}}(\mathrm{A},\mathrm{B})$.

Les structures introduites plus haut donnent lieu à des catégories : les catégories $\mathfrak{Gr}$ des groupes, $\mathfrak{AbGr}$ des groupes abéliens, $\mathfrak{Ann}$ des anneaux, $\mathfrak{Corps}$ des corps, $\mathfrak{Ev}_k$ des $k$-espaces vectoriels, $\mathfrak{Alg}_k$ des $k$-algèbres, $\mathfrak{Mod}_k$ des $k$-modules.

## 1.10. Foncteurs

Si $\mathfrak{C}$ et $\mathfrak{C}'$ sont deux catégories, un *foncteur* $\mathrm{F} : \mathfrak{C} \to \mathfrak{C}'$ est la donnée :

– pour tout objet $\mathrm{A} \in \mathrm{ob}\,\mathfrak{C}$, d'un objet $\mathrm{F}(\mathrm{A}) \in \mathrm{ob}\,\mathfrak{C}'$ ;

– pour tout morphisme $f \in \mathrm{Hom}_{\mathfrak{C}}(\mathrm{A},\mathrm{B})$, d'un morphisme $\mathrm{F}(f) \in \mathrm{Hom}_{\mathfrak{C}'}(\mathrm{F}(\mathrm{A}),\mathrm{F}(\mathrm{B}))$

de sorte que soient vérifiées les propriétés suivantes :

$$\mathrm{F}(\mathrm{Id}_{\mathrm{A}}) = \mathrm{Id}_{\mathrm{F}(\mathrm{A})} \quad \text{et} \quad \mathrm{F}(f) \circ \mathrm{F}(g) = \mathrm{F}(f \circ g).$$

Un tel foncteur est aussi appelé *foncteur covariant*. Il existe aussi des *foncteurs contravariants* qui changent le sens des flèches : si $f : \mathrm{A} \to \mathrm{B}$, $\mathrm{F}(f)$ est un morphisme $\mathrm{F}(\mathrm{B}) \to \mathrm{F}(\mathrm{A})$ et $\mathrm{F}(f \circ g) = \mathrm{F}(g) \circ \mathrm{F}(f)$.

Les foncteurs suivants sont appelés *foncteurs d'oubli* car ils consistent à oublier une partie de la structure d'un objet algébrique. Ils envoient un objet sur le même objet de la structure plus pauvre, un morphisme sur le même morphisme.

– $\mathfrak{AbGr} \to \mathfrak{Gr}$ : un groupe abélien est un groupe ;

– $\mathfrak{AbGr} \to \mathfrak{AbGr}$, $\mathfrak{Ev}_k \to \mathfrak{AbGr}$ : un anneau, un espace vectoriel sont des groupes abéliens ;

– $\mathfrak{Corps} \to \mathfrak{Ann}$, $\mathfrak{Alg}_k \to \mathfrak{Ann}$ : un corps, une $k$-algèbre sont aussi des anneaux.

Il existe aussi des foncteurs plus subtils, comme le foncteur $\mathfrak{Ann} \to \mathfrak{AbGr}$ qui associe à un anneau A le groupe multiplicatif $\mathrm{A}^\times$ des éléments inversibles de A.

## 1.11. Relations d'ordre

Une *relation d'ordre* sur un ensemble X est une relation $\leq$ vérifiant les axiomes

– $x \leq x$ ;

– si $x \leq y$ et $y \leq z$, alors $x \leq z$ ;

– si $x \leq y$ et $y \leq x$, alors $x = y$.

Si $\leq$ est une relation d'ordre, on définit la relation $\geq$ comme $x \leq y$ si et seulement si $y \geq x$.

Comme exemples, citons la relation d'ordre usuelle sur les réels et la divisibilité sur les entiers naturels non nuls. Citons aussi la relation d'inclusion sur les parties d'un ensemble.

Un ordre $\leq$ sur X est dit *total* si pour tout couple $(x, y)$ d'éléments de X, ou bien $x \leq y$, ou bien $y \leq x$.

Dans un ensemble ordonné $(\mathrm{X}, \leq)$, un élément *maximal* est un élément $x$ tel qu'il n'existe pas de $y \in \mathrm{X}$, $y \neq x$ vérifiant $y \geq x$. Un *plus grand élément* est un élément $x$ tel que pour tout $y \in \mathrm{X}$, $y \leq x$. Attention, lorsque la relation d'ordre n'est pas totale, ces deux notions sont distinctes.

On utilisera à plusieurs reprises le *lemme de Zorn*. C'est un résultat de logique, équivalent à l'axiome du choix, dont l'intérêt est d'impliquer l'existence de nombreux objets intéressants en mathématiques : bases et supplémentaires en théorie des espaces vectoriels, clôture algébrique d'un corps, idéaux maximaux d'un anneau, le théorème de Hahn–Banach en analyse fonctionnelle, etc. Il implique aussi l'existence de nombreux objets pathologiques tels des ensembles non mesurables ou — c'est le paradoxe de Banach–Tarski — deux partitions de la sphère $\mathrm{S}^2 \subset \mathbf{R}^3$ de la forme $\mathrm{S}^2 \sqcup_{i \in \mathrm{I}} \mathrm{X}_i = \sqcup_{i \in \mathrm{I}} (\mathrm{Y}_i \sqcup \mathrm{Z}_i)$ tel que pour tout $i$, $\mathrm{X}_i$, $\mathrm{Y}_i$ et $\mathrm{Z}_i$ soient images l'un de l'autre par un déplacement. C'est pourquoi certains mathématiciens le rejettent.

LEMME 1.11.1 (Zorn). — *Soit* $(\mathrm{X}, \leq)$ *un ensemble ordonné vérifiant la propriété suivante : toute partie de* X *totalement ordonnée admet un majorant dans* X *(on dit que* X *est* inductif*). Alors,* X *admet un élément maximal.*

# 2 Anneaux, idéaux, algèbres

*Ce chapitre introduit les notions d'anneaux et d'idéaux. Ces deux notions formalisent les méthodes de calcul bien connues avec les nombres entiers : on dispose d'une addition, d'une multiplication, de deux symboles* $0$ *et* $1$ *et des règles de calcul usuelles.*

## 2.1. Premières propriétés

DÉFINITION 2.1.1. — *On appelle anneau un groupe abélien* $\mathrm{A}$ *noté additivement muni d'une loi de multiplication* $\mathrm{A} \times \mathrm{A} \to \mathrm{A}$, $(a, b) \mapsto ab$ *vérifiant les propriétés suivantes :*

– *il existe un élément* $1 \in \mathrm{A}$ *tel que pour tout* $a \in \mathrm{A}$, $1a = a$ *(élément neutre pour la multiplication) ;*

– *pour tous* $a$ *et* $b$ *dans* $\mathrm{A}$, $ab = ba$ *(commutativité) ;*

– *pour tous* $a$, $b$ *et* $c$ *dans* $\mathrm{A}$, $a(b + c) = ab + ac$ *(distributivité).*

Les axiomes ci-dessous permettent un calcul analogue à celui dont on a l'habitude dans les entiers. Si $a$ est un élément d'un anneau A et si $n$ est un entier positif ou nul, on définit $a^n$ par récurrence en posant $a^0 = 1$ et, si $n \geq 1$, $a^n = a(a^{n-1})$.

On peut déduire de ces axiomes des propriétés familières.

*Exercice 2.1.2.* — a) Démontrer que pour tout $a \in \mathrm{A}$, $0a = 0$ (on dit que $0$ est *absorbant* pour la multiplication).

b) Si $e \in \mathrm{A}$ est un élément tel que pour tout $a \in \mathrm{A}$, $ea = a$, alors $e = 1$ (unicité de l'élément neutre pour la multiplication).

c) Pour tout $a \in \mathrm{A}$, on a $(-1)a = -a$.

d) Si $1 = 0$ dans A, alors $\mathrm{A} = \{0\}$. On dit que A est l'anneau nul.

e) Pour tout $a \in \mathrm{A}$ et pour tous entiers $m$, $n \geq 0$, on a $a^{m+n} = a^m a^n$.

f) La *formule du binôme* est valide : si $a$ et $b \in \mathrm{A}$ et $n \geq 0$, on a

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

Certains éléments d'un anneau ont des propriétés particulières intéressantes par rapport à la multiplication, ce qui justifie quelques définitions.

DÉFINITION 2.1.3. — *Soit* A *un anneau et soit $a$ un élément de* A.

*On dit que $a$ est* inversible, *ou que $a$ est une* unité *de* A, *s'il existe $b \in \mathrm{A}$ tel que $ab = 1$. Un tel $b$ est nécessairement unique, c'est l'*inverse *de $a$ ; on le note souvent $a^{-1}$.*

*On dit que $a$ est* diviseur de zéro *s'il existe $b \in \mathrm{A}$, $b \neq 0$ tel que $ab = 0$. On dit que $a$ est* simplifiable *s'il n'est pas diviseur de zéro, c'est-à-dire si la relation $ab = 0$ abec $b \in \mathrm{A}$ implique $b = 0$.*

*On dit enfin que $a$ est nilpotent s'il existe $n \geq 1$ tel que $a^n = 0$.*

PROPOSITION 2.1.4. — *L'ensemble des éléments inversibles d'un anneau* A *est un groupe pour la multiplication. On le note* $\mathrm{A}^\times$ *; c'est le* groupe des unités *de* A.

*Démonstration.* — Soit $a$ et $b$ deux éléments de A, d'inverses $a^{-1}$ et $b^{-1}$. Alors, $(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1}) = 1$, si bien que $ab$ est inversible d'inverse $a^{-1}b^{-1}$. La multiplication de A définit ainsi une loi interne sur $\mathrm{A}^\times$. De plus, 1 est inversible et est un élément neutre pour cette loi. Enfin, si $a \in \mathrm{A}^\times$, son inverse pour cette loi n'est autre que $a^{-1}$. Ainsi, $\mathrm{A}^\times$ est un groupe pour la multiplication. □

*Exercice 2.1.5.* — Soit A un anneau.

a) Soit $x \in \mathrm{A}$ un élément nilpotent. Si $n \geq 0$ est tel que $x^{n+1} = 0$, calculer $(1+x)(1-x+x^2-\cdots+(-1)^n x^n)$. En déduire que $1+x$ est inversible dans A.

b) Soit $x \in \mathrm{A}$ un élément inversible et $y \in \mathrm{A}$ un élément nilpotent, montrer que $x+y$ est inversible.

c) Si $x$ et $y$ sont deux éléments nilpotents de A, montrer que $x+y$ est nilpotent. (Si $n$ et $m$ sont deux entiers tels que $x^{n+1} = y^{m+1} = 0$, on utilisera la formule du binôme pour calculer $(x+y)^{n+m+1}$.)

Encore un peu de terminologie :

DÉFINITION 2.1.6. — *Soit* A *un anneau non nul.*

*On dit que* A *est* intègre *s'il n'a pas de diviseur de zéro autre que* 0 *(autrement dit, si tout élémément non nul est simplifiable).*

*On dit que* A *est* réduit *si* 0 *est le seul élément nilpotent de* A.

*On dit que* A *est un* corps *si tout élément non nul de* A *est inversible.*

En particulier, *l'anneau nul n'est ni intègre ni réduit.*

*Exercice 2.1.7.* — Soit A un anneau fini intègre. Alors, A est un corps.

*Solution.* — Soit $a$ un élément non nul de A. On doit prouver que $a$ est inversible dans A. Soit $\varphi\colon \mathrm{A} \to \mathrm{A}$ l'application telle que $\varphi(b) = ab$. Alors, $\varphi$ est injective : si $\varphi(b) = \varphi(b')$, on a $ab = ab'$, donc $a(b-b') = 0$. Comme A est intègre et $a \neq 0$, $b - b' = 0$. Par suite, le cardinal de $\varphi(\mathrm{A})$ est égal au cardinal de A. Comme $\varphi(\mathrm{A})$ est une partie de A, $\varphi(\mathrm{A}) = \mathrm{A}$. Ainsi, $\varphi$ est surjectif et il existe $b \in \mathrm{A}$ tel que $ab = 1$. □

*Exemple 2.1.8.* — Soit A un anneau intègre. L'anneau A[X] des polynômes en une indéterminée à coefficients dans A est intègre.

Avant de démontrer ce fait, rappelons que l'on dispose d'une fonction *degré* sur l'anneau A[X] : un polynôme non nul $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ peut s'écrire $\sum_{k=0}^{n} a_k \mathrm{X}^k$ avec $a_n \neq 0$ pour un unique entier $n \geq 0$ ; on pose alors $\deg \mathrm{P} = n$. Par convention, on pose $\deg(0) = -\infty$. De plus, si P et Q sont des polynômes de A[X], on a $\deg(\mathrm{P}+\mathrm{Q}) \leq \max(\deg \mathrm{P}, \deg \mathrm{Q})$ et $\deg(\mathrm{PQ}) \leq \deg \mathrm{P} + \deg \mathrm{Q}$ (ces formules sont vraies même si P, Q, P + Q ou PQ est nul, avec les conventions naturelles $\max(-\infty, x) = -\infty$ et $-\infty + x = -\infty$ pour tout $x \in \mathbf{N} \cup \{-\infty\}$).

*Démonstration.* — Si P et Q sont deux polynômes non nuls, on veut prouver que $\mathrm{PQ} \neq 0$. On peut écrire

$$\mathrm{P} = \sum_{k=0}^{\deg \mathrm{P}} a_k \mathrm{X}^k \quad \text{et} \quad \mathrm{Q} = \sum_{k=0}^{\deg \mathrm{Q}} b_k \mathrm{X}^k$$

avec $a_{\deg \mathrm{P}} \neq 0$ et $b_{\deg \mathrm{Q}} \neq 0$. Alors,

$$\mathrm{PQ} = \sum_{k=0}^{\deg \mathrm{P} + \deg \mathrm{Q}} \left( \sum_{m=0}^{\min(\deg \mathrm{P}, k)} a_m b_{k-m} \right) \mathrm{X}^k.$$

En particulier, le terme de degré $\deg \mathrm{P} + \deg \mathrm{Q}$ a pour coefficient $a_{\deg \mathrm{P}} b_{\deg \mathrm{Q}}$. Comme A est intègre, ce coefficient est non nul et $\mathrm{PQ} \neq 0$. □

Le raisonnement ci-dessus montre donc que si P et Q sont deux polynômes à coefficients dans un anneau intègre, $\deg(\mathrm{PQ}) = \deg \mathrm{P} + \deg \mathrm{Q}$. La notion de degré d'un polynôme intervient aussi dans le théorème de division euclidienne :

THÉORÈME 2.1.9. — *Soit* A *un anneau et soit* P *et* Q *deux polynômes de* A[X]. *On suppose que* $\mathrm{Q} \neq 0$ *et que le coefficient du terme de plus haut degré de* Q *est inversible*[(1)]. *Alors, il existe un unique couple de polynômes* (R, S) *dans* A[X] *vérifiant les propriétés*

- $\mathrm{P} = \mathrm{RQ} + \mathrm{S}$ ;
- $\deg \mathrm{S} < \deg \mathrm{Q}$.

[(1)] Un tel polynôme est appelé *unitaire*

*Démonstration.* — On commence par l'unicité. Si $P = RQ + S = R'Q + S'$, alors $Q(R' - R) = S' - S$ est de degré au plus $\max(\deg S, \deg S') < \deg Q$. Supposons $R \neq R'$, c'est-à-dire $R' - R \neq 0$. Alors, si $uX^{\deg Q}$ et $aX^m$ sont les termes de plus haut degré dans Q et $R' - R$ respectivement, le terme de plus haut degré dans $Q(R' - R)$ est donné par $auX^{m+\deg Q}$. Comme $u$ est inversible et $a \neq 0$, $au \neq 0$. Ainsi, $Q(R' - R)$ est de degré $m + \deg Q \geq \deg Q$. Cette contradiction montre que $R = R'$, puis $S = P - RQ = P - R'Q = S'$.

Montrons maintenant l'existence du couple $(R, S)$ comme dans le théorème. Notons toujours $uX^{\deg Q}$ le terme de plus haut degré de Q. On raisonne par récurrence sur le degré de P. Si $\deg P < \deg Q$, il suffit de poser $R = 0$ et $S = P$. Sinon, soit $aX^{\deg P}$ le terme de plus haut degré de P. Alors, $P' = P - au^{-1}X^{\deg P - \deg Q}Q$ est un polynôme de degré au plus $\deg P$ mais dont le coefficient du terme de degré $\deg P$ est égal à $a - au^{-1}u = 0$. Ainsi, $\deg P' < \deg P$. Par récurrence, il existe deux polynômes $R'$ et $S'$ dans $A[X]$ tels que

$$P' = R'Q + S' \quad \text{et} \quad \deg S' < \deg Q.$$

Alors, on a

$$P = P' + au^{-1}X^{\deg P - \deg Q}Q = (R' + au^{-1}X^{\deg P - \deg Q})Q + S'.$$

Il suffit maintenant de poser $R = R' + au^{-1}X^{\deg P - \deg Q}$ et $S' = S$. Le théorème est donc démontré. □

L'exercice suivant munit le produit de deux anneaux d'une structure d'anneau et en étudie quelques propriétés. Un *sous-anneau* B d'un anneau A est un sous-groupe de A pour l'addition qui contient 1 et est stable par la multiplication.

*Exercice 2.1.10* (Anneau produit). — 1) Soit A et B deux anneaux. On munit le groupe abélien $A \times B$ d'une loi interne en définissant pour $a$ et $a' \in A$, $b$ et $b' \in B$, $(a, b) \cdot (a', b') = (aa', bb')$.

a) Montrer que cette loi confère à $A \times B$ une structure d'anneau. Quel est l'élément neutre pour la multiplication ?

b) L'anneau A et B est-il intègre ? Quels sont ses éléments nilpotents ?

c) Montrer que les éléments $e = (1, 0)$ et $f = (0, 1)$ de $A \times B$ vérifient $e^2 = e$ et $f^2 = f$. On dit que ce sont des *idempotents*.

2) Soit A un anneau et $e \in A$ un idempotent.

a) Montrer que $1 - e$ est un idempotent de A.

b) Montrer que $eA = \{ea\,;\, a \in A\}$ est un sous-anneau de A.

c) Montrer que $A \simeq eA \times (1 - e)A$.[(2)]

[(2)] Le symbole $\simeq$ signifie « isomorphe ». Cette notion d'isomorphisme est définie un peu plus loin.

## 2.2. Idéaux

DÉFINITION 2.2.1. — *On appelle* idéal *d'un anneau* A *tout sous-groupe* $\mathrm{I} \subset \mathrm{A}$ *tel que pour tout* $a \in \mathrm{A}$ *et tout* $b \in \mathrm{I}$, $ab \in \mathrm{I}$.

Autrement dit, un idéal d'un anneau A est un sous-A-module de A (vu comme A-module sur lui-même). Remarquons aussi que 0 et A sont des idéaux de A. Une autre conséquence de la définition est que pour toute famille presque nulle $(a_s)_{s\in\mathrm{S}}$ d'éléments d'un idéal I, la somme $\sum_s a_s$ est encore un élément de I.

Comme $-1$ est un élément de A, pour prouver qu'une partie I de A est un idéal, il suffit d'établir les faits suivants :
- $0 \in \mathrm{I}$ ;
- si $a \in \mathrm{I}$ et $b \in \mathrm{I}$, $a + b \in \mathrm{I}$ ;
- si $a \in \mathrm{A}$ et $b \in \mathrm{I}$, $ab \in \mathrm{I}$.

*Exemple 2.2.2.* — Si A est un anneau et $x \in \mathrm{A}$, l'ensemble $(x) = \{ax\,;\, a \in \mathrm{A}\}$ est un idéal de A. Un tel idéal est dit *principal*.

*Exemple 2.2.3.* — *Si* K *est un corps, les seuls idéaux de* K *sont* $(0)$ *et* K. En effet, soit I un idéal de K distinct de 0 et soit $a$ un élément non nul de I. Soit $b$ un élément de K. Comme $a \neq 0$, on peut considérer l'élément $b/a$ de K et par définition d'un idéal $(b/a)a \in \mathrm{I}$. On a donc $b \in \mathrm{I}$, d'où $\mathrm{I} = \mathrm{K}$.

DÉFINITION 2.2.4. — *On dit que deux éléments* $a$ *et* $b$ *d'un anneau* A *sont* associés *s'il existe un élément inversible* $u \in \mathrm{A}^\times$ *tel que* $a = bu$.

La relation « être associé » est une relation d'équivalence.

*Exercice 2.2.5.* — Soit A un anneau et soit $a$, $b$ deux éléments de A. S'ils sont associés, montrer que les idéaux $(a)$ et $(b)$ sont égaux. Réciproquement, si A est intègre et si $(a) = (b)$, montrer que $a$ et $b$ sont associés.

*Exemple 2.2.6.* — Si I est un idéal de $\mathbf{Z}$, il existe un unique entier $n \geq 0$ tel que $\mathrm{I} = (n)$.

*Démonstration.* — Si $\mathrm{I} = (0)$, $n = 0$ convient.

Supposons maintenant $\mathrm{I} \neq (0)$. Si $\mathrm{I} = (n)$, on constate que les éléments strictement positifs de I sont $\{n; 2n; 3n; \ldots\}$ et que $n$ est le plus petit d'entre eux — ce qui montre l'unicité d'un éventuel entier $n$ comme dans l'énoncé.

Notons donc $n$ le plus petit élément de $\mathrm{I} \cap \mathbf{N}^*$. Comme $n \in \mathrm{I}$, $an \in \mathrm{I}$ pour tout $a \in \mathbf{Z}$ et $(n) \subset \mathrm{I}$. Réciproquement, soit $a$ est un élément de I. La *division euclidienne* de $a$ par $n$ s'écrit $a = qn + r$, avec $q \in \mathbf{Z}$ et $0 \leq r \leq n - 1$. Comme $a \in \mathrm{I}$ et comme $qn \in \mathrm{I}$, $r = a - qn$ appartient à I. Comme $n$ est le plus petit élément

strictement positif de I et comme $r < n$, on a nécessairement $r = 0$. Par suite, $a = qn \in (n)$ et $\mathrm{I} \subset (n)$. Ainsi, $\mathrm{I} = (n)$. □

On dispose d'un certain nombre d'opérations intéressantes sur les idéaux.

*2.2.7. Intersection.* — Si I et J sont deux idéaux de A, l'ensemble $\mathrm{I} \cap \mathrm{J}$ est encore un idéal de A. Plus généralement, l'*intersection* d'une famille (non vide) d'idéaux de A est encore un idéal de A.

*Démonstration.* — Soit $(\mathrm{I}_s)_s$ une famille d'idéaux de A et posons $\mathrm{I} = \bigcap_s \mathrm{I}_s$. L'intersection d'une famille de sous-groupes est encore un sous-groupe, donc I est un sous-groupe de A. Soit maintenant $x \in \mathrm{I}$ et $a \in \mathrm{A}$ arbitraires et montrons que $ax \in \mathrm{I}$. Pour tout $s$, $x \in \mathrm{I}_s$ et $\mathrm{I}_s$ étant un idéal, on a donc $ax \in \mathrm{I}_s$. Par suite, $ax$ appartient à tous les $\mathrm{I}_s$ donc $ax \in \mathrm{I}$. □

*2.2.8. Idéal engendré par une partie.* — Si S est une partie de A, il existe un plus petit idéal de A contenant S, noté $\langle \mathrm{S} \rangle$ et appelé *idéal engendré* par S. Cela signifie que $\langle \mathrm{S} \rangle$ est un idéal contenant S et que si I est un idéal contenant S, alors I contient déjà $\langle \mathrm{S} \rangle$. En effet, il suffit de poser

$$\langle \mathrm{S} \rangle = \bigcap_{\mathrm{S} \subset \mathrm{I} \subset \mathrm{A}} \mathrm{I}$$

où I parcourt l'ensemble (non vide) des idéaux de A contenant S. Cet ensemble est effectivement non vide car A est un idéal de A contenant S. De plus, $\langle \mathrm{S} \rangle$ est l'ensemble des combinaisons linéaires presque nulle $\sum_{s \in \mathrm{S}} a_s s$.

*Démonstration.* — Notons $\mathrm{I}_\mathrm{S}$ l'ensemble des idéaux de A qui contiennent S. Si $(a_s)$ est une famille presque nulle d'éléments de A, $\sum_{s \in \mathrm{S}} a_s s$ est un élement de tout idéal de A contenant S, donc de $\langle \mathrm{S} \rangle$, si bien que $\langle \mathrm{S} \rangle$ contient $\mathrm{I}_\mathrm{S}$.

Réciproquement, montrons que $\mathrm{I}_\mathrm{S}$ est un idéal de A. Il contient $0 = \sum_{s \in \mathrm{S}} 0s$ ; si $\sum a_s s$ et $\sum b_s s$ sont des éléments de $\mathrm{I}_\mathrm{S}$, la famille $(a_s + b_s)_{s \in \mathrm{S}}$ est une famille presque nulle d'éléments de A et $\sum (a_s + b_s)s \in \mathrm{I}_\mathrm{S}$ ; enfin, si $a \in \mathrm{A}$ et si $x = \sum a_s s \in \mathrm{I}_\mathrm{S}$, on a $ax = a(\sum a_s s) = \sum (a a_s)s \in \mathrm{I}_\mathrm{S}$ et $\mathrm{I}_\mathrm{S}$ est bien un idéal de A.

Comme $\mathrm{I}_\mathrm{S}$ contient S (si $t \in \mathrm{S}$, $t = \sum_{s \in \mathrm{S}} a_s t$ avec $a_t = 1$ et $a_s = 0$ si $s \neq t$). Par suite, $\langle \mathrm{S} \rangle$ est contenu dans $\mathrm{I}_\mathrm{S}$, d'où finalement l'égalité. □

*Exercice 2.2.9.* — Soit A un anneau.

a) Soit $x \in \mathrm{A}$. Montrer que tout idéal I de A contenant $x$ contient aussi $(x)$, de sorte que $(x)$ est le plus petit idéal de A contenant $x$.

b) Si $x_1, \dots, x_n$ sont des éléments de A, l'ensemble $(x_1, \dots, x_n) = \{a_1x_1 + \cdots + a_nx_n\,;\, a_1, \dots, a_n \in \mathrm{A}\}$ est le plus petit idéal de A contenant $x_1, \dots, x_n$.

c) Plus généralement, si $(x_i)_{i\in\mathrm{I}}$ est une famille d'éléments de A, l'ensemble des combinaisons linéaires $\sum a_i x_i$ où $(a_i)_{i\in\mathrm{I}}$ est une famille presque nulle d'éléments de A est le plus petit idéal de A contenant les $x_i$.

*2.2.10. Somme d'idéaux.* — Soit I et J deux idéaux de A. L'ensemble des sommes $a + b$ avec $a \in \mathrm{I}$ et $b \in \mathrm{J}$ est un idéal de A, noté $\mathrm{I} + \mathrm{J}$. C'est aussi l'idéal de A engendré par la partie $\mathrm{I} \cup \mathrm{J}$. Plus généralement, si $(\mathrm{I}_s)_{s\in\mathrm{S}}$ est une famille d'idéaux de A, l'ensemble des sommes (presque nulles) $\sum_s a_s$, où pour tout $s$, $a_s \in \mathrm{I}_s$, est un idéal de A noté $\sum_s \mathrm{I}_s$. C'est aussi l'idéal de A engendré par la partie $\bigcup_s \mathrm{I}_s$.

*Démonstration.* — Comme $0 = \sum_s 0$ et comme $0 \in \mathrm{I}_s$ pour tout $s$, $0 \in \sum_s \mathrm{I}_s$. Ensuite, si $a = \sum_s a_s$ et $b = \sum_s b_s$ sont deux éléments de $\sum_s \mathrm{I}_s$, on a $a + b = \sum_s (a_s + b_s)$ où pour tout $s$, $a_s + b_s \in \mathrm{I}_s$, presque tous les termes de cette somme étant nuls. Donc $a + b \in \sum_s \mathrm{I}_s$. Finalement, si $a = \sum_s a_s$ appartient à $\mathrm{I}_s$ et $b \in \mathrm{A}$, on a $ba = \sum_s (ba_s)$. Pour tout $s$, $ba_s \in \mathrm{I}_s$, donc $ba \in \sum_s \mathrm{I}_s$. Ainsi, $\sum_s \mathrm{I}_s$ est bien un idéal de A.

Pour montrer que c'est l'idéal de A engendré par la partie $\bigcup_s \mathrm{I}_s$, nous devons établir deux inclusions. Tout d'abord, si $t \in \mathrm{S}$ et $a \in \mathrm{I}_t$, on a $a = \sum_s a_s$ avec $a_s = 0$ si $s \neq t$ et $a_t = a$. Donc $a \in \sum_s \mathrm{I}_s$ et l'idéal $\sum_s \mathrm{I}_s$ contient $\mathrm{I}_t$. Par définition de l'idéal $\langle \bigcup_s \mathrm{I}_s \rangle$ (plus petit idéal qui contient la partie $\bigcup_s \mathrm{I}_s$), on a ainsi

$$\langle \bigcup_s \mathrm{I}_s \rangle \subset \sum_s \mathrm{I}_s.$$

Dans l'autre sens, si I est un idéal contenant $\bigcup_s \mathrm{I}_s$, montrons que I contient $\sum_s \mathrm{I}_s$. Soit alors $a = \sum_s a_s$ un élément de $\sum_s \mathrm{I}_s$. Tous les termes de cette somme appartiennent à I. Par définition d'un idéal, $a$ appartient à I et I contient $\sum_s \mathrm{I}_s$. □

*2.2.11. Produit d'idéaux.* — Soit I et J deux idéaux de A. L'ensemble des produits $ab$ avec $a \in \mathrm{I}$ et $b \in \mathrm{J}$ n'est pas forcément un idéal de A. L'idéal IJ est par définition l'idéal engendré par ces produits. C'est ainsi l'ensemble des combinaisons linéaires finies $\sum a_s b_s$ avec $a_s \in \mathrm{I}$ et $b_s \in \mathrm{J}$.

Proposition 2.2.12. — *Soit* A *un anneau, soit* I *et* J *deux idéaux de* A. *Alors,* $\mathrm{IJ} \subset \mathrm{I} \cap \mathrm{J}$.

*Si de plus* $I+J=A$, *auquel cas on dit que les idéaux* I *et* J *sont* comaximaux, *alors on a égalité :* $IJ = I \cap J$.

*Démonstration.* — Si $a \in I$ et $b \in J$, $ab$ appartient à I (c'est un multiple de $a \in I$) et appartient à J (c'est un multiple de $b \in J$). Donc $ab \in I \cap J$. Puisque les produits $ab$ avec $a \in I$ et $b \in J$ appartiennent à l'idéal $I \cap J$, l'idéal IJ qui est engendré par ces produits est contenu dans $I \cap J$.

Si $I+J=A$, il existe $x \in I$ et $y \in J$ tels que $x+y=1$. Soit alors $a \in I \cap J$. Écrivons

$$a = a1 = a(x+y) = ax + ay.$$

Comme $a \in I$ et $y \in J$, $ay \in IJ$ ; comme $a \in J$ et $x \in I$, $ax \in IJ$. Par suite, leur somme $ax+ay$ appartient à IJ et $a \in IJ$. Il en résulte que si I et J sont comaximaux, on a $I \cap J \subset IJ$, donc, compte-tenu de l'autre inclusion, $I \cap J = IJ$. □

*Exercice 2.2.13.* — Soit A un anneau, soit I un idéal de A et soit S une partie de A. On définit le *conducteur* de S dans I par la formule

$$J = (I : S) = \{a \in A\,;\ \text{pour tout } s \in S,\ as \in I\}.$$

Montrer que c'est un idéal de A.

*2.2.14. (Nil)radical.* — Le *nilradical* d'un anneau A est l'ensemble de ses éléments nilpotents. C'est un idéal de A.

Plus généralement, on définit le *radical* $\sqrt{I}$ de A par la formule

$$\sqrt{I} = \{a \in A\,;\ \text{il existe } n \geq 1,\ a^n \in I\}.$$

C'est un idéal de A qui contient I. Par définition même, le nilradical de A est donc égal au radical de l'idéal nul.

*Démonstration.* — Comme $0^1 = 0 \in I$, $0 \in \sqrt{I}$. Si $a \in \sqrt{I}$ et $b \in \sqrt{I}$, choisissons $n$ et $m \geq 1$ tels que $a^n \in I$ et $b^m \in I$. Alors, on a d'après la formule du binôme

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

Dans cette somme, tous les termes appartiennent à I : c'est vrai de ceux correspondant à $k \geq n$ puisque $a^k = a^n a^{n-k}$ et $a^n \in I$ ; de même, si $k \leq n$, $n+m-k \geq m$ et $b^{n+m-k} = b^m b^{n-k}$ appartient à I. On a donc $(a+b)^{n+m} \in I$, d'où $a+b \in \sqrt{I}$. Enfin, si $a \in \sqrt{I}$ et $b \in A$, choisissons $n \geq 1$ tel que $a^n \in I$. Alors, $(ba)^n = b^n a^n \in I$ et $ba \in \sqrt{I}$. □

*Exercice 2.2.15.* — Quel est le radical de l'idéal (12) dans $\mathbf{Z}$ ?

## 2.3. Morphismes

DÉFINITION 2.3.1. — *Soit* A *et* B *deux anneaux. Un* homomorphisme d'anneaux $f : \mathrm{A} \to \mathrm{B}$ *est une application vérifiant les propriétés suivantes*

- *on a* $f(0) = 0$ *et* $f(1) = 1$ *;*
- *pour tous* $a$ *et* $b$ *dans* A, *on a* $f(a+b) = f(a) + f(b)$ *et* $f(ab) = f(a)f(b)$.

Le mot *homomorphisme* est un synonyme pour morphisme. Si A est un anneau, l'application identique $\mathrm{Id}_\mathrm{A} : \mathrm{A} \to \mathrm{A}$ est un morphisme d'anneaux. La *composition* de deux morphismes d'anneaux est encore un morphisme d'anneaux. Cela permet de définir la *catégorie des anneaux.*

Conformément aux définitions de théorie des catégories, on dit qu'un morphisme d'anneaux $f : \mathrm{A} \to \mathrm{B}$ est un *isomorphisme* s'il existe un morphisme d'anneaux $g : \mathrm{B} \to \mathrm{A}$ tel que $f \circ g = \mathrm{Id}_\mathrm{B}$ et $g \circ f = \mathrm{Id}_\mathrm{A}$. Le morphisme $g$ est alors appelé morphisme réciproque de $f$. On note $f : \mathrm{A} \xrightarrow{\sim} \mathrm{B}$ pour signifier que le morphisme $f : \mathrm{A} \to \mathrm{B}$ est un isomorphisme ; si A et B sont *isomorphes*, c'est-à-dire s'il existe un isomorphisme $\mathrm{A} \xrightarrow{\sim} \mathrm{B}$, on écrit $\mathrm{A} \simeq \mathrm{B}$.

PROPOSITION 2.3.2. — *Un morphisme d'anneaux est un isomorphisme si et seulement si il est bijectif.*

*Démonstration.* — Si $f : \mathrm{A} \to \mathrm{B}$ est un isomorphisme, son morphisme réciproque est en particulier une bijection réciproque de $f$, donc $f$ est bijectif. Réciproquement, supposons que $f$ est bijectif et notons $g$ sa bijection réciproque. Il nous faut alors prouver que $g$ est un morphisme d'anneaux de B dans A.

Comme $f(0) = 0$, $g(0) = 0$. Si $a$ et $b \in \mathrm{B}$,

$$f(g(a+b)) = a + b = f(g(a)) + f(g(b)) = f(g(a) + g(b))$$

et

$$f(g(ab)) = ab = f(g(a))f(g(b)) = f(g(a)g(b)).$$

Comme $f$ est bijectif, $g(a+b) = g(a) + g(b)$ et $g(ab) = g(a)g(b)$. □

*Exercice 2.3.3.* — Soit A et B deux anneaux et $f : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux.

Si $a \in \mathrm{A}$ est inversible, montrer que $f(a)$ est inversible dans B. En déduire que la restriction de $f$ à $\mathrm{A}^\times$ définit un morphisme de groupes (noté encore $f$) $\mathrm{A}^\times \to \mathrm{B}^\times$.

PROPOSITION 2.3.4. — *Le* noyau *d'un morphisme d'anneaux* $f : \mathrm{A} \to \mathrm{B}$ *est l'ensemble des* $a \in \mathrm{A}$ *tels que* $f(a) = 0$. *C'est un* idéal *de* A *noté* $\operatorname{Ker} f$.

*Démonstration.* — Un morphisme d'anneaux étant un morphisme de groupes abéliens, $\operatorname{Ker} f$ est un sous-groupe de A. De plus, si $x \in \operatorname{Ker} f$ et si $a \in \mathrm{A}$, on a $f(ax) = f(a)f(x) = f(a)0 = 0$ donc $ax \in \operatorname{Ker} f$. Il en résulte que $\operatorname{Ker} f$ est un idéal de A. □

*2.3.5. Image, image réciproque.* — Soit $f : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux. Plus généralement, si J est un idéal de B, l'image réciproque

$$f^{-1}(\mathrm{J}) = \{a \in \mathrm{A}\,;\, f(a) \in \mathrm{J}\}$$

est un idéal de A.

*Démonstration.* — Comme $f(0) = 0 \in \mathrm{J}$, $0 \in f^{-1}(\mathrm{J})$. Si $a$ et $b \in f^{-1}(\mathrm{J})$, $f(a+b) = f(a) + f(b) \in \mathrm{J}$ puisque $f(a)$ et $f(b) \in \mathrm{J}$ et que J est un idéal de B. Enfin, si $a \in \mathrm{A}$ et $b \in f^{-1}(\mathrm{J})$, on a $f(ab) = f(a)f(b) \in \mathrm{J}$ puisque $f(b) \in \mathrm{J}$. □

En revanche, l'image d'un idéal par un morphisme d'anneaux n'est pas forcément un idéal. Si $f : \mathrm{A} \to \mathrm{B}$ est un morphisme d'anneaux et si I est un idéal de A, on notera $f(\mathrm{I})\mathrm{B}$, voire IB, l'idéal engendré dans B par $f(\mathrm{I})$.

## 2.4. Algèbres et sous-anneaux

On rappelle la définition d'un sous-anneau.

Définition 2.4.1. — *Soit* A *un anneau. Un sous-anneau de* A *est une partie* $\mathrm{B} \subset \mathrm{A}$ *contenant* 0, 1, *stable par addition, passage à l'opposé et multiplication.*

Si $f : \mathrm{A} \to \mathrm{B}$ est un morphisme d'anneaux, l'image $f(\mathrm{A})$ de A par $f$ est un sous-anneau de B. L'image réciproque $f^{-1}(\mathrm{C})$ d'un sous-anneau C de B est un sous-anneau de A.

Définition 2.4.2. — *Soit $k$ un anneau. Une* $k$-algèbre *est un anneau* A *muni d'un morphisme d'anneaux* $i : k \to \mathrm{A}$.

Formellement, une $k$-algèbre est le couple $(\mathrm{A}, i : k \to \mathrm{A})$. On dira cependant souvent « soit A une $k$-algèbre » en sous-entendant le morphisme $i$. Si $x \in k$ et $a \in \mathrm{A}$, on commetra ainsi l'abus d'écriture en notant $xa$ au lieu de $i(x)a$. Noter cependant que $i$ n'est pas forcément injectif.

Définition 2.4.3. — *Si* $(\mathrm{A}, i)$ *et* $(\mathrm{B}, j)$ *sont des $k$-algèbres, un* morphisme *de $k$-algèbres* $f : \mathrm{A} \to \mathrm{B}$ *est un morphisme d'anneaux tel que pour tout $x \in k$ et tout $a \in \mathrm{A}$,* $f(i(x)a) = j(x)f(a)$.

*Exercice 2.4.4.* — Vérifier que l'image $f(\mathrm{A})$ d'un morphisme de $k$-algèbres $f : \mathrm{A} \to \mathrm{B}$ est une sous-$k$-algèbre de B.

*Exemples 2.4.5.* — a) Si $k$ est un sous-anneau d'un anneau A, l'injection naturelle $k \hookrightarrow \mathrm{A}$ munit A d'une structure de $k$-algèbre.

b) L'anneau $k[\mathrm{X}]$ des polynômes à coefficients dans $k$ est une $k$-algèbre de manière naturelle. Plus généralement, $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est une $k$-algèbre.

c) Tout anneau est de manière unique une **Z**-algèbre. En effet, si A est un anneau, il existe un unique morphisme $i : \mathbf{Z} \to \mathrm{A}$. (On a nécessairement $i(0) = 0$, $i(1) = 1$ ; par récurrence, $i(n)$ est défini pour $n \geq 1$ et enfin, $i(n) = -i(-n)$ si $n \leq 0$.)

La $k$-algèbre des polynômes jouit d'une *propriété universelle* importante :

PROPOSITION 2.4.6. — *Soit* A *une $k$-algèbre et soit $n \geq 1$ un entier non nul. Pour tout $n$-uplet $(a_1, \ldots, a_n)$ d'éléments de* A*, il existe un unique morphisme de $k$-algèbres $f : k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ tel que pour tout $i \in \{1, \ldots, n\}$, $f(\mathrm{X}_i) = a_i$.*

*Démonstration.* — Si un tel morphisme existe, il doit vérifier

$$f(\lambda \mathrm{X}_1^{m_1} \ldots \mathrm{X}_n^{m_n}) = \lambda f(\mathrm{X}_1)^{m_1} \ldots f(\mathrm{X}_n)^{m_n} = \lambda a_1^{m_1} \ldots a_n^{m_n}.$$

Par suite, si $\mathrm{P} = \sum_{\mathbf{m}} \lambda_{\mathbf{m}} \mathrm{X}_1^{m_1} \ldots \mathrm{X}_n^{m_n}$, on doit avoir

$$f(\mathrm{P}) = \sum_{\mathbf{m}} \lambda_{\mathbf{m}} a_1^{m_1} \ldots a_n^{m_n},$$

ce qui prouve qu'il existe au plus un tel morphisme de $k$-algèbres, et que s'il existe, il est défini par cette dernière formule. Réciproquement, il est facile de prouver que cette formule définit un morphisme de $k$-algèbres. □

Ce morphisme est parfois appelé, surtout lorsque $\mathrm{A} = k$, morphisme d'*évaluation* en le point $(a_1, \ldots, a_n)$. L'image d'un polynôme P est notée $\mathrm{P}(a_1, \ldots, a_n)$. Il en résulte par exemple un morphisme de $k$-algèbres $k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathscr{F}(k^n, k)$ des polynômes dans la $k$-algèbre des fonctions de $k^n$ dans $k$. Les fonctions qui sont dans l'image de ce morphisme sont tout naturellement appelées *fonctions polynômiales*.

*2.4.7. Algèbre engendrée par une partie.* — Soit A une $k$-algèbre et S une partie de A. La $k$-algèbre $k[\mathrm{S}]$ est par définition la plus petite sous-$k$-algèbre de A qui contient S. C'est l'ensemble des combinaisons linéaires de la forme $\lambda s_1^{m_1} \ldots s_n^{m_n}$ pour $\lambda \in k$, les $s_i$ dans S et les $m_i$ dans **N**.

Si $\mathrm{S} = \{a_1, \ldots, a_n\}$, $k[\mathrm{S}]$ est aussi notée $k[a_1, \ldots, a_n]$. C'est l'image du morphisme d'évaluation $k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathrm{A}$ en $(a_1, \ldots, a_n)$.

*Démonstration.* — Notons $\varphi$ ce morphisme d'évaluation. Comme $\varphi(\mathrm{X}_i) = a_i$, $\operatorname{Im}\varphi$ est une sous-$k$-algèbre de A qui contient les $a_i$, donc $\operatorname{Im}\varphi$ contient $k[a_1, \ldots, a_n]$. Réciproquement, toute sous-$k$-algèbre de A qui contient $\{a_1; \ldots; a_n\}$ contient les éléments de A de la forme $\lambda a_1^{m_1} \ldots a_n^{m_n}$ et aussi leurs combinaisons linéaires. Par suite, $k[a_1, \ldots, a_n]$ contient $\operatorname{Im}\varphi$. On a ainsi égalité. □

*Exercice 2.4.8.* — Utiliser la propriété universelle pour démontrer qu'il existe un unique morphisme de $k$-algèbres $\varphi : k[X,Y] \to k[X][Y]$ tel que $\varphi(X) = X$ et $\varphi(Y) = Y$ et que c'est un isomorphisme.

PROPOSITION 2.4.9. — *Soit* K *un corps et soit* $\iota : \mathbf{Q} \to K$ *l'homomorphisme canonique. Alors,* K *contient un plus petit sous-corps* $K_0$.

– *si* $\iota$ *est injectif,* $K_0$ *est isomorphe à* $\mathbf{Q}$ *;*

– *si* $\iota$ *n'est pas injectif, il existe un unique nombre premier* $p$ *tel que* $\operatorname{Ker}\iota = (p)$ *et* $K_0$ *est de cardinal* $p$.

*Démonstration.* — L'intersection $L = \bigcap K_i$ d'une famille $(K_i)$ de sous-corps de K est un sous-corps de K : comme $1 \in K_i$ pour tout $i$, $1 \in L$. Si $x$ et $y$ sont dans L, $x - y$ est dans tout $K_i$ donc dans K. Si de plus $y \neq 0$, $x/y$ appartient à chaque $K_i$ donc $x/y \in L$. L'intersection de tous les sous-corps de K est donc un sous-corps de K. On le note $K_0$.

Supposons maintenant que $\iota$ est injectif et construisons un homomorphisme de corps $\tilde{\iota}$: $\mathbf{Q} \to K$. Pour cela, si $a/b$ est une fraction d'entiers avec $b \neq 0$, $\iota(b) \neq 0$ dans K et on pose $\tilde{\iota}(a/b) = \iota(a)/\iota(b)$. Cela ne dépend pas de la fraction choisie : si $a/b = c/d$, on a $ad = bc$ dans $\mathbf{Z}$, donc

$$\iota(a)\iota(d) = \iota(ad) = \iota(bc) = \iota(b)\iota(c)$$

et $\iota(a)/\iota(b) = \iota(c)/\iota(d)$.

C'est un homomorphisme de corps : pour la somme de deux éléments,

$$\begin{aligned}
\tilde{\iota}(a/b) + \tilde{\iota}(c/d) &= \frac{\iota(a)}{\iota(b)} + \frac{\iota(c)}{\iota(d)} \\
&= \frac{\iota(a)\iota(d) + \iota(b)\iota(c)}{\iota(b)\iota(d)} \\
&= \frac{\iota(ad + bc)}{\iota(bd)} \\
&= \tilde{\iota}\left(\frac{ad + bc}{bd}\right) \\
&= \tilde{\iota}((a/b) + (c/d))
\end{aligned}$$

et pour le produit,

$$\tilde{\iota}(a/b)\tilde{\iota}(c/d)) = \frac{\iota(a)}{\iota(b)}\frac{\iota(c)}{\iota(d)} = \frac{\iota(a)\iota(c)}{\iota(b)\iota(d)} = \frac{\iota(ac)}{\iota(bd)} = \tilde{\iota}(ac/bd) = \tilde{\iota}((a/b)(c/d)).$$

Par suite, $\tilde{\iota}$ est un homomorphisme de corps $\mathbf{Q} \to K$. Il est nécessairement injectif et définit donc un isomorphisme de $\mathbf{Q}$ sur un sous-corps $K_0'$ de K.

Nécessairement, $K_0 \subset K_0'$. Réciproquement, comme $K_0$ contient 1, il contient $\iota(\mathbf{Z})$ puis toutes les fractions $\iota(a)/\iota(b)$ avec $b \neq 0$. Par suite, $K_0 = K_0'$.

Supposons maintenant que $\iota$ n'est pas injectif. Son noyau est un idéal $(n)$ de $\mathbf{Z}$, où $n$ est défini comme le plus petit entier strictement positif tel que $\iota(n) = 0$. Soit $p$ un facteur premier de $n$. On peut écrire $n = pm$ avec $1 \leq m < n$. On a donc $0 = \iota(n) = \iota(p)\iota(m)$. Par minimalité de $n$, $\iota(m) \neq 0$ donc $\iota(p) = 0$. Cela implique $p \geq n$, donc $n = p$.

L'image $\iota(\mathbf{Z})$ de $\mathbf{Z}$ par l'homomorphisme $\iota$ est un sous-anneau de K. En fait, on a $\iota(\mathbf{Z}) = \{\iota(0); \ldots; \iota(p-1)\}$ : si $n \in \mathbf{Z}$, la division euclidienne de $n$ par $p$ s'écrit $n = pq + r$ avec $0 \leq r < p - 1$ et $\iota(n) = \iota(p)\iota(q) + \iota(r) = \iota(r)$. En particulier, le cardinal de $\iota(\mathbf{Z})$ est exactement $p$. Ainsi, $\iota(\mathbf{Z})$ est un sous-anneau fini d'un anneau intègre. En vertu de l'exercice 2.1.7, c'est un corps. Par minimalité de $K_0$, ce corps contient $K_0$, mais réciproquement $K_0$ contient 1, donc il contient $\iota(\mathbf{Z})$. □

Définition 2.4.10. — *Soit* K *un corps. Le plus petit sous-corps de* K *est appelé* sous-corps premier *de* K. *S'il est isomorphe à* $\mathbf{Q}$, *on dit que* K *est de* caractéristique 0 *; s'il est fini de cardinal* $p$, *on dit que* K *est de* caractéristique $p$.

## 2.5. Exercices

*Exercice 2.5.1.* — Montrer qu'un anneau intègre possédant un nombre fini d'idéaux est un corps. (*Si* $x \neq 0$, *introduire les idéaux* $(x^n)$ *pour* $n \geq 1$.)

*Exercice 2.5.2.* — Soient K un corps et A un anneau non nul. Montrer que tout homomorphisme d'anneaux de K dans A est injectif.

*Exercice 2.5.3.* — Soient $\mathbf{Z}[\sqrt{2}]$ et $\mathbf{Z}[\sqrt{3}]$ les sous-anneaux de $\mathbf{C}$ engendrés par $\mathbf{Z}$, et respectivement par $\sqrt{2}$ et $\sqrt{3}$.

**a)** Montrer que $\mathbf{Z}[\sqrt{2}] = \{a+b\sqrt{2}\,;\, a, b \in \mathbf{N}\}$ et que $\mathbf{Z}[\sqrt{3}] = \{a+b\sqrt{3}\,;\, a, b \in \mathbf{N}\}$.

**b)** Montrer qu'il n'existe pas de morphisme d'anneaux de $\mathbf{Z}[\sqrt{2}]$ dans $\mathbf{Z}[\sqrt{3}]$.

*Exercice 2.5.4.* — Soient I, J et L des idéaux de A. Démontrer les assertions suivantes :

**a)** $I \cdot J$ est contenu dans $I \cap J$ ;

**b)** on a $(I \cdot J) + (I \cdot L) = I \cdot (J + L)$ ;

**c)** $(I \cap J) + (I \cap L)$ est contenu dans $I \cap (J + L)$ ;

**d)** si J est contenu dans I, on a $J + (I \cap L) = I \cap (J + L)$ ;

**e)** soit K un corps. Supposons que l'on ait $A = K[X,Y]$. Posons $I = (X)$, $J = (Y)$ et $L = (X+Y)$. Déterminer $(I \cap J) + (I \cap L)$ et $I \cap (J+L)$, puis les comparer.

*Exercice 2.5.5.* — Soient B un anneau et $f : A \to B$ un homomorphisme d'anneaux. Pour tout idéal I de A, on note $f_*(I)$ l'idéal de B engendré par $f(I)$ et on

l'appelle extension de I dans B. Pour tout idéal J de B, on appelle contraction de J l'idéal $f^{-1}(\mathrm{J})$.

Étant donné un idéal I de A et un idéal J de B, montrer les assertions suivantes :

**a)** I est contenu dans $f^{-1}(f_*(\mathrm{I}))$ et J contient $f_*(f^{-1}(\mathrm{J}))$ ;

**b)** on a $f^{-1}(\mathrm{J}) = f^{-1}\big(f_*(f^{-1}(\mathrm{J}))\big)$ et $f_*(\mathrm{I}) = f_*\big(f^{-1}(f_*(\mathrm{I}))\big)$.

Soit $\mathscr{C}$ l'ensemble des idéaux de A qui sont des contractions d'idéaux de B et $\mathscr{E}$ l'ensemble des idéaux de B qui sont des extensions d'idéaux de A.

**c)** on a $\mathscr{C} = \{\mathrm{I}; \mathrm{I} = f^{-1}\big(f_*(\mathrm{I})\big)\}$ et $\mathscr{E} = \{\mathrm{J}; \mathrm{J} = f_*\big(f^{-1}(\mathrm{I})\big)\}$ ;

**d)** l'application $f_*$ définit une bijection de $\mathscr{C}$ sur $\mathscr{E}$ ; quel est son inverse ?

Soient $\mathrm{I}_1$ et $\mathrm{I}_2$ deux idéaux de A, et $\mathrm{J}_1$ et $\mathrm{J}_2$ deux idéaux de B. Montrer les assertions suivantes :

**e)** on a $f_*(\mathrm{I}_1 + \mathrm{I}_2) = f_*(\mathrm{I}_1) + f_*(\mathrm{I}_2)$ et $f^{-1}(\mathrm{J}_1 + \mathrm{J}_2)$ contient $f^{-1}(\mathrm{J}_1) + f^{-1}(\mathrm{J}_2)$ ;

**f)** $f_*(\mathrm{I}_1 \cap \mathrm{I}_2)$ est contenu dans $f_*(\mathrm{I}_1) \cap f_*(\mathrm{I}_2)$ et l'on a $f^{-1}(\mathrm{J}_1 \cap \mathrm{J}_2) = f^{-1}(\mathrm{J}_1) \cap f^{-1}(\mathrm{J}_2)$ ;

**g)** on a $f_*(\mathrm{I}_1 \cdot \mathrm{I}_2) = f_*(\mathrm{I}_1) \cdot f_*(\mathrm{I}_2)$ et $f^{-1}(\mathrm{J}_1 \cdot \mathrm{J}_2)$ contient $f^{-1}(\mathrm{J}_1) \cdot f^{-1}(\mathrm{J}_2)$ ;

**h)** $f_*(\sqrt{\mathrm{I}})$ est contenu dans $\sqrt{f_*(\mathrm{I})}$ et l'on a $f^{-1}(\sqrt{\mathrm{J}}) = \sqrt{f^{-1}(\mathrm{J})}$.

*Exercice 2.5.6.* — Soient I et J deux idéaux de A. On suppose que $\mathrm{I} + \mathrm{J} = \mathrm{A}$. Montrer que pour tout entier $n$, $\mathrm{I}^n + \mathrm{J}^n = \mathrm{A}$.

*Exercice 2.5.7.* — Soit A un anneau et $f = a_0 + a_1\mathrm{X} + \cdots + a_n\mathrm{X}^n \in \mathrm{A}[\mathrm{X}]$.

**a)** Montrer que $f$ est nilpotent si et seulement si tous les $a_i$ sont nilpotents.

**b)** Montrer que $f$ est inversible dans A[X] si et seulement $a_0$ est inversible dans A et $a_1, \ldots, a_n$ sont nilpotents. (*Si* $g = f^{-1} = b_0 + b_1\mathrm{X} + \cdots + b_m\mathrm{X}^m$, *montrer par récurrence sur* $k$ *que* $a_n^{k+1} b_{m-k} = 0$.)

**c)** Montrer que $f$ est diviseur de zéro si et seulement si il existe $a \in \mathrm{A}$, $a \neq 0$ tel que $af = 0$. (*Si* $fg = 0$ *avec* $g$ *de degré minimal, montrer que pour tout* $k$, $a_k g = 0$.)

## 2.6. Solutions

*Solution de l'exercice 2.5.1.* — Soit A un anneau intègre et $x \neq 0$ un élément de A qui n'est pas nul. Il faut montrer que $x$ est inversible. On introduit alors les idéaux $(x) \supset (x^2) \supset \ldots (x^n) \supset \ldots$. Il y en a une « infinité », et comme A est supposé n'avoir qu'un nombre fini d'idéaux, deux d'entre eux sont égaux, disons $(x^n) = (x^m)$ pour $m > n \geq 1$. Alors, il existe $a \in \mathrm{A}$ tel que $x^n = a \cdot x^m$, et $x^n(1 - ax^{m-n}) = 0$. Comme $x$ n'est pas nul, $x^{m-n}$ non plus et $1 = ax^{m-n}$. Ainsi $x \cdot (ax^{m-n-1}) = 1$ et $x$ est inversible.

*Solution de l'exercice 2.5.2.* — Soit $\varphi : \mathrm{K} \to \mathrm{A}$ un homomorphisme d'anneaux. Supposons que $\varphi$ n'est pas injectif et soit $x \in \mathrm{K}$ un élément non nul tel que

$\varphi(x) = 0$. Alors, $\varphi(1) = \varphi(x/x) = \varphi(x)\varphi(1/x) = 0$, donc $1 = 0$ dans A, ce qui contredit le fait que A n'est pas l'anneau nul.

*Autre méthode* : Le noyau de $\varphi$ est un idéal de K, donc $\operatorname{Ker}\varphi = (0)$ ou $\operatorname{Ker}\varphi = \mathrm{K}$. Comme $\varphi(1_\mathrm{K}) = 1_\mathrm{A} \neq 0_\mathrm{A}$, $1_\mathrm{K} \notin \operatorname{Ker}\varphi$ et $\operatorname{Ker}\varphi = (0)$, ce qui signifie que $\varphi$ est injectif.

*Solution de l'exercice 2.5.3.* — **a)** On démontre que tout élément de $\mathbf{Z}[\sqrt{2}]$ s'écrit d'une manière unique sous la forme $a+b\sqrt{2}$, pour $a$ et $b \in \sqrt{2}$. En effet, comme

$$\begin{aligned}(a + b\sqrt{2})(a' + b'\sqrt{2}) &= aa' + ba'\sqrt{2} + ab'\sqrt{2} + 2bb' \\ &= (aa' + 2bb') + (ab' + a'b)\sqrt{2},\end{aligned}$$

l'ensemble des $a+b\sqrt{2}$ est un sous-anneau de $\mathbf{C}$, donc égal à $\mathbf{Z}[\sqrt{2}]$. L'unicité de la décomposition résulte du fait que $\sqrt{2} \notin \mathbf{Q}$. On aurait sinon deux entiers non tous deux nuls $a$ et $b$ tels que $a + b\sqrt{2} = 0$. On peut supposer $a$ et $b$ premiers entre eux, et en particulier $a^2 = 2b^2$. Ainsi, $a$ est pair ; on écrit donc $a = 2a'$, d'où $2a'^2 = b^2$, ce qui implique que $b$ est pair, contrairement au fait que $a$ et $b$ étaient supposés premiers entre eux.

De même, tout élément de $\mathbf{Z}[\sqrt{3}]$ s'écrit de manière unique sous la forme $a + b\sqrt{3}$.

**b)** Supposons donné un homomorphisme d'anneaux $\varphi : \mathbf{Z}[\sqrt{2}] \to \mathbf{Z}[\sqrt{3}]$. Alors, il existe $a$ et $b$ tels que $\varphi(\sqrt{2}) = a+b\sqrt{3}$. Alors $\varphi(2) = \varphi(1+1) = 2\varphi(1) = 2$, mais

$$\varphi(2) = \varphi(\sqrt{2}\sqrt{2}) = \varphi(\sqrt{2})^2 = (a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3}.$$

Il faut donc résoudre le système d'équations

$$\begin{cases} a^2 + 3b^2 &= 2 \\ 2ab &= 0 \end{cases}$$

Ainsi, soit $a = 0$, soit $b = 0$. Si $a = 0$, on trouve $3b^2 = 2$, ce qui est impossible ($b = 0$ ne convient pas, et si $b \neq 0$, $3b^2 \geq 3$). Si $b = 0$, on trouve $a^2 = 2$ qui n'a pas de solution entière. Ainsi, $\varphi$ n'existe pas.

*Solution de l'exercice 2.5.4.* — **a)** Soit $x \in \mathrm{I}\cdot\mathrm{J}$ : $x$ s'écrit sous la forme $x = \sum_{i=1}^{n} \alpha_i\beta_i$ avec $\alpha_i \in \mathrm{I}$ et $\beta_i \in \mathrm{J}$. Pour chaque $i$ on a donc $\alpha_i\beta_i \in \mathrm{I}\cap\mathrm{J}$, d'où $x \in \mathrm{I}\cap\mathrm{J}$.

**b)** On a $\mathrm{I}\cdot\mathrm{J} \subset \mathrm{I}\cdot(\mathrm{J}+\mathrm{L})$ et $\mathrm{I}\cdot\mathrm{L} \subset \mathrm{I}\cdot(\mathrm{J}+\mathrm{L})$, donc $\mathrm{I}\cdot\mathrm{J}+\mathrm{I}\cdot\mathrm{L}$ est inclus dans $\mathrm{I}\cdot(\mathrm{J}+\mathrm{L})$. Réciproquement, soit $x \in \mathrm{I}\cdot(\mathrm{J}+\mathrm{L})$. On a donc $x = \sum_{i=1}^{n} \alpha_i(\beta_i + \gamma_i)$, avec $\alpha_i \in \mathrm{I}$, $\beta_i \in \mathrm{J}$ et $\gamma_i \in \mathrm{L}$. Ainsi,

$$x = \sum_{i=1}^{n} \alpha_i\beta_i + \sum_{i=1}^{n} \alpha_i\gamma_i \in \mathrm{I}\cdot\mathrm{J} + \mathrm{I}\cdot\mathrm{L}.$$

**c)** Soit $x = y+z$ avec $y \in I \cap J$ et $z \in I \cap L$. En particulier, $y+z \in I$ et $y+z \in J+L$, d'où $x \in I \cap (J+L)$.

**d)** D'après c), on a $J + (I \cap L) \subset I \cap (J+L)$. D'autre part, si $x \in I \cap (J+L)$, alors on peut écrire $x = y+z$, avec $y \in J$ et $z \in L$. En particulier, $z = x - y \in I$, donc $z \in I \cap L$, si bien que $x = y+z \in J + (I \cap L)$.

**e)** On a $I \cap J = (XY)$, $I \cap L = (X^2 + XY)$, d'où

$$I \cap J + I \cap L = (XY, X^2 + XY) = (X^2, XY).$$

D'autre part, $J + L = (Y, X+Y) = (X, Y) \supset I$, d'où $I \cap (J+L) = I = (X)$.

*Solution de l'exercice 2.5.5.* — **a)** Soit $x \in I$, $f(x) \in f(I) \subset f_*(I)$, d'où $x \in f^{-1}(f_*(I))$.

Soit $y \in f_*(f^{-1}(J))$. On peut donc écrire $y = \sum_{i=1}^{n} b_i f(x_i)$, pour $b_i \in B$ et $x_i \in f^{-1}(J)$. Ainsi, $f(x_i) \in J$ et $y \in J$.

**b)** La première inclusion de a) appliquée à $I = f^{-1}(J)$ donne $f-1(J) \subset f^{-1}(f_*(f^{-1}(J)))$. En appliquant $f^{-1}$ à la seconde, on obtient l'égalité souhaitée.

Si l'on applique $f_*$ à la première inclusion de a), on obtient $f_*(I) \subset f_*(f^{-1}(f_*(I)))$. Si l'on applique la seconde inclusion de a) à l'idéal $J = f(I)$, on obtient que $f_*(I)$ contient $f_*(f^{-1}(f_*(I)))$, d'où l'égalité.

**c)** D'après la première égalité de b), tout élément I de $\mathscr{E}$ vérifie $I = f^{-1}(f_*(I))$, tandis qu'il est clair que tout idéal I vérifiant $I = f^{-1}(f_*(I))$ est un contracté : c'est le contracté de $f_*(I)$.

D'autre part, tout idéal J de $\mathscr{E}$ vérifie $J = f_*(f^{-1}(J))$ (appliquer la seconde égalité de b) à un idéal I tel que $J = f_*(I)$), tandis que si un idéal J vérifie $J = f_*(f^{-1}(J))$, c'est l'extension de $f^{-1}(J)$, donc un élément de $\mathscr{E}$.

**d)** L'application $f_*$ envoie bien idéaux contractions d'idéaux de B dans les idéaux qui sont extensions d'idéaux de A et l'application $f^{-1}$ envoie les idéaux qui sont extensions d'idéaux de A dans ceux qui sont contractés d'idéaux de A. Montrons que $f_* f^{-1} : \mathscr{E} \to \mathscr{E}$ est l'identité. C'est en fait la seconde égalité de b). De même, la première égalité de b) entraîne que $f^{-1} f_* : \mathscr{E} \to \mathscr{E}$ est l'identité. Ainsi, $f_*$ est bijective, de bijection réciproque $f^{-1}$.

Les vérifications des relations des questions e) à h) sont immédiates.

*Solution de l'exercice 2.5.6.* — Si $I + J = A$, on peut écrire $1 = x + y$ avec $x \in I$ et $y \in J$. Alors, on a

$$1 = (x+y)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} x^k y^{2n-k}.$$

De plus, pour tout $k \in \{0, \ldots, 2n\}$, ou bien $x^k \in I^n$, ou bien $y^{2n-k} \in J^n$. Par suite, $1 \in I^n + J^n$ et $I^n + J^n = A$.

*Solution de l'exercice 2.5.7.* — **a)** Si $f = a_0 + a_1\mathrm{X} + \cdots + a_n\mathrm{X}^n$ est nilpotent, on voit tout de suite que $a_n$ est nilpotent car le terme (*a priori* dominant) de degré $nk$ dans $f^k$ a pour coefficient $a_n^k$. Par suite, $f - a_n\mathrm{X}^n$ est aussi nilpotent et par récurrence sur $n$, tous les $a_i$ sont nilpotents.

Dans l'autre sens, si tous les $a_i$ sont nilpotents, $f$ est une somme d'éléments nilpotents de $\mathrm{A}[\mathrm{X}]$ donc est nilpotent.

**b)** Si $a_0$ est inversible et $a_1, \ldots, a_n$ sont nilpotents, $f$ est la somme d'un élément inversible $u$ et d'un élément nilpotent $n$ de $\mathrm{A}[\mathrm{X}]$, donc est nilpotent. En effet, on peut écrire $u + n = u(1 + u^{-1}n)$, si bien qu'il suffit de prouver que $1 + u^{-1}n$ est inversible. Or, si $n^{k+1} = 0$,

$$1 - u^{-1}n + (u^{-1}n)^2 - \cdots + (-1)^k(u^{-1}n)^k$$

est un inverse de $1 + u^{-1}n$. (*Autre méthode :* si $u + n$ appartient à un idéal maximal $\mathfrak{m}$, $n \in \mathfrak{m}$ car un élément nilpotent appartient à tout idéal premier, donc $u \in \mathfrak{m}$ ce qui contredit le fait que $u$ est inversible.)

Réciproquement, soit $g = b_0 + b_1\mathrm{X} + \cdots + b_m\mathrm{X}^m$ l'inverse de $f$. Le terme de degré 0 dans $fg$ est $a_0b_0 = 1$, ce qui prouve que $a_0$ est inversible. Si $n = 0$, la question est résolue. Sinon, le terme de degré $m + n \geq 1$ dans $fg$ est nul, d'où $a_nb_m = 0$.

Comme indiqué, montrons par récurrence sur $k \geq 0$ que $a_n^{k+1}b_{m-k} = 0$ pour $k \leq m$. C'est vrai pour $k = 0$, et si c'est vrai pour $k - 1$, écrivons le terme de degré $m + n - k$ dans $fg$. Il est nul car $m + n - k \geq n \geq 1$, d'où

$$a_nb_{m-k} + a_{n-1}b_{m+1-k} + \cdots + a_0b_{m-k} = 0.$$

En multipliant cette relation par $a_n^k$ et en utilisant l'assertion de récurrence, on trouve que $a_n^{k+1}b_{m-k} = 0$.

Pour $k = m$, on a donc $a_n^{m+1} = 0$, ce qui prouve que $a_n$ est nilpotent. Par suite, $f - a_n\mathrm{X}^n$ est encore inversible et par récurrence sur $n$, $a_1, \ldots, a_n$ sont nilpotents.

**c)** Soit $g = b_0 + \cdots + b_m\mathrm{X}^m$ un polynôme non nul de degré minimal tel que $fg = 0$. Si $m = 0$, on a $b_0f = 0$, ainsi qu'il fallait démontrer.

Supposons donc $m > 0$ et commençons par montrer que pour tout $k$, $a_kg = 0$.

L'assertion est vraie pour $k > n$. Supposons la vraie pour $k + 1$. Alors,

$$0 = fg = (a_0 + a_1\mathrm{X} + \cdots + a_k\mathrm{X}^k)g$$

dont le coefficient *a priori* dominant est donné par $a_kb_m$. Par suite $a_kb_m = 0$ et $a_kg$ est un polynôme de degré $\leq m - 1$ tel que $f(a_kg) = 0$. L'hypothèse de minimalité sur $\deg g$ implique que $a_kg = 0$.

Une fois ceci prouvé, tous les produits $a_kb_\ell$ sont nuls. Par suite, on a $b_\ell f = 0$. Comme $g \neq 0$, l'un des $b_\ell$ est non nul et il existe bien $a \in \mathrm{A} \setminus \{0\}$ tel que $af = 0$.

La réciproque est évidente.

# 3 Anneau quotient, localisation

*Nous introduisons dans ce chapitre deux constructions fondamentales d'anneaux. Le passage au quotient, tout d'abord : étant donnés un anneau et une relation d'équivalence convenable sur cet anneau, l'objectif est de munir l'ensemble des classes d'équivalence d'une structure d'anneau. Cela revient en fait à « rendre nuls » les éléments d'un idéal de l'anneau sans modifier les autres règles de calcul. La localisation, ensuite : il s'agit cette fois de « rendre inversibles » une famille d'éléments de l'anneau.*

## 3.1. Anneaux quotients

Rappelons qu'une relation $\mathscr{R}$ sur un ensemble X est dite *relation d'équivalence* si elle est réflexive (pour tout $x$, $x \mathscr{R} x$), symétrique (si $x \mathscr{R} y$, alors $y \mathscr{R} x$) et transitive (si $x \mathscr{R} y$ et $y \mathscr{R} z$, alors $x \mathscr{R} z$). L'ensemble des classes d'équivalence de X pour la relation $\mathscr{R}$ est noté $X/\mathscr{R}$.

Soit maintenant A un anneau. On peut alors chercher les relations d'équivalence sur A qui sont *compatibles avec la structure d'anneau.* On veut ainsi que soient satisfaite la propriété :

$$\text{si } x \mathscr{R} y \text{ et } x' \mathscr{R} y', \text{ alors } x + x' \mathscr{R} y + y' \text{ et } xx' \mathscr{R} yy'.$$

Notons alors I la classe d'équivalence de 0. Si $x \mathscr{R} y$, comme $y \mathscr{R} y$, on a donc $x - y \mathscr{R} 0$, soit $x - y \in \mathrm{I}$, et réciproquement. Ainsi, $\mathscr{R}$ est définie par $x \mathscr{R} y$ si et seulement si $x - y \in \mathrm{I}$.

Montrons d'autre part que I est un idéal de A. On a déjà $0 \in \mathrm{I}$. De plus, si $x \in \mathrm{I}$ et $y \in \mathrm{I}$, $x \mathscr{R} 0$ et $y \mathscr{R} 0$, donc $(x + y) \mathscr{R} 0$, ce qui prouve que $x + y \in \mathrm{I}$. Enfin, si $x \in \mathrm{I}$ et $a \in \mathrm{A}$, $x \mathscr{R} 0$, d'où $ax \mathscr{R} a0$ ; comme $a0 = 0$, on a bien $ax \in \mathrm{I}$.

Réciproquement, les calculs ci-dessus montrent que l'on a le théorème suivant.

Théorème 3.1.1. — *Soit* A *un anneau et soit* I *un idéal de* A. *La relation* $\mathscr{R}$ *sur* A *définie par* $x \mathscr{R} y$ *si et seulement si* $x - y \in \mathrm{I}$ *est une relation d'équivalence compatible avec la structure d'anneau. L'ensemble quotient* $\mathrm{A}/\mathscr{R}$ *possède une unique structure d'anneau telle*

*que la surjection canonique* $\mathrm{cl} : \mathrm{A} \to \mathrm{A}/\mathscr{R}$ *est un morphisme d'anneaux. Ce morphisme est surjectif de noyau* I.

L'*anneau quotient* $\mathrm{A}/\mathscr{R}$ est noté A/I. Le morphisme $\mathrm{A} \to \mathrm{A/I}$ est aussi appelé *surjection canonique*.

Remarquons aussi que si $k$ est un anneau et $i : k \to \mathrm{A}$ un morphisme d'anneaux, de sorte que $(\mathrm{A}, i)$ est une $k$-algèbre, la composition $\mathrm{cl} \circ i : k \to \mathrm{A} \to \mathrm{A/I}$ munit A/I d'une (mieux, de l'unique) structure de $k$-algèbre pour laquelle la surjection canonique est un morphisme de $k$-algèbres.

L'importance de la structure d'anneau quotient vient notamment du *théorème de factorisation* que nous démontrons maintenant.

THÉORÈME 3.1.2. — *Soit* A *et* B *deux anneaux et soit* $f : \mathrm{A} \to \mathrm{B}$ *un homomorphisme d'anneaux. Si* I *est un idéal de* A *contenu dans* $\mathrm{Ker}\, f$*, il existe un unique homomorphisme d'anneaux* $\bar{f} : \mathrm{A/I} \to \mathrm{B}$ *tel que* $f = \bar{f} \circ \mathrm{cl}$.

Une façon visuelle et commode d'écrire cette dernière égalité est de dire que le diagramme

$$\begin{array}{ccc} \mathrm{A} & \xrightarrow{f} & \mathrm{B} \\ {\scriptstyle \mathrm{cl}}\downarrow & \nearrow_{\bar{f}} & \\ \mathrm{A/I} & & \end{array}$$

est *commutatif*.

*Démonstration.* — Nécessairement, $\bar{f}$ doit être tel que $\bar{f}(\mathrm{cl}(a)) = f(a)$ pour tout $a \in \mathrm{A}$. Comme tout élément de A/I est de la forme $\mathrm{cl}(a)$ pour un certain $a \in \mathrm{A}$, cela montre qu'il existe au plus un homomorphisme d'anneaux $\bar{f} : \mathrm{A/I} \to \mathrm{B}$ tel que $f = \bar{f} \circ \mathrm{cl}$.

Montrons maintnant l'existence de $\bar{f}$. Soit $x$ un élément de A/I. On sait qu'il existe $a \in \mathrm{A}$ tel que $x = \mathrm{cl}(a)$. Si $a'$ est un autre représentant de $x$, donc tel que $x = \mathrm{cl}(a')$, on a $a' - a \in \mathrm{I}$, donc, puisque $\mathrm{I} \subset \mathrm{Ker}\, f$, $f(a' - a) = 0$ et par conséquent, $f(a) = f(a')$. On peut ainsi poser $\bar{f}(x) = f(a)$ — le résultat est indépendant du représentant $a$ choisi. Il reste à montrer que $\bar{f}$ est un homomorphisme d'anneaux.

Comme $\mathrm{cl}(0_{\mathrm{A}}) = 0_{\mathrm{A/I}}$ et $\mathrm{cl}(1_{\mathrm{A}}) = 1_{\mathrm{A/I}}$, on a bien $f(0_{\mathrm{A/I}}) = 0_{\mathrm{B}}$ et $f(1_{\mathrm{A/I}}) = 1_{\mathrm{B}}$. De plus, si $x = \mathrm{cl}(a)$ et $y = \mathrm{cl}(b)$ sont deux éléments de A/I, on a $x + y = \mathrm{cl}(a + b)$ et

$$\begin{aligned} \bar{f}(x + y) = \bar{f}(\mathrm{cl}(a + b)) = f(a + b) = f(a) + f(b) = \bar{f}(\mathrm{cl}(a)) + \bar{f}(\mathrm{cl}(b)) \\ = f(x) + f(y) \end{aligned}$$

et, de même,

$$\bar{f}(xy) = f(ab) = f(a)f(b) = \bar{f}(x)\bar{f}(y).$$

Il en résulte que $\bar{f}$ est un homomorphisme d'anneaux. Le théorème est ainsi démontré. □

Le noyau de $\bar{f}$ sera calculé à la proposition 3.1.5. Notamment, on montrera que $\bar{f}$ *est injectif si et seulement si* $\mathrm{I} = \mathrm{Ker}\, f$. Soit $f : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux. On a vu (page 16) que $f(\mathrm{A})$ est un sous-anneau de B. Ainsi, on peut décomposer $f$ en

$$\mathrm{A} \xrightarrow{\mathrm{cl}} \mathrm{A}/\mathrm{Ker}\, f \xrightarrow{\bar{f}} f(\mathrm{A}) \hookrightarrow \mathrm{B}$$

c'est-à-dire en la composition d'un homomorphisme surjectif, d'un isomorphisme et d'un homomorphisme injectif.

Soit A un anneau et soit I un idéal de A. On s'intéresse maintenant aux idéaux de l'anneau A/I. Soit $\mathscr{J}$ un idéal de A/I. Alors, on sait que $\mathrm{cl}^{-1}(\mathscr{J})$ est un idéal de A. Par construction, il contient I puisque pour tout $a \in \mathrm{I}$, $\mathrm{cl}(a) = 0$ est un élément de $\mathscr{J}$.

La propriété importante est donnée par la proposition :

Proposition 3.1.3. — *Soit* A *un anneau et soit* I *un idéal de* A. *L'application* $\mathrm{cl}^{-1}$ *:*

$$\begin{array}{ccc} \textit{idéaux de } \mathrm{A}/\mathrm{I} & \to & \textit{idéaux de } \mathrm{A} \textit{ contenant } \mathrm{I} \\ \mathscr{J} & \mapsto & \mathrm{cl}^{-1}(\mathscr{J}) \end{array}$$

*est une bijection.*

Autrement dit, pour tout idéal J de A qui contient I, il existe un unique idéal $\mathscr{J}$ de A/I tel que $\mathrm{J} = \mathrm{cl}^{-1}(\mathscr{J})$. *De plus, on a* $\mathscr{J} = \mathrm{cl}(\mathrm{J})$ (image de l'idéal J par la surjection canonique, laquelle image se trouve être encore un idéal dans ce cas).

*Démonstration.* — Commencer par construire la bijection réciproque. Si J est un idéal de A, montrons d'abord que cl(J) est un idéal de A. On a bien $0 = \mathrm{cl}(0) \in \mathrm{cl}(\mathrm{J})$. D'autre part, si $x$ et $y$ appartiennent à cl(J), soit $a$ et $b$ des éléments de J tels que $x = \mathrm{cl}(a)$ et $y = \mathrm{cl}(b)$. Alors, $x+y = \mathrm{cl}(a)+\mathrm{cl}(b) = \mathrm{cl}(a+b)$ ; comme J est un idéal de A, $a+b$ appartient à J et $x+y$ appartient bien à cl(J). Enfin, soit $x$ un élément de cl(J) et $y$ un élément de A/I. Choisissons encore $a \in \mathrm{J}$ et $b \in \mathrm{A}$ tels que $x = \mathrm{cl}(a)$ et $y = \mathrm{cl}(b)$. On a $yx = \mathrm{cl}(b)\,\mathrm{cl}(a) = \mathrm{cl}(ba) \in \mathrm{cl}(\mathrm{J})$ puisque, J étant un idéal de A, $ba \in \mathrm{J}$.

Si $\mathscr{J}$ est un idéal de A/I, on a

$$\boxed{\mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{J})) = \mathscr{J}.}$$

Montrons les deux inclusions. Un élément $x$ de $\mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{J}))$ est de la forme $x = \mathrm{cl}(a)$ pour $a \in \mathrm{cl}^{-1}(\mathscr{J})$. On a donc $x \in \mathscr{J}$. Réciproquement, si $x \in \mathscr{J}$, soit $a \in \mathrm{A}$ tel que $x = \mathrm{cl}(a)$. Alors, $\mathrm{cl}(a) = x \in \mathscr{J}$, donc $a$ appartient à $\mathrm{cl}^{-1}(\mathscr{J})$ et $x$ appartient bien à $\mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{J}))$.

Enfin, si J est un idéal de A, on a

$$\boxed{\mathrm{cl}^{-1}(\mathrm{cl}(\mathrm{J})) = \mathrm{I} + \mathrm{J}.}$$

Là encore, montrons les deux inclusions. Si $x \in \mathrm{I}+\mathrm{J}$, on peut écrire $x = a + b$ avec $a \in \mathrm{I}$ et $b \in \mathrm{J}$. Il en résulte $\mathrm{cl}(x) = \mathrm{cl}(a) + \mathrm{cl}(b) = \mathrm{cl}(b) \in \mathrm{cl}(\mathrm{J})$. Donc $x \in \mathrm{cl}^{-1}(\mathrm{cl}(\mathrm{J}))$. Dans l'autre sens, soit $x \in \mathrm{cl}^{-1}(\mathrm{cl}(\mathrm{J}))$. Par définition, $\mathrm{cl}(x) \in \mathrm{cl}(\mathrm{J})$ et il existe $a \in \mathrm{J}$ tel que $\mathrm{cl}(x) = \mathrm{cl}(a)$. On a alors $\mathrm{cl}(x-a) = 0$, ce qui signifie que $x - a \in \mathrm{I}$. Finalement, $x = (x-a) + a$ appartient à $\mathrm{I}+\mathrm{J}$, ainsi qu'il fallait démontrer.

Si de plus J contient I, alors $\mathrm{I}+\mathrm{J} = \mathrm{J}$ et les deux formules établies montrent que l'application $\mathrm{cl}^{-1}$ définit une bijection de l'ensemble des idéaux de A/I vers l'ensemble des idéaux de A contenant I, dont la bijection réciproque est donnée par cl. □

Lorsque J est un idéal de A qui contient I, l'idéal $\mathrm{cl}(\mathrm{J})$ de A/I est aussi noté J/I. Cette notation intervient notamment lorsque l'homomorphisme cl est omis des notations. L'expression « soit J/I un idéal de A/I… » sous-entendra toujours que J est un idéal de A contenant I.

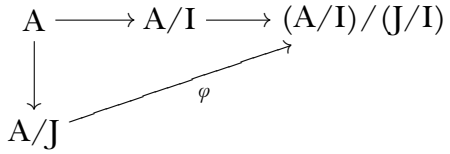
Proposition 3.1.4. — *Soit* A *un anneau, soit* I *un idéal de* A *et soit* J *un idéal de* A *contenant* I. *La composition des surjections canoniques* $\mathrm{A} \to \mathrm{A/I} \to (\mathrm{A/I})/(\mathrm{J/I})$ *a pour noyau* J. *Il en résulte un isomorphisme canonique*

$$\mathrm{A/J} \simeq (\mathrm{A/I})/(\mathrm{J/I}).$$

En résumé, un quotient d'un quotient est encore un quotient.

*Démonstration.* — La composée de deux homomorphismes surjectifs étant encore surjectif, le morphisme $\mathrm{A} \to (\mathrm{A/I})/(\mathrm{J/I})$ est surjectif. Un élément $a \in \mathrm{A}$ appartient au noyau si et seulement si $\mathrm{cl}(a) \in \mathrm{A/I}$ appartient au noyau de l'homomorphisme $\mathrm{A/I} \to (\mathrm{A/I})/(\mathrm{J/I})$, c'est-à-dire $\mathrm{cl}(a) \in (\mathrm{J/I})$. Comme $\mathrm{J/I} = \mathrm{cl}(\mathrm{J})$, cela signifie que $a \in \mathrm{cl}^{-1}(\mathrm{cl}(\mathrm{J})) = \mathrm{J}$ puisque J contient I.

Le théorème de factorisation affirme alors l'existence d'un unique homomorphisme $\varphi : \mathrm{A/J} \to (\mathrm{A/I})/(\mathrm{J/I})$ rendant le diagramme




commutatif. Cet homomorphisme est surjectif. Soit $x \in \mathrm{A/J}$ un élément tel que $\varphi(x) = 0$. Soit $a \in \mathrm{A}$ tel que $x = \mathrm{cl}_{\mathrm{J}}(a)$. Par définition de $\varphi$, on a $\varphi(x) = \mathrm{cl}_{\mathrm{J/I}} \circ \mathrm{cl}\,\mathrm{I}(a) = 0$, c'est-à-dire $a \in \mathrm{J}$. Ainsi, $x = 0$ et l'homomorphisme $\varphi$ est injectif. C'est donc un isomorphisme □

La dernière partie de la démonstration peut être généralisée en un complément important au théorème de factorisation

PROPOSITION 3.1.5. — *Soit* $f : A \to B$ *un morphisme d'anneaux et soit* I *un idéal de* A *contenu dans* $\operatorname{Ker} f$. *Soit* $\bar{f} : A/I \to B$ *l'homomorphisme fourni par le théorème de factorisation. Alors, le noyau de* $\bar{f}$ *est égal à* $(\operatorname{Ker} f)/I$.

*Démonstration.* — En effet, si $\bar{f}(x) = 0$, soit $a \in A$ tel que $x = \mathrm{cl}(a)$. On a alors $f(a) = 0$, d'où $a \in \operatorname{Ker} f$ et $x = \mathrm{cl}(a) \in \mathrm{cl}(\operatorname{Ker} f) = (\operatorname{Ker} f)/I$. Réciproquement, si $x \in (\operatorname{Ker} f)/I$, il existe $a \in \operatorname{Ker} f$ tel que $x = \mathrm{cl}(a)$. On a alors $\bar{f}(x) = f(a) = 0$ et $x \in \operatorname{Ker} \bar{f}$. □

Rappelons (proposition 2.2.12) que deux idéaux I et J d'un anneau A sont dits comaximaux si $I + J = A$. Ils donnent lieu à la forme générale du *théorème chinois.*

THÉORÈME 3.1.6. — *Soit* A *un anneau,* I *et* J *deux idéaux comaximaux de* A. *Il existe alors un unique isomorphismes de* A*-algèbres*

$$A/IJ \simeq A/I \times A/J.$$

COROLLAIRE 3.1.7. — *Si* I *et* J *sont deux idéaux comaximaux d'un anneau* A, *pour tout couple* $(x, y)$ *d'éléments de* A, *il existe* $a \in A$ *tel que* $a \in x + I$ *et* $a \in y + J$.

*Démonstration.* — Considérons le diagramme de A-algèbres :

$$\begin{array}{ccc} & A & \\ \swarrow & & \searrow \\ A/IJ & \overset{\varphi}{\dashrightarrow} & A/I \times A/J \end{array}$$

dans lequel on doit montrer l'existence d'une unique flèche pointillée qui le rende commutatif. Or, le morphisme $A \to A/I \times A/J$ envoie $a \in A$ sur $(\mathrm{cl}_I(a), \mathrm{cl}_J(a))$. Son noyau est donc $I \cap J$, et puisque I et J sont comaximaux, $I \cap J = IJ$ (proposition 2.2.12). Il existe ainsi un unique morphisme $\varphi$ rendant le diagramme commutatif et $\varphi(\mathrm{cl}_{IJ}(a)) = (\mathrm{cl}_I(a), \mathrm{cl}_J(a))$ pour tout $a \in A$.

Ce morphisme est un isomorphisme : comme $I + J = A$, il existe $x \in I$ et $y \in J$ tels que $x + y = 1$. Alors, on a les égalités $1 = \mathrm{cl}_I(x + y) = \mathrm{cl}_I(y)$ dans A/I et $1 = \mathrm{cl}_J(x+y) = \mathrm{cl}_J(x)$ dans A/J. Par suite, $\varphi(x) = (\mathrm{cl}_I(x), \mathrm{cl}_J(x)) = (0, \mathrm{cl}_J(x+y)) = (0, 1)$ tandis que $\varphi(y) = (1, 0)$. Si $a$ et $b$ sont dans A, il en résulte que

$$\varphi(bx + ay) = (0, \mathrm{cl}(b)) + (\mathrm{cl}(a), 0) = (\mathrm{cl}(a), \mathrm{cl}(b)).$$

Tout élément de $A/I \times A/J$ étant de la forme $(\mathrm{cl}(a), \mathrm{cl}(b))$, $\varphi$ est surjectif. □

## 3.2. Localisation

DÉFINITION 3.2.1. — *Soit* A *un anneau. Une partie* S *de* A *est dite* multiplicative *si elle vérifie les propriétés :*

– $1 \in S$ ;

– *pour tous* $a$ *et* $b$ *dans* S, $ab \in S$.

Étant donnés un anneau A et une partie multiplicative S de A, nous allons construire un anneau $S^{-1}A$ et un homomorphisme $i : A \to S^{-1}A$ tel que $i(S)$ est formé d'éléments inversibles dans $S^{-1}A$. Donnons d'abord quelques exemples :

*Exemple 3.2.2.* — a) Si $A = \mathbf{Z}$ et $S = \mathbf{Z} \setminus \{0\}$, l'anneau $S^{-1}A$ sera égal à $\mathbf{Q}$ et $i : \mathbf{Z} \to \mathbf{Q}$ l'injection usuelle.

b) Si S est formé d'éléments inversibles, alors $S^{-1}A = A$.

c) Si $A = \mathbf{Z}$ et $S = \{1; 10; 100; \ldots\}$ est l'ensemble des puissances de 10 dans $\mathbf{Z}$, alors $S^{-1}A$ sera l'ensemble des nombres décimaux, c'est-à-dire l'ensemble des nombres rationnels qui peuvent s'écrire sous la forme $a/10^n$ avec $a \in \mathbf{Z}$ et $n \in \mathbf{N}$.

Ainsi, ce qu'on veut imiter, c'est tout simplement le *calcul de fractions* que l'on apprend au collège.

*3.2.3. Construction.* — Sur l'ensemble $A \times S$, définissons la relation d'équivalence $\sim$ par :

$$(a, s) \sim (b, t) \quad \text{si et seulement s'il existe } u \in S \text{ tel que } \quad u(at - bs) = 0.$$

C'est en effet une relation d'équivalence.

– pour tout $(a, s) \in A \times S$, puisque $1 \in S$ et $1(as - as) = 0$, $(a, s) \sim (a, s)$. La relation est réflexive ;

– si $(a, s) \sim (b, t)$, choisissons $u \in S$ tel que $u(at - bs) = 0$. Alors, $u(bs - at) = 0$, d'où $(b, t) \sim (a, s)$. La relation est symétrique ;

– enfin, si $(a, s) \sim (b, t)$ et $(b, t) \sim (c, u)$, choisissons $v$ et $w \in S$ tels que $v(at - bs) = w(bu - ct) = 0$. Comme

$$t(au - cs) = u(at - bs) + s(bu - ct),$$

on a $vwt(au - cs) = 0$. Puisque $v$, $w$ et $t$ appartiennent à S, $vwt \in S$ et $(a, s) \sim (c, u)$. La relation est donc transitive.

On désigne par $S^{-1}A$ l'ensemble des classes d'équivalence (on trouve parfois la notation $A_S$) ; la classe du couple $(a, s)$ est notée $a/s$. On note $i : A \to S^{-1}A$ l'application qui à $a \in A$ associe la classe $a/1$. L'ensemble $A \times S$ n'est pas un anneau. En revanche, nous allons munir $S^{-1}A$ d'une structure d'anneau de sorte que $i$ est un homomorphisme d'anneaux. La définition provient des formules

habituelles pour la somme et le produit de fractions. L'élément 1 de $S^{-1}A$ est par définition $1/1$, l'élément 0 est $0/1$. On définit ensuite

$$(a/s) + (b/t) = (at + bs)/st, \quad (a/s) \cdot (b/t) = (ab/st).$$

Vérifions d'abord que cette définition a un sens : si $(a, s) \sim (a', s')$, il faut montrer que

$$(at + bs, st) \sim (a't + bs', s't) \quad \text{et} \quad (ab, st) \sim (a'b, s't).$$

On a alors

$$(at + bs)s't - (a't + bs')st = t^2(as' - a's).$$

Choisissons $u \in S$ tel que $u(as' - a's) = 0$ ; il en résulte que

$$u\left((at + bs)s't - (a't + bs')st\right) = 0$$

et donc $(at + bs, st) \sim (a't + bs', s't)$. De même,

$$u(abs't - a'bst) = ubt(as' - a's) = 0$$

et donc $(ab, st) \sim (a'b, st)$. Plus généralement, si $(a, s) \sim (a', s')$ et $(b, t) \sim (b', t')$, on a, en répétant ces vérifications (ou en remarquant la commutativité des opérations),

$$(a, s) + (b, t) \sim (a', s') + (b, t) \sim (a', s') + (b', t').$$

La vérification que ces lois confèrent une structure d'anneau à $S^{-1}A$ est un peu longue mais sans surprise et ne sera pas faite ici. Par exemple, la distributivité de l'addition sur la multiplication se démontre ainsi : si $a/s$, $b/t$ et $c/u$ sont trois éléments de $S^{-1}A$,

$$\frac{a}{s}\left(\frac{b}{t} + \frac{c}{u}\right) = \frac{a(bu + ct)}{stu} = \frac{abu}{stu} + \frac{act}{stu} = \frac{ab}{st} + \frac{ac}{su} = \frac{a}{s}\frac{b}{t} + \frac{a}{s}\frac{c}{u}.$$

L'application $i : A \to S^{-1}A$ telle que $i(a) = a/1$ pour tout $a \in A$ est un homomorphisme d'anneaux. En effet, $i(0) = 0/1 = 0$, $i(1) = 1/1 = 1$, et pour tous $a$ et $b$ dans A, on a

$$i(a + b) = (a + b)/1 = a/1 + b/1 = i(a) + i(b)$$

et

$$i(ab) = (ab)/1 = (a/1)(b/1) = i(a)i(b).$$

Enfin, si $s \in S$, on a $i(s) = s/1$ et $i(s)(1/s) = s/s = 1$. Donc pour tout $s \in S$, $i(s)$ est inversible dans $S^{-1}A$.

*3.2.4. Exemples de parties multiplicatives.* — a) Soit A un anneau intègre. La partie $S = A \setminus \{0\}$ est une partie multiplicative de A. L'anneau $S^{-1}A$ est alors un *corps*, appelé *corps des fractions* de A.

*Démonstration.* — Comme A est intègre, $1 \neq 0$ et $1 \in S$. D'autre part, si $a$ et $b$ sont deux éléments non nuls de A, on a par définition $ab \neq 0$. Ainsi, S est une partie multiplicative de A.

Un élément de $S^{-1}A$ est de la forme $a/s$ avec $a \in A$ et $s \neq 0$. S'il est nul, il existe un élément $b \in A \setminus \{0\}$ tel que $ab = 0$. Puisque A est intègre, on a alors $a = 0$. En particulier, $1/1 \neq 0$ dans $S^{-1}A$. Si $a/s$ n'est au contraire pas nul, on a $a \neq 0$ et $s/a$ est un élément de $S^{-1}A$ tel que $(a/s)(s/a) = as/as = 1$. Par suite, $a/s$ est inversible. Nous avons donc prouvé que $S^{-1}A$ est un corps. □

b) Soit A un anneau et $s \in A$ un élément non nilpotent. Alors, la partie $S = \{1; s; s^2; \ldots\}$ est une partie multiplicative qui ne contient pas 0 et l'anneau localisé $S^{-1}A$ est non nul (voir la remarque a) ci-dessous). On le note en général $A_s$.

c) Soit $f : A \to B$ un homomorphisme d'anneaux. Si S est une partie multiplicative de A, $f(S)$ est une partie multiplicative de B. Si T est une partie multiplicative de B, $f^{-1}(T)$ est une partie multiplicative de A. Lorsque le morphisme $f$ est implicite, par exemple lorsque B est explictement une A-algèbre, on s'autorisera l'abus d'écriture $S^{-1}B$ pour $T^{-1}B$.

d) Si I est un idéal d'un anneau A, l'ensemble $S = 1 + I$ des éléments $a \in A$ tels que $a - 1 \in I$ est une partie multiplicative. C'est l'image réciproque de la partie multiplicative $\{1\}$ de A/I par la surjection canonique $A \to A/I$.

*Remarques 3.2.5.* — a) À quelle condition l'anneau $S^{-1}A$ peut-il être nul ? Il résulte de la définition qu'une fraction $a/s$ est nulle dans $S^{-1}A$ si et seulement s'il existe $t \in S$ tel que $t(a1 - s0) = at = 0$. Dire que $S^{-1}A$ est l'anneau nul signifie alors que $1/1 = 1 = 0 = 0/1$, et donc qu'il existe $s \in S$ tel que $s \cdot 1 = s = 0$, autrement dit que $0 \in S$. On peut donc affirmer que *l'anneau* $S^{-1}A$ *est nul si et seulement si* 0 *appartient à* S.

Cela justifie *a posteriori* l'interdiction de diviser par zéro : si l'on s'autorisait cela, les règles du calcul de fractions rendraient toute fraction égale à 0 !

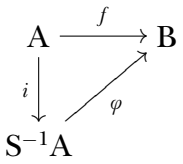
b) La définition de la relation d'équivalence dans la construction de l'anneau localisé peut sembler surprenante puisqu'elle est plus faible que l'« égalité du produit en croix » $at = bs$. Lorsque l'anneau est intègre et $0 \notin S$, ou plus généralement lorsque tous les éléments de S sont simplifiables, c'est équivalent. En revanche, dans le cas général, l'égalité du produit en croix ne fournirait pas une relation d'équivalence.

*Exercice 3.2.6.* — Soit A un anneau et soit S une partie multiplicative de A. Montrer que l'homomorphisme canonique $i : A \to S^{-1}A$ est injectif si et seulement si tout élément de S est simplifiable.

L'importance de cette construction vient de la *propriété universelle* qu'elle vérifie :

THÉORÈME 3.2.7. — *Soit* A *un anneau et* S *une partie multiplicative de* A. *Notons* $i : A \to S^{-1}A$ *l'homomorphisme d'anneaux que nous venons de construire. Alors, pour tout anneau* B *et tout homomorphisme* $f : A \to B$ *tel que* $f(S) \subset B^\times$, *il existe un unique homomorphisme* $\varphi : S^{-1}A \to B$ *tel que* $f = \varphi \circ i$.

On peut résumer cette dernière formule en disant que le diagramme




est commutatif.

*Démonstration.* — Si un tel $\varphi$ existe, il doit vérifier

$$\varphi(a/s)f(s) = \varphi(a/s)\varphi(i(s)) = \varphi(a/s)\varphi(s/1) = \varphi(a/1) = \varphi(i(a)) = f(a)$$

et donc

$$\varphi(a/s) = f(s)^{-1}f(a)$$

où $f(s)^{-1}$ désigne l'inverse de $f(s)$ dans B. Cela prouve qu'il existe un plus un tel homomorphisme $\varphi$. Pour montrer son existence, il suffit de vérifier que la formule indiquée définit un homomorphisme $\varphi : S^{-1}A \to B$ tel que $\varphi \circ i = f$.

Tout d'abord, si $(a/s) = (b/t)$, soit $u \in S$ tel que $u(at - bs) = 0$. Alors,

$$\begin{aligned} f(s)^{-1}f(a) &= f(s)^{-1}f(tu)^{-1}f(tu)f(a) = f(stu)^{-1}f(atu) \\ &= f(stu)^{-1}f(bsu) = f(t)^{-1}f(b), \end{aligned}$$

ce qui prouve que $\varphi$ est bien défini. Quant à la vérification des axiomes d'un homomorphisme d'anneaux, on a

$$\varphi(0) = f(0/1) = f(1)^{-1}f(0) = 0 \quad \text{et} \quad \varphi(1) = f(1/1) = f(1)^{-1}f(1) = 1.$$

Puis,

$$\begin{aligned} \varphi(a/s) + \varphi(b/t) &= f(s)^{-1}f(a) + f(t)^{-1}f(b) = f(st)^{-1}\left(f(at) + f(bs)\right) \\ &= f(st)^{-1}f(at + bs) = \varphi((at + bs)/st) = \varphi((a/s) + (b/t)). \end{aligned}$$

Enfin,

$$\begin{aligned}\varphi(a/s)\varphi(b/t) &= f(s)^{-1}f(a)f(t)^{-1}f(b) = f(st)^{-1}f(ab)\\ &= \varphi(ab/st) = \varphi((a/s)(b/t)).\end{aligned}$$

L'application $\varphi$ est donc un homomorphisme et le théorème est démontré. □

On peut enfin construire l'anneau localisé comme un quotient.

PROPOSITION 3.2.8. — *Soit* A *un anneau, a un élément de* A *et* $S = \{1; a; a^2; \ldots\}$ *la partie multiplicative de* A *formée des puissances de a. L'homomorphisme canonique*

$$\varphi\colon A[X] \to S^{-1}A, \quad P \mapsto P(1/a)$$

*est surjectif, de noyau l'idéal* $(1 - aX)$. *Il en résulte un isomorphisme*

$$\bar{\varphi}\colon A[X]/(1 - aX) \simeq S^{-1}A.$$

*Démonstration.* — Un élément de $S^{-1}A$ s'écrit $b/a^n$ pour un certain $n \geq 1$ et un élément $b \in A$. On a ainsi $b/a^n = \varphi(bX^n)$ et $\varphi$ est bien surjectif. Son noyau contient certainement $1 - aX$ puisque $\varphi(1 - aX) = 1 - a/a = 0$. Il contient par suite l'idéal $(1 - aX)$. Il en résulte par la propriété universelle des anneaux quotients un homomorphisme bien défini $\bar{\varphi}\colon A[X]/(1 - aX) \to S^{-1}A$. Nous allons montrer que $\bar{\varphi}$ est un isomorphisme. D'après la proposition 3.1.5, il en résultera que $\operatorname{Ker}\varphi = (1 - aX)$.

Définissons donc l'inverse de $\bar{\varphi}$. Soit $g$ l'homomorphisme canonique $A \to A[X]/(1 - aX)$ tel que pour tout $b \in A$, $b \mapsto \mathrm{cl}(b)$, la classe du polynôme constant $b$. Dans l'anneau $A[X]/(1 - aX)$, on a $\mathrm{cl}(aX) = 1$ et donc $\mathrm{cl}(a)$ est inversible, d'inverse $\mathrm{cl}(X)$. La propriété universelle de la localisation affirme qu'il existe un unique morphisme $\psi : S^{-1}A \to A[X]/(1 - aX)$ tel que pour tout $b \in A$, $\psi(b/1) = g(b)$. Par construction, si $b \in A$ et $n \geq 1$, $\psi(b/a^n) = b\,\mathrm{cl}(X^n) = \mathrm{cl}(bX^n)$.

Finalement, montrons que $\psi$ est l'inverse de $\bar{\varphi}$. Si $P \in A[X]$, $\psi(\bar{\varphi}(\mathrm{cl}(P))) = \psi(P(1/a))$. Par suite, si $P = \sum b_n X^n$, on a

$$\begin{aligned}\psi(\bar{\varphi}(\mathrm{cl}(P))) &= \psi(\varphi(P)) = \psi(P(1/a))\\ &= \psi\Big(\sum(b_n/a^n)\Big) = \sum\psi(b_n/a^n)\\ &= \sum\mathrm{cl}(bX^n) = \mathrm{cl}\Big(\sum b_n X^n\Big) = \mathrm{cl}(P)\end{aligned}$$

et $\psi \circ \bar{\varphi} = \mathrm{Id}$. Enfin,

$$\bar{\varphi}(\psi(b/a^n)) = \bar{\varphi}(\mathrm{cl}(bX^n)) = \varphi(aX^n) = b/a^n$$

et $\bar{\varphi} \circ \psi = \mathrm{Id}$. L'homomorphisme $\bar{\varphi}$ est donc un isomorphisme, ce qu'il fallait démontrer. □

La généralisation au cas d'une partie multiplicative quelconque est laissée en exercice.

*Exercice 3.2.9.* — Soit A un anneau, soit S une partie multiplicative de A.

a) On suppose qu'il existe $s$ et $t \in S$ tel que S est l'ensemble des $s^n t^m$ lorsque $n$ et $m$ parcourent $\mathbf{N}$. Montrer que l'homomorphisme $A[X,Y] \to S^{-1}A$, $P(X,Y) \mapsto P(1/s, 1/t)$ est surjectif et que son noyau contient l'idéal $(1 - sX, 1 - tY)$ engendré par $1 - sX$ et $1 - tY$ dans $A[X,Y]$. En déduire un isomorphisme $A[X,Y]/(1 - sX, 1 - tY) \simeq S^{-1}A$.

b) Plus généralement, soit $\langle 1 - sX_s \rangle_{s\in S}$ l'idéal de l'anneau de polynômes (en une infinité de variables) $A[(X_s)_{s\in S}]$ engendré par les polynômes $1 - sX_s$, lorsque $s$ parcourt S. Alors, l'homomorphisme canonique

$$A[(X_s)_{s\in S}] \to S^{-1}A, \quad P \mapsto P((1/s)_s)$$

induit un isomorphisme

$$A[(X_s)_{s\in S}]/\langle 1 - sX_s \rangle_{s\in S} \simeq S^{-1}A.$$

*3.2.10. Localisation et quotient.* — Enfin, étudions brièvement les idéaux de $S^{-1}A$. Un premier résultat est le suivant :

Proposition 3.2.11. — *Pour tout idéal $\mathscr{J}$ de $S^{-1}A$, il existe un idéal I de A tel que $\mathscr{J} = i(I)(S^{-1}A)$. On peut en fait prendre $I = i^{-1}(\mathscr{J})$.*

*Démonstration.* — Il faut montrer que

$$\boxed{\mathscr{J} = i(i^{-1}(\mathscr{J}))(S^{-1}A).}$$

Comme $i(i^{-1}(\mathscr{J})) \subset \mathscr{J}$, l'idéal engendré par $i(i^{-1}(\mathscr{J}))$ est contenu dans $\mathscr{J}$, d'où l'inclusion

$$i(i^{-1}(\mathscr{J}))(S^{-1}A) \subset \mathscr{J}.$$

Réciproquement, si $x \in \mathscr{J}$, choisissons $a \in A$ et $s \in S$ tels que $x = a/s$. On a alors $sx \in I$ et comme $sx = a/1 = i(a)$, $a$ appartient à $i^{-1}(\mathscr{J})$. Il en résulte que $sx \in i(i^{-1}(\mathscr{J}))$, puis $x = (sx)(1/s)$ appartient à $i(i^{-1}(\mathscr{J}))(S^{-1}A)$, ce qui établit l'autre inclusion. □

L'idéal $i(I)S^{-1}A$ sera aussi noté $IS^{-1}A$, en omettant le morphisme $i$. Il sera aussi noté $S^{-1}I$, cette dernière notation étant celle qui sera utilisée dans le cas plus général de la localisation des modules.

Proposition 3.2.12. — *Soit A un anneau, soit S une partie multiplicative de A et soit I un idéal de A. Soit $T = \mathrm{cl}(S) \subset A/I$ l'image de S par la surjection canonique $A \to A/I$. Il existe un unique isomorphisme*

$$\varphi : S^{-1}A/IS^{-1}A \xrightarrow{\sim} T^{-1}(A/I)$$

*tel que pour tout $a \in A$, $\varphi(\mathrm{cl}(a/1)) = \mathrm{cl}(a)/1$.*

Dit plus abstraitement, les deux anneaux $S^{-1}A/IS^{-1}A$ et $T^{-1}(A/I)$ sont des A-algèbres : un quotient ou un localisé d'une A-algèbre sont des A-algèbres. La proposition affirme alors qu'il existe un *unique isomorphisme de* A*-algèbres* entre ces deux anneaux.

*Démonstration.* — On peut donner une démonstration explicite, mais la méthode la plus élégante (et la plus abstraite) utilise les propriétés universelles des quotients et des localisés. Considérons le morphisme d'anneaux composé

$$A \to A/I \to T^{-1}(A/I), \quad a \mapsto \mathrm{cl}(a)/1.$$

Par ce morphisme, un élément $s \in S$ a pour image $\mathrm{cl}(s)/1$ qui est inversible dans $T^{-1}(A/I)$, d'inverse $1/\mathrm{cl}(s)$. La propriété universelle de la la localisation affirme qu'il existe un unique homomorphisme d'anneaux

$$\varphi_1 \colon S^{-1}A \to T^{-1}(A/I)$$

par lequel $a/1$ a pour image $\mathrm{cl}(a)/1$.

Par cet homomorphisme, un élément $a/1$ avec $a \in I$ a pour image

$$\varphi_1(a/1) = \varphi_1(a)/1 = \mathrm{cl}(a)/1 = 0$$

puisque $a \in I$ et donc $\mathrm{cl}(a) = 0$ dans $A/I$. Par suite, le noyau de $\varphi_1$ contient l'image de I dans $S^{-1}A$ ; il contient automatiquement l'idéal $IS^{-1}A$ qui est engendré par I dans $S^{-1}A$. D'après la propriété universelle des anneaux quotients, il existe un unique homomorphisme d'anneaux

$$\varphi \colon S^{-1}A/IS^{-1}A \to T^{-1}(A/I)$$

tel que pour tout $a/s \in S^{-1}A$, $\varphi(\mathrm{cl}(a/s)) = \mathrm{cl}(a)/\mathrm{cl}(s)$.

Nous avons montré qu'il existe un unique morphisme de A-algèbres $\varphi$ : $S^{-1}A/IS^{-1}A \to T^{-1}(A/I)$. On peut aussi résumer ces constructions par le diagramme commutatif

$$\begin{array}{ccccc} & & S^{-1}A & \longrightarrow & S^1A/IS^{-1}A \\ & \nearrow & & \searrow^{\varphi_1} & \downarrow \varphi \\ A & & & & \\ & \searrow & A/I & \longrightarrow & T^{-1}(A/I). \end{array}$$

Reprenons ce diagramme dans l'autre sens. Le noyau du morphisme de A-algèbres $A \to S^{-1}A/IS^{-1}A$ contient I, d'où un unique morphisme de A-algèbres

$$\psi_1 \colon A/I \to S^{-1}A/IS^{-1}A$$

(donc vérifiant que pour tout $a \in A$, $\psi_1(\mathrm{cl}(a)) = \mathrm{cl}(a/1)$). Si $s \in S$, $\psi_1(\mathrm{cl}(s)) = \mathrm{cl}(s/1)$ est inversible, d'inverse $\mathrm{cl}(1/s)$. Ainsi, l'image de T par $\psi_1$ est formée

d'éléments inversibles dans $S^{-1}A/IS^{-1}A$. Il existe donc un unique morphisme de A-algèbres

$$\psi : T^{-1}(A/I) \to S^{-1}A/IS^{-1}A$$

(c'est-à-dire tel que pour tout $a \in A$, $\psi(\mathrm{cl}(a)/1) = \mathrm{cl}(a/1)$). Ces constructions sont synthétisées par le diagramme commutatif

$$\begin{array}{ccc} & S^{-1}A & \longrightarrow S^1A/IS^{-1}A \\ A \nearrow & & \uparrow \psi \\ A \searrow & \overset{\psi_1}{\nearrow} & \\ & A/I & \longrightarrow T^{-1}(A/I). \end{array}$$

Finalement, si $a \in A$ et $s \in S$, on a $\varphi(\mathrm{cl}(a/s)) = \mathrm{cl}(a)/\mathrm{cl}(s)$ dans $T^{-1}(A/I)$ et $\psi(\mathrm{cl}(a)/\mathrm{cl}(s)) = \mathrm{cl}(a/s)$ dans $S^{-1}A/IS^{-1}A$ d'où il résulte que $\varphi \circ \psi$ et $\psi \circ \varphi$ sont l'identité. □

Cette dernière proposition reviendra plus tard sous le vocable *exactitude de la localisation*.

## 3.3. Exercices

*Exercice 3.3.1.* — Soit K un corps. Soient $a$ et $b$ deux éléments de K. Montrer les assertions suivantes :

**a)** l'anneau $K[X]/(X-a)$ est isomorphe à K ;
**b)** l'anneau $K[X,Y]/(Y-b)$ est isomorphe à $K[X]$ ;
**c)** l'anneau $K[X,Y]/(X-a,Y-b)$ est isomorphe à K.

*Exercice 3.3.2.* — Soit $n$ un entier $\geq 1$. On note $s : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ la surjection canonique.

**a)** Étant donné un entier $m$, montrer que $s(m)$ est inversible dans l'anneau $\mathbf{Z}/n\mathbf{Z}$ si et seulement si $n$ et $m$ sont premiers entre eux.
**b)** Montrer que l'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si $n$ est premier.
**c)** Si $n$ est premier, montrer que l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps.
**d)** Déterminer l'idéal $\sqrt{n\mathbf{Z}}$.

*Exercice 3.3.3.* — Soit K un corps. On pose $A = K[X,Y]/(X^2, XY, Y^2)$.

**a)** Déterminer les éléments inversibles de A ;
**b)** déterminer tous les idéaux principaux de A ;
**c)** déterminer tous les idéaux de A.

*Exercice 3.3.4.* — Soient K un corps et $\varphi : K[U,V] \to K[X]$ l'homomorphisme d'anneaux défini par les égalités $\varphi(U) = X^3$, $\varphi(V) = -X^2$ et $\varphi(a) = a$ pour tout $a$ dans K. Quels sont les noyau et image de $\varphi$. Soit A l'image de $\varphi$. Montrer que A est intègre et que son corps des fractions est isomorphe à K(X).

*Exercice 3.3.5.* — Soit S une partie multiplicative de A ne contenant pas 0. On note $\mathfrak{r}(A)$ l'ensemble des éléments nilpotents de A.

**a)** Si A est intègre, montrer que $S^{-1}A$ est intègre.

**b)** Si A est réduit, montrer que $S^{-1}A$ est réduit.

**c)** On note $f : A \to S^{-1}A$ l'homomorphisme naturel $a \mapsto a/1$. Montrer en fait que

$$\mathfrak{r}(S^{-1}A) = \mathfrak{r}(A)\, S^{-1}A.$$

## 3.4. Solutions

*Solution de l'exercice 3.3.1.* — **a)** Soit $\varphi : K[X] \to K$ l'homomorphisme d'anneaux défini par $\varphi(P) = P(a)$. Il est surjectif et son noyau contient l'idéal $(X - a)$. D'autre part, si $P \in \operatorname{Ker}\varphi$, i.e. si $P(\alpha) = 0$, le théorème de factorisation implique que P est de la forme $P(X) = Q(X)(X - a)$, autrement dit $P \in (X - a)$. Ainsi, $\varphi$ est un isomorhisme.

**b)** On définit $\psi : K[X,Y] \to K[X]$ par $P(X,Y) \mapsto P(X,b)$. Il est surjectif, son noyau contient l'idéal $(Y - b)$. Enfin, si $P(X,Y)$ est tel que $P(X,b) = 0$, prouvons que $P(X,Y)$ est multiple de $Y - b$. On peut en effet invoquer le théorème de factorisation dans l'anneau des polynômes en une variable à coefficients dans l'anneau intègre K[X]. Mais on peut le démontrer directement : on écrit

$$P(X,Y) = \sum_{k=0}^{m} P_k(Y)X^k, \qquad P_k \in K[Y].$$

Alors, $P(X,b) = \sum_{k=0}^{m} P_k(b)X^k = 0$, si bien que $P_k$ est multiple de $Y - b$, et donc P est multiple de $Y - b$.

**c)** On introduit $\eta : K[X,Y] \to K$ donné par $\eta(P) = P(a,b)$. C'est le composé $\varphi \circ \psi$. Son noyau contient l'idéal $(X - a, Y - b)$. Réciproquement, soit $P \in K[X,Y]$ tel que $P(a,b) = 0$. La division euclidienne de P par $Y - b$ dans $K[X][Y]$ nous permet d'écrire

$$P(X,Y) = (Y - b)Q(X,Y) + R(X,Y)$$

où $R(X,Y)$ est un polynôme de degré en Y strictement inférieur à 1, donc un polynôme $R(X)$ en X seulement. Alors, $P(a,b) = R(a) = 0$, ce qui implique que $R(X)$ s'écrit $(X - a)S(X)$. Finalement, on a bien $P(X,Y) \in (X - a, Y - b)$.

*Solution de l'exercice 3.3.2.* — **a)** Soit $m \in \mathbf{Z}$. Dire que $s(m)$ est inversible signifie qu'il existe $m' \in \mathbf{Z}$ tel que $s(m)s(m') = s(1)$. Cela implique qu'il existe $k \in \mathbf{Z}$ tel que $mm' = 1 + nk$, d'où une relation de Bézout entre $m$ en $n$ qui sont donc premiers entre eux.

Réciproquement, si $m$ et $n$ sont premiers entre eux, il existe $u \in \mathbf{Z}$ et $v \in \mathbf{Z}$ tels que $um + vn = 1$, d'où $s(u)s(m) = s(1) : s(m)$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$, d'inverse $s(u)$.

**b)** Supposons que $n$ est premier et montrons que $\mathbf{Z}/n\mathbf{Z}$ est intègre. Soient $a$ et $b$ tels que $s(a)s(b) = s(0)$. Cela signifie que $ab$ est un multiple de $n$, donc, $n$ étant premier, que $n$ divise $a$ ou que $n$ divise $b$ (théorème de Gauß). Ainsi, $s(a) = 0$ ou $s(b) = 0$.

Dans l'autre sens, si $n$ n'est pas premier, on peut écrire $n = n_1 n_2$ pour des entiers $n_1$ et $n_2$ tels que $1 < n_1 < n$ et $1 < n_2 < n$. En particulier, $s(n_1)$ et $s(n_2)$ sont non nuls dans $\mathbf{Z}/n\mathbf{Z}$. Or, $s(n_1)s(n_2) = s(n_1 n_2) = s(n) = s(0)$. Ainsi, $\mathbf{Z}/n\mathbf{Z}$ n'est pas intègre.

**c)** Supposons maintenant $n$ premier et montrons que $\mathbf{Z}/n\mathbf{Z}$ est un corps. Si $m$ est un élément de $\mathbf{Z}$ tel que $s(m) \neq 0$ dans $\mathbf{Z}/n\mathbf{Z}$, cela signifie que $n$ ne divise pas $m$, donc que $m$ et $n$ sont premiers entre eux. D'après le a), $s(m)$ est inversible dans $s(n)$. Par suite, $\mathbf{Z}/n\mathbf{Z}$ est un corps.

**d)** Soit $n = \prod_i p_i^{n_i}$ la décomposition de $n$ en facteurs premiers distincts (avec $n_i \geq 1$).

Soit $a \in \sqrt{n\mathbf{Z}}$. Il existe ainsi $k \geq 1$ tel que $a^k \in n\mathbf{Z}$, autrement dit tel que $a^k$ est multiple de $n$. Nécessairement, pour tout nombre premier $p$ divisant $n$, $a^k$ sera multiple de $p$, donc $a$ aussi. Ainsi, $a$ est multiple de $\prod_i p_i$.

Réciproquement, l'élément $a = \prod_i p_i$ appartient au radical de $n\mathbf{Z}$. Soit en effet $k = \max_i n_i$. Alors $a^k = \prod_i p_i^k$ est visiblement multiple de $n$.

On a ainsi montré que $\sqrt{n\mathbf{Z}} = \prod_i p_i \mathbf{Z}$.

On aurait aussi pu remarquer que si $p$ est premier, l'idéal $p\mathbf{Z}$ contient l'idéal $n\mathbf{Z}$ si et seulement si $p|n$. Ainsi, le radical de $n\mathbf{Z}$ est l'intersection des idéaux $p\mathbf{Z}$ pour les nombres premiers divisant $n$. D'après le lemme chinois, c'est l'idéal $(\prod_i p_i)$.

*Solution de l'exercice 3.3.3.* — **a)** Notons $x$ et $y$ l'image de X et Y dans A. On a donc $x^2 = xy = y^2 = 0$. Tout élément de A s'écrit de manière unique sous la forme $a + bx + cy$, avec $(a, b, c) \in \mathrm{K}^3$. Si $a' + b'x + c'y$ est un autre élément de A, on a

$$(a + bx + cy)(a' + b'x + c'y) = aa' + (ab' + a'b)x + (ac' + a'c)y,$$

si bien que $a + bx + cy$ est inversible si et seulement si le système

$$aa' = 1, \quad ab' + a'b = 0, \quad ac' + a'c = 0$$

a une solution $(a', b', c')$. Il faut $a \neq 0$, et dans ce cas, $a' = 1/a$, $b' = -b/a^2$ et $c' = -c/a^2$ est solution. Ainsi, *$a + bx + cy$ est inversible si et seulement si $a \neq 0$.*

**b)** Les idéaux 0 et A sont principaux, engendrés respectivement par 0 et 1. Soit maintenant I un idéal principal de A distinct de 0 et de A. Il est engendré par un élément $a + bx + cy$ de A non nul et non inversible, donc $a = 0$. Remarquons que l'on a

$$(\alpha + \beta x + \gamma y)(bx + cy) = (\alpha b)x + (\alpha c)y = \alpha(bx + cy).$$

Ainsi, l'élément (non nul) $b'x + c'y$ appartient à l'idéal engendré par $bx + cy$ si et seulement si le couple $(b', c')$ est multiple du couple $(b, c)$. Alors, $\alpha \neq 0$, si bien que ces éléments diffèrent par multiplication de l'élément inversible $\alpha$ et définissent le même idéal. On peut ainsi supposer que $b = 1$, ou que $b = 0$, auquel cas on suppose $c = 0$ ou $c = 1$.

*Les idéaux principaux de* A *sont donc* $(0)$, $(x + \lambda y)$ *avec* $\lambda \in \mathrm{K}$, $(y)$ *et* A *lui-même.*

**c)** Soit I un idéal non principal, en particulier, $\mathrm{I} \neq \mathrm{A}$. Il contient ainsi deux éléments $bx + cy$ et $b'x + c'y$ non proportionnels. Ainsi, par combinaisons linéaires, I contient tous les éléments de la forme $\beta x + \gamma y$, c'est-à-dire l'idéal $(x, y)$. Il est maximal (tout autre élément est inversible), donc le seul idéal de A non principal est $(x, y)$.

*Solution de l'exercice 3.3.4.* — On constate qu'un polynôme multiple de $\mathrm{U}^2 + \mathrm{V}^3$ est dans le noyau de $\varphi$. Réciproquement, si $\varphi(\mathrm{P}) = 0$, effectuons la division euclidienne de P par $\mathrm{U}^2 + \mathrm{V}^3$ dans $\mathrm{K}[\mathrm{V}][\mathrm{U}]$. On trouve deux polynômes $\mathrm{P}_2$ et $\mathrm{P}_3 \in \mathrm{K}[\mathrm{U}, \mathrm{V}]$, avec $\mathrm{P}_3 = 0$ ou $\deg_{\mathrm{U}} \mathrm{P}_3 < 2$ tels que

$$\mathrm{P}(\mathrm{U}, \mathrm{V}) = (\mathrm{U}^2 + \mathrm{V}^3)\mathrm{P}_2(\mathrm{U}, \mathrm{V}) + \mathrm{P}_3(\mathrm{U}, \mathrm{V}).$$

On écrit $\mathrm{P}_3(\mathrm{U}, \mathrm{V}) = \mathrm{A}(\mathrm{V}) + \mathrm{UB}(\mathrm{V})$, et on a donc $\varphi(\mathrm{P}) = \mathrm{A}(-\mathrm{X}^2) + \mathrm{X}^3\mathrm{B}(-\mathrm{X}^2) = 0$. Nécessairement, en considérant les parties paires et impaires de $\varphi(\mathrm{P})$, on trouve que $\mathrm{A} = \mathrm{B} = 0$. Autrement dit, $\operatorname{Ker}\varphi = (\mathrm{U}^2 + \mathrm{V}^3)$.

Soit $\mathrm{P} = \sum a_{i,j}\mathrm{U}^i\mathrm{V}^j$. On voit que $\varphi(\mathrm{P}) = \sum_{i,j} a_{i,j}(-1)^j\mathrm{X}^{3i+2j}$. Tous les degrés $\geq 2$ sont possibles, si bien que l'image de $\varphi$ est formée des polynômes dont le terme de degré 1 est nul. Notons $\mathrm{A} = \Im\varphi$. C'est un sous-anneau de $\mathrm{K}[\mathrm{X}]$ qui est intègre, donc A est intègre.

Son corps des fractions est un sous-corps de $\mathrm{K}(\mathrm{X})$. Pour montrer que c'est $\mathrm{K}(\mathrm{X})$ lui-même, il suffit de montrer que X y appartient. Or, $\mathrm{X} = \mathrm{X}^3/\mathrm{X}^2 = -\varphi(\mathrm{U})/\varphi(\mathrm{V})$.

*Solution de l'exercice 3.3.5.* — **a)** Soit $a/s$ et $b/t$ deux élémentsde $\mathrm{S}^{-1}\mathrm{A}$ de produit nul. Il existe ainsi $u \in \mathrm{S}$ tel que $u(ab) = 0$. Comme A est intègre et $u \neq 0$, $ab = 0$. Ainsi, $a = 0$ ou $b = 0$ et donc $a/s = 0$ ou $b/t = 0$. L'anneau $\mathrm{S}^{-1}\mathrm{A}$ est intègre.

**b)** Soit $a/s \in \mathrm{S}^{-1}\mathrm{A}$ un élément nilpotent. Il existe alors $t \in \mathrm{S}$ tel que $ta^n = 0$. Cela implique que $(ta)^n = 0$, donc que $ta$ est nilpotent. Comme A est réduit, $ta = 0$, d'où $a/s = 0$ dans $\mathrm{S}^{-1}\mathrm{A}$, et $\mathrm{S}^{-1}\mathrm{A}$ est réduit.

**c)** Soit $a/s$ un élément nilpotent de $\mathrm{S}^{-1}\mathrm{A}$. Cela signifie qu'il existe $n \geq 0$ et $t \in \mathrm{S}$ tel que $ta^n = 0$. A fortiori, $ta$ est nilpotent dans A. Autrement dit, tout élément nilpotent de $\mathrm{S}^{-1}\mathrm{A}$ est multiple de l'image d'un élément nilpotent de A par un élément de S (qui est inversible dans $\mathrm{S}^{-1}\mathrm{A}$). Il en résulte que l'idéal engendré par $f(\mathfrak{r}(\mathrm{A}))$ contient $\mathfrak{r}(\mathrm{S}^{-1}\mathrm{A})$. L'autre inclusion est évidente.

# 4 Idéaux premiers, maximaux

*La première partie de cette leçon est consacrée aux notions d'idéaux premiers et maximaux. Ces notions généralisent le concept classique de nombre premier. Leur importance est apparue au XIX^e siècle avec les travaux de KUMMER en arithmétique.*
*Dans la seconde partie, on introduit le langage de la géométrie algébrique et on démontre le théorème des zéros de HILBERT.*

## 4.1. Idéaux premiers, idéaux maximaux

La notion d'idéal premier généralise celle de nombre premier. En effet, par définition d'un nombre premier, si un produit d'entiers $ab$ est multiple de $p$, $a$ ou $b$ est multiple de $p$. Cela amène à la définition :

DÉFINITION 4.1.1. — *Soit* A *un anneau et soit* I *un idéal de* A. *On dit que* I *est un idéal* premier *s'il vérifie les propriétés :*
- $I \neq A$ ;
- *si* $a$ *et* $b$ *sont deux éléments de* A *tels que* $ab \in I$, *alors ou bien* $a \in I$, *ou bien* $b \in I$.

La condition $I \neq A$ est analogue à la convention qui dit que 1 n'est pas un nombre premier. Par ailleurs, la seconde condition s'utilise parfois sous la forme équivalente (contraposée) : *si* $a$ *et* $b$ *sont deux éléments de* A *n'appartenant pas à* I, *alors leur produit* $ab$ *n'appartient pas à* I.

*Remarque 4.1.2.* — Un idéal I de A est premier si et seulement si $A \setminus I$ est une partie multiplicative.

THÉORÈME 4.1.3. — *Un idéal* I *d'un anneau* A *est premier si et seulement si l'anneau quotient* A/I *est intègre.*

*Démonstration.* — Dire que A/I est intègre signifie d'abord que $A/I \neq 0$, c'est-à-dire que $I \neq A$, et ensuite que si un produit $xy$ d'éléments de A/I est nul,

alors $x$ ou $y$ est nul. Écrivons $x = \mathrm{cl}(a)$ et $y = \mathrm{cl}(b)$ avec $a$ et $b$ dans A. Comme $xy = \mathrm{cl}(a)\,\mathrm{cl}(b) = \mathrm{cl}(ab)$, $xy = 0$ équivaut à $ab \in \mathrm{I}$. □

*Exemples 4.1.4.* — a) L'idéal (0) d'un anneau A est premier si et seulement si A est intègre.

b) Il a été démontré dans l'exercice 3.3.2 que pour tout $n \geq 1$, l'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si $n$ est premier. Comme $\mathbf{Z}$ est intègre, les idéaux premiers de $\mathbf{Z}$ sont donc, d'une part l'idéal (0), et d'autre part les idéaux $(p)$ où $p$ parcourt l'ensemble des nombres premiers.

c) Si $k$ est un corps, les idéaux (X) et (X,Y) de $k[\mathrm{X},\mathrm{Y}]$ sont premiers (cf. l'exercice 3.3.1).

PROPOSITION 4.1.5. — *Soit* $f : \mathrm{A} \to \mathrm{B}$ *un homomorphisme d'anneaux. Si* I *est un idéal premier de* B, $f^{-1}(\mathrm{I})$ *est un idéal premier de* A.

*Démonstration.* — *Première méthode (naïve).* Comme $f(1) = 1$ n'appartient pas à I, $1 \notin f^{-1}(\mathrm{I})$ et $f^{-1}(\mathrm{I}) \neq \mathrm{A}$. D'autre part, soit $a$ et $b$ deux éléments de A tels que $ab \in f^{-1}(\mathrm{I})$. On a ainsi $f(ab) = f(a)f(b) \in \mathrm{I}$. Comme I est supposé premier, $f(a) \in \mathrm{I}$ ou $f(b) \in \mathrm{I}$, ce qui signifie $a \in f^{-1}(\mathrm{I})$ ou $b \in f^{-1}(\mathrm{I})$.

*Seconde méthode.* L'idéal $f^{-1}(\mathrm{I})$ est le noyau de l'homomorphisme composé $\mathrm{A} \to \mathrm{B} \to \mathrm{B/I}$. On en déduit un homomorphisme injectif $\mathrm{A}/f^{-1}(\mathrm{I}) \hookrightarrow \mathrm{B/I}$ et $\mathrm{A}/f^{-1}(\mathrm{I})$ est isomorphe à un sous-anneau de B/I. Comme un sous-anneau d'un anneau intègre est intègre et comme B/I est intègre, $\mathrm{A}/f^{-1}(\mathrm{I})$ est intègre. L'idéal $f^{-1}(\mathrm{I})$ est donc premier. □

DÉFINITION 4.1.6. — *Soit* A *un anneau. Un idéal* I *de* A *est dit* maximal *s'il est distinct de* A *et si les seuls idéaux de* A *qui contiennent* I *sont* I *et* A.

On remarquera que cela signifie que I est un élément maximal de l'ensemble des idéaux de A distincts de A pour la relation d'ordre donnée par l'inclusion.

Comme pour les idéaux premiers, on peut donner une caractérisation des idéaux maximaux en termes de quotients.

THÉORÈME 4.1.7. — *Un idéal* I *d'un anneau* A *est maximal si et seulement si l'anneau quotient* A/I *est un corps.*

*Démonstration.* — Supposons que A/I est un corps. Comme l'anneau nul n'est pas un corps, $\mathrm{A/I} \neq 0$ et $\mathrm{I} \neq \mathrm{A}$. Soit d'autre part un idéal J de A contenant I. Si $\mathrm{J} \neq \mathrm{I}$, il existe ainsi $a \in \mathrm{J} \setminus \mathrm{I}$. Sa classe $\mathrm{cl}(a) \in \mathrm{A/I}$ est donc non nulle, donc inversible puisque A/I est un corps. Soit $b \in \mathrm{A}$ tel que $\mathrm{cl}(a)\,\mathrm{cl}(b) = 1$. On a donc $ab - 1 \in \mathrm{I}$ et comme $a \in \mathrm{J}$, $1 = ab - (ab - 1) \in \mathrm{J}$. Par suite, $\mathrm{J} = \mathrm{A}$.

Montrons réciproquement que si $\mathrm{I} \neq \mathrm{A}$ et si tout idéal de A contenant I est égal à I ou A, alors A/I est un corps. Déjà, A/I est non nul. Si maintenant

$x \in A/I$ est non nul, il existe $a \in A$ tel que $x = \mathrm{cl}(a)$, et l'on a $a \notin I$. L'idéal $I + (a)$ contient I ; comme il contient $a$, il est distinct de I. Par hypothèse, on a donc $I + (a) = A$, ce qui signifie qu'il existe $b \in I$ et $c \in A$ tels que $1 = b + ac$. Alors, dans l'anneau A/I, on a $1 = \mathrm{cl}(1) = \mathrm{cl}(b + ac) = \mathrm{cl}(a)\,\mathrm{cl}(c) = x\,\mathrm{cl}(c)$, ce qui prouve que $x$ est inversible dans A/I. □

*Exemple 4.1.8.* — a) L'idéal (0) d'un anneau A n'est maximal que si A est un corps.

b) Un idéal maximal est nécessairement premier.

c) Les idéaux maximaux de $\mathbf{Z}$ sont les idéaux $(p)$ avec $p$ premier. En effet, l'idéal (0) n'est pas maximal puisque $\mathbf{Z}$ n'est pas un corps. D'autre part, si $p$ est un nombre premier, l'anneau $\mathbf{Z}/p\mathbf{Z}$ est un corps d'après l'exercice 3.3.2. On le note $\mathbf{F}_p$.

*Remarque 4.1.9.* — Ainsi, si K est un corps de caractéristique $p$, le sous-corps premier de K est isomorphe à $\mathbf{F}_p$.

THÉORÈME 4.1.10 (Krull). — *Tout anneau non nul possède au moins un idéal maximal.*

En particulier, tout anneau non nul possède au moins un idéal premier.

*Démonstration.* — La preuve repose sur le lemme de Zorn. Soit A un anneau non nul et notons $\mathscr{I}$ l'ensemble des idéaux de A distincts de A. On munit $\mathscr{I}$ de l'ordre donné par l'inclusion.

L'ensemble $\mathscr{I}$ est inductif. Tout d'abord, il est non vide puisque (0) est un idéal de A distinct de A. D'autre part, si $(I_s)_{s\in S}$ est une famille (non vide) totalement ordonnée d'idéaux de A distincts de A et montrons qu'elle admet un majorant dans $\mathscr{I}$, à savoir l'idéal $\bigcup_{s\in S} I_s$. En effet, $I = \bigcup_s I_s$ est bien un idéal[(1)] : on a $0 \in I_s$ pour tout $s \in S$, donc a fortiori $0 \in I$. Ensuite, si $a \in I$ et $b \in I$, choisissons $s$ et $t \in S$ tels que $a \in I_s$ et $b \in I_t$. Que $\mathscr{I}$ soit totalement ordonnée implique que $I_s \subset I_t$ ou $I_t \subset I_s$. Dans le premier cas, on a donc $a \in I_t$ si bien que $a + b \in I_t$ et donc $a + b \in I$. Dans le second cas, on a de même $a + b \in I_s \subset I$. Enfin, si $a \in I$ et $b \in A$, soit $s$ tel que $a \in I_s$. On a $ab \in I_s$ et donc $ab \in I$. Ainsi, I est bien un idéal de A ; il contient tous les $I_s$. Reste à montrer qu'il appartient à $\mathscr{I}$ c'est-à-dire que $I \neq A$. Or, si $I = A$, on aurait $1 \in I$ ; il existerait alors $s \in S$ tel que $1 \in I_s$ ce qui impliquerait $I_s = A$. Cette contradiction montre que $I \neq A$.

Le lemme de Zorn implique alors que $\mathscr{I}$ possède un élément maximal. Soit $\mathfrak{m}$ un tel élément. C'est un idéal maximal : si I est un idéal contenant $\mathfrak{m}$ et distinct de $\mathfrak{m}$, on ne peut avoir $I \in m$ puisque $\mathfrak{m}$ est supposé maximal dans $\mathscr{I}$. Donc $I \notin \mathscr{I}$, ce qui signifie $I = A$. □

(1) Rappelons que la réunion d'une famille d'idéaux n'est pas en général un idéal, on utilise ici de manière cruciale le fait que la famille soit totalement ordonnée.

On peut appliquer ce théorème dans deux situations étudiées au chapitre précédent, à savoir celui d'un anneau quotient et celui d'un anneau localisé. On peut tout d'abord compléter les propositions 3.1.3 et 3.2.11.

PROPOSITION 4.1.11. — *Soit* $A$ *un anneau.*

*a) Soit* $I$ *un idéal de* $A$ *et notons* $\mathrm{cl} : A \to A/I$ *la surjection canonique. La bijection donnée par* $\mathrm{cl}^{-1}$ *entre idéaux de* $A/I$ *et idéaux de* $A$ *contenant* $I$ *induit des bijections entre*

– *idéaux premiers de* $A/I$ *et idéaux premiers de* $A$ *contenant* $I$ *;*

– *idéaux maximaux de* $A/I$ *et idéaux maximaux de* $A$ *contenant* $I$.

*b) Soit* $S$ *une partie multiplicative de* $A$ *et* $i : A \to S^{-1}A$ *l'homomorphisme canonique. Si* $\mathscr{I}$ *est un idéal premier de* $S^{-1}A$*, l'idéal* $I = i^{-1}(\mathscr{I})$ *est l'unique idéal premier de* $A$ *disjoint de* $S$ *tel que* $IS^{-1}A = \mathscr{I}$.

*Démonstration.* — a) Soit $J$ un idéal de $A$ contenant $I$. Il faut montrer que $J$ est premier (resp. maximal) si et seulement si $J/I$ l'est. Or, on a démontré dans la proposition 3.1.4 que $A/J$ est isomorphe à $(A/I)/(J/I)$. En vertu des critères (théorèmes 4.1.3 et 4.1.7) sur l'anneau quotient pour qu'un idéal soit premier (resp. maximal), l'idéal $J/I$ est premier (resp. maximal) dans $A/I$ si et seulement l'idéal $J$ est premier (resp. maximal) dans $A$.

b) On a démontré dans la proposition 3.2.11 que l'idéal $I$ vérifie $IS^{-1}A = \mathscr{I}$. D'autre part, il est premier d'après la proposition 4.1.5. De plus, il est disjoint de $S$ : si $s \in I$, $s/1 \in \mathscr{I}$. Comme $s/1$ est inversible dans $S^{-1}A$, on a alors $\mathscr{I} = A$ ce qui est absurde.

Il suffit donc de montrer que c'est le seul idéal premier ayant ces propriétés. Soit $J$ un idéal premier disjoint de $S$ tel que $JS^{-1}A = \mathscr{I} = IS^{-1}A$ et montrons que $I = J$. Soit $a \in J$. Alors, $a/1$ appartient à $\mathscr{I}$, donc il existe $x \in I$ et $s \in S$ tel que $a/1 = x/s$. Par suite, il existe $t \in S$ tel que $tsa = tx$, donc $(ts)a \in I$. Comme $ts \in S$, $ts \notin I$ et comme $I$ est premier, $a \in I$. Ainsi $J \subset I$. L'autre inclusion se démontre de même par symétrie. □

On en déduit le résultat suivant :

COROLLAIRE 4.1.12. — *Soit* $A$ *un anneau.*

*a) Si* $I$ *est un idéal de* $A$ *distinct de* $A$*, il existe un idéal maximal* $\mathfrak{m}$ *de* $A$ *contenant* $I$.

*b) Si* $S$ *est une partie multiplicative de* $A$ *ne contenant pas* $0$*, il existe un idéal premier de* $A$ *disjoint de* $S$.

*Démonstration.* — a) Comme $I \neq A$, l'anneau $A/I$ est non nul et possède donc un idéal maximal. D'après la proposition précédente, celui-ci est de la forme $\mathfrak{m}/I$ où $\mathfrak{m}$ est un idéal maximal de $A$ contenant $I$.

b) Comme $0 \notin S$, l'anneau localisé $S^{-1}A$ n'est pas l'anneau nul. Soit $\mathfrak{m}$ un idéal maximal de $S^{-1}A$. Son image réciproque $i^{-1}(\mathfrak{m})$ dans A par l'homomorphisme canonique $i : A \to S^{-1}A$ est alors un idéal premier I de A disjoint de S. □

Un autre corollaire est la caractérisation suivante des éléments inversible d'un anneau.

PROPOSITION 4.1.13. — *Soit* A *un anneau. Un élément* $a \in A$ *est inversible si et seulement si il n'appartient à aucun idéal maximal de* A.

*Démonstration.* — Supposons que $a$ est inversible. Alors, $(a) = A$ et le seul idéal de A contenant $a$ est égal à A lui-même. Par suite, $a$ ne peut appartenir à aucun idéal maximal de A.

Réciproquement, si $a$ n'est pas inversible, $(a) \neq A$. D'après le corollaire précédent, il existe un idéal maximal $\mathfrak{m}$ de A contenant l'idéal $(a)$. On a donc $a \in \mathfrak{m}$. □

On peut aussi en déduire une formule intéressante concernant le radical d'un idéal.

THÉORÈME 4.1.14. — *Soit* A *un anneau et soit* I *un idéal de* A. *Alors,*

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$$

*où l'intersection est prise sur l'ensemble des idéaux premiers de* A *qui contiennent* I.

*En particulier, le nilradical de* A *est l'intersection de ses idéaux premiers.*

*Démonstration.* — On commence par montrer l'inclusion facile selon laquelle $\sqrt{I}$ est contenu dans tout idéal premier de A qui contient I. Soit donc $\mathfrak{p}$ un tel idéal premier. Soit $a \in \sqrt{I}$. Il existe ainsi $n \geq 1$ tel que $a^n \in I$ et donc $a^n \in \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, $a \in \mathfrak{p}$.

L'autre inclusion est plus difficile. Si $a$ est un élément de $A \setminus \sqrt{I}$, il faut montrer qu'il existe un idéal premier de A contenant I mais ne contenant pas $a$. Soit $\mathrm{cl} : A \to A/I$ l'homomorphisme canonique. Dire que $a \notin \sqrt{I}$ signifie que pour tout $n \geq 1$, $a^n \notin I$, ou encore $\mathrm{cl}(a)^n \neq 0$ dans A/I. Ainsi, $\mathrm{cl}(a)$ n'est pas nilpotent dans A/I. Soit S la famille multiplicative $S = \{1; a; a^2; \ldots\}$ dans A. La famille $T = \mathrm{cl}(S) = \{1; \mathrm{cl}(a); \mathrm{cl}(a)^2; \ldots\}$ est alors une famille multiplicative de A/I et elle ne contient pas 0. Il en résulte que l'anneau $T^{-1}(A/I)$ possède un idéal maximal $\mathfrak{m}$. Considérons l'homomorphisme composé $A \to A/I \to T^{-1}(A/I)$. L'image réciproque de $\mathfrak{m}$ dans A/I est un idéal premier de A/I disjoint de T. L'image réciproque de $\mathfrak{m}$ dans A est ainsi idéal premier $\mathfrak{p}$ de A contenant I disjoint de S. Comme $a \in S$, $a \notin \mathfrak{p}$. □

## 4.2. Le théorème des zéros de Hilbert

On s'intéresse maintenant aux idéaux des anneaux de polynômes, et notamment à leurs idéaux premiers ou maximaux.

*Exemple 4.2.1.* — Tout idéal non nul de l'anneau $\mathbf{C}[X]$ est de la forme $(P)$ pour un unique polynôme unitaire $P$. Parmi ceux-ci, les idéaux premiers sont les $(X-a)$ pour $a \in \mathbf{C}$ ; ils sont aussi maximaux. L'idéal nul est premier mais non maximal.

*Démonstration.* — On va utiliser un argument de division euclidienne, comme dans l'exemple 2.2.6. Soit $I$ un idéal non nul de $\mathbf{C}[X]$. Soit $P$ un polynôme non nul unitaire appartenant à $I$ de degré minimal. On va montrer que $I = (P)$. En effet, si $Q \in I$, il existe par division euclidienne des polynômes $R$ et $S \in \mathbf{C}[X]$ tels que $Q = PR + S$ avec $\deg S < \deg P$. Alors $S = Q - PR \in I$ et l'inégalité $\deg S < \deg P$ implique que $S = 0$. On a donc $Q = PR \in (P)$.

L'unicité du générateur unitaire $P$ est facile. Si $(P) = (Q)$ pour deux polynômes unitaires $P$ et $Q$, on peut écrire $P = QA$ et $Q = PB$ pour deux polynômes $A$ et $B$. On a alors $\deg A = \deg P - \deg Q \geq 0$ et $\deg B = \deg Q - \deg P \geq 0$, d'où $\deg P = \deg Q$, et le fait que $A$ et $B$ sont constants. Comme $P$ et $Q$ sont tous deux unitaires, $A = B = 1$ et $P = Q$.

Soit maintenant $I = (P)$ un idéal premier de $\mathbf{C}[X]$. Soit $P = \prod_{j=1}^{n}(X - a_j)$ la décomposition de $P$ en produit de facteurs du premier degré (on utilise ici que $\mathbf{C}$ est algébriquement clos). Si $n = 1$, $P = X - a_1$ et $I = (X - a_1)$. Sinon, si $n > 1$, $X - a_1 \notin (P)$ et $\prod_{j=2}^{n}(X - a_j) \notin (P)$ alors que $(X - a_1)\prod_{j=2}^{n}(X - a_j) = P$ appartient à $(P)$. Cela contredit le fait que $I$ est premier.

Réciproquement, si $a \in \mathbf{C}$, l'idéal $(X - a)$ est premier, et même maximal. En effet, l'application $\mathbf{C}[X] \to \mathbf{C}$ telle que $P \mapsto P(a)$ est surjectif et a pour noyau $(X - a)$. On a ainsi un homomorphisme injectif et surjectif $\mathbf{C}[X]/(X - a) \to \mathbf{C}$. C'est donc un isomorphisme et l'idéal $(X - a)$ est maximal. □

De ce résultat, va surtout se généraliser la description des idéaux maximaux.

THÉORÈME 4.2.2 (Théorème des zéros de Hilbert). — *Soit $n \geq 1$ et soit $I$ un idéal maximal de l'anneau $\mathbf{C}[X_1, \ldots, X_n]$. Il existe alors un unique élément $(a_1, \ldots, a_n) \in \mathbf{C}^n$ tel que $I = (X_1 - a_1, \ldots, X_n - a_n)$.*

*Démonstration.* — L'anneau $\mathbf{C}[X_1, \ldots, X_n]$ est une $\mathbf{C}$-algèbre et sa dimension en tant que $\mathbf{C}$-espace vectoriel est infinie dénombrable. En effet, il admet comme base la famille des monômes $X_1^{a_1} \ldots X_n^{a_n}$ indexée par $\mathbf{N}^n$, donc dénombrable. *A*

*fortiori*, l'anneau quotient $K = \mathbf{C}[X_1, \ldots, X_n]/I$ est une $\mathbf{C}$-algèbre de dimension finie ou dénombrable.

Considérons l'homomorphisme de $\mathbf{C}$-algèbres composé

$$\varphi : \mathbf{C}[X_1] \to \mathbf{C}[X_1, \ldots, X_n] \to \mathbf{C}[X_1, \ldots, X_n]/I = K.$$

Comme I est maximal, K est un corps. Si $\varphi$ est injectif, il s'étend en une injection du corps des fractions de $\mathbf{C}[X_1]$ dans le corps K. On aurait ainsi une sous-$\mathbf{C}$-algèbre de K isomorphe à $\mathbf{C}(X_1)$, le corps des fractions rationnelles en une indéterminée. Or, ce corps admet la famille libre formée des $1/(X - a)$ pour $a$ parcourant $\mathbf{C}$. Comme le corps $\mathbf{C}$ est non dénombrable, $\mathbf{C}(X_1)$ est un $\mathbf{C}$-espace vectoriel de dimension non dénombrable. Par suite, K contient un sous-$\mathbf{C}$-espace vectoriel de dimension non dénombrable, ce qui est absurde. Donc $\varphi$ n'est pas injectif.

Comme K est un corps, il est intègre et le noyau de $\varphi$ est un idéal premier de $\mathbf{C}[X_1]$. D'après l'exemple précédent, il existe $a_1 \in \mathbf{C}$ tel que $\varphi(X_1 - a_1) = 0$. On a donc $X_1 - a_1 \in I$.

Le même argument appliqué à $X_2, \ldots, X_n$ montre qu'il existe $a_2, \ldots, a_n$ dans $\mathbf{C}$ tels que $X_2 - a_2 \in I$, …, $X_n - a_n \in I$. L'idéal I contient ainsi l'idéal $(X_1 - a_1, \ldots, X_n - a_n)$.

Pour conclure, il faut montrer que cet idéal est bien maximal. Or, l'homomorphisme $\theta$ de $\mathbf{C}$-algèbres d'évaluation en $(a_1, \ldots, a_n)$

$$\theta\colon \mathbf{C}[X_1, \ldots, X_n] \to \mathbf{C}, \quad P \mapsto P(a_1, \ldots, a_n)$$

est surjectif. Son noyau J est un idéal maximal puisque $\theta$ induit un isomorphisme $\mathbf{C}[X_1, \ldots, X_n]/J$.

Il est clair que J contient les polynômes $X_1 - a_1$, …, $X_n - a_n$. Réciproquement, si $P \in J$, c'est-à-dire si $P(a_1, \ldots, a_n) = 0$, effectuons la division euclidienne de P par $X_1 - a_1$ en raisonnant dans $\mathbf{C}[X_2, \ldots, X_n][X_1]$. Il existe alors des polynômes Q et R dans $\mathbf{C}[X_1, \ldots, X_n]$ tels que $P = (X_1 - a_1)Q + R$ et le degré de R en $X_1$ est nul, c'est-à-dire que R ne dépend pas de $X_1$. Alors, $R(a_2, \ldots, a_n) = 0$ et par récurrence, R appartient à $(X_2 - a_2, \ldots, X_n - a_n)$. Par suite, P appartient à $(X_1 - a_1, \ldots, X_n - a_n)$. Ainsi, $J = (X_1 - a_1, \ldots, X_n - a_n)$ et $\theta$ induit un isomorphisme $\mathbf{C}[X_1, \ldots, X_n]/J \simeq \mathbf{C}$ ce qui prouve que J est maximal.

Enfin, l'unicité de la famille $(a_1, \ldots, a_n) \in \mathbf{C}^n$ provient du fait que les idéaux $(X_1 - a_1, \ldots, X_n - a_n)$ sont maximaux. Si en effet $X_1 - b_1$ appartient à l'idéal maximal $I = (X_1 - a_1, \ldots, X_n - a_n)$, on a alors $b_1 - a_1 \in I$. Si $b_1 \neq a_1$, $b_1 - a_1$ est inversible, $I = \mathbf{C}[X_1, \ldots, X_n]$ ce qui est absurde. Donc $b_1 = a_1$. □

Ce théorème est à la base d'une correspondance admirable entre certains idéaux de $\mathbf{C}[X_1, \ldots, X_n]$ et certaines parties de $\mathbf{C}^n$.

DÉFINITION 4.2.3. — *Un* ensemble algébrique *est une partie de* $\mathbf{C}^n$ *de la forme*

$$\mathscr{Z}(S) = \{(a_1, \ldots, a_n) \in \mathbf{C}^n \,;\, \textit{pour tout } P \in S,\ P(a_1, \ldots, a_n) = 0\},$$

*où* S *est une partie de* $\mathbf{C}[X_1, \ldots, X_n]$.

PROPOSITION 4.2.4. — *a) Si* $S \subset S'$, $\mathscr{Z}(S') \subset \mathscr{Z}(S)$.

*b) L'ensemble vide et* $\mathbf{C}^n$ *sont des ensembles algébriques.*

*c) Si* $\langle S \rangle$ *est l'idéal engendré par* S *dans* $\mathbf{C}[X_1, \ldots, X_n]$, *on a* $\mathscr{Z}(\langle S \rangle) = \mathscr{Z}(S)$.

*d) L'intersection d'une famille d'ensembles algébriques, la réunion de deux ensembles algébrques sont des ensembles algébriques.*

*e) Si* I *est un idéal de* $\mathbf{C}[X_1, \ldots, X_n]$, $\mathscr{Z}(I) = \mathscr{Z}(\sqrt{I})$.

*Démonstration.* — a) Soit $(a_1, \ldots, a_n) \in \mathscr{Z}(S')$ et montrons que $(a_1, \ldots, a_n) \in \mathscr{Z}(S)$. Si $P \in S$, on doit montrer que $P(a_1, \ldots, a_n)$, ce qui est vrai puisque $P \in S'$.

b) On a $\emptyset = \mathscr{Z}(\{1\})$ (le polynôme constant 1 ne s'annule en aucun point de $\mathbf{C}^n$) et $\mathbf{C}^n = \mathscr{Z}(\{0\})$ (le polynôme nul s'annule partout).

c) Comme $S \subset \langle S \rangle$, on a $\mathscr{Z}(\langle S \rangle) \subset \mathscr{Z}(S)$. Réciproquement, soit $(a_1, \ldots, a_n) \in \mathscr{Z}(S)$ et montrons que $(a_1, \ldots, a_n) \in \mathscr{Z}(\langle S \rangle)$. Soit $P \in \langle S \rangle$ ; il existe des polynômes $P_s \in S$ et $Q_s \in \mathbf{C}[X_1, \ldots, X_n]$ tels que $P = \sum P_s Q_s$. Alors,

$$P(a_1, \ldots, a_n) = \sum_s P_s(a_1, \ldots, a_n) Q_s(a_1, \ldots, a_n) = 0$$

et donc $(a_1, \ldots, a_n) \in \mathscr{Z}(\langle S \rangle)$.

d) Soit $(Z_j)$ une famille d'ensembles algébriques et pour tout $j$, $S_j$ une partie de $\mathbf{C}[X_1, \ldots, X_n]$ telle que $Z_j = \mathscr{Z}(S_j)$. Nous allons montrer que

$$\bigcap_j \mathscr{Z}(S_j) = Z(\bigcup_j S_j).$$

En effet, dire que $(a_1, \ldots, a_n)$ appartient à $\bigcap_j \mathscr{Z}(S_j)$, c'est dire que pour tout $j$ et tout $P \in S_j$, $P(a_1, \ldots, a_n) = 0$. C'est donc dire que pour tout $P \in \bigcup_j S_j$, $P(a_1, \ldots, a_n) = 0$, ce qui équivaut à $(a_1, \ldots, a_n) \in \mathscr{Z}(\bigcup_j S_j)$.

Soit S et S′ deux parties de $\mathbf{C}[X_1, \ldots, X_n]$. Soit $T = \{PP' \,;\, P \in S,\ P' \in S'\}$. On va montrer que $\mathscr{Z}(S) \cup \mathscr{Z}(S') = \mathscr{Z}(T)$. Si en effet $(a_1, \ldots, a_n) \in \mathscr{Z}(S)$ et $Q \in T$, on peut écrire $Q = PP'$ avec $P \in S$ et $P' \in S'$. Alors, $Q(a_1, \ldots, a_n) = P(a_1, \ldots, a_n)P'(a_1, \ldots, a_n) = 0$ puisque $(a_1, \ldots, a_n) \in \mathscr{Z}(S)$. Autrement dit, $\mathscr{Z}(S) \subset \mathscr{Z}(T)$. De même, $\mathscr{Z}(S') \subset \mathscr{Z}(T)$ et donc $\mathscr{Z}(S) \cup \mathscr{Z}(S') \subset \mathscr{Z}(T)$. Réciproquement, soit $(a_1, \ldots, a_n) \in \mathscr{Z}(T)$. Pour montrer que $(a_1, \ldots, a_n) \in \mathscr{Z}(S) \cup \mathscr{Z}(S')$, il suffit de montre que si $(a_1, \ldots, a_n) \notin \mathscr{Z}(S')$, alors $(a_1, \ldots, a_n) \in \mathscr{Z}(S)$. Or, si $(a_1, \ldots, a_n) \notin \mathscr{Z}(S')$, il existe un polynôme $P' \in S'$ tel que $P'(a_1, \ldots, a_n) \neq 0$. Alors, pour tout $P \in S$, $PP' \in T$, d'où $(PP')(a_1, \ldots, a_n) = 0 = P(a_1, \ldots, a_n)P'(a_1, \ldots, a_n)$ et donc $P(a_1, \ldots, a_n) = 0$, ainsi qu'il fallait démontrer.

e) Comme $I \subset \sqrt{I}$, on a $\mathscr{Z}(\sqrt{I}) \subset \mathscr{Z}(I)$. Réciproquement, soit $(a_1, \ldots, a_n) \in \mathscr{Z}(I)$. Si $P \in \sqrt{I}$, soit $m \geq 1$ tel que $P^m \in I$. On a alors $P^m(a_1, \ldots, a_n) = 0$, d'où $P(a_1, \ldots, a_n) = 0$ et $(a_1, \ldots, a_n) \in \mathscr{Z}(\sqrt{I})$. □

*Remarque 4.2.5* (pour les férus de topologie). — La proposition précédente peut s'interpréter en disant qu'il existe une topologie sur $\mathbf{C}^n$ dont les fermés sont les ensembles algébriques. Cette topologie est appelée *topologie de Zariski*.

Voilà le premier sens de la correspondance : à tout idéal I de $\mathbf{C}[X_1, \ldots, X_n]$ on associe l'ensemble algébrique $\mathscr{Z}(I)$. Une reformulation du théorème des zéros de Hilbert est la suivante :

THÉORÈME 4.2.6. — *Si* I *est un idéal de* $\mathbf{C}[X_1, \ldots, X_n]$ *distinct de* $\mathbf{C}[X_1, \ldots, X_n]$, *l'ensemble algébrique* $\mathscr{Z}(I)$ *est non vide.*

*Démonstration.* — Soit $\mathfrak{m}$ un idéal maximal contenant I. D'après le théorème des zéros, il existe $(a_1, \ldots, a_n) \in \mathbf{C}^n$ tel que $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$. Par suite, si $P \in I$, P appartient à $\mathfrak{m}$ et $P(a_1, \ldots, a_n) = 0$. Ainsi, $(a_1, \ldots, a_n)$ appartient à $\mathscr{Z}(I)$ qui est donc non vide. □

Dans l'autre sens, à toute partie de $\mathbf{C}^n$ est associée un idéal.

DÉFINITION 4.2.7. — *Soit* V *une partie de* $\mathbf{C}^n$. *On définit une partie*

$$\mathscr{I}(V) = \{P \in \mathbf{C}[X_1, \ldots, X_n] \,;\, \textit{pour tout } (a_1, \ldots, a_n) \in V,\ P(a_1, \ldots, a_n) = 0\}.$$

PROPOSITION 4.2.8. — *a) Pour tout* $V \subset \mathbf{C}^n$, $\mathscr{I}(V)$ *est un idéal tel que* $\mathscr{I}(V) = \sqrt{\mathscr{I}(V)}$.

*b) Si* $V \subset V'$, $\mathscr{I}(V') \subset \mathscr{I}(V)$.

*c) Si* V *et* V′ *sont deux parties de* $\mathbf{C}^n$, *on a* $\mathscr{I}(V \cup V') = \mathscr{I}(V) \cap \mathscr{I}(V')$.

*Démonstration.* — a) En fait, $\mathscr{I}(V)$ est l'intersection des noyaux des morphismes d'évaluation aux $(a_1, \ldots, a_n) \in V$. C'est donc un idéal.

b) Soit $P \in \mathscr{I}(V')$. Si $(a_1, \ldots, a_n) \in V$, comme $V \subset V'$, $P(a_1, \ldots, a_n) = 0$ et $P \in \mathscr{I}(V)$.

c) Cela découle de la définition. Un polynôme P appartient à $\mathscr{I}(V \cup V')$ si et seulement s'il s'annule en tout point de V *et* de V′. □

PROPOSITION 4.2.9. — *a) Pour tout idéal* I *de* $\mathbf{C}[X_1, \ldots, X_n]$, *on a* $I \subset \mathscr{I}(\mathscr{Z}(I))$.

*b) Pour toute partie* V *de* $\mathbf{C}^n$, *on a* $V \subset \mathscr{Z}(\mathscr{I}(V))$.

*Démonstration.* — a) Soit $P \in I$ et montrons $P \in \mathscr{I}(\mathscr{Z}(I))$. Pour cela, il faut montrer que P s'annule en tout point de Z(I). Or, si $(a_1, \ldots, a_n) \in \mathscr{Z}(I)$, on a $P(a_1, \ldots, a_n)$ puisque $P \in I$.

b) Soit $(a_1, \ldots, a_n) \in V$ et montrons que $(a_1, \ldots, a_n)$ appartient à $\mathscr{Z}(\mathscr{I}(V))$. Il faut donc motnrer que pour tout $P \in \mathscr{I}(V)$, $P(a_1, \ldots, a_n) = 0$. Mais c'est clair puisque $(a_1, \ldots, a_n) \in V$. □

Nous allons utiliser le théorème des zéros de Hilbert pour démontrer le théorème suivant.

THÉORÈME 4.2.10. — *Si* I *est un idéal de* $\mathbf{C}[X_1, \ldots, X_n]$, *on a*

$$\boxed{\mathscr{I}(\mathscr{Z}(I)) = \sqrt{I}}.$$

Avant d'en donner la démonstration, montrons qu'il donne lieu à une bijection entre ensembles algébriques et idéaux égaux à leur racine.

COROLLAIRE 4.2.11. — *Les applications* $V \mapsto \mathscr{I}(V)$ *et* $I \mapsto \mathscr{Z}(I)$ *définissent des bijections réciproques l'une de l'autre entre ensembles algébriques de* $\mathbf{C}^n$ *et idéaux* I *de* $\mathbf{C}[X_1, \ldots, X_n]$ *tels que* $I = \sqrt{I}$.

*Démonstration du corollaire.* — Soit I un idéal de $\mathbf{C}[X_1, \ldots, X_n]$ tel que $I = \sqrt{I}$. D'après le théorème précédent,

$$\mathscr{I}(\mathscr{Z}(I)) = \sqrt{I} = I.$$

Soit maintenant V un ensemble algébrique et I un idéal tel que $V = \mathscr{Z}(I)$. On a alors

$$\mathscr{I}(V) = \mathscr{I}(\mathscr{Z}(I)) = \sqrt{I}$$

d'où encore

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

Le corollaire est ainsi établi. □

*Démonstration du théorème.* — L'inclusion $\sqrt{I} \subset \mathscr{I}(\mathscr{Z}(I))$ est facile. Si $P \in \sqrt{I}$, soit $m \geq 1$ tel que $P^m \in I$. Alors, si $(a_1, \ldots, a_n) \in \mathscr{Z}(I)$, $P^m(a_1, \ldots, a_n) = 0$ d'où $P(a_1, \ldots, a_n) = 0$. Il en résulte que $P \in \mathscr{I}(\mathscr{Z}(I))$.

Réciproquement, soit P un polynôme de $\mathscr{I}(\mathscr{Z}(I))$. On veut montrer qu'il existe $m \geq 1$ tel que $P^m \in I$. Considérons l'idéal J de $\mathbf{C}[X_1, \ldots, X_n, T]$ engendré par I et par le polynôme $1 - TP$. On a $\mathscr{Z}(J) = \emptyset$. En effet, si $(a_1, \ldots, a_n, t) \in \mathbf{C}^{n+1}$ appartient à $\mathscr{Z}(J)$, on doit avoir $Q(a_1, \ldots, a_n) = 0$ pour tout polynôme $Q \in I \subset \mathbf{C}[X_1, \ldots, X_n] \subset \mathbf{C}[X_1, \ldots, X_n, T]$, et donc $(a_1, \ldots, a_n) \in \mathscr{Z}(I)$. On doit aussi avoir $1 - tP(a_1, \ldots, a_n) = 0$. Mais $P \in I$, donc $P(a_1, \ldots, a_n) = 0$ et l'on a une contradiction $(1 = 0)$.

D'après le théorème des zéros, $J = \mathbf{C}[X_1, \ldots, X_n, T]$ et il existe des polynômes $Q_j \in I$, $R_i \in \mathbf{C}[X_1, \ldots, X_n, T]$ et $R \in \mathbf{C}[X_1, \ldots, X_n, T]$ tels que

$$1 = (1 - TP)R + \sum_i Q_j R_i.$$

C'est une égalité de polynômes dans $\mathbf{C}[X_1, \ldots, X_n, T]$. On peut y substituer $T = 1/P$ pour obtenir une égalité de fractions rationnelles dans $\mathbf{C}(X_1, \ldots, X_n)$ :

$$1 = \sum_i Q_i(X_1, \ldots, X_n) R_i(X_1, \ldots, X_n, 1/P(X_1, \ldots, X_n)).$$

Il convient alors d'écrire pour tout $i$

$$R_i(X_1, \ldots, X_n, T) = \sum_{m=0}^{M} R_{i,m}(X_1, \ldots, X_n) T^m$$

pour un certain entier $M \geq 1$ (le même pour tous les $i$). En multipliant par $P^M$, on en déduit la relation

$$P(X_1, \ldots, X_n)^M = \sum_i \sum_{m=0}^{M} Q_i(X_1, \ldots, X_n) R_{i,m}(X_1, \ldots, X_n) P(X_1, \ldots, X_n)^{M-m},$$

relation valable de nouveau dans l'anneau des polynômes $\mathbf{C}[X_1, \ldots, X_n]$. Comme les $Q_i$ appartiennent à I, cette relation montre que $P^M$ appartient à I et donc $P \in \sqrt{I}$. □

## 4.3. Exercices

*Exercice 4.3.1.* — Étant donné un idéal I de A, on note $\sqrt{I}$ son radical (ou sa racine). Soient I, J et L des idéaux de A. Démontrer les assertions suivantes :

**a)** si I est contenu dans J, $\sqrt{I}$ est contenu dans $\sqrt{J}$ ;

**b)** on a $\sqrt{I \cdot J} = \sqrt{I \cap J}$ ;

**c)** on a $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ ;

**d)** $\sqrt{\sqrt{I}} = \sqrt{I}$ ;

**e)** si $\mathfrak{p}$ est un idéal premier de A, on a $\sqrt{\mathfrak{p}} = \mathfrak{p}$ ;

**f)** on a $\sqrt{I} + \sqrt{J} \subset \sqrt{I + J}$ ;

**g)** on a $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$ ;

**h)** on a

$$\sqrt{(I \cap J) + (I \cap L)} = \sqrt{I \cap (J + L)} \ ;$$

**i)** Soient $(\mathfrak{p}_i)_{1 \leq i \leq n}$, $n$ idéaux premiers de A. On suppose que I est contenu dans l'intersection des $\mathfrak{p}_i$ et que cette intersection est contenue dans $\sqrt{I}$. Montrer que l'on a l'égalité $\sqrt{I} = \cap \mathfrak{p}_i$.

*Exercice 4.3.2.* — Supposons que A soit un produit fini d'anneaux $A_i$ : on a $A = A_1 \times \cdots \times A_n$.

**a)** Montrer que les idéaux de A sont de la forme $I_1 \times \cdots \times I_n$, où les $I_j$ sont des idéaux de A.

**b)** Déterminer les idéaux premiers et maximaux de A.

**c)** Supposons de plus que les $A_i$ soient des corps. Montrer que A n'a qu'un nombre fini d'idéaux.

*Exercice 4.3.3.* — Soient $\mathfrak{p}$ un idéal premier de A, et $(I_k)_{1\leq k\leq n}$ $n$ idéaux de A. On suppose que $\mathfrak{p}$ contient l'idéal produit $\prod_{1\leq k\leq n} I_k$. Montrer que $\mathfrak{p}$ contient l'un des idéaux $I_k$.

*Exercice 4.3.4.* — Soient $(\mathfrak{p}_i)_{1\leq i\leq n}$ $n$ idéaux premiers de A. Soit I un idéal de A contenu dans la réunion des idéaux $\mathfrak{p}_i$. Montrer que I est contenu dans l'un des $\mathfrak{p}_i$.

*Exercice 4.3.5.* — Soit A un anneau intègre et $\mathfrak{p}$ un idéal premier principal non nul. Soit I un idéal principal de A contenant $\mathfrak{p}$. Montrer que $I = A$ ou $I = \mathfrak{p}$.

*Exercice 4.3.6.* — **a)** Soient I et J deux idéaux comaximaux de A. Montrer que l'on a $I : J = I$. Soit L un idéal tel que $I \cdot L$ soit contenu dans J. Montrer que L est contenu dans J.

**b)** Soient $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers de A dont aucun n'est inclus dans l'autre. Montrer que $\mathfrak{p} : \mathfrak{q} = \mathfrak{p}$ et $\mathfrak{q} : \mathfrak{p} = \mathfrak{q}$. Si K est un corps, donner un exemple de deux idéaux premiers de K[X,Y] dont aucun n'est contenu dans l'autre et qui ne sont pas comaximaux.

**c)** Soit $a$ un élément de A non diviseur de zéro de A. on suppose que $(a)$ est un idéal premier et que l'on a $(a) = I \cdot J$ où I et J sont deux idéaux de A. Montrer que l'on a $I = A$ ou bien $J = A$. (*Indication : commencer par prouver que* $I = (a)$ *ou* $J = (a)$.)

*Exercice 4.3.7.* — On dit qu'un anneau est local s'il n'a qu'un seul idéal maximal.

**a)** Montrer qu'un anneau est local si et seulement si l'ensemble de ses éléments non inversibles est un idéal

**b)** Soit A un anneau et $\mathfrak{p}$ un idéal premier de A. Soit $A_{\mathfrak{p}}$ l'anneau localisé de A par rapport à la partie multiplicative $A \setminus \mathfrak{p}$. Montrer que $A_{\mathfrak{p}}$ est un anneau local, d'idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$.

*Exercice 4.3.8.* — On dira qu'une partie S de A est saturée si $xy \in S$ implique $x \in S$ et $y \in S$.

**a)** Montrer qu'une partie S de A est multiplicative et saturée si et seulement $A \setminus S$ est réunion d'idéaux premiers de A.

**b)** Soit S une partie multiplicative de A. Soit $\tilde{S}$ l'ensemble des $x \in A$ pour lesquels il existe $y \in A$ tel que $xy \in S$. Montrer que $\tilde{S}$ est la plus petite partie multiplicative saturée contenant S.

**c)** Montrer que $A \setminus \tilde{S}$ est la réunion des idéaux premiers de A disjoints de S.

**d)** Montrer que l'homomorphisme canonique

$$S^{-1}A \to \tilde{S}^{-1}A$$

est un isomorphisme.

*Exercice 4.3.9* (Anneaux de Jacobson). — Si A est un anneau, on note $\mathfrak{N}(A) = \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p}$ (nilradical) et $\mathfrak{J}(A) = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$ (radical de Jacobson).

**a)** Montrer l'équivalence de :

(1) Tout idéal premier est intersection d'idéaux maximaux.

(2) Pour tout quotient B de A on a $\mathfrak{N}(B) = \mathfrak{J}(B)$.

*On dit alors que* A *est un anneau de Jacobson.*

**b)** Montrer que $\mathbf{C}[X_1, \ldots, X_n]$ est un anneau de Jacobson. (*Utiliser le théorème des zéros de Hilbert.*)

*Exercice 4.3.10.* — Soit A un anneau et $\mathfrak{J}$ l'intersection des idéaux maximaux de A (radical de Jacobson). Montrer qu'un élément $a \in A$ appartient à $\mathfrak{J}$ si et seulement si pour tout $x \in A$, $1 - ax$ est inversible.

*Exercice 4.3.11.* — Soient $P, Q, R$ trois polynômes de $\mathbf{C}[x_1, \ldots, x_n]$. On suppose que P est irréductible et que R n'est pas multiple de P. On suppose que pout tout $a \in \mathbf{C}^n$ tel que $P(a) = 0$ et $Q(a) \neq 0$, alors $R(a) = 0$. Montrer que Q est multiple de P.

## 4.4. Solutions

*Solution de l'exercice 4.3.1.* — **a)** Soit $x \in \sqrt{I}$. Il existe $n \geq 1$ tel que $x^n \in I$, mais comme $I \subset J$, $x^n \in J$, et donc $x \in \sqrt{J}$.

**b)** D'après le a) de l'exercice 2.5.4, on a $I \cdot J \subset I \cap J$, et donc $\sqrt{I \cdot J} \subset \sqrt{I \cap J}$. Réciproquement, si $x \in \sqrt{I \cap J}$, il existe $n \geq 1$ tel que $x^n \in I \cap J$. Alors, $x^{2n} = x^n \cdot x^n \in I \cdot J$, si bien que $x \in \sqrt{I \cdot J}$.

**c)** On a $I \cap J \subset I$, donc $\sqrt{I \cap J} \subset \sqrt{I}$, et de même pour J, soit $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$. Dans l'autre sens, si $x \in \sqrt{I} \cap \sqrt{J}$, il existe $n \geq 1$ tel que $x^n \in I$ et $m \geq 1$ tel que $x^m \in J$. Alors, $x^{n+m} \in I \cdot J \subset I \cap J$, d'où $x \in \sqrt{I \cap J}$.

**d)** Comme $\sqrt{I} \supset I$, on a $\sqrt{\sqrt{I}} \supset \sqrt{I}$. Dans l'autre sens, soit $x \in \sqrt{\sqrt{I}}$. Il existe donc $n \geq 1$ tel que $x^n \in \sqrt{I}$, ce qui signifie qu'il existe $m \geq 1$ tel que $(x^n)^m \in I$. Comme $(x^n)^m = x^{nm}$ et comme $nm \geq 1$, $x \in \sqrt{I}$.

**e)** On a déjê $\sqrt{\mathfrak{p}} \supset \mathfrak{p}$. Réciproquement, si $x \in \sqrt{\mathfrak{p}}$, soit $n \geq 1$ minimal tel que $x^n \in \mathfrak{p}$. Si $x \notin \mathfrak{p}$, ce qui signifie $n > 1$, on peut écrire $x^n = x \cdot x^{n-1}$. Comme $\mathfrak{p}$ est premier et que $x \notin \mathfrak{p}$, on a $x^{n-1} \in \mathfrak{p}$. Or, $1 \leq n - 1 < n$, ce qui contredit la minimalité de $n$.

**f)** On a $I \subset I + J$, donc $\sqrt{I} \subset \sqrt{I + J}$, et de même pour J, si bien que $\sqrt{I} + \sqrt{J} \subset \sqrt{I + J}$.

**g)** On a les inclusions

$$I \subset \sqrt{I} \subset \sqrt{I} + \sqrt{J} \subset \sqrt{\sqrt{I} + \sqrt{J}},$$

d'où l'on déduit que $I + J \subset \sqrt{\sqrt{I} + \sqrt{J}}$ et donc

$$\sqrt{I+J} \subset \sqrt{\sqrt{\sqrt{I} + \sqrt{J}}} = \sqrt{\sqrt{I} + \sqrt{J}}.$$

Dans l'autre sens, la question précédente donne $\sqrt{I} + \sqrt{J} \subset \sqrt{I+J}$, d'où en reprenant les racines,

$$\sqrt{\sqrt{I} + \sqrt{J}} \subset \sqrt{\sqrt{I+J}} = \sqrt{I+J}.$$

**h)**

$$\begin{aligned}
\sqrt{I \cap (J+L)} &= \sqrt{I \cdot (J+L)} && \text{d'après b)} \\
&= \sqrt{I \cdot J + I \cdot L} \\
& && \text{d'après l'exercice 2.5.4, question b)} \\
&= \sqrt{\sqrt{I \cdot J} + \sqrt{I \cdot L}} && \text{(question g)} \\
&= \sqrt{\sqrt{I \cap J} + \sqrt{I \cap L}} && \text{(question b)} \\
&= \sqrt{(I \cap J) + (I \cap L)} && \text{(question g).}
\end{aligned}$$

**i)** Comme $I \subset \bigcap \mathfrak{p}_i$, on a

$$\sqrt{I} \subset \sqrt{\bigcap \mathfrak{p}_i} \underset{\text{c)}}{\subset} \bigcap \sqrt{\mathfrak{p}_i} \underset{\text{e)}}{\subset} \bigcap \mathfrak{p}_i.$$

On a donc l'égalité.

*Solution de l'exercice 4.3.2.* — **a)** Commençons par étudier le cas $n = 2$. Nous en déduirons le cas général par récurrence. Soit I un idéal de A. Notons $I_1$ et $I_2$ les images de I par les projections $A_1 \times A_2 \to A_1$ (resp. $A_1 \times A_2 \to A_2$). Montrons que $I_1$ est un idéal de $A_1$. Soient en effet $x_1, y_1 \in I_1$ et $\lambda, \mu \in A_1$. Alors,

il existe par définition $x_2$ et $y_2 \in A_2$ tels que $x = (x_1, x_2) \in I$ et $y = (y_1, y_2) \in I$. Par suite, I contient l'élément

$$\begin{aligned}
(\lambda, 0)x + (\mu, 0)y &= (\lambda, 0)(x_1, x_2) + (\mu, 0)(y_1, y_2) \\
&= (\lambda x_1, 0) + (\mu y_1, 0) = (\lambda x_1 + \mu x_2, 0),
\end{aligned}$$

ce qui prouve que $\lambda x_1 + \mu y_1 \in I_1$. De même pour $I_2$.

Montrons maintenant que $I = I_1 \times I_2$. Soit $x = (x_1, x_2) \in I$. On a ainsi $x_1 \in I_1$ et $x_2 \in I_2$, d'où $x \in I_1 \times I_2$. Dans l'autre sens, si $(x_1, x_2) \in I_1 \times I_2$, il existe $y_1$ tel que $(x_1, y_1) \in I$, et $y_2$ tel que $(y_2, x_2) \in I$. Ainsi,

$$(x_1, x_2) = (1, 0) \cdot (x_1, y_1) + (0, 1) \cdot (y_2, x_2) \in I.$$

Lorsque $n > 2$, on procède par récurrence : les idéaux de $A_1 \times A_2 \times \cdots \times A_n$ sont de la forme $I_1 \times J$, où $I_1$ est un idéal de $A_1$ et J un idéal de $A_2 \times \cdots \times A_n$. Par récurrence, J est de la forme $I_2 \times \cdots \times I_n$.

**b)** Soit $I = I_1 \times \cdots \times I_n$ un idéal de A. L'anneau quotient A/I est alors égal à $(A/I_1) \times \ldots (A/I_n)$. Un produit d'anneaux intègres n'est intègre que si tous les anneaux sauf un seul sont nuls. (Quand $n = 2$, on a $(1, 0) \cdot (0, 1) = (0, 0)$ ; si l'anneau

produit est intègre, il faut que $1_{A_1} = 0$ ou $1_{A_2} = 0$.)

Ainsi, les idéaux premiers de A sont de la forme $A_1 \times \cdots \times I_j \ldots A_n$ (tous les $A_i$, sauf en $j$, ou on a un idéal $I_j$).

Le quotient vaut $A_j/I_j$, ce qui implique que $I_j$ est premier dans $A_j$. La réciproque est claire, et les idéaux premiers de A sont donc de la forme $A_1 \times A_2 \cdots \times \mathfrak{p}_j \times \cdots \times A_n$, avec $\mathfrak{p}_j$ premier dans $A_j$.

Parmi ces idéaux premiers, ne sont maximaux que ceux tels que $A_j/\mathfrak{p}_j$ est un corps, c'est-à-dire $\mathfrak{p}_j$ maximal dans $A_j$.

**c)** Un corps $k$ n'a que deux idéaux : (0) et $k$ tout entier. Ainsi, un produit de corps $k_1 \times \cdots \times k_n$ a exactement $2^n$ idéaux. Parmi ceux-ci, $n$ sont premiers, d'ailleurs maximaux.

*Solution de l'exercice 4.3.3.* — Supposons par l'absurde que $\mathfrak{p}$ ne contient aucun des $I_k$. Il existe ainsi pour tout $k$ un élément $x_k \in I_k$ tel que $x_k \notin \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, le produit $x = x_1 \ldots x_n$ n'appartient pas à $\mathfrak{p}$. Or, $x \in \prod I_k \subset \mathfrak{p}$, ce qui est une contradiction.

*Solution de l'exercice 4.3.4.* — Quitte à remplacer les $\mathfrak{p}_i$ par un sous-ensemble, il n'est pas restrictif de supposer qu'aucun des $\mathfrak{p}_i$ n'est inclus dans un autre (sinon on garde le plus grand, et on enlève le plus petit qui ne sert à rien).

Raisonnons alors par l'absurde : si I n'est contenu dans aucun $\mathfrak{p}_i$, il existe pour tout $i$ un élément $x_i \in I$ tel que $x_i \notin \mathfrak{p}_i$.

Comme $\mathfrak{p}_j \not\subset \mathfrak{p}_1$ pour $j \geq 2$, on peut trouver $a_1 \in \mathfrak{p}_2 \ldots \mathfrak{p}_n$ tel que $a_1 \notin \mathfrak{p}_1$ (considérer $b_j \in \mathfrak{p}_j$ qui n'appartient pas à $\mathfrak{p}_1$ et faire le produit). De même, pour tout $1 \leq i \leq n$, on trouve $a_i \notin \mathfrak{p}_i$ tel que $a_i$ appartienne à tous les autres $\mathfrak{p}_j$.

Considérons l'élément $x = \sum a_i x_i$. Comme $x_i \in I$ pour tout $i$, c'est un élément de I.

Pourtant, comme $\mathfrak{p}_1$ est premier et que ni $a_1$ ni $x_1$ n'appartiennent à $\mathfrak{p}_1$, $a_1 x_1$ n'appartient pas à $\mathfrak{p}_1$. Et il est clair que $a_2 x_2 + \cdots + a_n x_n$ appartient à $\mathfrak{p}_1$ puisque

tous les $a_i$ $(i \geq 2)$ y appartiennent. Ainsi, $x \notin \mathfrak{p}_1$. Le même résultat vaut pour tout $i$ et $x \notin \bigcup \mathfrak{p}_i$, ce qui contredit l'hypothèse que $\mathrm{I} \subset \bigcup_i \mathfrak{p}_i$.

*Solution de l'exercice 4.3.5.* — On écrit $\mathfrak{p} = (a)$. Soit $\mathrm{I} = (b)$ un idéal principal de A contenant $\mathfrak{p}$. Comme $(a) \subset (b)$, on peut écrire $a = bu$, avec $u \in \mathrm{A}$. Comme $(a)$ est premier, soit $b \in (a)$, soit $u \in (a)$. Dans le premier cas, $\mathrm{I} = \mathfrak{p}$. Dans l'autre, on peut écrire $u = av$, d'où l'égalité $a = abv$ et A étant intègre et $a \neq 0$, $bv = 1$. L'élément $b$ est inversible et $\mathrm{I} = \mathrm{A}$.

*Solution de l'exercice 4.3.6.* — **a)** On rappel que $\mathrm{I} : \mathrm{J}$ est l'ensemble des éléments $a \in \mathrm{A}$ tels que $a\mathrm{J} \subset \mathrm{I}$. Or, I et J étant comaximaux, il existe $u \in \mathrm{I}$ et $v \in \mathrm{J}$ tels que $u + v = 1$. Ainsi, si $av \in \mathrm{I}$, on a $a = au + av \in \mathrm{I}$ et donc $\mathrm{I} : \mathrm{J} \subset \mathrm{I}$. L'autre inclusion est claire, si bien que $\mathrm{I} : \mathrm{J} = \mathrm{I}$.

Soit L un idéal tel que $\mathrm{I} \cdot \mathrm{L} \subset \mathrm{J}$. Si $a \in \mathrm{L}$, on a donc $a\mathrm{I} \subset \mathrm{J}$, soit $a \in \mathrm{J} : \mathrm{I}$. D'après la première partie de la question (en échangeant les rôles de I et J), $a \in \mathrm{J}$, d'où $\mathrm{L} \subset \mathrm{J}$.

**b)** On a déjà $\mathfrak{p} \subset \mathfrak{p} : \mathfrak{q}$. Soit réciproquement $a \in \mathfrak{p} : \mathfrak{q}$. Ainsi, pour tout $x \in \mathfrak{q}$, $ax \in \mathfrak{p}$. Comme $\mathfrak{q}$ n'est pas inclus dans $\mathfrak{p}$, on peut choisir $x \in \mathfrak{q}$ tel que $x \notin \mathfrak{p}$. Alors, $\mathfrak{p}$ étant premier, $a \in \mathfrak{p}$, ce qu'il fallait démontrer.

L'autre assertion $\mathfrak{q} : \mathfrak{p} = \mathfrak{q}$ est symétrique.

On prend $\mathrm{I} = (\mathrm{X})$ et $\mathrm{J} = (\mathrm{Y})$. Ils sont premiers, non comaximaux et pourtant, aucune des inclusions $\mathrm{I} \subset \mathrm{J}$ et $\mathrm{J} \subset \mathrm{I}$ n'est vraie.

**c)** On a clairement $(a) \subset \mathrm{I}$ et $(a) \subset \mathrm{J}$. Supposons que $\mathrm{I} \neq (a)$ et $\mathrm{J} \neq (a)$. Il existe ainsi $x \in \mathrm{I}$ et $y \in \mathrm{J}$ tels que $x \notin (a)$ et $y \notin (a)$. Alors leur produit $xy \in \mathrm{I} \cdot \mathrm{J} \subset (a)$, contrairement à l'hypothèse que $(a)$ est un idéal premier. (On vient de redémontrer le résultat de l'exercice 4.3.3 dans notre cas particulier.)

Supposons donc pour fixer les idées que $\mathrm{I} = (a)$ et prouvons que $\mathrm{J} = \mathrm{A}$. Comme $\mathrm{I} \cdot \mathrm{J} = (a)$, on peut écrire $a = \sum_{i=1}^{n} x_i y_j$, avec $x_i \in \mathrm{I}$ et $y_j \in \mathrm{J}$. Ainsi, on écrit $x_i = ax_i'$, d'où la relation $a \sum_{i=1}^{n} x_i' y_i = a$. Comme $a$ n'est pas diviseur de 0 dans A, on peut simplifier par $a$,

d'où la relation

$$1 = \sum_{i=1}^{n} x_i' y_i$$

qui prouve que $1 \in \mathrm{J}$, et donc que $\mathrm{J} = \mathrm{A}$.

*Solution de l'exercice 4.3.7.* — **a)** Soit A un anneau local et notons $\mathfrak{m}$ son idéal maximal. Montrons qu'un élément $x \in \mathrm{A}$ est inversible si et seulement si $x \notin \mathfrak{m}$. En effet, si $x \in \mathrm{A}$ est inversible, il ne peut pas appartenir à $\mathfrak{m}$ qui est distinct de A. Réciproquement, si $x \in \mathrm{A}$ n'est pas inversible, il appartient à un idéal maximal de A, donc à $\mathfrak{m}$.

Dans l'autre sens, soit A un anneau tel que l'ensemble de ses éléments non inversibles soit un idéal I. Comme un élément de A est inversible si et seulement si il n'appartient à aucun idéal maximal, I est nécessairement la réunion des idéaux maximaux de A. Soit alors $\mathfrak{m}$ un idéal maximal de A. On a $\mathfrak{m} \subset I$. Comme $\mathfrak{m}$ est maximal et $I \neq A$, $\mathfrak{m} = I$. Autrement dit, I est l'unique idéal maximal de A qui est donc un anneau local.

**b)** Notons S la partie multiplicative $A \setminus \mathfrak{p}$. On sait que tout idéal strict (*i.e.* distinct de l'idéal (1)) de $A_\mathfrak{p}$ est de la forme $IA_\mathfrak{p}$ pour I un idéal de A disjoint de S. Cela signifie donc $I \subset \mathfrak{p}$. Par suite, tout idéal strict de $A_\mathfrak{p}$ est contenu dans l'idéal strict $\mathfrak{p}A_\mathfrak{p}$ qui est donc nécessairement l'unique idéal maximal de $A_\mathfrak{p}$.

*Solution de l'exercice 4.3.8.* — **a)** Supposons que $S = A \setminus \bigcup_i \mathfrak{p}_i$, pour des idéaux premiers $\mathfrak{p}_i$ de A. Montrons que S est multiplicative. En effet, $1 \in S$. Soient $x \in S$, $y \in S$, cela signifie que pour tout $i$, $x \notin \mathfrak{p}_i$ ; alors, $\mathfrak{p}_i$ étant premier, $xy \notin \mathfrak{p}_i$, d'où $xy \in S$. Montrons que S est saturée. Si $xy \in S$, cela signifie que $xy \notin \mathfrak{p}_i$, et il est nécessaire que ni $x$, ni $y$ n'appartienne à $\mathfrak{p}_i$, d'où $x \in S$ et $y \in S$.

Réciproquement, soit S une partie multiplicative et saturée. Si $a \notin S$, on cherche un idéal premier de A disjoint de S et contenant $a$. L'image de S dans $A/(a)$ est encore une partie multiplicative, et comme S est saturée, elle ne contient pas 0 : si $x \in S \cap (a)$, alors $x = ay \in S$, d'où $a \in S$. On sait alors qu'il existe un idéal premier de $A/(a)$ disjoint de l'image de S. (Ce fait intervient dans la démonstration que le nilradical est l'intersection des idéaux premiers, on prend un élément maximal parmi les idéaux disjoints de l'image de S et on prouve que cet idéal est premier.) L'image réciproque dans A de cet idéal premier de $A/(a)$ est alors un idéal premier de A disjoint de S et qui contient $a$. Autrement dit, $A \setminus S$ est réunion d'idéaux premiers.

**b)** Montrons que $\tilde{S}$ est une partie multiplicative : soient $x$ et $x'$ dans $\tilde{S}$. Alors, il existe $y$ et $y'$ dans A tels que $xy \in S$ et $x'y' \in S$. Comme S est une partie multiplicative, on a ainsi $xy(x'y') \in S$, ce qui implique $xy \in \tilde{S}$. Montrons ensuite que $\tilde{S}$ est une partie saturée : si $xy \in \tilde{S}$, il existe $a \in A$ tel que $xya \in S$. Alors, $x(ay) \in S$, ce qui implique $x \in \tilde{S}$, et $y(ax) \in S$, d'où $y \in \tilde{S}$.

Enfin, soit T une partie multiplicative saturée qui contient S et montrons que $\tilde{S} \subset T$. Soient en effet $x \in \tilde{S}$, et $a \in A$ tel que $ax \in S$. Comme $S \subset T$, $ax \in T$, et comme T est saturée, $x \in T$.

**c)** D'après la première question, $A \setminus \tilde{S}$ est la réunion des idéaux premiers disjoints de $\tilde{S}$. Si un idéal premier est disjoint de $\tilde{S}$, il est a fortiori disjoint de S. Il reste à prouver que si un idéal premier $\mathfrak{p}$ est disjoint de S, il est disjoint de $\tilde{S}$. Or, si $x \in \mathfrak{p} \cap \tilde{S}$, il existe $a \in A$ tel que $ax \in S$, et alors, $ax \in \mathfrak{p} \cap S$, ce qui prouve que $\mathfrak{p}$ et S ne sont pas disjoints.

**d)** Montrons que l'homomorphisme

$$\varphi : \mathrm{S}^{-1}\mathrm{A} \to \tilde{\mathrm{S}}^{-1}\mathrm{A}$$

est injectif et surjectif. Soit $x/y \in \tilde{\mathrm{S}}^{-1}\mathrm{A}$, avec $x \in \mathrm{A}$ et $y \in \tilde{\mathrm{S}}$; choisissons $a \in \mathrm{A}$ tel que $ay \in \mathrm{S}$. Alors, $x/y = ax/ay$ est l'image d'un élément de $\mathrm{S}^{-1}\mathrm{A}$, donc $\varphi$ est surjectif. Soit $x/y \in \mathrm{S}^{-1}\mathrm{A}$ dont l'image dans $\tilde{\mathrm{S}}^{-1}\mathrm{A}$ est nulle. Il existe ainsi $a \in \tilde{\mathrm{S}}$ tel que $ax = 0$. Si $b \in \mathrm{A}$ est tel que $ab \in \mathrm{S}$, on a aussi $abx = 0$, ce qui prouve que $x/y = 0$ dans $\mathrm{S}^{-1}\mathrm{A}$, et donc $\varphi$ est injectif.

*Solution de l'exercice 4.3.9.* — **a)** Supposons (i) et montrons (ii). Soit $\mathrm{B} = \mathrm{A}/\mathrm{I}$ un quotient de A. On a comme toujours $\mathfrak{N}(\mathrm{B}) \subset \mathfrak{J}(\mathrm{B})$. Les idéaux premiers (resp. maximaux) sont en bijection avec les idéaux premiers (resp. maximaux) de A qui contiennent I. D'après (i), si $\mathfrak{p}$ est un idéal premier qui contient I, il est égal à une intersection d'idéaux maximaux, qui contiennent nécessairement I. Finalement, $\mathfrak{N}(\mathrm{B})$ est une intersection d'idéaux maximaux qui contiennent I, donc contient $\mathfrak{J}(\mathrm{B})$. On a donc prouvé que $\mathfrak{N}(\mathrm{B}) = \mathfrak{J}(\mathrm{B})$.

Dans l'autre sens, supposons (ii) et soit $\mathfrak{p}$ un idéal premier de A. Le radical nilpotent de $\mathrm{A}/\mathfrak{p}$ est nul (car $\mathrm{A}/\mathfrak{p}$ est intègre). Donc le radical de Jacobson de $\mathrm{A}/\mathfrak{p}$ aussi, ce qui signifie que

$$\bigcap_{\mathfrak{m} \subset \mathfrak{p}} \mathfrak{m} = \mathfrak{p}.$$

Par suite, $\mathfrak{p}$ est intersection d'idéaux maximaux et (i) est vérifié.

**b)** Soit $\mathfrak{p}$ un idéal premier de $\mathbf{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Notons V l'ensemble algébrique $\mathscr{Z}(\mathfrak{p})$ qu'il définit. D'après le théorème des zéros, on a

$$\mathscr{I}(\mathrm{V}) = \sqrt{\mathfrak{p}} = \mathfrak{p}$$

puisque $\mathfrak{p}$ est premier. Or, $\mathscr{I}(\mathscr{Z}(\mathfrak{p}))$ est l'ensemble des $\mathrm{P} \in \mathbf{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ tels que pour tout $(a_1, \ldots, a_n) \in \mathrm{V}$, $\mathrm{P}(a_1, \ldots, a_n) = 0$. C'est donc l'intersection des idéaux maximaux de $\mathbf{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ de la forme $(\mathrm{X}_1 - a_1, \ldots, \mathrm{X}_n - a_n)$ avec $(a_1, \ldots, a_n) \in \mathrm{V}$. Par suite, $\mathfrak{p}$ est intersection d'idéaux maximaux.

*Solution de l'exercice 4.3.10.* — Soit $a$ un élément de $\mathfrak{J}$ et soit $x \in \mathrm{A}$. On veut montrer que $1 - ax$ est inversible. Soit $\mathfrak{m}$ un idéal maximal de A. Comme $ax$ appartient à $\mathfrak{J} \subset \mathfrak{m}$ et $1 \notin \mathfrak{m}$, $1 - ax$ n'appartient pas à $\mathfrak{m}$. Ceci prouve que $1 - ax$ n'appartient à aucun idéal maximal de A. Il est donc inversible.

Réciproquement, soit $a$ un élément de A n'appartenant pas à $\mathfrak{J}$. Il existe alors un idéal maximal $\mathfrak{m}$ de A tel que $a \notin \mathfrak{m}$. Par l'homomorphisme $\mathrm{cl} : \mathrm{A} \to \mathrm{A}/\mathfrak{m}$, l'image $\mathrm{cl}(a)$ de $a$ est non nulle. Comme $\mathfrak{m}$ est un idéal maximal de A, $\mathrm{A}/\mathfrak{m}$ est un corps et $\mathrm{cl}(a)$ est inversible dans $\mathrm{A}/\mathfrak{m}$. Il existe donc $b \in \mathrm{A}$ tel que $\mathrm{cl}(a)\,\mathrm{cl}(b) = 1$ dans $\mathrm{A}/\mathfrak{m}$, c'est-à-dire $1 - ab \in \mathfrak{m}$. Par conséquent, $1 - ab$ n'est

pas inversible et il existe donc $x \in \mathrm{A}$ (à savoir $x = b$) tel que $1 - ax$ n'est pas inversible.

*Solution de l'exercice 4.3.11.* — L'hypothèse peut se retraduire en disant que si $a \in \mathbf{C}^n$ vérifie $\mathrm{P}(a) = 0$, alors $\mathrm{Q}(a) = 0$ ou $\mathrm{R}(a) = 0$, c'est-à-dire $\mathrm{QR}(a) = 0$. Autrement dit, $\mathscr{V}((\mathrm{P})) \subset \mathscr{V}((\mathrm{QR}))$. D'après le théorème des zéros de Hilbert, $\sqrt{(\mathrm{QR})} \subset \sqrt{(\mathrm{P})}$. Il existe en particulier un entier $m$ tel que $(\mathrm{QR})^m \in (\mathrm{P})$, i.e. P divise $(\mathrm{QR})^m$.

Comme P est irréductible et $\mathbf{C}[x_1, \ldots, x_n]$ est un anneau factoriel, l'idéal (P) est premier et P divise Q ou P divise R. Comme par hypothèse P ne divise pas R, P divise donc Q, cqfd.

# 5 Anneaux principaux, factoriels

*Comme l'indique son titre, ce chapitre est consacré aux anneaux principaux et factoriels. Par définition, dans un anneau principal, tout idéal est engendré par un seul élément. Les anneaux factoriels sont ceux qui donnent lieu à une « décomposition en facteurs premiers ».*
*On donne deux exemples d'application de ces notions. L'une, arithmétique et due à* Fermat, *concerne les nombres entiers qui sont de la forme $a^2 + b^2$, pour deux entiers $a$ et $b$. L'autre, géométrique, est un théorème de* Bézout *concernant le nombre de solutions communes à deux polynômes de $\mathbf{C}[X,Y]$ sans facteur commun.*

## 5.1. Définitions

Définition 5.1.1. — *On dit qu'un anneau est* principal *s'il est intègre et si tous ses idéaux sont principaux.*

*Exemples 5.1.2.* — a) On a vu (exemples 2.2.6 et 4.2.1) que l'anneau des entiers relatifs $\mathbf{Z}$ et l'anneau des polynômes en une indéterminée à coefficients dans un corps $k$ sont des anneaux principaux.

b) Soit $k$ un corps. L'anneau $k[X,Y]$ n'est pas principal. En effet, l'idéal $(X,Y)$ n'est pas principal.

*Démonstration.* — Soit par l'absurde $P \in k[X,Y]$ tel que $(X,Y) = (P)$. Il existe alors $Q$ et $R$ dans $k[X,Y]$ tels que $X = PQ$ et $Y = PR$. En écrivant $P = a_0(X) + a_1(X)Y + \dots$ comme un polynôme en $Y$ à coefficients dans $k[X]$, la relation $X = PQ$ montre que $\deg_Y P + \deg_Y Q = 0$, donc $P$ ne fait pas intervenir $Y$. De même, la relation $Y = PR$ montre que $P$ ne fait pas intervenir $X$. Finalement, $P$ est un polynôme constant, non nul et $(P) = (1)$. Cela implique qu'il existe $A$ et $B$ dans $k[X,Y]$ tels que $1 = XA(X,Y) + YB(X,Y)$. Or, le terme constant du membre de droite

est nul, tandis que celui du membre de gauche est égal à 1. Cette contradiction montre que l'idéal (X,Y) n'est pas principal □

Les deux exemples d'anneaux principaux que nous connaissons à présent sont même des *anneaux euclidiens.*

PROPOSITION 5.1.3. — *Soit* A *un anneau intègre et* $\varphi : A \setminus \{0\} \to \mathbf{N}$ *une fonction telle que pour tous* $a$ *et* $b$ *dans* A, *avec* $b \neq 0$, *il existe* $q$ *et* $r \in A$ *tels que*

– $a = bq + r$ ;

– $r = 0$ *ou* $\varphi(r) < \varphi(b)$.

*Alors,* A *est principal.*

*Démonstration.* — On reprend les arguments des exemples 2.2.6 et 4.2.1. Soit I un idéal de A dont on veut montrer qu'il est principal. Comme l'idéal nul est principal, on peut supposer que $I \neq \{0\}$. Soit alors un élément $a \in I \setminus \{0\}$ un élément tel que $\varphi(a)$ est minimal. On a bien sûr $(a) \subset I$, et on va montrer que $I = (a)$. Soit $b$ un élément de I et choisissons $q$ et $r$ tels que $b = aq + r$ comme dans l'énoncé. Si $r \neq 0$, on a $\varphi(r) < \varphi(a)$, ce qui est absurde puisque $r = b - aq$ appartient à I. Donc $r = 0$ et $b = aq \in (a)$. Par suite, $I = (a)$ ; tout idéal de A est principal. Comme A est intègre, A est principal. □

*Exemple 5.1.4* (Anneau des entiers de Gauß). — L'anneau $\mathbf{Z}[i]$ engendré par $\mathbf{Z}$ et $i$ dans $\mathbf{C}$ est un anneau principal.

*Démonstration.* — L'ensemble des nombres complexes de la forme $a + ib$ avec $(a, b) \in \mathbf{Z}^2$ est un sous-anneau de $\mathbf{C}$ : il est stable par addition, soustraction et multiplication puisque

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc).$$

C'est donc l'anneau $\mathbf{Z}[i]$ engendré par $\mathbf{Z}$ et $i$ dans $\mathbf{C}$. Soit $\varphi : \mathbf{Z}[i] \to \mathbf{N}$ défini par $\varphi(a + ib) = |a + ib|^2 = a^2 + b^2$.

Commençons par une remarque : soit $z = x + iy$ un nombre complexe. Il existe des entiers relatifs $a$ et $b$ tels que $|x - a| \leq 1/2$ et $|y - b| \leq 1/2$. Posons $u = a + ib$. Alors, on a $|z - u|^2 \leq 1/4 + 1/4 = 1/2$.

Montrons maintenant que $\varphi$ vérifie l'hypothèse de la proposition. Soit $a$ et $b$ deux éléments de $\mathbf{Z}[i]$, $b$ étant non nul. Soit $z$ le nombre complexe $a/b$, et définissons $q$ le nombre complexe $u$ obtenu comme dans la remarque et $r = a - bq$. Ce sont des éléments de $\mathbf{Z}[i]$. Alors, on a

$$|r|^2 = |a - bq|^2 = |b|^2 \, |(a/b) - q|^2 \leq |b|^2 / 2 < |b|^2 .$$

Par suite, $\varphi(r) < \varphi(b)$.

La proposition précédente implique donc que $\mathbf{Z}[i]$ est un anneau principal. □

## 5.2. Anneaux factoriels

DÉFINITION 5.2.1. — *Soit* A *un anneau intègre. Un élément* $a$ *de* A *est dit* irréductible *s'il vérifie les propriétés suivantes :*

– $a$ *n'est pas inversible ;*

– *si* $b$ *et* $c$ *sont des éléments de* A *tels que* $a = bc$*, l'un des deux,* $b$ *ou* $c$*, est inversible.*

*Exemples 5.2.2.* — a) L'élément 0 n'est jamais irréductible : il s'écrit $0 \cdot 0$ et 0 n'est pas inversible.

b) Un entier relatif est irréductible si et seulement s'il est un nombre premier ou l'opposé d'un nombre premier.

c) Soit $k$ un corps. Dans l'anneau $k[X]$, un polynôme est irréductible s'il est de degré $\geq 1$ et s'il ne s'écrit pas comme produit de deux polynômes de degrés $\geq 1$.

PROPOSITION 5.2.3. — *Soit* $k$ *un corps.*

*a) Dans l'anneau* $k[X]$*, un polynôme ayant une racine dans* $k$ *est irréductible si et seulement si il est de degré* 1*.*

*b) Un polynôme de degré* 2 *ou* 3 *dans* $k[X]$ *est irréductible si et seulement si il n'a pas de racine dans* $k$*.*

*c) Dans l'anneau* $\mathbf{C}[X]$*, les polynômes irréductibles sont les polynômes de degré* 1*. Dans l'anneau* $\mathbf{R}[X]$*, les polynômes irréductibles sont les polynômes de degré* 1 *et les polynômes du second degré sans racine réelle.*

*Démonstration.* — a) Si un polynôme de degré 1 est un produit QR, on a $\deg(Q) + \deg(R) = 1$ et nécessairement, l'un des degrés $\deg(Q)$ ou $\deg(R)$ est nul, ce qui signifie que Q ou R est inversible. Les polynômes de degré 1 sont donc irréductibles.

Réciproquement, si P a une racine $z$ dans $k$, on peut factoriser $P = (X-z)Q+R$ avec $\deg R < 1$, c'est-à-dire R constant. On a alors $P(z) = R(z) = 0$, d'où la factorisation $P = (X - z)Q$. Comme $\deg Q = \deg P - 1$, P n'est pas irréductible dès que $\deg P \geq 2$.

b) Soit maintenant P un polynôme de degré 2 ou 3. S'il existe deux polynômes non constants Q et R tels que $P = QR$, on a $\deg(Q) + \deg(R) = \deg(P) \leq 3$ et $\deg(Q), \deg(P) \geq 1$. Cela implique que $\deg(Q) = 1$ ou $\deg(R) = 1$ et ou bien Q, ou bien R a une racine dans $k$. Par suite, P a une racine dans $k$.

c) On utilise le fait que $\mathbf{C}$ est un corps algébriquement clos (théorème de d'Alembert–Gauß). Tout polynôme non constant de $\mathbf{C}[X]$ est produit de polynômes de degré 1. Un polynôme de degré $\geq 2$ n'est par conséquent pas irréductible.

Pour $\mathbf{R}[X]$, on utilise le résultat pour $\mathbf{C}[X]$. On a déjà démontré que les polynômes de degré 1 sont irréductibles, ainsi que les polynômes de degré 2

sans racine. Les polynômes de degré 2 ayant une racine ne sont pas irréductibles. Soit maintenant $P \in \mathbf{R}[X]$ de degré $\geq 3$ et soit $z$ une racine de P dans $\mathbf{C}$. Si $z \in \mathbf{R}$, P n'est pas irréductible. Si $z \in \mathbf{C} \setminus \mathbf{R}$, on a $P(\bar{z}) = \overline{P(z)} = 0$, donc $\bar{z}$ est une racine de P, distincte de $z$. On peut alors factoriser $P = (X - z)(X - \bar{z})Q$ avec $Q \in \mathbf{C}[X]$ de degré $\deg P - 2 \geq 1$. Comme P et $(X-z)(X-\bar{z}) = X^2 - 2\Re(z)X + |z|^2$ appartiennent à $\mathbf{R}[X]$, Q appartient à $\mathbf{R}[X]$. Cette factorisation montre que P n'est pas irréductible. □

*Exercice 5.2.4.* — Soit A un anneau et soit $P \in A[X]$ un polynôme de degré supérieur ou égal à 2. On suppose que P a une racine dans A. Montrer que P n'est pas irréductible.

DÉFINITION 5.2.5. — *Soit* A *un anneau intègre.*

*On dit qu'un anneau* A *est* factoriel *si tout élément non nul de* A *peut s'écrire, d'une façon essentiellement unique, comme produit d'éléments irréductibles de* A.

Autrement sit, si $a$ est un élément non nul de A, il existe $n \geq 0$, des éléments irréductibles $p_1, \ldots, p_n$ de A et un élément inversible $u \in A$ tels que

$$a = up_1 \ldots p_n.$$

(Si $n = 0$, cela signifie que $a = u$ est inversible.) L'unicité est bien entendu à l'ordre et à des éléments inversibles près. Précisément, on demande que si $a = up_1 \ldots p_n = u'p'_1 \ldots p'_m$, alors

– on a $m = n$ ;

– il existe une permutation $\sigma : \{1; \ldots; n\} \to \{1; \ldots; n\}$ et pour tout $i \in \{1; \ldots; n\}$ un élément inversible $u_i$ tels que $p_{\sigma(i)} = u_i p_i$.

On sait que $\mathbf{Z}$ est un anneau factoriel (c'est le théorème bien connu de décomposition en facteurs premiers). Si $k$ est un corps, $k[X]$ est aussi un anneau factoriel. Plus généralement :

THÉORÈME 5.2.6. — *Les anneaux principaux sont factoriels.*

La démonstration est en deux parties. D'abord on démontre l'existence d'une décomposition en facteurs irréductibles, ensuite, on établit l'unicité.

*Démonstration de l'existence.* — Soit A un anneau principal et soit $a$ un élément non nul de A dont on suppose par l'absurde qu'il n'est pas produit d'éléments irréductibles. On pose $a_1 = a$. Il en résulte que $a$ n'est ni inversible (un inversible $u$ se décompose comme produit de zéro facteur irréductible : $u = u$) ni irréductible (on pourrait le décomposer comme produit d'un facteur irréductible égal à lui-même). Ainsi, il existe $b$ et $c$ non inversibles dans A tels que $a = bc$. Comme $a$ n'est pas produit d'éléments irréductibles, au moins l'un des deux, $b$ ou $c$ n'est pas produit d'éléments irréductibles ; Notons $a_2$ cet élément. Comme $b$ et $c$ ne

sont pas inversibles, l'idéal $(a_2)$ contient strictement l'idéal $(a_1)$. Par récurrence, on construit ainsi une suite $(a_1; a_2; \dots)$ d'éléments de A tels que l'on ait une suite strictement croissante d'idéaux

$$(a_1) \subsetneq (a_2) \subsetneq \dots$$

Soit I la réunion de ces idéaux. Comme la réunion est croissante, c'est un idéal de A (l'argument a déjà été expliqué page 45 : pour la somme, si $x$ et $y$ sont dans I, ils sont dans un certain $(a_n)$, donc $x+y \in (a_n)$ et donc $x+y \in \mathrm{I}$). Comme A est principal, il existe $x \in \mathrm{A}$ tel que $\mathrm{I} = (x)$. Alors, $x \in \bigcup_n (a_n)$, donc il existe un entier $n$ tel que $x \in (a_n)$ ce qui permet d'écrire $x = a_n u$ pour $u \in \mathrm{A}$. Par ailleurs, $a_n \in (x)$ donc il existe $v \in \mathrm{A}$ tel que $a_n = xv$. On a alors $x = a_n u = xuv$. Comme $x$ est non nul (sinon I serait nul) et comme A est intègre, on peut simplifier par $x$, d'où l'égalité $uv = 1$. Ainsi, $u$ et $v$ sont inversibles et $(a_n) = (x)$, alors que l'on a l'inclusion stricte $(a_n) \subsetneq (a_{n+1}) \subset \mathrm{I} = (x)$. Cette contradiction montre que tout élément non nul d'un anneau principal admet une décomposition comme produit d'éléments irréductibles. □

Pour démontrer l'unicité, nous aurons besoin du *lemme de Gauß*.

Lemme 5.2.7 (Lemme de Gauß). — *Soit* A *un anneau principal et soit* $p \in \mathrm{A}$ *un élément irréductible. Alors si* $a$ *et* $b$ *sont deux éléments de* A *tels que* $p$ *divise* $ab$, $p$ *divise* $a$ *ou* $p$ *divise* $b$. *En d'autre termes, l'idéal* $(p)$ *est premier.*

*Démonstration.* — Supposons que $p$ ne divise pas $a$ et considérons l'idéal $(p, a)$. Comme A est principal, il existe $c \in \mathrm{A}$ tel que $(p, a) = (c)$. Par suite, il existe $x$ et $y \in \mathrm{A}$ tels que $p = cx$ et $a = cy$. Comme $p$ ne divise pas $a$, il ne divise pas $c$ ; puisque $p$ est irréductible, il divise $x$. Il existe alors $u \in \mathrm{A}$ tel que $x = pu$ et, simplifiant par $p$ l'égalité $p = cpu$, on obtient que $1 = cu$. Autrement dit, $c$ est inversible et $(p, a) = \mathrm{A}$.

Ainsi, il existe $f$ et $g$ dans A tels que $1 = pf + ag$. Multiplions cette égalité par $b$, on trouve que $b = pfb + abg$. Comme $ab$ est multiple de $p$, $b$ est multiple de $p$. □

*Démonstration de l'unicité.* — On raisonne par récurrence sur le nombre minimal de facteurs irréductibles intervenant dans une décomposition en facteurs premiers d'un élément.

Supposons donc d'abord que $a$ est inversible (cas de zéro facteur premier) et soit $a = u' p'_1 \dots p'_m$ une autre décomposition. Si $m \geq 1$, les $p'_i$ sont inversibles, ce qui est absurde. Donc $m = 0$.

Soit maintenant $a = up_1 \dots p_n = u' p'_1 \dots p'_m$ deux décompositions d'un élément $a$ en produits d'éléments irréductibles, $n \geq 1$ étant supposé minimal. D'après le lemme de Gauß, l'élément irréductible $p_n$ divise nécessairement l'un des $p'_1$,

$\ldots$, $p'_m$. Quitte à les renuméroter, on peut supposer que $p_n$ divise $p'_m$. Il existe ainsi $u_n \in \mathrm{A}$ tel que $p_n = u_n p'_m$ et, $p_n$ étant irréductible, $u_n$ est nécessairement inversible. On peut alors simplifier par $p_n$, d'où une relation

$$(a/p_n) = up_1 \ldots p_{n-1} = u' u_n p'_1 \ldots p'_{m-1}.$$

Par récurrence, on a $m - 1 = n - 1$, c'est-à-dire $m = n$ et, quitte à renuméroter les $p'_j$, il existe pour tout $j \in \{1; \ldots; n-1\}$ un élément inversible $u_j \in \mathrm{A}^\times$ tel que $p_j = u_j p'_j$. Les deux décompositions de $a$ sont donc équivalentes. □

La démonstration que nous venons de faire montre en fait un résultat plus général (mais pas très utile dans ce cours).

*Exercice 5.2.8.* — Un anneau intègre A est factoriel si et seulement si il vérifie les deux propriétés suivantes :
– toute suite d'idéaux principaux dans A est stationnaire ;
– tout élément irréductible de A engendre un idéal premier (lemme de Gauß).

En particulier, *la vérification du lemme de Gauß suffit à assurer l'unicité d'une décomposition en facteurs irréductibles.*

*5.2.9. L'unicité dans la décomposition en facteurs irréductibles.* — Il est commode de normaliser la décomposition en facteurs irréductibles dans un anneau factoriel A. Pour cela, choisissons une famille $(\pi_i)$ d'éléments irréductibles de A de sorte que :
– si $i \neq j$, $\pi_i$ et $\pi_j$ ne sont pas associés ;
– tout élément irréductible de A est associé à l'un des $\pi_i$.
Alors, tout élément non nul de A s'écrit de manière unique sous la forme $u \prod_i \pi_i^{r_i}$ où $u$ est un élément inversible de A et les $r_i$ des entiers positifs ou nuls, seul un nombre fini d'entre eux étant nuls.

Si A est l'anneau $\mathbf{Z}$, un choix courant pour les $\pi_i$ consiste à prendre tous les nombres premiers. L'élément inversible $u$ peut valoir $\pm 1$ et correspond au signe.

Si A est l'anneau des polynômes à coefficients dans un corps $k$, on peut prendre pour les $\pi_i$ l'ensemble des polynômes irréductibles *unitaires*. L'élément $u$ appartient alors à $k^*$ et correspond au coefficient dominant.

L'intérêt de cette normalisation est qu'un élément $a = u \prod_i \pi_i^{r_i}$ divise un élément $b = v \prod_i \pi_i^{s_i}$ si et seulement si pour tout $i$, $r_i \leq s_i$. (En effet, si $c \in \mathrm{A}$ est tel que $b = ac$, soit $c = w \prod_i \pi_i^{t_i}$ la décomposition en facteurs irréductibles de $c$, on a alors

$$b = v \prod_i \pi_i^{s_i} = uw \prod_i \pi_i^{r_i + t_i},$$

d'où, par unicité, $s_i = r_i + t_i \geq r_i$ pour tout $i$. Réciproquement, il suffit de poser $c = vu^{-1} \prod_i \pi_i^{s_i - r_i}$.)

*5.2.10. Ppcm, pgcd.* — Soit A un anneau factoriel. Si $a$ et $b$ sont deux éléments (non nuls) de A, on va définir leur ppcm et leur pgcd. Pour simplifier, on suppose avoir normalisé la décomposition en facteurs irréductibles comme ci-dessus. Soit

$$a = u \prod_i \pi_i^{r_i} \quad \text{et} \quad b = v \prod_i \pi_i^{s_i}$$

les décompositions en facteurs irréductibles de $a$ et $b$. On définit

$$\operatorname{pgcd}(a,b) = \prod_i \pi_i^{\min(s_i,r_i)} \quad \text{et} \quad \operatorname{ppcm}(a,b) = \prod_i \pi_i^{\max(s_i,r_i)}.$$

Ils méritent leur nom, à savoir : *tout élément non nul de* A *qui divise a et b divise leur pgcd, tout élément de* A *multiple de a et de b est multiple de leur ppcm.*

Définition 5.2.11. — *Deux éléments a et b sont dits* premiers entre eux *si leur pgcd est égal à* 1.

Proposition 5.2.12. — *Soit* A *un anneau factoriel et soit a, b deux éléments non nuls de* A. *L'idéal engendré par* $\operatorname{pgcd}(a,b)$ *est le plus petit idéal principal contenant l'idéal* $(a,b)$. *L'idéal engendré par* $\operatorname{ppcm}(a,b)$ *est le plus grand idéal principal contenu dans l'idéal* $(a) \cap (b)$.

*En particulier, si* A *est un anneau principal, deux éléments a et b sont premiers entre eux si et seulement si les idéaux* $(a)$ *et* $(b)$ *sont comaximaux.*

*Démonstration.* — C'est une reformulation de ce qui a été dit plus haut. Notons

$$a = u \prod_i \pi_i^{r_i} \quad \text{et} \quad b = v \prod_i \pi_i^{s_i}$$

les décompositions en facteurs irréductibles de $a$ et $b$. Un idéal principal $(x)$ contient $(a,b)$ si et seulement si $a$ et $b$ sont multiples de $x$. Si

$$x = w \prod_i \pi_i^{t_i}$$

est la décomposition en facteurs irréductibles de $x$, cela signifie que pour tout $i$, $r_i \geq t_i$ et $s_i \geq t_i$, ce qui équivaut encore à $\min(r_i, s_i) \geq t_i$, soit encore au fait que $x$ divise le pgcd de $a$ et $b$.

Un idéal principal $(x)$ est contenu dans $(a) \cap (b)$ si et seulement si $x$ est multiple de $a$ et de $b$. Avec les mêmes notations, cela signifie que pour tout $i$, $t_i \geq r_i$ et $t_i \geq s_i$, soit encore $t_i \geq \max(r_i, s_i)$, soit encore au fait que $x$ est multiple du ppcm de $a$ et $b$. □

*Remarque 5.2.13.* — Si l'on ne fixe pas une forme particulière pour la décomposition en facteurs irréductibles, le ppcm et le pgcd de deux éléments sera bien défini à multiplication par un élément inversible près : c'est un élément du monoïde quotient $A/A^\times$ (pour la multiplication).

*Exercice 5.2.14.* — Généraliser la définition du pgcd et du ppcm et la proposition précédente au cas d'une famille quelconque. (Le ppcm pourra éventuellement être nul.)

## 5.3. Sommes de carrés

Le but de ce paragraphe est de démontrer, à l'aide des propriétés de l'anneau $\mathbf{Z}[i]$ le théorème suivant :

THÉORÈME 5.3.1 (Fermat, 1640). — *Soit $p$ un nombre premier impair. Il existe $a$ et $b$ dans $\mathbf{Z}$ tels que $p = a^2 + b^2$ si et seulement si $p \equiv 1 \pmod 4$*

*Plus généralement, un entier $n \geq 1$ est somme de deux carrés d'entiers si et seulement si les exposants des nombres premiers congrus à $-1$ modulo $4$ dans la décomposition en facteurs premiers de $n$ sont pairs.*

*5.3.2. La norme.* — On définit une application $\mathrm{N} : \mathbf{Z}[i] \to \mathbf{N}$ par $\mathrm{N}(z) = z\bar{z} = |z|^2$. Si $z = a + ib$, on a donc $\mathrm{N}(z) = a^2 + b^2$. De plus, si $z$ et $z'$ sont deux éléments de $\mathbf{Z}[i]$, alors $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$.

*5.3.3. Éléments inversibles de $\mathbf{Z}[i]$.* — Soit $z \in \mathbf{Z}[i]$ un élément inversible. Alors, il existe $z' \in \mathbf{Z}[i]$ tel que $zz' = 1$. Par suite, $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z') = \mathrm{N}(1) = 1$ et $\mathrm{N}(z)$ est inversible dans $\mathbf{N}$, c'est-à-dire $\mathrm{N}(z) = 1$. Posons $z = a + ib$ avec $(a, b) \in \mathbf{Z}^2$. On a $\mathrm{N}(z) = a^2 + b^2$ ce qui laisse quatre possibilités, $a = \pm 1$ et $b = 0$, ou $a = 0$ et $b = \pm 1$, qui correspondent à $z \in \{1; -1; i; -i\}$. Ces quatre éléments étant inversibles, on a démontré que

*les éléments inversibles de $\mathbf{Z}[i]$ sont $1$, $-1$, $i$ et $-i$.*

Nous déterminons maintenant la décomposition des nombres premiers $p$ en facteurs irréductibles dans $\mathbf{Z}[i]$.

PROPOSITION 5.3.4. — *Soit $p$ un nombre premier.*
- *Si $p = 2$, on a $p = (1 + i)(1 - i)$, $1 + i$ et $1 - i$ sont irréductibles ;*
- *si $p \equiv 1 \pmod 4$, il existe $\pi \in \mathbf{Z}[i]$ irréductible tel que $p = \pi\bar{\pi}$ ;*
- *si $p \equiv 3 \pmod 4$, $p$ est irréductible dans $\mathbf{Z}[i]$ ;*

*Démonstration.* — On commence par une remarque : si un élément $z \in \mathbf{Z}[i]$ est tel que $\mathrm{N}(z)$ est premier, alors $z$ est irréductible. En effet, on pourrait sinon écrire $z = z_1 z_2$, ni $z_1$ ni $z_2$ n'étant inversibles, et on aurait $\mathrm{N}(z) = \mathrm{N}(z_1)\mathrm{N}(z_2)$,

c'est-à-dire une décomposition du nombre premier $\mathrm{N}(z)$ en un produit de deux facteurs dont aucun n'est égal à 1 !

Par suite, $1+i$ et $1-i$ (dont la norme est 2) sont irréductibles dans $\mathbf{Z}[i]$, ce qui établit le premier alinéa de la proposition.

Supposons maintenant $p$ impair. Nous allons compléter la démonstration en admettant provisoirement deux lemmes. □

LEMME 5.3.5. — *Soit $p$ un nombre premier. On a un isomorphisme*

$$\mathbf{Z}[i]/(p) \simeq \mathbf{F}_p[\mathrm{X}]/(\mathrm{X}^2+1).$$

*Par suite, l'idéal $(p)$ est premier dans $\mathbf{Z}[i]$ si et seulement si $-1$ n'est pas un carré dans $\mathbf{F}_p$.*

LEMME 5.3.6. — *Soit $p$ un nombre premier impair. Alors, $-1$ est un carré dans $\mathbf{F}_p$ si et seulement si $p \equiv 1 \pmod 4$.*

*Fin de la démonstration de la proposition.* — Ces deux lemmes montrent que $p$ est irréductible dans $\mathbf{Z}[i]$ si et seulement si $p \equiv 3 \pmod 4$, ce qui établit déjà le troisième alinéa du théorème.

Si $p \equiv 1 \pmod 4$, $p$ n'est pas irréductible dans $\mathbf{Z}[i]$. Soit $\pi$ un diviseur irréductible de $p$. Alors, $\bar{\pi}$ est aussi un diviseur irréductible de $p$ : d'une factorisation $p = \pi z$, on en déduit une autre $p = \bar{\pi}\bar{z}$. De plus, $\pi$ et $\bar{\pi}$ ne sont pas associés. (En effet, si $\bar{\pi} = \pm\pi$, $\pi \in \mathbf{Z}$, donc $\pi$ est un entier non inversible qui divise $p$, c'est-à-dire $\pi = \pm p$, ce qui est absurde puisque $p$ n'est pas irréductible dans $\mathbf{Z}[i]$. Si $\bar{\pi} = \varepsilon i\pi$ avec $\varepsilon = \pm 1$, écrivons $\pi = a+ib$, $\bar{\pi} = a-ib$ et $a+ib = \varepsilon i(a-ib)$, d'où $a = \varepsilon b$, $\pi = (1+i\varepsilon)a$ et $\mathrm{N}(\pi) = 2\mathrm{N}(a)$ est pair alors qu'il doit diviser $\mathrm{N}(p) = p^2$.) Par suite, $\pi\bar{\pi}$ divise $p$. Soit $a \in \mathbf{Z}[i]$ tel que $p = a\pi\bar{\pi}$. On a alors $p^2 = \mathrm{N}(\pi\bar{\pi})\mathrm{N}(a) = \mathrm{N}(\pi)^2\mathrm{N}(a)$ et $\mathrm{N}(\pi) \neq 1$. Donc $\mathrm{N}(\pi) = p$, $\mathrm{N}(a) = 1$ et $a$ est inversible dans $\mathbf{Z}[i]$. Comme $\pi\bar{\pi}$ est un entier strictement positif, on a en fait $a = p/\pi\bar{\pi} > 0$, d'où $a = 1$. Le théorème est donc démontré. □

*Preuve du lemme 5.3.5.* — On commence par remarquer que le noyau du morphisme d'anneaux $\mathbf{Z}[\mathrm{X}] \to \mathbf{Z}[i]$ donné par $\mathrm{P} \mapsto \mathrm{P}(i)$ est l'idéal $(\mathrm{X}^2+1)$. Cet idéal est manifestement contenu dans le noyau de cet homomorphisme et réciproquement, si $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$ vérifie $\mathrm{P}(i) = 0$, la division euclidienne de P par le polynôme unitaire $\mathrm{X}^2+1$ s'écrit

$$\mathrm{P} = (\mathrm{X}^2+1)\mathrm{Q} + \mathrm{R}, \qquad \mathrm{Q} \in \mathbf{Z}[\mathrm{X}], \qquad \mathrm{R} = a\mathrm{X}+b, \quad (a,b) \in \mathbf{Z}^2.$$

Par suite, $\mathrm{P}(i) = ai+b = 0$ et $a = b = 0$, donc $\mathrm{R} = 0$ et $\mathrm{P} \in (\mathrm{X}^2+1)$. On en déduit des isomorphismes

$$\begin{aligned}\mathbf{Z}[i]/(p) \simeq \big(\mathbf{Z}[\mathrm{X}]/(\mathrm{X}^2+1)\big)/(p) &\simeq \mathbf{Z}[\mathrm{X}]/(p,\mathrm{X}^2+1)\\ &\simeq \big(\mathbf{Z}[\mathrm{X}]/(p)\big)/(\mathrm{X}^2+1) \simeq \mathbf{F}_p[\mathrm{X}]/(\mathrm{X}^2+1)\end{aligned}$$

et le lemme est démontré.

Ainsi, l'idéal $(p)$ est premier dans $\mathbf{Z}[i]$ si et seulement si l'idéal $(X^2+1)$ est premier dans $\mathbf{F}_p[X]$. Comme $\mathbf{F}_p$ est un corps, $\mathbf{F}_p[X]$ est un anneau factoriel et cela équivaut au fait que $X^2+1$ est un polynôme irréductible dans $\mathbf{F}_p[X]$. Comme il est de degré 2, cela revient à dire qu'il n'a pas de racine dans $\mathbf{F}_p$, c'est-à-dire que $-1$ n'est pas un carré dans $\mathbf{F}_p$. □

*Preuve du lemme 5.3.6.* — Soit $\sim$ la relation sur $\mathbf{F}_p^*$ définie par

$$x \sim y \qquad \Leftrightarrow \qquad x = \pm y \quad \text{ou} \quad x = \pm 1/y.$$

C'est une relation d'équivalence : elle est évidemment réflexive et symétrique. De plus, elle est transitive : si $x = \pm y$ et $y = \pm z$, on a $x = \pm z$ ; si $x = \pm y$ et $y = \pm 1/z$, on a $x = \pm 1/z$ ; si $x = \pm 1/y$ et $y = \pm z$, on a $x = \pm 1/z$ ; et si $x = \pm 1/y$ et $y = \pm 1/z$, on a $x = \pm z$.

La classe d'équivalence d'un élément $x$ a pour cardinal 2 si $x = \pm 1/x$ et 4 sinon. Ainsi, la classe de 1 et la classe d'un éventuel élément $x \in \mathbf{F}_p^*$ tel que $x^2 = -1$ ont pour cardinal 2, les autres, en nombre $d$, ont pour cardinal 4. Comme les classes d'équivalences forment une partition de $\mathbf{F}_p^*$ qui est de cardinal $p-1$, il en résulte que

$$p - 1 = \begin{cases} 2 + 4d & \text{si } -1 \text{ n'est pas un carré dans } \mathbf{F}_p ; \\ 2 + 2 + 4d & \text{si } -1 \text{ est un carré.} \end{cases}$$

Ainsi, $-1$ est un carré dans $\mathbf{F}_p$ si et seulement si $p \equiv 1 \pmod 4$. □

Nous pouvons maintenant démontrer le théorème 5.3.1. Soit $p$ un nombre impair. Si $p = a^2 + b^2$, on a $p = (a+ib)(a-ib)$ et donc $p$ n'est pas irréductible dans $\mathbf{Z}[i]$, d'où $p \equiv 1 \pmod 4$. Réciproquement, si $p \equiv 1 \pmod 4$, soit $\pi \in \mathbf{Z}[i]$ tel que $p = \pi\bar{\pi}$ et posons $\pi = a + ib$. Alors, $p = a^2 + b^2$. Remarquons aussi que $2 = 1^2 + 1^2$ est la somme de deux carrés d'entiers.

Soit $n$ un entier $\geq 1$. On peut l'écrire sous la forme $k^2 m$, où $m = p_1 \dots p_r$ est un entier sans facteurs carrés, c'est-à-dire un produit de nombre premiers distincts. Si ces nombres premiers sont ne sont pas congrus à $-1$ modulo 4, il existe pour tout $j$ un élément $z_j = a_j + ib_j \in \mathbf{Z}[i]$ tel que $\mathrm{N}(z_j) = z_j\overline{z_j} = a_j^2 + b_j^2 = p_j$. Posons alors $z = k \prod_{j=1}^{r} z_j$. On a $\mathrm{N}(z) = k^2 \prod_{j=1}^{r} \mathrm{N}(z_j) = k^2 \prod_{j=1}^{r} p_j = k^2 m = n$. Comme $z \in \mathbf{Z}[i]$, il existe $a$ et $b$ dans $\mathbf{Z}$ tels que $z = a + ib$ et $n = a^2 + b^2$.

Réciproquement, supposons que $n = a^2 + b^2$ est somme de deux carrés et soit $p$ un nombre premier congru à $-1$ modulo 4 divisant $n$. On va montrer (par récurrence sur $n$) que l'exposant de $p$ dans la décomposition en facteurs premiers de $n$ est pair. C'est vrai si $n = 1$. Si $\mathrm{cl} : \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ désigne la surjection canonique, on a donc $\mathrm{cl}(a)^2 + \mathrm{cl}(b)^2 = 0$. Supposons que $\mathrm{cl}(a) \neq 0$. Alors, $\mathrm{cl}(a)$ est inversible

dans $\mathbf{Z}/p\mathbf{Z}$ et $\mathrm{cl}(b)/\mathrm{cl}(a)$ est un élément de $\mathbf{F}_p$ dont le carré est $-1$, ce qui est absurde puisque $p \equiv -1 \pmod 4$ (lemme 5.3.6). Ainsi, $\mathrm{cl}(a) = \mathrm{cl}(b) = 0$ ; $a$ et $b$ sont multiples de $p$. On peut donc écrire $a = pa'$, $b = pb'$ et $n = p^2(a'^2 + b'^2)$. Alors, $m = n/p^2$ est un entier qui est somme de deux carrés et $m < n$. Par récurrence, l'exposant de $p$ dans la décomposition en facteurs premiers de $m$ est pair. Comme $n = mp^2$, il en est de même pour $n$.

Citons pour terminer un autre théorème du même genre : le théorème des quatre carrés.

THÉORÈME 5.3.7 (Lagrange, 1770). — *Tout entier positif est somme de quatre carrés : pour tout $n \geq 1$, il existe $a$, $b$, $c$ et $d \in \mathbf{Z}$ tels que $n = a^2 + b^2 + c^2 + d^2$*

## 5.4. Anneaux de polynômes

Dans ce paragraphe, A est un anneau factoriel et l'on s'intéresse à l'anneau $\mathrm{A}[\mathrm{X}]$. Tout d'abord, on rappelle que *les éléments inversibles de* $\mathrm{A}[\mathrm{X}]$ *sont les polynômes constants égaux à un élément inversible de* $\mathrm{A}^\times$. (Comme A est intègre, si P et Q sont deux polynômes de $\mathrm{A}[\mathrm{X}]$, on a $\deg(\mathrm{PQ}) = \deg(\mathrm{P}) + \deg(\mathrm{Q})$. Par suite, si $\mathrm{PQ} = 1$, $\deg(\mathrm{P}) = \deg(\mathrm{Q}) = 0$, P et Q sont des éléments de A, inverses l'un de l'autre dans A, donc inversibles. Voir aussi l'exercice 2.5.7,)

DÉFINITION 5.4.1. — *Soit* A *un anneau factoriel et soit* P *un polynôme dans* $\mathrm{A}[\mathrm{X}]$. *Le* contenu *de* P, *noté* $\mathrm{ct}(\mathrm{P})$, *est par définition le pgcd des coefficients de* P. *Un polynôme est dit* primitif *si son contenu est* 1, *c'est-à-dire si ses coefficients sont premiers entre eux.*

PROPOSITION 5.4.2. — *Soit* A *un anneau factoriel et soit* P *et* Q *deux polynômes de* $\mathrm{A}[\mathrm{X}]$. *Alors,* $\mathrm{ct}(\mathrm{PQ}) = \mathrm{ct}(\mathrm{P})\,\mathrm{ct}(\mathrm{Q})$.

*Démonstration.* — Par définition, il existe des polynômes primitifs $\mathrm{P}_1$ et $\mathrm{Q}_1$ dans $\mathrm{A}[\mathrm{X}]$ tels que $\mathrm{P} = \mathrm{ct}(\mathrm{P})\mathrm{P}_1$ et $\mathrm{Q} = \mathrm{ct}(\mathrm{Q})\mathrm{Q}_1$. Alors, $\mathrm{PQ} = \mathrm{ct}(\mathrm{P})\,\mathrm{ct}(\mathrm{Q})\mathrm{P}_1\mathrm{Q}_1$ et $\mathrm{ct}(\mathrm{PQ})$ est ainsi égal à $\mathrm{ct}(\mathrm{P})\,\mathrm{ct}(\mathrm{Q})\,\mathrm{ct}(\mathrm{P}_1\mathrm{Q}_1)$. Il suffit donc de montrer que $\mathrm{P}_1\mathrm{Q}_1$ est encore un polynôme primitif.

Soit $\pi$ un élément irréductible de A. Nous allons montrer que $\pi$ ne divise pas tous les coefficients de $\mathrm{P}_1\mathrm{Q}_1$. Comme $\mathrm{P}_1$ est primitif, la réduction $\mathrm{cl}(\mathrm{P}_1)$ de $\mathrm{P}_1$ modulo $\pi$ est un polynôme non nul à coefficients dans l'anneau $\mathrm{A}/(\pi)$. De même, $\mathrm{cl}(\mathrm{Q}_1)$ est un polynôme non nul à coefficients dans $\mathrm{A}/(\pi)$. Or, $\pi$ est irréductible dans A qui est un anneau factoriel. Par suite, $\mathrm{A}/(\pi)$ est un anneau intègre et l'anneau de polynômes $(\mathrm{A}/(\pi))[\mathrm{X}]$ est aussi intègre (exemple 2.1.8). Il en résulte que le produit $\mathrm{cl}(\mathrm{P}_1)\,\mathrm{cl}(\mathrm{Q}_1) = \mathrm{cl}(\mathrm{P}_1\mathrm{Q}_1)$ est encore non nul dans $(\mathrm{A}/\pi)[\mathrm{X}]$. Cela signifie exactement que $\pi$ ne divise pas tous les coefficients de $\mathrm{P}_1\mathrm{Q}_1$, ce qu'on voulait démontrer. □

Cette proposition fondamentale va nous permettre de déterminer les éléments irréductibles de $A[X]$.

PROPOSITION 5.4.3. — *Soit* $A$ *un anneau factoriel et soit* $K$ *son corps des fractions. Les éléments irréductibles de* $A[X]$ *sont*

- *les éléments irréductibles de* $A$ *;*
- *les polynômes primitifs de* $A[X]$ *qui sont irréductibles en tant que polynômes de* $K[X]$.

*Démonstration.* — On commence par montrer que ces éléments sont irréductibles, puis on montrera qu'il n'y en a pas d'autres.

Soit donc $a$ un élément de A qui est irréductible et soit P et Q deux polynômes de $A[X]$ tels que $a = PQ$. Alors, $\deg(P) + \deg(Q) = \deg(PQ) = 0$, donc P et Q sont tous deux de degré 0, c'est-à-dire des éléments de A. Comme $a$ est irréductible dans A, P ou Q est inversible dans A, donc aussi dans $A[X]$ et $a$ est bien irréductible dans $A[X]$.

Soit maintenant $P \in A[X]$ un polynôme primitif qui est irréductible dans $K[X]$. Si $P = QR$ avec Q et R dans $A[X]$, cela fournit *a fortiori* une décomposition dans $K[X]$ si bien que Q ou R est inversible dans $K[X]$, autrement dit, Q ou R est constant. Supposons pour fixer les notations que R est un élément de A, noté $a$ ; on a donc $P = aQ$. Par suite, le contenu de P vaut

$$\mathrm{ct}(P) = \mathrm{ct}(aQ) = a\,\mathrm{ct}(Q)$$

et $a$ est nécessairement inversible dans A donc dans $A[X]$. Ainsi, P est irréductible dans $A[X]$.

Réciproquement, soit P un élément irréductible de $A[X]$. Il existe un polynôme primitif $P_1 \in A[X]$ tel que $P = \mathrm{ct}(P)P_1$. Par suite, $\mathrm{ct}(P) = 1$ ou $P_1$ est inversible dans $A[X]$.

Supposons d'abord que P n'est pas primitif. Alors, $P_1$ est inversible dans $A[X]$, ce qui signifie que $P_1$ est un polynôme constant, inversible dans A. Il reste à montrer que $\mathrm{ct}(P)$ est irréductible, mais s'il ne l'était pas, on pourrait écrire $\mathrm{ct}(P) = ab$ où ni $a$ ni $b$ n'est inversible dans A. Cela fournirait une factorisation $P = a(bP_1)$ comme produit de deux éléments non inversibles, ce qui contredit l'hypothèse que P est irréductible.

Supposons maintenant que $P_1$ n'est pas inversible dans $A[X]$, c'est-à-dire $\deg(P) > 0$. On a déjà vu que $\mathrm{ct}(P) = 1$, donc $P = P_1$ et il faut montrer que P est irréductible dans $K[X]$. Soit $P = QR$ une factorisation de P en produit de deux éléments de $K[X]$. On peut écrire $Q = qQ_1$ et $R = rR_1$, où $q$ et $r$ sont deux éléments de K et $Q_1$ et $R_1$ sont deux polynômes primitifs de $A[X]$. On a ainsi $P = (qr)Q_1R_1$. Écrivons alors $qr = a/b$ où $a$ et $b$ sont deux éléments de A. On a $bP = aQ_1R_1$. Par suite, ces deux polynômes ont même contenu, $b$ et

$a$ respectivement[(1)], c'est-à-dire $qr \in \mathrm{A}^\times$. Comme P est irréductible dans A[X], cette factorisation montre que $\mathrm{Q}_1$ ou $\mathrm{R}_1$ est inversible dans A[X], donc dans K[X] ; par suite, $\mathrm{Q} = q\mathrm{Q}_1$ ou $\mathrm{R} = r\mathrm{R}_1$ est inversible dans K[X]. □

THÉORÈME 5.4.4. — *Si* A *est un anneau factoriel,* A[X] *est un anneau factoriel.*

*Démonstration.* — Notons K le corps des fractions de A. Soit P un élément de A[X]. Il admet une décomposition en facteurs irréductibles dans K[X] : $\mathrm{P} = c\prod_{i=1}^{r}\mathrm{P}_i$ où les $\mathrm{P}_i$ sont des polynômes de A[X] qui sont primitifs et irréductibles dans K[X] et $c \in \mathrm{K}$. Écrivons $c = a/b$ avec $a$ et $b \in \mathrm{A}$ premiers entre eux. Alors, $b\mathrm{P} = a\prod_i \mathrm{P}_i$. Ces deux polynômes ont même contenu, c'est-à-dire que $b\,\mathrm{ct}(\mathrm{A}) = a\prod_i \mathrm{ct}(\mathrm{P}_i) = a$. Par suite, $c = a/b$ appartient à A et il admet une décomposition en facteurs irréductibles $c = u\prod_{j=1}^{s}\pi_j$ avec $u \in \mathrm{A}^\times$ et les $\pi_j \in \mathrm{A}$ irréductibles. On a finalement l'égalité

$$\mathrm{P} = u\prod_{j=1}^{s}\pi_j\prod_{i=1}^{r}\mathrm{P}_i.$$

D'après la proposition précédente, les $\pi_j$ et les $\mathrm{P}_i$ sont iréductibles dans A[X]. Cette égalité prouve donc que P admet une décomposition en facteurs irréductibles dans A[X].

Pour montrer l'unicité, il suffit d'établir que le lemme de Gauß est vérifié : si un élément irréductible de A[X] divise un produit, il divise l'un des facteurs. Soit d'abord $\pi$ un élément irréductible de A qui divise un produit PQ de deux polynômes de A[X]. Il s'ensuit que $\pi$ divise $\mathrm{ct}(\mathrm{PQ}) = \mathrm{ct}(\mathrm{P})\,\mathrm{ct}(\mathrm{Q})$. Par suite $\pi$ divise ct(P) ou ct(Q) et donc il divise P ou Q.

Soit maintenant un polynôme primitif $\Pi \in \mathrm{A}[\mathrm{X}]$, irréductible dans K[X] qui divise un tel produit PQ. Il divise par conséquent l'un des facteurs dans K[X], soit P pour fixer les notations : $\mathrm{P} = \mathrm{R}\Pi$ avec $\mathrm{R} \in \mathrm{K}[\mathrm{X}]$. On écrit alors $\mathrm{R} = (a/b)\mathrm{R}_1$ où $\mathrm{R}_1 \in \mathrm{A}[\mathrm{X}]$ est primitif, et $a$ et $b$ sont deux éléments de A premiers entre eux. On a alors $b\mathrm{P} = b\mathrm{R}\Pi = a\mathrm{R}_1\Pi$. L'égalité des contenus montre que $a = b\,\mathrm{ct}(\mathrm{P})$ et donc $a/b = \mathrm{ct}(\mathrm{P})$ appartient à A. On a donc $\mathrm{R} \in \mathrm{A}[\mathrm{X}]$, ce qui prouve que $\Pi$ divise P dans A[X]. □

COROLLAIRE 5.4.5 (Gauß). — *Si* A *est un anneau factoriel,* $\mathrm{A}[\mathrm{X}_1,\ldots,\mathrm{X}_n]$ *est un anneau factoriel. En particulier, si* $k$ *est un corps,* $k[\mathrm{X}_1,\ldots,\mathrm{X}_n]$ *est un anneau factoriel.*

*Démonstration.* — C'est immédiant par récurrence sur $n$ en utilisant l'isomorphisme

$$\mathrm{A}[\mathrm{X}_1,\ldots,\mathrm{X}_n] \simeq (\mathrm{A}[\mathrm{X}_1,\ldots,\mathrm{X}_{n-1}])[\mathrm{X}_n].$$

(1) à multiplication par un élément inversible de $\mathrm{A}^\times$ bien entendu

□

*Exercice 5.4.6.* — a) Soit $k$ un corps. Les éléments X et Y de $k[X,Y]$ sont premiers entre eux mais l'idéal $(X,Y)$ n'est pas égal à $(1)$. En déduire que $k[X,Y]$ n'est pas un anneau principal.

b) Si ce n'était déjà fait, résoudre l'exercice 4.3.11.

## 5.5. Résultant. Un théorème de Bézout

DÉFINITION 5.5.1. — *Soit* $P = a_nX^n + \cdots + a_0$ *et* $Q = b_mX^m + \cdots + b_0$ *deux polynômes de* $A[X]$ *de degrés inférieurs ou égaux à* $n$ *et* $m$ *respectivement. Leur* résultant *(de taille* $(n,m)$*) est le déterminant*

$$\mathrm{Res}_{n,m}(P,Q) = \begin{vmatrix} a_0 & & & 0 & b_0 & & & 0 \\ a_1 & a_0 & & & b_1 & b_0 & & \\ \vdots & & \ddots & & \vdots & & \ddots & \\ a_{m-1} & & & a_0 & b_{m-1} & & b_0 & \\ \vdots & & & \vdots & b_m & & & \ddots \\ \vdots & & & \vdots & & \ddots & & b_0 \\ a_n & a_{n-1} & & a_{n-m+1} & & b_m & & \vdots \\ & a_n & & \vdots & & & \ddots & \vdots \\ & & \ddots & \vdots & & & & \ddots \\ 0 & & & a_n & 0 & & & b_m \end{vmatrix}$$

($m$ colonnes) ($n$ colonnes)

(Précisément, le vecteur colonne $(a_0,\ldots,a_n)$ est recopié $m$ fois décalé puis le vecteur colonne $(b_0,\ldots,b_m)$ est recopié $n$ fois décalé.)

PROPOSITION 5.5.2. — *Soit* $k$ *un corps et soit* $P,Q$ *deux polynômes de* $k[X]$ *de degrés inférieurs ou égaux à* $n$ *et* $m$ *respectivement. Alors,* $\mathrm{Res}_{n,m}(P,Q)$ *est nul si et seulement si*

- *ou bien* $P$ *et* $Q$ *ne sont pas premiers entre eux ;*
- *ou bien* $a_n = b_m = 0$.

*Démonstration.* — Remarquons pour commencer que $\mathrm{Res}_{n,m}(P,Q)$ est le déterminant de l'application linéaire

$$\rho\colon k[X]_{m-1} \times k[X]_{n-1} \to k[X]_{m+n-1}, \qquad (U,V) \mapsto UP + VQ$$

dans les bases $(1,\ldots,X^{m-1};1,\ldots,X^{n-1})$ au départ et $(1,X,\ldots,X^{m+n-1})$ à l'arrivée. (Si $p$ est un entier, $k[X]_p$ désigne le $k$-espace vectoriel des polynômes de degré inférieur ou égal à $p$ ; il est de dimension $p+1$.) Nous allons calculer le rang de $\rho$.

Si $P = Q = 0$, alors $m = n = 0$ et la définition du déterminant montre que $\mathrm{Res}_{n,m}(P, Q) = 0$. Supposons maintenant qu'ils ne sont pas tous deux nuls et soit D leur pgcd On écrit $P = DP_1$ et $Q = DQ_1$ où $P_1$ et $Q_1$ sont deux polynômes de $k[X]$ premiers entre eux. Alors, si U et $V \in k[X]$ vérifient $UP + VQ = 0$, on a $UP_1 + VQ_1 = 0$. Par suite, $Q_1$ divise U et $P_1$ divise V. On a donc $U = Q_1 S$ et $V = P_1 T$, mais nécessairement, $T = -S$, d'où finalement $U = Q_1 S$ et $V = -P_1 S$. Alors, $U \in k[X]_{m-1}$ si et seulement si $\deg(S) \leq m - 1 - \deg(Q_1)$, tandis que $V \in k[X]_{n-1}$ si et seulement si $\deg(S) \leq n - 1 - \deg(P_1)$. On remarque que

$$\begin{aligned} m - 1 - \deg(Q_1) &= m - \deg(Q) + \deg(Q) - \deg(Q_1) - 1 \\ &= (m - \deg(Q)) + \deg(D) - 1 \end{aligned}$$

et de même, $n - 1 - \deg(P_1) = (n - \deg(P)) + \deg(D) - 1$. Posons

$$s = \min(n - \deg(P), m - \deg(Q))$$

de sorte que $s = 0$ à moins que $a_n = b_m = 0$. Finalement, avec ces notations, le noyau de $\rho$ est isomorphe à $k[X]_{s+\deg(D)-1}$, donc est de dimension $s + \deg D$.

Il en résulte que $\mathrm{Res}_{n,m}(P, Q)$ est nul si et seulement si $s + \deg D > 0$, c'est-à-dire si $a_n = b_m = 0$ ou si D est de degré non nul. □

Corollaire 5.5.3. — *Soit $k$ un corps algébriquement clos et A l'anneau $k[Y]$. Soit P et Q deux polynômes de $k[X, Y] = A[X]$. Écrivons ainsi*

$$P = P_n(Y)X^n + \cdots + P_0(Y) \quad \textit{et} \quad Q = Q_m(Y)X^m + \cdots + Q_0(Y)$$

*où les $P_i$ et les $Q_j$ sont des éléments de $k[Y]$. Soit $R = \mathrm{Res}_{m,n}(P, Q) \in k[Y]$ le résultant de taille $(n, m)$ du couple $(P, Q)$. Alors, un élément $y \in k$ est racine de R si et seulement si*

- *ou bien les polynômes $P(X, y)$ et $Q(X, y)$ ont une racine commune dans $k$ ;*
- *ou bien $P_n(y) = Q_m(y) = 0$.*

*Démonstration.* — Il résulte de la formule définissant le résultant que

$$R(y) = \big(\mathrm{Res}_{n,m}(P, Q)\big)(y) = \mathrm{Res}_{n,m}(P(X, y), Q(X, y)).$$

Il suffit donc d'appliquer le théorème précédent aux polynômes $P(X, y)$ et $Q(X, y)$ de $k[X]$. □

Théorème 5.5.4 (Bézout). — *Soit P et Q deux polynômes premiers entre eux de $\mathbf{C}[X, Y]$. Notons $p$ et $q$ leurs degrés*[(2)]*. Alors, l'ensemble des racines communes à P et Q (c'est-à-dire les couples $(x, y) \in \mathbf{C}^2$ tels que $P(x, y) = Q(x, y) = 0$) est fini et est de cardinal au plus $pq$.*

[(2)] Le degré d'un monôme $X^r Y^s$ est $r + s$ ; le degré d'une somme de monômes $P = \sum a_{rs} X^r Y^s \in \mathbf{C}[X, Y]$ avec $a_{rs} \neq 0$ est le maximum des degrés des monômes.

*Démonstration.* — Comme P et Q sont premiers entre eux dans $\mathbf{C}[X,Y]$, ils le sont aussi dans $\mathbf{C}(Y)[X]$ et leur résultant R par rapport à X est un polynôme non nul $R_Y$ de $\mathbf{C}[Y]$. Ainsi, les racines communes à P et Q n'ont qu'un nombre fini d'ordonnées $y$ possibles. Le même argument en échangeant les rôles de X et Y montre qu'il n'y qu'un nombre fini d'abscisses possibles. Par suite, l'ensemble $\Sigma$ des racines communes à P et Q est fini.

Montrons maintenant que le cardinal de $\Sigma$ est inférieur ou égal au produit des degrés de P et Q.

Faisons tout d'abord un changement de variables linéaire de sorte qu'une droite horizontale ne contienne au plus qu'un point de $\Sigma$. (Il n'y a qu'un nombre fini de directions est à éviter, donc c'est possible.) Les polynômes P et Q sont changés, mais leurs degrés restent égaux à $p$ et $q$ respectivement. Il suffit maintenant de montrer que l'ensemble des ordonnées des points de $\Sigma$ est de cardinal au plus $pq$.

Écrivons

$$P = P_n(Y)X^n + \cdots + P_0(Y) \quad \text{et} \quad Q = Q_m(Y)X^m + \cdots + Q_0(Y)$$

où $P_n$ et $Q_m$ sont non nuls. Soit $R = \mathrm{Res}_{n,m}(P,Q)$ (résultant par rapport à X). Si $y \in \mathbf{C}$ est l'ordonnée d'un point de $\Sigma$, $P(X,y)$ et $Q(X,y)$ ont une racine commune et par suite, $R(y) = 0$. Il suffit donc de montrer que R est un polynôme de degré inférieur ou égal à $pq$.

On constate d'abord que les $P_i$ sont de degrés $\leq p-i$ et que les $Q_j$ sont de degrés $\leq q-j$. Explicitons le coefficient $R_{ij}$ à la ligne $i$ et à la colonne $j$ du déterminant qui définit R :

– pour $1 \leq j \leq m$, on a $R_{ij} = P_{i-j}$ si $0 \leq i-j \leq n$ et $R_{ij} = 0$ sinon ;

– pour $m+1 \leq j \leq m+n$, on a $R_{ij} = Q_{j-j+m}$ si $0 \leq i-j+m \leq m$ et $R_{ij} = 0$ sinon.

En particulier, le degré de $R_{ij}$ est majoré par

$$\deg(R_{ij}) \leq \begin{cases} p-i+j & \text{si } 1 \leq j \leq m\,; \\ q-m-i+j & \text{si } m+1 \leq j \leq m+n. \end{cases}.$$

Le déterminant R est une somme de produits de la forme $\prod_{j=1}^{m+n} R_{\sigma(i)i}$, $\sigma$ étant une permutation de $\{1;\ldots;m+n\}$. Or, le degré d'un tel produit est majoré par

$$\begin{aligned} \sum_{j=1}^{m+n} \deg(R_{\sigma(j)j}) &\leq \sum_{j=1}^{m} (p-\sigma(j)+j) + \sum_{j=m+1}^{m+n} (q-m-\sigma(j)+j) \\ &\leq pm + n(q-m) - \sum_{j=1}^{m+n} \sigma(j) + \sum_{j=1}^{m+n} j \\ &\leq pq - (p-n)(q-m) \leq pq. \end{aligned}$$

Il en résulte que $\deg(R) \leq pq$. Le théorème est démontré. □

Donnons quelques résultats complémentaires sur le résultant.

PROPOSITION 5.5.5. — *Soit* A *un anneau et soit* P, Q *deux polynômes de* A[X] *de degrés inférieurs ou égaux à* $n$ *et* $m$ *respectivement. Alors, le résultant* $\mathrm{Res}_{n,m}(P,Q)$ *appartient à l'idéal*

$$(P,Q)_{A[X]} \cap A.$$

*Démonstration.* — On peut calculer le déterminant qui définit le résultant dans tout anneau qui contient A, et notamment dans A[X]. Ajoutons alors à la première ligne X fois la seconde, $X^2$ fois la troisième, etc. Il s'ensuit que $\mathrm{Res}_{n,m}(P,Q)$ est le déterminant d'une matrice à coefficients dans A[X] dont la première ligne est

$$P \quad XP \quad \dots \quad X^{m-1}P \quad Q \quad XQ \quad \dots \quad X^{n-1}Q$$

En développant le déterminant par rapport à cette ligne, on constate que $\mathrm{Res}_{n,m}(P,Q)$ est de la forme $UP+VQ$ pour deux polynômes U et V dans A[X]. Ainsi, il appartient bien à l'idéal $(P,Q)_{A[X]}$ engendré par P et Q dans A[X]. Comme il appartient aussi à A, il appartient à l'idéal $(P,Q)_{A[X]} \cap A$ de A. □

PROPOSITION 5.5.6. — *Soit* A *un anneau et soit* P *et* Q *deux polynômes de* A[X] *qui sont scindés :* $P = a_n \prod_{i=1}^{n}(X-t_i)$ *et* $Q = b_m \prod_{j=1}^{m}(X-u_j)$. *Alors,*

$$\mathrm{Res}_{n,m}(P,Q) = (-1)^{mn} a_n^m b_m^n \prod_{i,j}(t_i-u_j) = b_m^n \prod_{j=1}^{m} P(u_j) = a_n^m (-1)^{mn} \prod_{i=1}^{n} Q(t_j).$$

*Démonstration.* — L'égalité des trois expressions de droite est évidente. Nous allons montrer qu'elles sont égales à $\mathrm{Res}_{n,m}(P,Q)$ par récurrence sur $n$. Si $n=0$, $P=a_0$, $\mathrm{Res}_{0,m}(P,Q) = a_0^m$, donc la formule est vérifiée. Nous allons maintenant montrer par des combinaisons linéaires sur le déterminant que

$$\mathrm{Res}_{n+1,m}((X-t)P,Q) = (-1)^m Q(t)\,\mathrm{Res}_{n,m}(P,Q).$$

En effet, si $P = a_nX^n + \cdots + a_0$, on a

$$(X-t)P = a_nX^{n+1} + (a_{n-1}-ta_n)X^n + \cdots + (a_0-ta_1)X + a_0$$

et $\mathrm{Res}_{n+1,m}((\mathrm{X}-t)\mathrm{P},\mathrm{Q})$ est égal à

$$\begin{vmatrix}
-ta_0 & & & & & b_0 & & \\
a_1-ta_0 & -ta_0 & & & & b_1 & \ddots & \\
\vdots & a_0-ta_1 & -ta_0 & & & \vdots & & b_0 \\
 & & \ddots & & & \vdots & & \vdots \\
 & & & & -ta_0 & \vdots & & \\
a_{n-1}-ta_n & & & & \vdots & \vdots & & \\
a_n & \ddots & & & & \vdots & & \\
 & \ddots & \ddots & & & b_{m-1} & & \vdots \\
 & & & \ddots & & b_m & & \vdots \\
 & & & \ddots & a_{n-1}-ta_n & & \ddots & b_{m-1} \\
 & & & & a_n & & & b_m
\end{vmatrix}$$

(Il y a $m$ colonnes « $a$ » tandis que les colonnes « $b$ » sont au nombre de $n+1$.) En partant du bas, ajoutons à chaque ligne $t$ fois la suivante. Cela ne change pas la valeur du déterminant et $\mathrm{R}es_{n+1,m}((\mathrm{X}-t)\mathrm{P},\mathrm{Q})$ est donc égal à

$$\begin{vmatrix}
0 & \dots & 0 & b_0+tb_1+\cdots+t^mb_m & t(b_0+tb_1+\dots) & \dots & t^n(b_0+\dots) \\
a_0 & & & (b_1+tb_2+\dots) & (b_0+tb_1+\dots) & & t^{n-1}(b_0+\dots) \\
\vdots & \ddots & a_0 & \vdots & & & \\
\vdots & & \vdots & b_m & & & \vdots \\
a_n & & \vdots & & \ddots & & b_{m-1}+tb_m \\
 & & a_n & & & & b_m
\end{vmatrix}$$

Dans la première ligne, $\mathrm{Q}(t)$ est en facteur, si bien que le résultant cherché vaut

$$\mathrm{Q}(t)\begin{vmatrix}
0 & \dots & 0 & 1 & t & \dots & t^n \\
a_0 & & & (b_1+tb_2+\dots) & (b_0+tb_1+\dots) & & t^{n-1}(b_0+\dots) \\
\vdots & \ddots & a_0 & \vdots & & & \\
\vdots & & \vdots & b_m & & & \vdots \\
a_n & & \vdots & & \ddots & & b_{m-1}+tb_m \\
 & & a_n & & & & b_m
\end{vmatrix}$$

On peut alors soustraire à chaque colonne de type « $b$ » $t$ fois la précédente, en partant de la droite, d'où le déterminant

$$\mathrm{Q}(t)\begin{vmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_0 & & & b_1+tb_2+\dots & b_0 & & \\ \vdots & \ddots & a_0 & \vdots & b_1 & \ddots & \\ \vdots & & \vdots & \vdots & & & \ddots \\ & & \vdots & & & \ddots & b_{m-1} \\ a_n & & & & & \ddots & b_m \\ & & a_n & & & & \end{vmatrix}$$

Il reste à developper suivant la première ligne pour obtenir

$$(-1)^m \mathrm{Q}(t)\,\mathrm{Res}_{m,n}(\mathrm{P},\mathrm{Q}).$$

Par récurrence, la proposition est démontrée. □

## 5.6. Exercices

*Exercice 5.6.1.* — Montrer que l'anneau $\mathbf{C}[\mathrm{X},\mathrm{Y}]/(\mathrm{Y}-\mathrm{X}^2)$ est principal.

*Exercice 5.6.2.* — On pose $\mathrm{A}=\mathbf{C}[\mathrm{X},\mathrm{Y}]/(\mathrm{XY}-1)$. On note $x$ l'image de X dans A.

**a)** Montrer que $x$ est inversible dans A. Montrer que tout élément $a$ non nul de A peut s'écrire de façon unique sous la forme $a=x^m\mathrm{P}(x)$, où $m$ est dans $\mathbf{Z}$ et où P est un polynôme à coefficients dans $\mathbf{C}$ dont le terme constant est non nul. On note $e(a)$ le degré de P.

**b)** Soient $a$ et $b$ deux éléments de A, avec $b\neq 0$. Montrer qu'il existe des éléments $q$ et $r$ dans A tels que $a=bq+r$ avec $r=0$ ou bien $e(r)<e(b)$.

**c)** En déduire que A est principal.

*Exercice 5.6.3.* — Soit K un compact de $\mathbf{C}$ et $\mathscr{H}$ l'anneau des fonctions holomorphes sur K (c'est-à-dire sur un voisinage ouvert de K). Montrer que $\mathscr{H}$ est principal.

*Exercice 5.6.4.* — Soit K un corps. On pose $\mathrm{A}=\mathrm{K}[\mathrm{X},\mathrm{Y}]/(\mathrm{X}^2+5\mathrm{Y}^2)$. L'anneau A est-il

**a)** intègre,

**b)** réduit,

**c)** factoriel ?

(On pourra donner des conditions sur K).

*Exercice 5.6.5* (Critère d'irréductibilité d'Eiseinstein). — Soient A un anneau factoriel et K son corps des fractions. Soit

$$f(\mathrm{X}) = \sum_{0 \leq k \leq n} a_k \mathrm{X}^k$$

un polynôme de degré $n \geq 1$ à coefficients dans A. Soit $p$ un élément irréductible de A. On suppose que $p$ ne divise pas $a_n$, que $p$ divise $a_k$ si $0 \leq k < n$ et que $p^2$ ne divise pas $a_0$. Montrer que $f$ est irréductible dans K[X].

*Exercice 5.6.6.* — Soit $\mathrm{A} = \mathbf{Z}[i\sqrt{5}]$ l'anneau engendré par $\mathbf{Z}$ et $i\sqrt{5}$ dans $\mathbf{C}$.

**a)** Montrer qu'un élément de A s'écrit de manière unique sous la forme $a + ib\sqrt{5}$ avec $a$ et $b \in \mathbf{Z}$.

**b)** Montrer que les seuls éléments inversibles de A sont 1 et $-1$.

(*Si* $z \in \mathrm{A}$, *introduire* $\mathrm{N}(z) = z\bar{z}$.)

**c)** Montrer que les éléments 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles dans A.

**d)** Montrer que A n'est pas factoriel.

## 5.7. Solutions

*Solution de l'exercice 5.6.1.* — En fait, l'anneau $\mathbf{C}[\mathrm{X},\mathrm{Y}]/(\mathrm{Y} - \mathrm{X}^2)$ est isomorphe à $\mathbf{C}[\mathrm{X}]$ dont on sait bien qu'il est principal.

Introduisons en effet l'homomorphisme

$$\varphi : \mathbf{C}[\mathrm{X},\mathrm{Y}] \to \mathbf{C}[\mathrm{X}], \quad \mathrm{P}(\mathrm{X},\mathrm{Y}) \mapsto \mathrm{P}(\mathrm{X},\mathrm{X}^2).$$

On voit que $\varphi$ est surjectif, et que son noyau contient l'idéal $(\mathrm{Y} - \mathrm{X}^2)$. Si maintenant $\mathrm{P} \in \operatorname{Ker}\varphi$, effectuons la division euclidienne de P par $\mathrm{Y} - \mathrm{X}^2$ dans l'anneau $\mathrm{K}[\mathrm{X}][\mathrm{Y}]$. (Bien que K[X] ne soit pas un corps, on peut effectuer la division car le coefficient dominant de $\mathrm{Y} - \mathrm{X}^2$ dans l'anneau $\mathrm{K}[\mathrm{X}][\mathrm{Y}]$ est égal à 1, donc est inversible dans K[X].) On écrit ainsi $\mathrm{P}(\mathrm{X},\mathrm{Y}) = (\mathrm{Y} - \mathrm{X}^2)\mathrm{Q}(\mathrm{X},\mathrm{Y}) + \mathrm{R}(\mathrm{X},\mathrm{Y})$ où $\mathrm{R}(\mathrm{X},\mathrm{Y})$ est un polynôme de $\mathrm{K}[\mathrm{X}][\mathrm{Y}]$ de degré en Y strictement inférieur à $1 = \deg_{\mathrm{Y}}(\mathrm{Y} - \mathrm{X}^2)$, donc nul. Ainsi, $\mathrm{R}(\mathrm{X},\mathrm{Y})$ est un polynôme en X uniquement. On calcule alors $\varphi(\mathrm{P}) = \varphi(\mathrm{R}) = \mathrm{R}(\mathrm{X},\mathrm{X}^2) = \mathrm{R}(\mathrm{X}) = 0$. Donc $\mathrm{R} = 0$ et P est multiple de $\mathrm{Y} - \mathrm{X}^2$, ainsi qu'il fallait démontrer.

*Solution de l'exercice 5.6.2.* — **a)** Notons $y$ l'image de Y dans A. On a donc $xy = 1$, si bien que $x$ est inversible, d'inverse $y$. Soit maintenant $a \in \mathrm{A}$. On peut donc écrire

$$a = \sum_{i,j} \alpha_{i,j} x^i y^j = \sum_{\substack{i,j \in \mathbf{N} \\ \text{somme finie}}} \alpha_{i,j} x^{i-j} = \sum_{\substack{k \in \mathbf{Z} \\ \text{somme finie}}} \beta_k x^k,$$

avec $\beta_k = \sum_j \alpha_{j+k,j}$. Soit $m$ le plus petit entier tel que $\beta_m \neq 0$ et $\mathrm{P}(\mathrm{X}) = \sum_{\substack{k\geq 0 \\ \text{somme finie}}} \beta_{k+m}\mathrm{X}^k$. On a bien $a = x^m\mathrm{P}(x)$, avec $\mathrm{P}(0) = \beta_m \neq 0$. Il reste a voir que cette écriture est unique. En effet, si $x^m\mathrm{P}(x) = x^n\mathrm{Q}(x)$, avec $m \leq n$, on obtient alors

$$\begin{aligned}
& x^m\big(\mathrm{P}(x) - x^{n-m}\mathrm{Q}(x)\big) = 0 \\
\Leftrightarrow\ & \mathrm{P}(x) - x^{n-m}\mathrm{Q}(x) = 0 && \text{car } x \text{ est inversible} \\
\Leftrightarrow\ & \mathrm{XY} - 1 \text{ divise } \mathrm{P}(\mathrm{X}) - \mathrm{X}^{n-m}\mathrm{Q}(\mathrm{X}) \\
\Leftrightarrow\ & \mathrm{P}(\mathrm{X}) - \mathrm{X}^{n-m}\mathrm{Q}(\mathrm{X}) = 0 && \text{car il est de degré } 0 \text{ en Y} \\
\Leftrightarrow\ & n = m \text{ et } \mathrm{Q}(\mathrm{X}) = \mathrm{P}(\mathrm{X})
\end{aligned}$$

en utilisant que le terme constant de P est non nul.

**b)** Si $a = 0$, on choisit $q = r = 0$. Supposons donc $a \neq 0$. D'après a), on peut écrire $a = x^m\mathrm{P}(x)$ et $b = x^n\mathrm{S}(x)$ ; la division euclidienne de P par S (dans $\mathbf{C}[\mathrm{X}]$) s'écrit $\mathrm{P} = \mathrm{SQ} + \mathrm{R}$, avec $\mathrm{R} = 0$ ou $\deg \mathrm{R} < \deg \mathrm{S}$. On a ainsi $x^m\mathrm{P}(x) = x^n\mathrm{S}(x)\, x^{m-n}\mathrm{Q}(x) + x^m\mathrm{R}(x)$. Posons $q = x^{m-n}\mathrm{Q}(x)$ et $r = x^m\mathrm{R}(x)$, de sorte que $a = bq + r$. Si $r \neq 0$, c'est-à-dire $\mathrm{R}(\mathrm{X}) \neq 0$, on a alors $e(r) \leq \deg \mathrm{R} < \deg \mathrm{S} = e(b)$.

**c)** Soit $\mathrm{I} \subset \mathrm{A}$ un idéal. Si $\mathrm{I} = (0)$, il est principal. Supposons donc $\mathrm{I} \neq (0)$. On choisit $\rho \in \mathrm{I} \setminus \{0\}$ tel que $e(\rho)$ soit minimal. Soit alors $a \in \mathrm{I}$. On peut écrire $a = \rho q + r$, avec $r = 0$ ou $e(r) < e(\rho)$. Comme $r = a - \rho q \in \mathrm{I}$, on a $r = 0$ et $\mathrm{I} = (\rho)$.

*Solution de l'exercice 5.6.3.* — Soit I un idéal de $\mathscr{H}$ et $(f_i)$ une famille de générateurs de I.

Une fonction $f \in \mathscr{H}$ non nulle n'a qu'un nombre finis de zéros, avec multiplicités. On peut ainsi trouver un unique polynôme $p_f \in \mathbf{C}[z]$ tel que $f/p_f$ est holomorphe sans zéros, ce qui implique que $f/p_f$ est une unité de $\mathscr{H}$. En particulier, les $p_{f_i}$ sont aussi des générateurs de I, ce qui permet de supposer que pour tout $i$, $f_i$ est un polynôme.

Considérons l'idéal J engendré dans $\mathbf{C}[z]$ par les $f_i$. Comme $\mathbf{C}[z]$ est un anneau principal, il existe $f \in \mathbf{C}[z]$ tel que $\mathrm{J} = f\mathbf{C}[z]$. On a $f \in (f_1, f_2, \dots)$, donc $f \in \mathrm{I}$ et $\mathrm{I} \supset f\mathscr{H}$. Comme il existe pour tout $i$ un polynôme $h_i$ tel que $f_i = fh_i$, on a $f_i \in f\mathbf{C}[z] \subset f\mathscr{H}$, et donc $\mathrm{I} \subset f\mathscr{H}$.

Par conséquent, I est principal.

*Solution de l'exercice 5.6.4.* — **a)** L'anneau A est intègre si et seulement si l'idéal $(\mathrm{X}^2 + 5\mathrm{Y}^2)$ est premier dans $\mathrm{K}[\mathrm{X},\mathrm{Y}]$. Comme cet anneau est factoriel, c'est équivalent au fait que $\mathrm{X}^2 + 5\mathrm{Y}^2$ est irréductible.

S'il existe $\alpha \in \mathrm{K}$ tel que $\alpha^2 = -5$, alors $\mathrm{X}^2 + 5\mathrm{Y}^2 = (\mathrm{X} + \alpha\mathrm{Y})(\mathrm{X} - \alpha\mathrm{Y})$, et $\mathrm{X}^2 + 5\mathrm{Y}^2$ n'est pas irréductible. Réciproquement, dans une décomposition de $\mathrm{X}^2 + 5\mathrm{Y}^2$

en facteurs irréductibles, le degré en X et en Y des facteurs doit être égal à 1, c'est-à-dire

$$X^2 + 5Y^2 = (X + \alpha Y)(X + \alpha' Y) = X^2 + (\alpha + \alpha')XY + \alpha\alpha' Y^2,$$

d'où $\alpha^2 = -5$ et $\alpha' = -\alpha$.

Ainsi, A est intègre si et seulement si $-5$ n'a pas de racine carrée dans K.

**b)** Si A est intègre, il est réduit.

Si A n'est pas intègre, $X^5 + 5Y^2 = (X + \alpha Y)(X - \alpha Y)$. Si $P \in K[X,Y]$ est tel que $P^n \in (X^2 + 5Y^2)$, nécessairement $(X + \alpha Y)$ divise $P^n$, et $(X - \alpha Y)$ divise $P^n$, d'où le fait que P est multiple de $X + \alpha Y$ et de $X - \alpha Y$.

Si la caractéristique de K est différente de 2 et 5, $\alpha \neq -\alpha$ donc $X + \alpha Y$ et $X - \alpha Y$ sont premiers entre eux et P est multiple de $X^2 + 5Y^2$ (on utilise encore le fait que K[X,Y] est factoriel). Ainsi, A est réduit.

Si la caractéristique de K est égale à 2, $-5 = 1$ est un carré dans K est $A = K[X,Y]/((X + Y)^2)$ n'est pas réduit.

**c)** Un anneau factoriel étant nécessairement intègre, A n'est pas factoriel si $-5$ est un carré dans K.

Supposons donc que $-5$ n'est pas un carré dans K. Notons $x$ et $y$ les images dans A de X et de Y. On a alors

$$(x + y)(x - y) = x^2 - y^2 = 6y^2.$$

L'idéal $(y)$ n'est pas premier dans A car $A/(y) = K[X,Y]/(Y, X^2 + 5Y^2) = K[X]/(X^2)$ n'est pas intègre. Or, prouvons que $y$ est irréductible dans A. Cela assurera que A n'est pas factoriel.

Donnons nous donc $P_1, P_2 \in K[X,Y]$ tels que $P_1P_2 - Y \in (X^2 + 5Y^2)$. La division euclidienne de $P_1$ et $P_2$ par $X^2 + 5Y^2$ dans $K[X][Y]$ permet de supposer que $P_1(X,Y) = A_1(X) + B_1(X)Y$, et de même pour $P_2$. On a alors

$$\begin{aligned} P_1(X,Y)P_2(X,Y) - Y &= A_1(X)A_2(X) + (A_1(X)B_2(X) + A_2(X)B_1(X))Y \\ &\quad + B_1(X)B_2(X)Y^2 - Y \\ &= (A_1(X)A_2(X) - \frac{1}{5}B_1(X)B_2(X)X^2) \\ &\quad + (A_1(X)B_2(X) + A_2(X)B_1(X) - 1)Y. \end{aligned}$$

Comme cet élément est multiple de $X^2 + 5Y^2$, la considération des degrés en Y montre qu'il est nul. On a donc les équations (dans K[X])

$$(*) \qquad 5A_1A_2 = B_1B_2X^2, \qquad A_1B_2 + A_2B_1 = 1.$$

Aucun de ces polynômes n'est nul. Par exemple, si $B_2 = 0$, alors $A_2$ ne peut pas être nul, donc $A_1 = 0$ et $A_2B_1 = 1$, ce qui implique que $A_2$ et $B_1$ sont

constants, et donc que $P_2$ est une unité de A. De même, si $A_2 = 0$, $B_1$ doit être nul, d'où le fait que $A_1$ est une constante non nulle, et que $P_1$ est une unité.

Soit P un polynôme irréductible divisant $B_2$. D'après la première relation et le lemme de Gauß, P divise ou $A_1$ ou $A_2$. Mais s'il divise $A_2$, il devra diviser 1, d'où, $v_P(B_2) \leq v_P(A_1)$. (Si $P \in K[Y]$ est un polynôme irréductible, on note $v_P(Q)$ l'exposant du polynôme Q dans la décomposition en facteurs irréductibles.) De même, $v_P(B_1) \leq v_P(A_2)$. En fait, il y a égalité si $P \neq X$, et la seconde relation implique que $A_1$ et $A_2$ ne sont pas tous deux multiples de X.

En particulier, on peut écrire (quitte à échanger $P_1$ et $P_2$), $B_2 = \lambda A_1$ et $A_2 = \mu X^2 B_1$. Les deux relations (∗) se récrivent

$$(**) \qquad 5\mu = \lambda, \qquad \lambda A_1^2 + \mu X^2 B_1^2 = 1.$$

On a ainsi $\lambda = 5\mu$, d'où l'équation $A_1^2 + \frac{1}{5}X^2B_1^2 = 1/\mu$.

Or, la relation

$$(A_1(x) + B_1(x)y) \times (A_1(x) - B_1(x)y) = A_1(x)^2 + \frac{1}{5}B_1(x)^2x^2 = 1/\mu$$

montre que $P_1(x, y)$ est une unité dans A. Ainsi, $y$ est bien irréductible.

*Solution de l'exercice 5.6.5.* — Rappelons que A[X] est factoriel, et que tout élément irréductible dans A est encore irréductible dans A[X]. Rappelons aussi que $A[X]/pA[X] \simeq (A/pA)[X]$.

Écrivons donc $f(X) = g(X)h(X)$ avec $g, h \in K[X]$. On peut écrire $g(X) = g_0(X)/a$, où $g_0 \in A[X]$, $a \in A$, et aucun facteur irréductible de $a$ ne divise $g_0$. De même, on écrit $h(X) = h_0(X)/b$. Ainsi, $abf(X) = g_0(X)h_0(X)$. Si $p$ est un élément irréductible qui divise $ab$, il divise $g_0h_0$, donc d'après le lemme de Gauß, il divise $g_0$ ou $h_0$. En le divisant, on obtient une relation semblable, avec un facteur irréductible de moins, ce qui permet par récurrence de supposer que $ab$ est inversible, soit en divisant encore, $a = b = 1$.

On a ainsi une relation $f(X) = g(X)h(X)$, avec $g \in A[X]$ et $h \in A[X]$.

Réduisons cette égalité modulo $p$. On trouve, en factorisant $X^n$ dans $(A/pA)[X]$, que $X^n = \overline{g}(X)\overline{h}(X)$. On en déduit $\overline{g} = \overline{\alpha}X^k$ et $\overline{h} = \overline{\beta}X^{n-k}$. (Unicité de la décomposition en facteurs irréductibles dans $(\mathrm{Frac}(A/p))[X]$, mais on peut le démontrer directement.) D'où des égalités

$$g(X) = \alpha X^k + pg_1(X), \quad g(X) = \beta X^{n-k} + ph_1(X)$$

avec $g_1$ et $h_1 \in A[X]$ et $\alpha, \beta \in A$. Cela implique

$$g(X)h(X) = \alpha\beta X^n + p(X^{n-k}g_1(X) + X^k h_1(X)) + p^2 g_1(X)h_1(X).$$

L'hypothèse que le terme constant de $f$ n'est pas multiple de $p^2$ implique que $k = 0$, ou que $k = n$. Si $k = n$, on a donc $g(X) = \alpha X^n + pg_1(X)$, avec $\deg g_1 < n$.

Ainsi, $\deg g = n$, et donc $\deg h = 0$, ce qui signifie que $h$ est inversible dans K[X]. Dans l'autre cas ($k = 0$), on trouve que $g$ est constant.

Nous avons donc prouvé que $f$ est irréductible dans K[X].

*Solution de l'exercice 5.6.6.* — **a)** Il suffit de montrer que l'ensemble des $a + ib\sqrt{5}$ avec $a$ et $b$ dans $\mathbf{Z}$ est un sous-anneau de $\mathbf{C}$ car il contient manifestement $\mathbf{Z}$ et $i\sqrt{5}$. Or, cet ensemble, muni de l'addition, est un sous-groupe abélien de $\mathbf{C}$; d'autre part, il contient 1 et la formule

$$(a + ib\sqrt{5})(c + id\sqrt{5}) = (ab - 5bd) + i(bc + ad)\sqrt{5}$$

montre qu'il est stable par multiplication. C'est donc un sous-anneau de $\mathbf{C}$.

Enfin, montrons l'unicité d'une telle écriture. Si $a + ib\sqrt{5} = c + id\sqrt{5}$, on a $(a - c) = i(d - b)\sqrt{5}$, d'où $(a - c)^2 + 5(d - b)^2 = 0$. Cela implique $a = c$ et $b = d$.

**b)** Soit $z = a + ib\sqrt{5}$ un élément inversible de A, et soit $u = c + id\sqrt{5}$ son inverse. Remarquons que $z\bar{z} = a^2 + 5b^2$ est entier positif ou nul. Par suite, si $zu = 1$, on a $(z\bar{z})(u\bar{u}) = 1$ et $z\bar{z}$ est égal à 1, soit $a^2 + 5b^2 = 1$. Si $b \neq 0$, on a $a^2 + 5b^2 \geq 5$, ce qui est absurde. Donc $b = 0$ et $a^2 = 1$, d'où $a = \pm 1$ et $z = \pm 1$.

**c)** Supposons que $2 = (a + ib\sqrt{5})(c + id\sqrt{5})$. Alors, on a $4 = 2\bar{2} = (a^2 + 5b^2)(c^2 + 5d^2)$. Si $b \neq 0$, $a^2 + 5b^2 \geq 5$ et $(a^2 + 5b^2)(c^2 + 5d^2) \geq 5$, ce qui est absurde et $b = 0$. De même, $d = 0$. Alors, la relation $2 = ac$ jointe au fait que 2 est premier dans $\mathbf{Z}$ montre que $a = \pm 1$ ou $c = \pm 1$. Nous avons donc prouvé que 2 est irréductible dans $\mathbf{Z}[i\sqrt{5}]$.

De même, si $3 = (a + ib\sqrt{5})(c + id\sqrt{5})$, on a

$$9 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Si $b \neq 0$, $a^2 + 5b^2 \geq 5$ et si $c + id\sqrt{5}$ n'est pas inversible, $c^2 + 5d^2 \geq 2$ et l'on a $9 \geq 10$, ce qui est absurde. Donc $b = d = 0$, $3 = ac$ et comme 3 est premier, $a = \pm 1$ ou $c = \pm 1$. Ainsi, 3 est irréductible dans $\mathbf{Z}[i\sqrt{5}]$.

Si maintenant $1 + i\sqrt{5} = (a + ib\sqrt{5})(c + id\sqrt{5})$, on a

$$(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Si $c + id\sqrt{5}$ n'est pas inversible, $c^2 + 5d^2 \geq 2$. Cela implique $a^2 + 5b^2 \leq 3$, d'où $b = 0$ et $a = \pm 1$. Donc $a + ib\sqrt{5}$ est inversible et $1 + i\sqrt{5}$ est irréductible. On montre de même que $1 - i\sqrt{5}$ est irréductible..

**d)** Remarquons que $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Si $\mathbf{Z}[i\sqrt{5}]$ était factoriel, 2 diviserait $1 + i\sqrt{5}$ ou $1 - i\sqrt{5}$. Or, un multiple de 2 dans A est de la forme $a + ib\sqrt{5}$ avec $a$ et $b$ deux entiers *pairs*. Par suite, ni $1 + i\sqrt{5}$ ni $1 - i\sqrt{5}$ ne sont multiples de 2. Cette contradication montre que $\mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel.

# 6 Modules

*Le modules sont aux anneaux ce que les espaces vectoriels sont aux corps. Ce chapitre d'introduction aux modules en donne la définition et les premières propriétés. On montre aussi comment construire des modules par passage au quotient ou par localisation. Le produit tensoriel sera introduit plus tard dans le cours.*

## 6.1. Premiers pas

DÉFINITION 6.1.1. — *Soit* A *un anneau. Un* A-module *est un groupe abélien* M *muni d'une application (multiplication externe)*

$$\mathrm{A} \times \mathrm{M} \to \mathrm{M}, \qquad (a, m) \mapsto am$$

*vérifiant les propriétés suivantes : pour tous* $a, b \in \mathrm{A}$ *et tous* $m, n \in \mathrm{M}$*, on a*

- $(a+b)m = am + bm$ *et* $a(m+n) = am + an$ *(distributivité);*
- $(ab)m = a(bm)$ *(associativité);*
- $1m = m$ *(élément neutre).*

*Exemples 6.1.2.* — a) Un anneau A est un A-module ; un idéal de A est un A-module.

b) Un groupe abélien possède une unique structure de **Z**-module.

c) Si A est un corps, A-module équivaut à A-espace vectoriel.

d) Si $f\colon \mathrm{A} \to \mathrm{B}$ est un homomorphisme d'anneaux, la multiplication externe $\mathrm{A} \times \mathrm{B} \to \mathrm{B}$ définie par $(a, b) \mapsto f(a)b$ munit B d'une structure de A-module.

e) Plus généralement, si $f\colon \mathrm{A} \to \mathrm{B}$ est un homomorphisme d'anneaux et si M est un B-module, la multiplication externe $\mathrm{A} \times \mathrm{M} \to \mathrm{M}$ définie par $(a, m) \mapsto f(a)m$ munit M d'une structure de A-module.

*Exercice 6.1.3.* — Soit M un A-module. Montrer que $(-1)m = -m$.

*Remarque 6.1.4.* — Soit A un anneau et soit M un A-module. Si $a \in A$, notons $\mu_a : M \to M$ l'application définie par $\mu_a(m) = am$. C'est un endomorphisme de M en tant que groupe abélien. En fait, l'application $a \mapsto \mu_a$ définit un homomorphisme d'anneaux $A \to \mathrm{End}(M)$, ce dernier anneau n'étant pas forcément commutatif.

On constate ainsi que, M étant un groupe abélien, se donner une structure de A-module sur M équivaut à se donner un homomorphisme d'anneaux $A \to \mathrm{End}(M)$.

Définition 6.1.5. — *Soit* A *un anneau et soit* M *un* A*-module. Un* sous-module *de* M *est une partie* N *de* M *vérifiant :*

– N *est un sous-groupe abélien de* M *;*

– *pour tout* $a \in A$ *et tout* $m \in N$, $am \in N$.

*Exemples 6.1.6.* — a) Si M est un A-module, la partie de M réduite à 0 en est un sous-module. De même, M est un sous-module de lui-même.

b) Si A est un anneau, les idéaux de A sont les sous-A-modules de A.

c) Si A est un corps, les sous-modules d'un A-espace vectoriel en sont les sous-espaces vectoriels.

Lemme 6.1.7. — *Soit* M *un* A*-module et soit* N *une partie de* M*. Pour montrer que* N *est un sous-module de* M*, il suffit de montrer les propriétés suivantes :*

– $0 \in N$ *;*

– *si* $a \in A$ *et* $m \in N$, $am \in N$ *;*

– *si* $m \in N$ *et* $n \in N$, $m + n \in N$.

*Démonstration.* — En effet, la seconde propriété appliquée à $a = -1$ et $m \in N$ montre que $-m \in N$. Jointe aux deux autres propriétés, on constate que N est un sous-groupe abélien de M. La seconde propriété implique alors que c'en est un sous-module. □

*Exercice 6.1.8.* — Soit A un anneau et soit M un A-module.

a) Montrer que l'ensemble $(0 : M)$ des $a \in A$ tels que pour tout $m \in M$, $am = 0$ est un idéal de A (*annulateur de* M). On le note aussi $\mathrm{Ann}(M)$.

b) Plus généralement, soit N un sous-A-module de M. Montrer que l'ensemble $(N : M)$ des $a \in A$ tels que pour tout $m \in M$, $am \in N$ est un idéal de A.

Définition 6.1.9. — *Soit* A *un anneau et soit* M *et* N *deux* A*-modules. Un* homomorphisme *de* M *dans* N *est une application* $f : M \to N$ *telle que pour tous* $a$ *et* $b$ *dans* A *et tous* $m$ *et* $n$ *dans* M*, on a*

$$f(am + bn) = af(m) + bf(n).$$

*On note* $\mathrm{Hom}_A(M, N)$ *l'ensemble des homomorphismes de* M *dans* N.

*Un homomorphisme de* M *dans* M *est appelé* endomorphisme *de* M. *On note* $\mathrm{End}_A(M)$ *l'ensemble des endomorphismes du* A*-module* M.

*Exemple 6.1.10.* — Soit A un anneau et soit M, N deux A-modules. Si $f$ et $g$ sont deux homomorphismes $M \to N$, soit $f+g$ l'application définie par $m \mapsto f(m)+g(m)$. Si $f$ est un homomorphisme $M \to N$ et si $a \in A$, soit $af$ l'application donnée par $m \mapsto af(m)$. Ce sont des homomorphisme de A-modules de M dans N.

Ces lois munissent $\mathrm{Hom}_A(M,N)$ d'une structure de A-module

Lemme 6.1.11. — *Soit* A *un anneau et soit* M, N, P *trois* A*-modules. Si* $f\colon M \to N$ *et* $g\colon N \to P$ *sont des homomorphismes, leur composé* $g \circ f\colon M \to P$ *est un homomorphisme de* A*-modules.*

Définition 6.1.12. — *On dit qu'un homomorphisme de* A*-modules* $f\colon M \to N$ *est un homomorphisme est un isomorphisme s'il existe un homomorphisme* $g\colon N \to M$ *tel que* $f \circ g = \mathrm{Id}_N$ *et* $g \circ f = \mathrm{Id}_M$.

Proposition 6.1.13. — *Un homomorphisme est un isomorphisme si et seulement si il est bijectif.*

*Démonstration.* — Si $f\colon M \to N$ est un isomorphisme, de réciproque $g$, il est clair que $g$ est la bijection réciproque de $f$.

Réciproquement, si $f\colon M \to N$ est un homomorphisme bijectif, soit $g$ sa bijection réciproque. Alors, $g$ est un homomorphisme. En effet, si $n$, $n' \in N$ et $a$, $a' \in A$, on a

$$f\big(ag(n)+a'g(n')\big) = af(g(n))+a'f(g(n')) = an+a'n'$$

donc $ag(n)+a'g(n') = g(an+a'n')$, ce qui établit la linéarité de $g$. □

Proposition 6.1.14. — *Soit* A *un anneau, soit* M, N *deux* A*-modules et soit* $f\colon M \to N$ *un homomorphisme de* A*-modules. Pour tout* A*-module* X*, les applications*

$$f^*\colon \mathrm{Hom}_A(N,X) \to \mathrm{Hom}_A(M,X), \qquad \varphi \mapsto \varphi \circ f$$

*et*

$$f_*\colon \mathrm{Hom}_A(X,M) \to \mathrm{Hom}_A(X,N), \qquad \varphi \mapsto f \circ \varphi$$

*sont des homomorphismes de* A*-modules. Si de plus* $g\colon N \to P$ *est un second homomorphisme de* A*-modules, on a les égalités* $f^* \circ g^* = (g \circ f)^*$ *et* $g_* f_* = (g \circ f)_*$.

Définition 6.1.15. — *Soit* A *un anneau et soit* M *un* A*-module. Le* A*-module dual de* M*, noté* $M^\vee$*, est le* A*-module* $\mathrm{Hom}_A(M,A)$.

*Remarque 6.1.16.* — On peut reformuler la proposition 6.1.14 dans le langage des catégories. Si X est un A-module fixé, l'« application » qui associe à un A-module M le A-module $\mathrm{Hom}_A(M,X)$ et à un morphisme $f\colon M \to N$ l'homomorpisme $f^*\colon \mathrm{Hom}_A(N,X) \to \mathrm{Hom}_A(M,X)$ est un foncteur contravariant de la catégorie $\mathfrak{Mod}_A$ des A-modules dans elle-même. Pour $X = A$, on obtient ainsi un foncteur « dual », $M \rightsquigarrow M^\vee = \mathrm{Hom}_A(M,A)$ de la catégorie des A-modules dans elle-même.

Associer à un A-module M le A-module $\mathrm{Hom}_A(X,M)$ définit au contraire un foncteur covariant.

Définition 6.1.17. — *Soit $f\colon M \to N$ un homomorphisme de* A*-modules. On appelle* noyau *de $f$, noté* $\mathrm{Ker}\, f$*, l'ensemble des $m \in M$ tels que $f(m) = 0$.*

Proposition 6.1.18. — *Soit $f\colon M \to N$ un homomorphisme de* A*-modules.*

*Si $M'$ est un sous-module de* M*, $f(M')$ est un sous-module de* N*. Si $N'$ est un sous-module de* N*, $f^{-1}(N')$ est un sous-module de* M*.*

*En particulier, le noyau* $\mathrm{Ker}\, f$ *et l'image* $\mathrm{Im}\, f = f(M)$ *de $f$ sont des sous-modules (de* M *et* N *respectivement).*

*Démonstration.* — Montrons que $f(M')$ est un sous-module de N. Comme $f(0_M) = 0_N$ et $0_M \in M'$, $0_N \in f(M')$. D'autre part, si $n$ et $n' \in f(M')$, il existe $m$ et $m' \in M'$ tels que $n = f(m)$ et $n' = f(m')$. Par suite,

$$n + n' = f(m) + f(m') = f(m + m') \in f(M').$$

Enfin, si $n = f(m)$ appartient à $f(M')$ et si $a \in A$, $an = af(m) = f(am)$ appartient à $f(M')$ puisque $am \in M'$.

Montrons que $f^{-1}(N')$ est un sous-module de M. Comms $f(0_M) = 0_N \in N'$, $0_M \in f^{-1}(N')$. D'autre part, si $m$ et $m' \in f^{-1}(N')$ et si $a$ et $b \in A$, on a

$$f(am + bm') = af(m) + bf(m') \in N'$$

puisque $f(m)$ et $f(m')$ appartiennent à $N'$ et que $N'$ est un sous-module de N. Donc $am + bm'$ appartient à $f^{-1}(N')$. □

## 6.2. Opérations sur les modules

Proposition 6.2.1. — *Soit* A *un anneau, soit* M *un* A*-module et soit $(N_s)_{s\in S}$ une famille de sous-modules de* M*. Alors, l'intersection $N = \bigcap_s N_s$ est un sous-module de* M*.*

*Démonstration.* — Comme $0 \in N_s$ pour tout $s$, $0 \in N$. Soit $m$ et $n$ deux éléments de N. Pour tout $s$, $m$ et $n$ appartiennent au sous-module $N_s$, donc $m+n$ aussi et $m+n$ appartient à leur intersection N. Enfin, soit $m \in N$ et $a \in A$. Pour tout $s$, $m \in N_s$, donc $am \in N_s$ et finalement, $am \in N$. Ainsi, N est un sous-A-module de M. □

PROPOSITION 6.2.2. — *Soit* A *un anneau, soit* M *un* A*-module et soit* X *une partie de* M. *Il existe un plus-petit sous-*A*-module* $\langle X \rangle$ *de* M *contenant* X *: c'est l'intersection de la famille (non vide) des sous-modules de* M *qui contiennent* X. *C'est aussi l'ensemble des sommes* $\sum_{x \in X} a_x x$ *où* $(a_x)_x$ *est une famille presque nulle d'éléments de* A.

*Par définition,* $\langle X \rangle$ *est le sous-module de* M *engendré par* X.

*Démonstration.* — Il existe des sous-modules de M qui contiennent X, par exemple M lui-même. Par suite, l'intersection $\langle X \rangle$ de ces sous-modules est un sous-module de M et contient X. Par construction, $\langle X \rangle$ est contenu dans tout sous-module de M qui contient X. C'est ainsi le plus petit d'entre eux.

Si $(a_x)_x$ est une famille presque nulle d'éléments de A, $\sum_{x \in X} a_x x$ est une combinaison linéaire d'éléments de $\langle X \rangle$, donc appartient à $\langle X \rangle$. Ceci prouve que l'ensemble $\langle X \rangle'$ des telles combinaisons linéaires est contenu dans $\langle X \rangle$. Réciproquement, il suffit de montrer que cet ensemble est un sous-module de M. Comme il contient X, on aura l'autre inclusion. Tout d'abord, $0 = \sum_x 0x$ appartient à $\langle X \rangle'$. Par ailleurs, si $m$ et $n$ sont deux éléments de $\langle X \rangle'$, il existe deux familles presque nulles $(a_x)_x$ et $(b_x)_x$ telles que $m = \sum_x a_x x$ et $n = \sum_x b_x x$. Alors, la famille $(a_x + b_x)_x$ est presque nulle et l'on a

$$m + n = \Big(\sum_x a_x x\Big) + \Big(\sum_x b_x x\Big) = \sum_x (a_x + b_x) x$$

donc $m + n$ appartient à $\langle X \rangle'$. Enfin, si $m \in \langle X \rangle'$ et $a \in A$, soit $(a_x)_x$ une famille presque nulle telle que $m = \sum_x a_x x$. On a alors $am = \sum_x (a a_x) x$, donc $am \in \langle X \rangle'$. □

DÉFINITION 6.2.3. — *Soit* A *un anneau,* M *un* A*-module et soit* $(M_s)_s$ *une famille de sous-module de* M. *La* somme *des* $M_s$, $\sum_s M_s$, *est le sous-module de* M *engendré par la réunion* $\bigcup_s M_s$ *des* $M_s$.

C'est aussi l'ensemble des combinaisons linéaires $\sum_s m_s$ où $(m_s)_s$ est une famille presque nulle d'éléments de M telle que $m_s \in M_s$ pour tout $s$.

*Exercice 6.2.4.* — La réunion de deux sous-modules n'est en général pas un sous-module.

a) Donner un exemple (on pourra se placer dans le cadre des espaces vectoriels).

b) Si $(M_n)_{n \in \mathbf{N}}$ est une famille de sous-modules d'un A-module M telle que $M_n \subset M_p$ si $n \leq p$, montrer que $\bigcup_n M_n$ est un sous-A-module de M.

DÉFINITION 6.2.5. — *Soit* A *un anneau,* M *un* A*-module et* I *un idéal de* A. *On définit le sous-module* IM *de* M *comme l'ensemble des combinaisons linéaires* $\sum a_i m_i$ *où pour tout* $i$, $a_i \in \mathrm{I}$ *et* $m_i \in \mathrm{M}$.

DÉFINITION 6.2.6. — *Soit* A *un anneau et soit* $(\mathrm{M}_s)$ *une famille de* A*-modules. Le produit des* $\mathrm{M}_s$ *est l'ensemble* $\prod_s \mathrm{M}_s$ *des lois :*

$$(m_s)_s + (n_s)_s = (m_s + n_s)_s, \qquad a(m_s)_s = (am_s)_s$$

*qui en font un* A*-module.*

*La somme directe des* $\mathrm{M}_s$ *est le sous-module* $\bigoplus_s \mathrm{M}_s$ *de* $\prod \mathrm{M}_s$ *formé des éléments* $(m_s)_s$ *tels que pour tout* $s$ *sauf pour un nombre fini,* $m_s = 0$.

*Remarque 6.2.7.* — Si tous les $\mathrm{M}_s$ sont isomorphes à un même module M, on a $\prod_s \mathrm{M}_s = \mathrm{M}^{\mathrm{S}}$. Le sous-module $\bigoplus \mathrm{M}_s$ est noté $\mathrm{M}^{(\mathrm{S})}$.

LEMME 6.2.8. — *Pour tout* $t$, *définissons des applications*

$$i_t \colon \mathrm{M}_t \to \bigoplus_s \mathrm{M}_s, \qquad p_t \colon \prod_s \mathrm{M}_s \to \mathrm{M}_t$$

*définis par* $i_t(m) = (m_s)$ *où* $m_t = m$ *et* $m_s = 0$ *si* $s \neq t$ *et* $p_t((m_s)) = m_t$. *Ce sont des homomorphismes de* A*-modules.*

*Démonstration.* — Soit $m$, $n$ dans $\mathrm{M}_t$, $a$ et $b$ dans A. Alors,

$$i_t(am + bn) = (0, \dots, 0, am + bn, 0, \dots)$$

(dans le membre de droite, le $am + bn$ est dans la composante indexée par $t$)

$$\begin{aligned} &= a(0, \dots, 0, m, 0, \dots) + b(0, \dots, 0, n, 0, \dots, 0) \\ &= ai_t(m) + bi_t(n). \end{aligned}$$

Par suite, $i_t$ est un homomorphisme de A-modules. La démonstration que $p_t$ est un homomorphisme est laissée en exercice. □

Produits et des sommes directes de modules satisfont une *propriété universelle* que nous énonçons maintenant.

THÉORÈME 6.2.9. — *Soit* A *un anneau et soit* $(\mathrm{M}_s)$ *une famille de* A*-modules.*

*a) Pour tout* A*-module* M *et toute famille* $(f_s)$ *de morphismes* $f_s \colon \mathrm{M} \to \mathrm{M}_s$, *il existe un unique morphisme* $f \colon \mathrm{M} \to \prod_s \mathrm{M}_s$ *tel que pour tout* $s$, $p_s \circ f = f_s$.

*b) Pour tout* A*-module* M *et toute famille* $(f_s)$ *de morphismes* $f_s \colon \mathrm{M}_s \to \mathrm{M}$, *il existe un unique morphisme* $f \colon \bigoplus_s \mathrm{M}_s \to \mathrm{M}$ *tel que pour tout* $s$, $f \circ i_s = f_s$.

*Démonstration.* — a) Supposons que $f\colon \mathrm{M} \to \prod_s \mathrm{M}_s$ vérifie $p_s \circ f = f_s$. Alors, si $f(m) = (m_s)_s$, on a nécessairement

$$m_s = p_s((m_s)_s) = p_s(f(m)) = (p_s \circ f)(m) = f_s(m),$$

ce qui montre que $f$, s'il existe, est unique. Réciproquement, définissons $f(m)$ comme la famille $(f_s(m))_s$. Il faut montrer que l'application ainsi définie $f\colon \mathrm{M} \to \prod_s \mathrm{M}_s$ est un homomorphisme de A-modules. Or, pour tous $a$ et $b$ dans A et tous $m$ et $n$ dans M, on a

$$\begin{aligned} f(am + bn) &= \big(f_s(am + bn)\big)_s = \big(af_s(m) + bf_s(n)\big)_s \\ &= a\big(f_s(m)\big)_s + b\big(f_s(n)\big)_s = af(m) + bf(n), \end{aligned}$$

ce qui prouve que $f$ est un homomorphisme de A-modules.

b) Supposons que $f\colon \bigoplus_s \mathrm{M}_s \to \mathrm{M}$ vérifie $f \circ i_s = f_s$. Alors, l'image par $f$ d'un élément $(0, \dots, 0, m, 0, \dots) = i_s(m)$ (où $m \in \mathrm{M}_s$ est dans la composante indexée par $s$) est nécessairement égale à $f_s(m)$. Un élément de $\bigoplus \mathrm{M}_s$ est une famille $(m_s)_s$ avec $m_s \in \mathrm{M}_s$, tous les $m_s$ étant nuls, sauf un nombre fini. Par suite, un tel élément est égal à $\sum_s i_s(m_s)$ (la somme est en fait finie) et son image par $f$ est égale à

$$f\Big(\sum_s i_s(m_s)\Big) = \sum_s (f \circ i_s)(m_s) = \sum_s f_s(m_s),$$

ce qui montre l'unicité. Récipriquement, l'application $f\colon \bigoplus \mathrm{M}_s \to \mathrm{M}$ définie par

$$f((m_s)_s) = \sum_s f_s(m_s) \qquad \text{(somme finie)}$$

est un homomorphisme de A-modules qui vérifie $f \circ i_s = f_s$ pour tout $s$. En effet, si $a$ et $b$ sont dans A et $(m_s)_s$, $(n_s)_s$ sont deux éléments de $\bigoplus_s \mathrm{M}_s$, on a

$$\begin{aligned} f(a(m_s)_s + b(n_s)_s) &= f((am_s + bn_s)_s) \\ &= \sum_s f_s(am_s + bn_s) = \sum_s \big(af_s(m_s) + bf_s(n_s)\big) \\ &= a\sum_s f_s(m_s) + b\sum_s f_s(n_s) \\ &= af((m_s)_s) + bf((n_s)_s). \end{aligned}$$

□

*Remarque 6.2.10.* — Ce théorème peut se reformuler ainsi : pour tout A-module M, les applications canoniques

$$\mathrm{Hom}_{\mathrm{A}}\Big(\bigoplus_s \mathrm{M}_s, \mathrm{M}\Big) \to \prod_s \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}_s, \mathrm{M}), \qquad f \mapsto (f \circ i_s)_s$$

et

$$\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \prod_s \mathrm{M}_s) \to \prod_s \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{M}_s), \qquad f \mapsto (p_s \circ f)_s$$

sont des isomorphismes.

## 6.3. Générateurs, bases, modules libres

DÉFINITION 6.3.1. — *Soit* A *un anneau et soit* M *un* A*-module. Soit* S *une partie de* M.
*On dit que* S *est*
– génératrice *si* $\mathrm{M} = \langle \mathrm{S} \rangle$ *;*
– libre *si pour toute famille presque nulle* $(a_s)_{s\in \mathrm{S}}$ *d'éléments de* A*, la relation* $\sum_{s\in \mathrm{S}} a_s s = 0$ *implique que* $a_s = 0$ *pour tout* $s$ *;*
– liée *si elle n'est pas libre ;*
– *être une* base *de* M *si pour tout élément* $m$ *de* M*, il existe une unique famille presque nulle* $(a_s)_{s\in \mathrm{S}}$ *dans* A *telle que* $m = \sum a_s s$.

*Exercice 6.3.2.* — Soit A un anneau et M un A-module. Si $m \in \mathrm{M}$, à quelle condition sur $\mathrm{Ann}(m)$ la famille $\{m\}$ est-elle libre ?

PROPOSITION 6.3.3. — *Soit* A *un anneau,* M *un* A*-module et* S *une partie de* M*. Soit* $\varphi_{\mathrm{S}}$ *l'homomorphisme canonique*

$$\mathrm{A}^{(\mathrm{S})} \to \mathrm{M}, \qquad (a_s)_{s\in \mathrm{S}} \mapsto \sum_{s\in \mathrm{S}} a_s s.$$

*Alors,*
– $\varphi_{\mathrm{S}}$ *est injectif si et seulement si* S *est libre ;*
– $\varphi_{\mathrm{S}}$ *est surjectif si et seulement si* S *est génératrice ;*
– $\varphi_{\mathrm{S}}$ *est un isomorphisme si et seulement si* S *est une base.*

*Démonstration.* — Le noyau de $\varphi_{\mathrm{S}}$ est l'ensemble des familles $(a_s)$ telles que $\sum_s a_s s = 0$. Dire que S est libre équivaut donc à dire que $\mathrm{Ker}\,\varphi_{\mathrm{S}} = (0)$, c'est-à-dire que $\varphi_{\mathrm{S}}$ est injectif.

L'image de $\varphi_{\mathrm{S}}$ est l'ensemble des combinaisons linéaires d'éléments de S. Par suite, $\mathrm{Im}\,\varphi_{\mathrm{S}} = \langle \mathrm{S} \rangle$ et $\varphi_{\mathrm{S}}$ est surjectif si et seulement si S est génératrice.

Enfin, la définition du fait que S est une base revient exactement à dire que $\varphi_{\mathrm{S}}$ est bijectif, donc un isomorphisme. □

COROLLAIRE 6.3.4. — *Une base est une partie libre et génératrice.*

*Remarques 6.3.5.* — a) Si A est un anneau quelconque, tout module n'admet pas forcément une base.

b) Si A est un corps, c'est un résultat fondamental de la théorie des espaces vectoriels que tout espace vectoriel admet une base.

DÉFINITION 6.3.6. — *Un module qui possède une base est dit* libre.

THÉORÈME 6.3.7. — *Soit* A *un anneau et soit* M *un* A*-module. Si* M *est libre, toutes les bases de* M *ont même cardinal. C'est par définition le* rang *de* M.

*Démonstration.* — Soit $\mathfrak{m}$ un idéal maximal de A, notons $k$ le corps $A/\mathfrak{m}$ et posons $V = M/\mathfrak{m}M$. On peut le considérer naturellement comme un $A/\mathfrak{m}$-module, donc comme un $k$-espace vectoriel.

Soit $(m_i)_{i\in I}$ une base de M et montrons que $(\mathrm{cl}(m_i))_{i\in I}$ est une base de V. Tout élément de V s'écrit $\mathrm{cl}(m)$ pour un certain $m \in M$. Par suite, $m$ est une combinaison linéaire des $m_i$ et $\mathrm{cl}(m)$ une combinaison linéaire des $\mathrm{cl}(m_i)$ qui forme donc une partie génératrice de V. De plus, si $(x_i)_{i\in I}$ est une famille presque nulle d'éléments de $k$ telle que $\sum x_i \,\mathrm{cl}(m_i) = 0$, choisissons pour tout $i$ un élément $a_i \in A$ tel que $x_i = \mathrm{cl}(a_i)$, avec en outre $a_i = 0$ si $x_i = 0$. On a alors $\mathrm{cl}(\sum a_i m_i) = \sum x_i \,\mathrm{cl}(m_i) = 0$ donc $m = \sum a_i m_i \in \mathfrak{m}M$. Il existe par suite une famille presque nulle $(b_i)_{i\in I}$ d'éléments de $\mathfrak{m}$ telle que $m = \sum b_i m_i$. Comme la famille $(m_i)_{i\in I}$ est une base de M, $a_i = b_i$ pour tout $i$, puis $x_i = cl(a_i) = \mathrm{cl}(b_i) = 0$ étant donné que $b_i \in \mathfrak{m}$. Ainsi, la famille $(\mathrm{cl}(m_i))$ est une base de V.

Si $(n_j)_{j\in J}$ est une autre base de M, la famille $(\mathrm{cl}(n_j))$ est tout autant une base de V.

Comme deux bases d'un espace vectoriel ont même cardinal, I et J sont équipotents. □

Plus généralement, on peut poser la définition :

DÉFINITION 6.3.8. — *Soit* A *un anneau et soit* M *un* A*-module*

*On dit qu'une famille* $(M_s)$ *de sous-modules de* M *est en* somme directe *si l'homomorphisme canonique* $\bigoplus_s M_s \to M$ *est un isomorphisme. On note* $M = \bigoplus_s M_s$.

*Si* N *et* P *sont deux sous-modules de* M *tels que* $M = N \oplus P$, *on dit aussi* P *et* N *sont* supplémentaires.

*Un sous-module de* M *qui possède un supplémentaire est dit* facteur direct.

## 6.4. Quotients de modules

*6.4.1. Relation d'équivalence compatible.* — Soit A un anneau et soit M un A-module. On s'intéresse aux relations d'équivalence sur M qui sont compatibles avec la structure de module, c'est-à-dire que pour tous $m$, $m'$, $n$ et $n'$ dans M,

$$\text{si } m \sim m' \text{ et } n \sim n', \text{ alors } am + bn \sim am' + bn'.$$

Soit N l'ensemble des $m \in M$ tels que $m \sim 0$. Comme une relation d'équivalence est réflexive, $0 \in N$. Si $m$ et $n$ appartiennent à N, on a $m \sim 0$, $n \sim 0$ et donc

pour tous $a$ et $b$ dans A, $am + bn \sim (a0 + b0) = 0$, c'est-à-dire $am + bn \in \mathrm{N}$. Cela prouve que N est un sous-module de M. De plus, si $m$ et $n$ sont deux éléments de M tels que $m \sim n$, on a $m + (-n) \sim n + (-n)$, d'où $m - n \in \mathrm{N}$.

Réciproquement, soit N un sous-A-module de M et soit $\sim$ la relation d'équivalence sur M définie par $m \sim n$ si et seulement si $m - n \in \mathrm{N}$. Notons M/N l'ensemble des classes d'équivalence et $\mathrm{cl}_{\mathrm{N}} : \mathrm{M} \to \mathrm{M/N}$ l'application canonique.[(1)] Les calculs qui précèdent montrent le théorème suivant.

THÉORÈME 6.4.2. — *Soit* A *un anneau,* M *un* A*-module et* N *un sous-module de* M. *La relation* $\sim$ *sur* M *définie par* $m \sim n$ *si et seulement si* $m - n \in \mathrm{N}$ *est une relation d'équivalence sur* M *compatible avec la structure de module. L'ensemble quotient* M/N *possède une unique structure de* A*-module telle que l'application* $\mathrm{cl} : \mathrm{M} \to \mathrm{M/N}$ *est un homomorphisme de* A*-modules.*

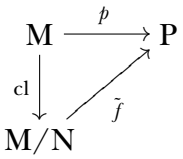
*L'homomorphisme* cl *est surjectif et de noyau* N.

On démontre maintenant un *théorème de factorisation*, propriété universelle des modules quotients.

THÉORÈME 6.4.3. — *Soit* A *un anneau,* M *un* A*-module et* N *un sous-module de* M. *Pour tout* A*-module* P *et tout homomorphisme* $f : \mathrm{M} \to \mathrm{P}$ *tel que* $\mathrm{N} \subset \mathrm{Ker}\, f$*, il existe un unique homomorphisme de modules* $\tilde{f} : \mathrm{M/N} \to \mathrm{P}$ *tel que* $f = \tilde{f} \circ \mathrm{cl}$.

*De plus,* $\mathrm{Im}\, \tilde{f} = \mathrm{Im}\, f$ *et* $\mathrm{Ker}\, \tilde{f} = \mathrm{cl}(\mathrm{Ker}\, f)$. *En particulier,* $\tilde{f}$ *est injectif si et seulement si* $\mathrm{Ker}\, f = \mathrm{N}$.

On peut représenter l'égalité du théorème en disant que le diagramme




est commutatif. L'intérêt de ce théorème est qu'il permet de factoriser un homomorphisme de A-modules $f : \mathrm{M} \to \mathrm{N}$ en la composition

$$\mathrm{M} \xrightarrow{\mathrm{cl}} \mathrm{M/\,Ker}\, f \xrightarrow{\tilde{f}} \mathrm{Im}\, f \hookrightarrow \mathrm{N}$$

d'un homomorphisme surjectif, d'un isomorphisme et d'un homomorphisme injectif.

*Démonstration.* — Nécessairement, on doit avoir $\tilde{f}(\mathrm{cl}(m)) = f(m)$ pour tout $m$ dans M. Comme tout élément de M/N est de la forme $\mathrm{cl}(m)$ pour un certain $m \in \mathrm{M}$, cela montre qu'il existe au plus un homomorphisme de A-modules $\tilde{f} : \mathrm{M/N} \to \mathrm{P}$ tel que $\tilde{f} \circ \mathrm{cl} = f$.

(1) S'il n'y a pas de confusion possible, on pourra noter simplement cl cette application.

Montrons l'existence de $\tilde{f}$. Soit $x \in \mathrm{M/N}$ et soit deux éléments $m$ et $m'$ de M tels que $x = \mathrm{cl}(m) = \mathrm{cl}(m')$. Alors, $m - m' \in \mathrm{N}$ et donc, puisque $\mathrm{N} \subset \mathrm{Ker}\, f$, $f(m - m') = 0$. On a alors $f(m) = f(m')$ et l'on peut définir $\tilde{f}$ en posant $\tilde{f}(x) = f(m)$ — cela ne dépend en effet pas de l'élément $m \in \mathrm{M}$ choisi parmi ceux qui vérifient $x = \mathrm{cl}(m)$. Il reste à montrer que $\tilde{f}$ est un homomorphisme de A-modules. Or, soit $x$ et $y \in \mathrm{M/N}$, soit $a$ et $b$ dans A. Choisissons $m \in \mathrm{M}$ tel que $x = \mathrm{cl}(m)$ et $n \in \mathrm{M}$ tel que $y = \mathrm{cl}(n)$. Alors, $ax+by = a\,\mathrm{cl}(m)+b\,\mathrm{cl}(n) = \mathrm{cl}(am+bn)$ et

$$\tilde{f}(ax + by) = \tilde{f}(\mathrm{cl}(am + bn)) = f(am + bn) = af(m) + bf(n) = a\tilde{f}(x) + b\tilde{f}(y).$$

Ainsi, $\tilde{f}$ est un homomorphisme de A-modules.

On a évidemment $\mathrm{Im}\, f \subset \mathrm{Im}\, \tilde{f}$. D'autre part, si $p$ appartient à $\mathrm{Im}\, \tilde{f}$, choisissons $x \in \mathrm{M/N}$ tel que $p = \tilde{f}(x)$ puis $m \in \mathrm{M}$ tel que $x = \mathrm{cl}(m)$. Alors, $p = \tilde{f}(\mathrm{cl}(m)) = f(m)$ appartient à $\mathrm{Im}\, f$, d'où l'autre inclusion et finalement l'égalité $\mathrm{Im}\, f = \mathrm{Im}\, \tilde{f}$.

Enfin, si $\tilde{f}(x) = 0$, on peut écrire $x = \mathrm{cl}(m)$ avec $m \in \mathrm{M}$ et la relation $\tilde{f} \circ \mathrm{cl} = f$ implique $f(m) = 0$, d'où $x \in \mathrm{cl}(\mathrm{Ker}\, f)$. Dans l'autre sens, si $x = \mathrm{cl}(m)$ avec $m \in \mathrm{Ker}\, f$, on a $\tilde{f}(x) = \tilde{f}(\mathrm{cl}(m)) = f(m) = 0$, donc $x \in \mathrm{Ker}\, \tilde{f}$. Ainsi, $\mathrm{Ker}\, \tilde{f} = \mathrm{cl}(\mathrm{Ker}\, f)$. □

La proposition suivante décrit les sous-modules d'un module quotient tel que M/N.

PROPOSITION 6.4.4. — *Soit* A *un anneau,* M *un* A*-module,* N *un sous-module de* M. *L'application* $\mathrm{cl}^{-1}$ *:*

$$\begin{array}{ccc} \textit{sous-modules de } \mathrm{M/N} & \to & \textit{sous-modules de } \mathrm{M} \textit{ contenant } \mathrm{N} \\ \mathscr{P} & \mapsto & \mathrm{cl}^{-1}(\mathscr{P}) \end{array}$$

*est une bijection.*

Ainsi, pour tout sous-module P de M qui contient N, il existe un unique sous-module $\mathscr{P}$ de M/N tel que $\mathrm{P} = \mathrm{cl}^{-1}(\mathscr{P})$. De plus, on $\mathscr{P} = \mathrm{cl}(\mathrm{P})$. *Le sous-module* $\mathrm{cl}(\mathrm{P})$ *de* M/N *sera noté* P/N. Cette notation est cohérente. En effet, la restriction de cl à P est un homomorphisme $\mathrm{cl}\,|\mathrm{P}\colon \mathrm{P} \to \mathrm{M/N}$ de noyau $\mathrm{P} \cap \mathrm{N} = \mathrm{N}$ et d'image $\mathrm{cl}(\mathrm{P})$. D'après le théorème de factorisation, $\mathrm{cl}\,|_{\mathrm{P}}$ induit un isomorphisme $\mathrm{P/N} \to \mathrm{cl}(\mathrm{P})$.

*Démonstration.* — La démonstration est une conséquence immédiate des deux formules suivantes : si P est un sous-module de M,

$$\boxed{\mathrm{cl}^{-1}(\mathrm{cl}(\mathrm{P})) = \mathrm{P} + \mathrm{N}}$$

et si $\mathscr{P}$ est un sous-module de M/N,

$$\boxed{\mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{P})) = \mathscr{P}.}$$

En effet, si $P \subset N$, $P + N = P$ et ces formules montrent que l'application $cl^{-1}$ comme dans l'énoncé admet cl comme bijection réciproque.

Montrons la première formule. Si $m \in cl^{-1}(cl(P))$, on a $cl(m) \in cl(P)$. Il existe donc $p \in P$ tel que $cl(m) = cl(p)$ et par suite, $cl(m - p) = 0$. Cela signifie que $n = m - p \in N$ et $m = p + n$ appartient à $P + N$. Réciproquement, si $m = p + n$ appartient à $P + N$, $cl(m) = cl(p + n) = cl(p)$ appartient à $cl(P)$, donc $m \in cl^{-1}(cl(P))$.

Montrons la seconde formule. Par définition, on a $cl(cl^{-1}(\mathscr{P})) \subset \mathscr{P}$. Réciproquement, si $x \in \mathscr{P}$, soit $m \in M$ tel que $x = cl(m)$. Alors, $cl(m) \in \mathscr{P}$, autrement dit, $m \in cl^{-1}(\mathscr{P})$ et donc $x = cl(m) \in cl(cl^{-1}(\mathscr{P}))$. □

Enfin, nous pouvons calculer le « quotient d'un quotient ».

PROPOSITION 6.4.5. — *Soit* A *un anneau,* N, P, M *trois* A*-modules tels que* $N \subset P \subset M$. *Alors, on a un isomorphisme canonique*

$$(M/N)/(P/N) \simeq (M/P)$$

*tel que pour tout* $m \in M$, $cl_{P/N}(cl_N(m)) \mapsto cl_P(m)$.

*Démonstration.* — Considérons l'homomorphisme composé

$$\varphi : M \to (M/N) \to (M/N)/(P/N), \qquad m \mapsto cl_{P/N}(cl_N(m)).$$

Il est surjectif, comme composé de deux homomorphismes surjectif. Un élément $m$ est dans son noyau si et seulement si $cl_N(m) \in \operatorname{Ker} cl_{P/N} = P/N = cl_N(P)$, c'est-à-dire $m \in P$ puisque P contient N. Ainsi, $\operatorname{Ker}\varphi = P$ et le théorème de factorisation 6.4.3 affirme l'existence d'un unique homomorphisme bijectif $\tilde{\varphi} : M/P \to (M/N)/(P/N)$ tel que $\tilde{\varphi}(cl_P(m)) = cl_{P/N}(cl_N(m))$. C'est l'isomorphisme cherché. □

## 6.5. Localisation des modules

*6.5.1. Calcul de fractions.* — Soit A un anneau et soit M un A-module. Soit S une partie multiplicative de A. Nous allons construire, par un calcul de fractions similaire à celui qui nous a permis de définir l'anneau localisé $S^{-1}A$, un $S^{-1}A$-module $S^{-1}M$ ainsi qu'un homomorphisme de A-modules $M \to S^{-1}M$.

Soit sur l'ensemble $M \times S$ la relation

$$(m, s) \sim (n, t) \quad \Leftrightarrow \quad \text{il existe } u \in S \text{ tel que } u(tm - sn) = 0.$$

On vérifie comme page 30 que c'est une relation d'équivalence, on note $S^{-1}M$ l'ensemble des classes d'équivalence et $m/s \in S^{-1}M$ la classe d'équivalence du couple $(m, s) \in M \times S$.

On définit sur $S^{-1}M$ deux lois : tout d'abord, si $m$, $n \in M$ et $s$, $t \in S$,

$$(m/s) + (n/t) = (tm + sn)/(st)$$

et, si $m \in M$, $a \in A$, $s$ et $t \in S$,

$$(a/t)(m/s) = (am)/(ts).$$

THÉORÈME 6.5.2. — *Muni de ces lois,* $S^{-1}M$ *est un* $S^{-1}A$*-module. L'application* $i : M \to S^{-1}M$ *telle que* $i(m) = (m/1)$ *est un homomorphisme de* A*-modules,* $S^{-1}M$ *étant considéré comme un* A*-module grâce à l'homomorphisme canonique d'anneaux* $A \to S^{-1}A$.

La démonstration est laissée en *exercice*. Les calculs sont semblables à ceux fait lors de la localisation des anneaux.

*Remarque 6.5.3.* — Rappelons quelques exemples de parties multiplicatives. Tout d'abord, si $s \in A$, la partie $S = \{1; s; s^2; \ldots\}$ est multiplicative. La localisation est dans ce cas notée avec un $s$ en indice : $M_s = S^{-1}M$ est un $A_s$-module. Si $\mathfrak{p}$ est un idéal premier de A, $S = A \setminus \mathfrak{p}$ est aussi une partie multiplicative. On note $A_\mathfrak{p}$ l'anneau localisé et $M_\mathfrak{p}$ le $A_\mathfrak{p}$-module obtenu par calcul de fractions à partir d'un A-module M.

*Exercice 6.5.4.* — Soit A un anneau, M un A-module, S une partie multiplicative de A. Considérons l'homomorphisme canonique $i : M \to S^{-1}M$.

a) Un élément $m \in M$ appartient à $\operatorname{Ker} i$ si et seulement s'il existe $s \in S$ tel que $sm = 0$.

b) L'homomorphisme $i$ est un isomorphisme si et seulement si pour tout élément de S, l'homomorphisme $\mu_s : M \to M$, $m \mapsto sm$, est un isomorphisme.

PROPOSITION 6.5.5. — *Soit* A *un anneau,* S *une partie multiplicative de* A. *Soit* $f : M \to N$ *un homomorphisme de* A*-modules. Il existe alors un unique homomorphisme de* $S^{-1}A$*-modules* $\tilde{f} : S^{-1}M \to S^{-1}N$ *tel que pour tout* $m \in M$ *et tout* $s \in S$, $\tilde{f}(m/s) = f(m)/s$.

Autrement dit, le diagramme

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle i} \\ S^{-1}M & \xrightarrow{\tilde{f}} & S^{-1}N \end{array}$$

est commutatif.

*Démonstration.* — Il faut vérifier que cette définition a un sens. Si $m/s = n/t$, soit $u \in S$ tel que $u(tm - sn) = 0$. Alors,

$$\frac{f(m)}{s} = \frac{utf(m)}{uts} = \frac{f(utm)}{uts} = \frac{f(usn)}{uts} = \frac{f(n)}{t},$$

ce qui prouve que $\tilde{f}$ est bien définie. Alors, si $m$, $n \in \mathrm{M}$, $s$, $t \in \mathrm{S}$, on a

$$\begin{aligned}\tilde{f}\left(\frac{m}{s}+\frac{n}{t}\right) &= \tilde{f}\left(\frac{tm+sn}{st}\right) = \frac{f(tm+sn)}{st} \\ &= \frac{tf(m)}{st}+\frac{sf(n)}{st} = \frac{f(m)}{s}+\frac{f(n)}{t} = \tilde{f}\left(\frac{m}{s}\right)+\tilde{f}\left(\frac{n}{t}\right)\end{aligned}$$

et $\tilde{f}$ est donc additive. Enfin, si $m \in \mathrm{M}$, $a \in \mathrm{A}$, $s$ et $t \in \mathrm{S}$, on a

$$\tilde{f}\left(\frac{a}{t}\,\frac{m}{s}\right) = \tilde{f}\left(\frac{am}{st}\right) = \frac{f(am)}{st} = \frac{af(m)}{st} = \frac{a}{t}\,\frac{f(m)}{s} = \frac{a}{t}\tilde{f}\left(\frac{m}{s}\right)$$

et $\tilde{f}$ est A-linéaire. □

La localisation des modules donne lieu à une propriété universelle du même genre de celle établie pour les anneaux.

THÉORÈME 6.5.6. — *Soit* A *un anneau,* S *une partie multiplicative de* A, $f : \mathrm{M} \to \mathrm{N}$ *un homomorphisme de* A*-modules. On suppose que pour tout* $s \in \mathrm{S}$, *l'homomorphisme* $\mu_s : \mathrm{N} \to \mathrm{N}$, $n \mapsto sn$, *est un isomorphisme. Alors, il existe un unique homomorphisme de* A*-modules* $\varphi : \mathrm{S}^{-1}\mathrm{M} \to \mathrm{N}$ *tel que* $\tilde{f}(m/1) = f(m)$ *pour tout* $m \in \mathrm{M}$.

*Démonstration.* — En fait, si $\tilde{f} : \mathrm{S}^{-1}\mathrm{M} \to \mathrm{S}^{-1}\mathrm{N}$ désigne l'homomorphisme fourni par la proposition précédente et $i : \mathrm{N} \to \mathrm{S}^{-1}\mathrm{N}$ l'homomorphisme canonique, la propriété voulue pour $\varphi$ équivaut à l'égalité $i \circ \varphi = \tilde{f}$. Comme $i$ est dans ce cas un isomorphisme, on a $\varphi = i^{-1} \circ \tilde{f}$. □

*Exercice 6.5.7.* — Le démontrer par du calcul en vérifiant que la formule $\varphi(m/s) = \mu_s^{-1}(f(m))$ convient.

La localisation se comporte très bien vis à vis des sous-modules ; c'est la deuxième occurence de l'*exactitude de la localisation*.

PROPOSITION 6.5.8. — *Soit* A *un anneau,* S *une partie multiplicative de* A. *Soit* M *un* A*-module et* N *un sous-module de* M.

*Alors, l'homomorphisme canonique* $\mathrm{S}^{-1}\mathrm{N} \to \mathrm{S}^{-1}\mathrm{M}$ *provenant de l'injection* $\mathrm{N} \to \mathrm{M}$ *est injectif et définit un isomorphisme de* $\mathrm{S}^{-1}\mathrm{N}$ *sur un sous-module de* $\mathrm{S}^{-1}\mathrm{M}$, *noté encore* $\mathrm{S}^{-1}\mathrm{N}$.

*De plus, on a un isomorphisme canonique*

$$\mathrm{S}^{-1}\mathrm{M}/\mathrm{S}^{-1}\mathrm{N} \simeq \mathrm{S}^{-1}(\mathrm{M}/\mathrm{N}).$$

*Démonstration.* — Soit $n \in \mathrm{N}$ et $s \in \mathrm{S}$. L'image de $n/s \in \mathrm{S}^{-1}\mathrm{N}$ dans $\mathrm{S}^{-1}\mathrm{M}$ est égale à $n/s$ mais où $n$ est vu comme un élément de M. Elle est nulle si et seulement s'il existe $t \in \mathrm{S}$ tel que $tn = 0$ dans M, mais aussi dans N ! Par suite, cet homomorphisme est injectif. C'est ainsi un isomorphisme de $\mathrm{S}^{-1}\mathrm{M}$ sur son image dans $\mathrm{S}^{-1}\mathrm{M}$.

Considérons maintenant l'homomorphisme égal à la composition des homomorphismes canoniques

$$\mathrm{M} \xrightarrow[m\mapsto m/1]{} \mathrm{S}^{-1}\mathrm{M} \xrightarrow{\mathrm{cl}} \mathrm{S}^{-1}\mathrm{M}/\mathrm{S}^{-1}\mathrm{N}.$$

Par construction, un élément $n$ a pour image 0, d'où, par la propriété universelle des modules quotients, un unique homomorphisme $\mathrm{M}/\mathrm{N} \to \mathrm{S}^{-1}\mathrm{M}/\mathrm{S}^{-1}\mathrm{N}$ par lequel $\mathrm{cl}_{\mathrm{N}}(m) \mapsto \mathrm{cl}_{\mathrm{S}^{-1}\mathrm{N}}(m/1)$. Comme S agit par automorphisme sur le $\mathrm{S}^{-1}\mathrm{A}$-module $\mathrm{S}^{-1}\mathrm{M}/\mathrm{S}^{-1}\mathrm{N}$, on en déduit un unique homomorphisme $\varphi\colon \mathrm{S}^{-1}(\mathrm{M}/\mathrm{N}) \to \mathrm{S}^{-1}\mathrm{M}/\mathrm{S}^{-1}\mathrm{N}$ tel que $(\mathrm{cl}_{\mathrm{N}}(m)/1) \mapsto \mathrm{cl}_{\mathrm{S}^{-1}\mathrm{N}}(m/1)$.

Montrons que $\varphi$ est un isomorphisme. Il est surjectif car $\mathrm{cl}_{\mathrm{N}}(m)/s$ a pour image $\mathrm{cl}_{\mathrm{S}^{-1}\mathrm{N}}(m/s)$. Il est injectif : si $\mathrm{cl}_{\mathrm{N}}(m)/s$ a pour image 0, $m/s \in \mathrm{S}^{-1}\mathrm{N}$. Il existe ainsi $n \in \mathrm{N}$ et $t \in \mathrm{S}$ tels que $m/s = n/t$. Soit alors $u \in \mathrm{S}$ tel que $u(tm - sn) = 0$. Il en résulte l'égalité

$$\frac{\mathrm{cl}_{\mathrm{N}}(m)}{s} = \frac{\mathrm{cl}_{\mathrm{N}}(utm)}{stu} = \frac{\mathrm{cl}_{\mathrm{N}}(sun)}{stu)} = \frac{0}{stu} = 0,$$

d'où l'injectivité. □

Proposition 6.5.9. — *Soit* A *un anneau,* S *une partie multiplicative de* A. *Soit* M *un* A*-module et soit* $(\mathrm{N}_i)$ *une famille de sous-modules de* M. *Alors, on a une égalité de sous-modules de* $\mathrm{S}^{-1}\mathrm{M}$ *:*

$$\sum_i \mathrm{S}^{-1}\mathrm{N}_i = \mathrm{S}^{-1} \sum \mathrm{N}_i.$$

*Démonstration.* — Notons $\mathrm{N} = \sum \mathrm{N}_i$. Pour tout $i$, $\mathrm{N}_i \subset \mathrm{N}$, d'où une inclusion $\mathrm{S}^{-1}\mathrm{N}_i \subset \mathrm{S}^{-1}\mathrm{N}$. Par suite, $\sum_i \mathrm{S}^{-1}\mathrm{N}_i \subset \mathrm{S}^{-1}\mathrm{N}$. Réciproquement, soit $n/s \in \mathrm{S}^{-1}\mathrm{N}$. On peut écrire $n = \sum_i n_i$, où pour tout $i$, $n_i \in \mathrm{N}_i$, la somme étant presque nulle. Alors, $n/s = \sum_i (n_i/s)$ appartient à $\sum \mathrm{S}^{-1}\mathrm{N}_i$ et l'autre inclusion est démontrée. □

Proposition 6.5.10. — *Soit* A *un anneau,* S *une partie multiplicative de* A *et soit* M *un* A*-module. Notons* $i\colon \mathrm{M} \to \mathrm{S}^{-1}\mathrm{M}$ *l'homomorphisme canonique de* A*-modules.*

*Si* $\mathscr{N}$ *est un sous-*$\mathrm{S}^{-1}\mathrm{A}$*-module de* $\mathrm{S}^{-1}\mathrm{M}$*, alors* $\mathrm{N} = i^{-1}(\mathscr{N})$ *est un sous-*A*-module de* M *tel que* $\mathscr{N} = \mathrm{S}^{-1}\mathrm{N}$.

*Démonstration.* — Il est clair que $\mathrm{S}^{-1}\mathrm{N} \subset \mathscr{N}$ : si $m \in \mathrm{N}$, on a $m/1 \in \mathscr{N}$, donc pour tout $s \in \mathrm{S}$, $m/s \in \mathscr{N}$.

Réciproquement, soit $x \in \mathscr{N}$. On peut écrire $x = m/s$ avec $m \in \mathrm{M}$ et $s \in \mathrm{S}$. Par suite, $sx = m/1$ appartient à N et $x = (sx)/s$ appartient à $\mathrm{S}^{-1}\mathrm{N}$. □

## 6.6. Exercices

*Exercice 6.6.1.* — Soit A et B deux anneaux et $f : A \longrightarrow B$ un homomorphisme d'anneaux.

**a)** Montrer que la loi $a.b = f(a).b$ (où $a \in A$ et $b \in B$) munit B d'une structure de A-module. B muni de sa structure d'anneau et de cette structure de A-module est appelé une A-algèbre

**b)** Montrer que si $B \neq 0$ et si A est un corps $k$ alors $f$ est injectif (càd : une $k$-algèbre non nulle contient un corps isomorphe à $k$).

**c)** Montrer que tout B-module N est muni naturellement d'une structure de A-module. Quel est l'annulateur $(0_A : N)$ de ce module ?

*Exercice 6.6.2.* — Soient $M_1, \dots, M_r$ des A-modules et $I_1 = (0 : M_1), \dots, I_r = (0 : M_r)$ leurs annulateurs. On suppose que les $I_\alpha$ sont deux à deux comaximaux.

On pose : $M = \bigoplus_{\alpha=1}^{r} M_\alpha$, $I = \bigcap_{\alpha=1}^{r} I_\alpha$, $N_\alpha = \bigoplus_{\beta\neq\alpha} M_\beta$ et $J_\alpha = \bigcap_{\beta\neq\alpha} I_\beta$.

**a)** Montrer que pour tout $\alpha$, $I_\alpha$ et $J_\alpha$ sont comaximaux.

Si J est un idéal de A on notera $(0 : J)$ le sous-A-module de M égal à $\{m \in M, J \cdot m = 0\}$.

Montrer les formules suivantes :

**b)** $J_\alpha = (0 : N_\alpha)$ et $N_\alpha = (0 : J_\alpha)$ ;

**c)** $N_\alpha = I_\alpha \cdot M$ et $J_\alpha \cdot M = \bigcap_{\beta\neq\alpha} N_\beta \simeq M_\alpha$.

*Exercice 6.6.3.* — Soit M un A-module et $m \in M$ un élément dont l'annulateur est réduit à $(0)$. Montrer l'équivalence des propriétés suivantes :

(1) A$m$ possède un supplémentaire dans M ;

(2) il existe $f \in M^* = \mathrm{Hom}(M, A)$ tel que $f(m) = 1$.

Montrer qu'alors $M = Am \oplus \mathrm{Ker}\, f$.

*Exercice 6.6.4* (Bidual). — Soit M un A-module. On note $M^\vee = \mathrm{Hom}_A(M, A)$ son dual et $M^{\vee\vee} = \mathrm{Hom}_A(M^\vee, A)$ son bidual, c'est-à-dire le dual de son dual.

**a)** Soit $m \in M$. Montrer que l'application

$$\lambda_m : M^\vee \to A, \qquad \varphi \mapsto \varphi(m)$$

est A-linéaire. En déduire un homomorphisme de A-modules $\lambda$: $M \to M^{\vee\vee}$ donné par $m \mapsto \lambda_m$.

**b)** Dans cette question et la suivante, on suppose que $M = A^n$, $n \geq 1$. Soit $(e_1, \dots, e_n)$ la base canonique de $A^n$, c'est-à-dire $e_i = (0, \dots, 0, 1, 0, \dots)$, le 1 étant en position $i$. Soit $\varphi_i$ l'application linéaire $A^n \to A$ définie par $(a_1, \dots, a_n) \mapsto a_i$. Montrer que $(\varphi_1, \dots, \varphi_n)$ est une base de $M^\vee$.

**c)** Toujours lorsque $M = A^n$, montrer que $\lambda$ est un isomorphisme.

Un tel module M pour lequel l'homomorphisme canonique $M \to M^{\vee\vee}$ est un isomorphisme est dit *réflexif*.

**d)** Donner un exemple de module pour lequel $\lambda$ n'est pas injectif ; pas surjectif.

*Exercice 6.6.5.* — Soit M un A-module. Soit $f \in \mathrm{End}_A(M)$ ; on définit sa transposée ${}^t f$ par ${}^t f(\varphi) = \varphi \circ f$, pour tout $\varphi \in M^\vee = \mathrm{Hom}_A(M, A)$.

**a)** Montrer que l'ensemble des polynômes P de A[X] tels que $P(f) = 0$ est un idéal que l'on notera $I(f)$.

**b)** Montrer que $I(f) \subset I({}^t f)$.

**c)** Montrer que si M est réflexif, $I(f) = I({}^t f)$.

*Exercice 6.6.6.* — Soit A un anneau intègre et M un A-module. On dit que $x \in M$ est de torsion si $(0 : x) \neq 0$. On note T(M) l'ensemble des éléments de torsion de M. Si $T(M) = 0$ on dit que M est sans torsion.

**a)** Montrer que l'ensemble des éléments de torsion de M est un sous-module de M.

**b)** Montrer que M/T(M) est sans torsion.

**c)** Montrer que si $f : M \to N$ est un morphisme de A-modules alors $f(T(M)) \subset T(N)$.

**d)** Montrer qu'une suite exacte $0 \to M' \to M \to M''$ induit une suite exacte $0 \to T(M') \to T(M) \to T(M'')$.

*Exercice 6.6.7.* — Soient M et N deux A-modules.

**a)** Soit $u \in \mathrm{End}_A M$. Montrer qu'il existe une unique structure de A[X]-module sur M telle que $X \cdot m = u(m)$ (et $1 \cdot m = m$) pour tout $m \in M$. On notera $M_u$ le A[X]-module M muni de cette structure.

Montrer que cette application $u \mapsto M_u$ induit une bijection entre les structures de A[X]-module sur M et les endomorphismes $u \in \mathrm{End}\, M$.

**b)** Soient $u \in \mathrm{End}_A M$ et $v \in \mathrm{End}_A N$. Déterminer tous les homomorphismes de A[X] modules de $M_u$ dans $N_v$.

**c)** Si $M = N$, à quelle condition $M_u \simeq M_v$ ?

**d)** Comment pouvez-vous interpréter les résultats de l'exercice lorsque $A = k$ est un corps et $M = k^n$ est l'espace vectoriel standard de dimension $n$ sur $k$ ?

*Exercice 6.6.8.* — Soit $f : M \to N$ un homomorphisme de A-modules.

**a)** Montrer qu'il existe $g : N \to M$ tel que $g \circ f = \mathrm{Id}_M$ si et seulement si $f$ est injectif et $\mathrm{Im}(f)$ admet un supplémentaire dans N.

**b)** Montrer qu'il existe $g : N \to M$ tel que $f \circ g = \mathrm{Id}_N$ si et seulement si $f$ est surjectif et $\mathrm{Ker}(f)$ admet un supplémentaire dans M.

*Exercice 6.6.9.* — Soit A un anneau et M un A-module. Soit I un idéal de A. On suppose que $M_{\mathfrak{m}} = 0$ pour tout idéal maximal $\mathfrak{m}$ contenant I. Montrer que $M = IM$.

*Exercice 6.6.10.* — Montrer qu'un idéal non nul I d'un anneau A est un sous-module libre de A si et seulement si I est principal et engendré par un élément non diviseur de zéro de A.

*Exercice 6.6.11.* — Soit A un anneau intègre et K son corps des fractions. On suppose $K \neq A$. Montrer que K n'est pas libre comme A-module.

*Exercice 6.6.12.* — Donner des exemples :

**a)** de modules non-libres ;

**b)** d'une famille libre à $n$ éléments dans $A^n$ qui ne soit pas une base ;

**c)** d'une partie génératrice minimale qui ne soit pas une base ;

**d)** de sous-module n'ayant pas de supplémentaire ;

**e)** de module libre ayant un sous-module qui ne l'est pas ;

*Exercice 6.6.13* (Extensions de modules libres). — Soient L et M deux A-modules, $f : L \to M$ un homomorphisme d'anneaux.

**a)** On suppose que $\operatorname{Ker} f$ et $\operatorname{Im} f$ sont de type fini. Montrer que L est de type fini.

**b)** On suppose que $\operatorname{Ker} f \simeq A^p$ et $\operatorname{Im} f \simeq A^q$. Montrer que $L \simeq A^{p+q}$.

## 6.7. Solutions

*Solution de l'exercice 6.6.1.* — **a)** On a les égalités

$$\begin{aligned} 1 \cdot b &= f(1)b = b \\ (a+a') \cdot b &= f(a+a')b = (f(a)+f(a'))b \\ &= f(a)b + f(a')b = a \cdot b + a' \cdot b \\ (aa') \cdot b &= f(aa')b = f(a)f(a')b = f(a)(a' \cdot b) \\ &= a \cdot (a' \cdot b) \end{aligned}$$

qui prouvent que cette loi munit B d'une structure de A-module.

**b)** Le noyau de $f$ est un idéal de A. Comme A est un corps, on a deux possibilités : $\operatorname{Ker} f = A$ ou $\operatorname{Ker} f = 0$. Comme $f(1_A) = 1_B \neq 0$, $1_A \notin \operatorname{Ker} f$, et donc $\operatorname{Ker} f = 0$.

**c)** Soit N un B-module. On vérifie que la loi $a \cdot n = f(a)n$ munit N d'une structure de A-module (on garde la même loi d'addition).

Soit $x \in (0_A : N)$. On a

$$\begin{aligned} x \in (0_A : N) &\Leftrightarrow \quad \forall n \in N, \quad x \cdot n = 0 \\ &\Leftrightarrow \quad \forall n \in N, \quad f(x)n = 0 \\ &\Leftrightarrow \quad f(x) \in (0_B : N) \\ &\Leftrightarrow \quad x \in f^{-1}(0_B : N). \end{aligned}$$

L'annulateur de N comme A-module est l'image réciproque par $f$ de l'annulateur de N vu comme B-module.

*Solution de l'exercice 6.6.2.* — **a)** Si $\beta \neq \alpha$, $I_\alpha$ et $I_\beta$ sont comaximaux. On peut donc écrire $1 = x_\beta + y_\beta$ avec $x_\beta \in I_\alpha$ et $y_\beta \in I_\beta$. Alors, en développant le produit

$$1 = \prod_{\beta \neq \alpha} (x_\beta + y_\beta),$$

on voit que 1 est la somme d'un élément de $\prod_{\beta \neq \alpha} I_\beta \subset J_\alpha$, à savoir $\prod_{\beta \neq \alpha} y_\beta$, et d'un élément de $I_\alpha$ (car c'est une somme de termes qui sont tous multiples de l'un des $x_\beta$).

**b)** Un élément $a \in A$ appartient à $(0 : N_\alpha)$ si et seulement $an = 0$ pour tout $n \in N_\alpha$, c'est-à-dire, pour tout $\beta \neq \alpha$ et tout $m \in M_\beta$, $am = 0$. Ainsi, $(0 : N_\alpha)$ est l'intersection des $(0 : M_\beta) = I_\beta$ pour $\beta \neq \alpha$, et donc $(0 : N_\alpha) = J_\alpha$.

Un élément $\sum m_\beta$ appartient à $(0 : J_\alpha)$ si et seulement si pour tout $\beta$, $J_\alpha m_\beta = 0$. Si $\alpha \neq \beta$, l'inclusion $J_\alpha \subset I_\beta$ montre que tout $m_\beta$ convient. Pour $\beta = \alpha$, l'égalité $I_\alpha + J_\alpha = A$ implique $I_\alpha m_\alpha + 0 = A m_\alpha$, d'où $m_\alpha = 0$. Ainsi, $(0 : J_\alpha) = \bigoplus_{\beta \neq \alpha} M_\beta = N_\alpha$.

**c)** Comme $I_\alpha + J_\alpha = A$, on a

$$N_\alpha = I_\alpha N_\alpha + J_\alpha N_\alpha == I_\alpha N_\alpha.$$

De même, on a pour tous $\alpha \neq \beta$,

$$M_\beta = (I_\beta + I_\alpha) M_\beta = I_\alpha M_\beta,$$

si bien que

$$I_\alpha M = \bigoplus_\alpha I_\alpha M_\beta = \bigoplus_{\alpha \neq \beta} M_\alpha = N_\alpha.$$

Enfin, $J_\alpha M = \bigoplus J_\alpha M_\beta = J_\alpha M_\alpha$ car $J_\alpha \subset I_\beta$ si $\beta \neq \alpha$. De plus, $J_\alpha + I_\alpha = 1$ implique que $J_\alpha M_\alpha = M_\alpha$.

*Solution de l'exercice 6.6.3.* — Soit N un supplémentaire de $Am$, de sorte que $M = Am \oplus N$. Comme l'annulateur de $m$ est nul, l'homomorphisme $A \to Am$, $a \mapsto am$ est un isomorphisme. On peut alors définir une forme linéaire $f$ sur M par $f(am, n) = a$. On a bien $f(m) = 1$.

Réciproquement, s'il existe un tel $f$, le noyau de $f$ est un sous-module N de M. De plus, si $am \in Am \cap N = 0$, $f(am) = a = 0$ et donc $Am \cap N = 0$. Enfin, si $m' \in M$,

on écrit $m' = f(m')m + (m' - f(m')m)$. Puisque $f(m) = 1$, $f(m' - f(m')m) = 0$ et $m' - f(m')m \in \mathrm{N}$, ce qui prouve que $\mathrm{A}m + \mathrm{N} = \mathrm{M}$. Donc $\mathrm{M} = \mathrm{A}m \oplus \mathrm{Ker}\, f$.

*Solution de l'exercice 6.6.4.* — **a)** Si $\varphi$, $\psi \in \mathrm{M}^\vee$ et si $a$, $b \in \mathrm{A}$, on a

$$\lambda_m(a\varphi + b\psi) = (a\varphi + b\psi)(m) = a\varphi(m) + b\psi(m) = a\lambda_m(\varphi) + b\lambda_m(\psi)$$

donc $\lambda_m$ est une application linéaire $\mathrm{M}^\vee \to \mathrm{A}$.

L'application $\lambda\colon \mathrm{M} \to \mathrm{M}^{\vee\vee}$ telle que $m \mapsto \lambda_m$ est linéaire. En effet, si $m$, $n \in \mathrm{M}$ et si $a$, $b \in \mathrm{A}$, $\lambda_{am+bn}$ est l'application linéaire donnée par $\varphi \mapsto \varphi(am + bn)$. Pour $\varphi \in \mathrm{M}^\vee$, on a donc

$$\lambda_{am+bn}(\varphi) = \varphi(am + bn) = a\varphi(m) + b\varphi(n) = a\lambda_m(\varphi) + b\lambda_n(\varphi) = (a\lambda_m + b\lambda_n)(\varphi)$$

et donc $\lambda_{am+bn} = a\lambda_m + b\lambda_n$ ce qui prouve que $\lambda$ est linéaire.

**b)** Soit $\varphi : \mathrm{A}^n \to \mathrm{A}$ une forme linéaire sur $\mathrm{A}^n$. On a pour tout $m = (a_1, \ldots, a_n) \in \mathrm{A}^n$, $a_i = \varphi_i(m)$. Par suite,

$$\varphi(m) = \varphi(a_1, \ldots, a_n) = \varphi(a_1 e_1 + \cdots + a_n e_n) = \varphi_1(m)\varphi(e_1) + \cdots + \varphi_n(m)\varphi(e_n)$$

et

$$\varphi = \varphi(e_1)\varphi_1 + \cdots + \varphi(e_n)\varphi_n.$$

Cette expression montre que toute forme linéaire sur $\mathrm{A}^n$ est combinaison linéaire des $\varphi_i$. Il y a de plus unicité : si

$$a_1\varphi_1 + \cdots + a_n\varphi_n = 0,$$

en appliquant $e_i$, on trouve $a_i = 0$. Par suite, les $\varphi_i$ forment une base de $\mathrm{M}^\vee$.

**c)** La question précédente appliquée à $\mathrm{M}^\vee \simeq \mathrm{A}^n$ montre qu'une base de $\mathrm{M}^{\vee\vee}$ est formée des formes linéaires $\psi_i : \mathrm{M}^\vee \to \mathrm{A}$ définies par $\psi_i(\varphi_j) = 1$ si $i = j$ et 0 sinon. Or, on remarque que

$$\lambda_{e_i}(\varphi_j) = \varphi_j(e_i) = \begin{cases} 1 & \text{si } i = j\,; \\ 0 & \text{sinon} \end{cases}$$

et donc $\lambda_{e_i}(\varphi_j) = \psi_i(\varphi_j)$, c'est-à-dire $\lambda_{e_i} = \psi_i$.

Par suite, $\lambda$ est un isomorphisme.

**d)** Prenons $\mathrm{A} = \mathbf{Z}$, $\mathrm{M} = \mathbf{Z}/2\mathbf{Z}$. Soit $f : \mathrm{M} \to \mathbf{Z}$ une application linéaire. Comme pour tout $m$ dans M, $2m = 0$, on a $f(2m) = 2f(m) = 0$ dans $\mathbf{Z}$, donc $f(m) = 0$. Ainsi, $f = 0$. Cela montre que $\mathrm{M}^\vee = 0$, puis $\mathrm{M}^{\vee\vee} = 0$. L'homomorphisme canonique $\mathrm{M} \to \mathrm{M}^{\vee\vee}$ est l'application nulle, donc n'est pas injectif.

Si A est un corps $k$, prenons $\mathrm{M} = k^{(\mathrm{I})}$ où I est une partie infinie dénombrable. C'est un $k$-espace vectoriel de dimension dénombrable. On a $\mathrm{M}^\vee \simeq k^{\mathrm{I}}$, donc $\mathrm{M}^\vee$ est de dimension infinie non dénombrable et contient un sous-espace vectoriel isomorphe à $k^{(\mathrm{I})}$. Alors, $\mathrm{M}^{\vee\vee}$ contient un sous-espace isomorphe à $k^{\mathrm{I}}$, donc est

de dimension infinie non dénombrable. L'homomorphisme $M \to M^{\vee\vee}$ ne peut donc pas être surjectif.

*Solution de l'exercice 6.6.5.* — **a)** Comme $I(f)$ est le noyau de l'application linéaire $A[X] \to \mathrm{End}_A M$ donnée par $P \mapsto P(f)$, c'est un idéal de $A[X]$.

**b)** Soit $P \in I(f)$ et montrons que $P \in I({}^t f)$. En effet, si $\varphi \in M^\vee$, et si $P = \sum a_n X^n$,

$$\begin{aligned} P({}^t f)(\varphi) &= \sum a_n {}^t f^n(\varphi) = \sum a_n \varphi \circ f^n \\ &= \varphi \circ \Big( \sum a_n f^n \Big) = \varphi \circ P(f) = 0. \end{aligned}$$

**c)** Si M est réflexif, $M^{\vee\vee}$ s'identifie à M, et par cette identification, ${}^{tt}f = f$, si bien que $I({}^t f) \subset I(f)$. Par suite, $I(f) = I({}^t f)$.

*Solution de l'exercice 6.6.6.* — **a)** On a $0 \in T(M)$. Soient $m$ et $m' \in T(M)$ ; soient $a$ et $a' \in A$. Soient $x$ et $x' \in A \setminus \{0\}$ tels que $xm = 0$ et $x'm' = 0$. Alors, $(xx')(am + a'm') = ax'(xm) + a'x(x'm') = 0$, et $xx' \neq 0$ puisque $x$ et $x'$ sont non nuls et que A est intègre. Par suite, $am + a'm' \in T(M)$. Ainsi, $T(M)$ est un sous-A-module de M.

**b)** Soient $\mathrm{cl}(m) \in M/T(M)$, avec $m \in M$, et $a \in A \setminus \{0\}$, tels que $a\,\mathrm{cl}(m) = 0$. Cela signifie que $am \in T(M)$. Il existe ainsi $x \in A \setminus \{0\}$ tel que $x(am) = 0 = (ax)m$. Comme $ax \neq 0$, $m \in T(M)$ et $\mathrm{cl}(m) = 0$. Ainsi, $M/T(M)$ est sans torsion.

**c)** Soit $m \in T(M)$, $a \in A$ tel que $a \neq 0$ et $am = 0$. Alors, $af(m) = 0$, ce qui prouve que $f(m) \in T(N)$. Par conséquent, $f(T(M)) \subset T(N)$.

**d)** Considérons une suite exacte $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$. L'application naturelle $T(M') \to T(M)$ est la restriction de l'injection $i : M' \to M$ à $T(M') \subset M'$. Elle est donc injective.

Soit $m \in T(M)$ dont l'image $p(m)$ dans $T(M'') \subset M''$ est nulle. Cela signifie qu'il existe $m' \in M'$ tel que $m = i(m')$. Comme $m \in T(M)$, il existe $a \in A$, $a \neq 0$ tel que $am = 0$. Ainsi, $i(am') = ai(m') = am = 0$ et donc $am' \in \mathrm{Ker}\, i = 0$. Donc $am' = 0$ et $m' \in T(M')$. Cela prouve que $\mathrm{Ker}(p|_{T(M)}) = \mathrm{Im}(i|_{T(M')})$ (exactitude au milieu).

*Solution de l'exercice 6.6.7.* — **a)** Soit $P \in A[X]$. Si $X \cdot m = u(m)$, alors $X^n \cdot m = u^n(m)$, si bien que $P \cdot m = P(u)(m)$ et il y a au plus une structure de $A[X]$-module sur M telle que $X \cdot m = u(m)$.

Réciproquement, en posant $P \cdot m = P(u)(m)$, on définit bien une structure de $A[X]$-module sur M, puisque $(P + P') \cdot m = (P + P')(u)(m) = P(u)(m) + P'(u)(m)$ et que $(PP') \cdot m = (PP')(u)(m) = P(u)(P'(u)(m)) = P \cdot (P' \cdot m)$.

Réciproquement, étant donnée une structure de $A[X]$-module sur M, définissons $u(m)$ pour $m \in M$ par $X \cdot m = u(m)$. Il est immédiat que $u$ est A-linéaire, soit $u \in \mathrm{End}_A(M)$.

**b)** Soit $\varphi : \mathrm{M}_u \to \mathrm{N}_v$. Si $a$, $a' \in \mathrm{A}$ et $m$, $m' \in \mathrm{M}$ on a $\varphi(am + a'm') = \varphi(a' \cdot m + a' \cdot m') = a \cdot \varphi(m) + a' \cdot \varphi(m') = a\varphi(m) + a'\varphi(m')$, si bien que $\varphi$ est A-linéaire.

D'autre part, $\varphi(\mathrm{X} \cdot m) = \varphi(u(m)) = \mathrm{X} \cdot \varphi(m) = v(\varphi(m))$, si bien que $\varphi \circ u = v \circ \varphi$.

Réciproquement, tout homomorphisme A-linéaire $\mathrm{M} \to \mathrm{N}$ tel que $\varphi \circ u = v \circ \varphi$ induit un homomorphisme A[X]-linéaire $\mathrm{M}_u \to \mathrm{N}_v$.

**c)** On a $\mathrm{M}_u \simeq \mathrm{N}_v$ si et seulement s'il existe $\varphi : \mathrm{M} \to \mathrm{N}$ tel que $\varphi \circ u = v \circ \varphi$ qui soit bijectif et dont la bijection réciproque $\psi : \mathrm{N} \to \mathrm{M}$ vérifie $\psi \circ v = u \circ \psi$. Cette dernière condition est automatiquement vérifiée si $\varphi$ est bijectif. Ainsi, $\mathrm{M}_u \simeq \mathrm{M}_v$ si et seulement s'il existe un isomorphisme de A-modules $\varphi : \mathrm{M} \to \mathrm{M}$ tel que $v = \varphi \circ u \circ \varphi^{-1}$.

**d)** Si $\mathrm{A} = k$ est un corps et $\mathrm{M} = k^n$, les endomorphismes de M s'identifient à leur matrice. On trouve que $\mathrm{M}_u \simeq \mathrm{M}_v$ si et seulement si les matrices de $u$ et de $v$ sont conjuguées.

*Solution de l'exercice 6.6.8.* — **a)** Supposons qu'il existe $g\colon \mathrm{N} \to \mathrm{M}$ tel que $g \circ f = \mathrm{Id}_\mathrm{M}$. Si $m \in \operatorname{Ker} f$, $m = g(f(m)) = g(0) = 0$, donc $f$ est injectif. De plus, un élément $n \in \mathrm{N}$ peut s'écrire

$$n = f(g(n)) + (n - f(g(n)))$$

comme la somme d'un élément de $\operatorname{Im}(f)$ et d'un élément de $\operatorname{Ker} g$ puisque

$$g\big(n - f(g(n))\big) = g(n) - g(f(g(n)) = 0.$$

De plus, si $n \in \operatorname{Im} f \cap \operatorname{Ker} g$, soit $m \in \mathrm{M}$ tel que $n = f(m)$. On a alors $0 = g(n) = g(f(m)) = m$, donc $n = 0$. Par suite, $\operatorname{Im}(f) \oplus \operatorname{Ker}(g) = \mathrm{N}$ et $\operatorname{Im}(f)$ possède un supplémentaire dans N.

Réciproquement, supposons que $f$ est injectif et que $\operatorname{Im}(f)$ admet un supplémentaire P dans N. Définissons $g\colon \mathrm{N} \to \mathrm{M}$ comme suit. Soit $n \in \mathrm{N}$, on peut l'écrire de manière unique $n = f(m) + p$ avec $m \in \mathrm{M}$ et $p \in \mathrm{P}$. Posons $g(n) = m$. Alors, $g$ est A-linéaire : si $n = f(m) + p$ et $n' = f(m') + p'$, on a

$$an + a'n' = a(f(m) + p) + a'(f(m') + p') = f(am + a'm') + (ap + a'p')$$

et $g(an + a'n') = am + a'm' = ag(n) + a'g(n')$. De plus, si $m \in \mathrm{M}$, la décomposition $f(m) = f(m) + 0$ montre que $g(f(m)) = m$ si bien que $g \circ f = \mathrm{Id}_\mathrm{M}$.

**b)** Supposons que $f$ admet un inverse à droite $g$ tel que $f \circ g = \mathrm{Id}_\mathrm{N}$. Si $n \in \mathrm{N}$, on a donc $f(g(n)) = n$ et ainsi $n \in \operatorname{Im} f$, ce qui montre que $f$ est surjectif. De plus, si $m \in \mathrm{M}$, on peut écrire

$$m = g(f(m)) + (m - g(f(m)))$$

comme la somme d'un élément de $\operatorname{Im} g$ et d'un élément de $\operatorname{Ker} f$ puisque

$$f\big(m - g(f(m))\big) = f(m) - f(g(f(m)) = f(m) - f(m) = 0.$$

De plus, si $m \in \operatorname{Ker} f \cap \operatorname{Im} g$, écrivons $m = g(n)$ pour $n \in \mathrm{N}$. Alors, $0 = f(m) = f(g(n)) = n$, donc $m = g(n) = 0$ et $\operatorname{Ker} f \cap \operatorname{Im} g = 0$. Cela montre que $\operatorname{Ker} f \oplus \operatorname{Im} g = \mathrm{M}$ et $\operatorname{Ker} f$ possède un supplémentaire dans M.

Réciproquement, supposons que $f$ est surjectif et que $\operatorname{Ker}(f)$ admet un supplémentaire P dans M. Si $n \in \mathrm{N}$, alors montrons que $n$ admet un unique antécédent par $f$ dans P : en effet, si $m = f(n)$, décomposons $m = m_0 + p$ avec $m_0 \in \operatorname{Ker} f$ et $p \in \mathrm{P}$ ; on a alors $n = f(m) = f(p)$. Si $p$ et $p'$ sont deux antécédents, $p - p' \in \mathrm{P}$ a pour image 0 dans N donc $p - p' \in \operatorname{Ker} f \in \mathrm{P}$ et $p = p'$. Définissons $g\colon \mathrm{N} \to \mathrm{M}$ tel que $g(n)$ est l'unique élément de P tel que $f(g(n)) = n$.

Si $n$, $n' \in \mathrm{N}$ et si $a$, $a' \in \mathrm{A}$, soit $p$, $p'$ les éléments de P tels que $f(p) = n$, $f(p') = n'$. Alors, $ap + a'p'$ est un élément de P tel que $f(ap + a'p') = an + a'n'$, donc par définition,

$$g(an + a'n') = ap + a'p' = ag(n) + a'g(n').$$

Ainsi, $g$ est un homomorphisme de A-modules tel que $f \circ g = \mathrm{Id}_{\mathrm{N}}$.

*Solution de l'exercice 6.6.9.* — Soit $m$ un élément de M et $\mathrm{J} = (\mathrm{IM} : m) = \{a \in \mathrm{A} ; am \in \mathrm{IM}\}$. C'est un idéal de J qui contient évidemment I. Si $m \notin \mathrm{IM}$, on a de plus $\mathrm{J} \neq \mathrm{A}$ et il existe par suite un idéal maximal $\mathfrak{m}$ de A contenant J. Comme $\mathrm{J} \supset \mathrm{I}$, $\mathfrak{m} \supset \mathrm{I}$ et $\mathrm{M}_{\mathfrak{m}} = 0$. Par suite, l'image de $m$ dans $\mathrm{M}_{\mathfrak{m}}$ est nulle, ce qui signifie qu'il existe $a \notin \mathfrak{m}$ tel que $am = 0$. En particulier, $am \in \mathrm{IM}$ et $a \in \mathrm{J}$. Ceci contredit l'inclusion $\mathrm{J} \subset \mathfrak{m}$ et $\mathrm{J} = \mathrm{A}$. Autrement dit, $m \in \mathrm{IM}$.

*Solution de l'exercice 6.6.10.* — On rappelle qu'un idéal de A est la même chose qu'un sous-A-module de A.

Soit $\mathrm{I} \subset \mathrm{A}$ un idéal de A principal et engendré par un élément $a$ non diviseur de 0. Montrons que $a$ est une base de I sur A. En effet, l'application $\mathrm{A} \to \mathrm{I}$ définie par $x \mapsto ax$ est surjective (I étant engendré par $a$) ; elle est injective car si $ax = 0$, alors $x = 0$ (puisque $a$ n'est pas diviseur de 0 dans A).

Réciproquement, soit $\mathrm{I} \subset \mathrm{A}$ un idéal non nul de A qui est libre comme A-module. Soit $(a_j)_{j \in \mathrm{J}}$ une base de I. Comme $\mathrm{I} \neq 0$, J est non vide. Montrons que J est un singleton. Si J a deux éléments distints, $j$ et $k$, on peut écrire $0 = a_j(a_k) - a_k(a_j) = 0(a_k) + 0(a_j)$, si bien que 0 s'écrit de deux manières distinctes comme combinaison linéaire d'éléments de la base $(a_j)_{j \in \mathrm{J}}$, ce qui contredit le fait que I est un A-module libre. Soit alors $a$ la base de I. Cela entraîne que I est principal. De plus, si $ax = 0$, avec $x \neq 0$, on a deux expressions de $0 \in \mathrm{I}$ comme combinaison linéaire de $a$, ce qui est impossible si I est libre. Ainsi, $a$ n'est pas diviseur de 0 dans A.

*Solution de l'exercice 6.6.11.* — Si $x$ et $y$ sont deux éléments de K, écrivons $x = a/b$ et $y = c/d$ avec $a$, $b$, $c$ et $d$ des éléments de A tels $b \neq 0$, $d \neq 0$. On a ainsi

$bcx = ac = ady$. Si $a$ ou $c$ est non nul, cette relation prouve que la famille $\{x, y\}$ est liée ; si $a = c = 0$, on a $x = y = 0$ et la famille $\{x, y\}$ est encore liée.

Par suite, toute famille libre de K a au plus un élément. Comme $K \neq 0$, une famille génératrice de K a au moins un élément. Ainsi, une base de K, si elle existe a exactement un élément.

Soit donc $x \in K$, $x \neq 0$ et montrons que $x$ n'engendre pas K comme A-module. Si c'était le cas, on aurait $x^2 \in Ax$, donc $x \in A$. Mais alors, $Ax \subset A$ Comme $A \neq K$, $Ax \neq K$. Donc K n'a pas de base comme A-module.

*Solution de l'exercice 6.6.12.* — Si l'anneau est un corps, on sait par la théorie des espaces vectoriels que de tels exemples n'existent pas. On résoud les premières questions de l'exercice avec $A = \mathbf{Z}$.

**a)** Le module $\mathbf{Z}/2\mathbf{Z}$ n'est pas libre. (Il est fini non nul et si $e_1$ est un vecteur d'une base d'un $\mathbf{Z}$-module libre M, il fournit un isomorphisme $\mathbf{Z} \simeq e_1\mathbf{Z} \subset M$ et un sous-module infini de M.)

**b)** Dans $\mathbf{Z}^n$, notons $(e_1, \dots, e_n)$ la base canonique. Alors, la famille $(2e_1, \dots, 2e_n)$ est libre mais n'est pas une base : le vecteur $(1, \dots, 1)$ n'est pas dans le sous-module engendré par ces éléments.

**c)** Dans $\mathbf{Z}$, la famille $(2, 3)$ est génératrice et minimale puisque $2\mathbf{Z}$ et $3\mathbf{Z}$ ne sont pas isomorphes à $\mathbf{Z}$. Pourtant, la famille $(2, 3)$ n'est pas libre, comme le montre la relation $3 \times 2 - 2 \times 3 = 0$.

**d)** Le sous-module $2\mathbf{Z} \subset \mathbf{Z}$ ne peut pas avoir de supplémentaire : le quotient $\mathbf{Z}/2\mathbf{Z}$ est un $\mathbf{Z}$-module fini et tout sous-$\mathbf{Z}$-module non nul de $\mathbf{Z}$ est infini.

**e)** Pour cette question, on ne peut pas prendre $A = \mathbf{Z}$. Choisissons $A = \mathbf{Z}[X]$. C'est un A-module libre. Pourtant, l'idéal $(2, X)$ n'est pas libre. S'il l'était, il serait engendré par un seul élément $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{Z}[X]$ dont 2 et X seraient multiples. Nécessairement $n = 0$ puis $a_0 = 1$. Or, $1 \notin (2, X)$ puisque la relation $1 = 2P + XQ$ entraÓne que $1 = 2P(0)$, relation absurde.

*Solution de l'exercice 6.6.13.* — **a)** Soit $(\ell_1, \dots, \ell_r)$ une famille génératrice de $\operatorname{Ker} f$ et $(m_1, \dots, m_s)$ une famille génératrice de $\operatorname{Im} f$. Pour tout $i \in \{1, \dots, s\}$, soit $\ell'_i \in L$ tel que $f(\ell'_i) = m_i$. Montrons que la famille $(\ell_1, \dots, \ell_r, \ell'_1, \dots, \ell'_s)$ engendre L.

En effet, si $\ell \in L$, $f(\ell) \in M$. On peut donc écrire $f(\ell) = \sum_{i=1}^{s} a_i m_i$ et $\ell' = \ell - \sum_{i=1}^{s} a_i \ell'_i \in \operatorname{Ker} f$. On écrit alors $\ell' = \sum_{i=1}^{r} b_i \ell_i$, si bien que

$$\ell = \sum_{i=1}^{s} a_i \ell'_i + \sum_{i=1}^{r} b_i \ell_i.$$

**b)** On raisonne comme dans la question précédente. Soit $(\ell_1, \dots, \ell_p)$ une base de $\operatorname{Ker} f$ et $(m_1, \dots, m_q)$ une base de $\operatorname{Im} f$. On écrit $m_i = f(\ell'_i)$ pour $1 \leq i \leq$

$q$. D'après la question précédente, la famille $(\ell_1, \ldots, \ell_p, \ell'_1, \ldots, \ell'_q)$ engendre L. D'autre part, si on a une relation de dépendance linéaire

$$\sum_{i=1}^{p} a_i \ell_i + \sum_{i=1}^{q} b_i \ell'_i = 0,$$

on lui applique $f$. On obtient alors

$$\sum_{i=1}^{q} b_i m_i = 0$$

d'où $b_1 = \cdots = b_q = 0$ puisque la famille $(m_1, \ldots, m_q)$ est libre. Alors, $\sum_{i=1}^{p} a_i \ell_i = 0$ et, la famille $(\ell_1, \ldots, \ell_p)$ étant libre, $a_i = 0$ pour tout $i$, ce qu'il fallait démontrer.

# 7 Modules de type fini. Anneaux noethériens

*On commence par donner quelques résultats sur les modules de type fini sur un anneau quelconque, notamment l'important théorème de* NAKAYAMA. *Nous introduisons ensuite les modules et anneaux noethériens. Cette condition, apparemment très simple, procure aux modules et anneaux envisagés énormément de propriétés supplémentaires. Un bon exemple d'anneau noethérien est fourni par les algèbres de type fini sur un corps. Nous démontrons à ce sujet un théorème de* HILBERT.

## 7.1. Modules de type fini

DÉFINITION 7.1.1. — *Soit* A *un anneau. On dit qu'un* A*-module* M *est de* type fini *s'il existe une partie finie* $S \subset M$ *telle que* $M = \langle S \rangle$.

PROPOSITION 7.1.2. — *Soit* A *un anneau, soit* M *un* A*-module et soit* N *un sous-module de* M.

*a) On suppose que* M *est de type fini. Alors,* M/N *est de type fini.*

*b) On suppose que* N *et* M/N *sont de type fini. Alors,* M *est de type fini.*

*Démonstration.* — Notons $\mathrm{cl} : M \to M/N$ la surjection canonique.

a) En fait, $M/N = \langle \mathrm{cl}(S) \rangle$. En effet, si $\mathscr{P}$ est un sous-module de M/N qui contient cl(S), $\mathrm{cl}^{-1}(\mathscr{P})$ est un sous-module de M qui contient $\mathrm{cl}^{-1}(\mathrm{cl}(S))$, donc qui contient P. Comme S engendre M, $\mathrm{cl}^{-1}(\mathscr{P}) = M$ et $\mathscr{P} = \mathrm{cl}(M) = M/N$.

b) Comme M/N est supposé de type fini, il existe une partie finie $\bar{S}$ de M/N telle que $\langle \bar{S} \rangle = M/N$. Puisque l'homomorphisme cl est surjectif, il existe pour tout $\bar{s} \in \bar{S}$ un élément $s \in M$ tel que $\bar{s} = \mathrm{cl}(s)$. L'ensemble de ces $s$ est alors une partie finie S de M telle que cl(S) engendre M. Soit aussi T une partie finie de N telle que $\langle T \rangle = N$. Montrons maintenant que $\langle S \cup T \rangle = M$.

Soit P un sous-module de M contenant $\langle S \cup T \rangle$. Donc P contient T, et par définition, P contient $\langle T \rangle = N$. Ceci implique l'égalité $\mathrm{cl}^{-1}(\mathrm{cl}(P)) = P + N = P$. Or,

$\mathrm{cl}(\mathrm{P})$ est un sous-module de $\mathrm{M}/\mathrm{N}$ qui contient $\mathrm{cl}(\mathrm{S}) = \bar{\mathrm{S}}$. Par suite, $\mathrm{cl}(\mathrm{P}) = \mathrm{M}/\mathrm{N}$. Finalement, $\mathrm{P} = \mathrm{cl}^{-1}(\mathrm{cl}(\mathrm{P})) = \mathrm{cl}^{-1}(\mathrm{M}/\mathrm{N}) = \mathrm{M}$. □

*Remarque 7.1.3.* — On peut démontrer cette proposition de manière concrète : prendre un élément et l'écrire comme combinaison linéaire plus ou moins explicite. Nous préférons plutôt une approche fondée la définition de « module engendré » comme intersection de sous-modules car elle prépare mieux aux manipulations ultérieures de suites croissantes de sous-modules.

COROLLAIRE 7.1.4. — *a) Si* M *et* N *sont des* A*-modules de type fini,* $\mathrm{M} \times \mathrm{N}$ *est un* A*-module de type fini.*

*b) Si* M *est un* A*-module de type fini et si* $n$ *est un entier,* $n \geq 1$*,* $\mathrm{M}^n$ *est de type fini.*

*c) Si* M *est un* A*-module, et si* P *et* N *sont deux sous-modules de* M *de type fini, alors* $\mathrm{P} + \mathrm{N}$ *est de type fini.*

*Démonstration.* — a) Considérons l'homomorphisme $f\colon \mathrm{M} \times \mathrm{N} \to \mathrm{N}$ défini par $f(m,n) = n$. Il est surjectif et son noyau est l'ensemble des $(m,0)$, donc est isomorphe à M. D'après la proposition précédente, $\mathrm{M} \times \mathrm{N}$ est de type fini.

b) Il se démontre par récurrence sur $n$. C'est vrai si $n = 1$ et si c'est vrai pour $n$, l'égalité $\mathrm{M}^{n+1} = \mathrm{M}^n \times \mathrm{M}$ montre que c'est vrai pour $n+1$.

c) Par définition, l'image de l'homomorphisme $\mathrm{P} \times \mathrm{N} \to \mathrm{M}$ défini par $(p,n) \mapsto p+n$ est égale à $\mathrm{P} + \mathrm{N}$. Comme $\mathrm{P} \times \mathrm{N}$ est de type fini, $\mathrm{P} + \mathrm{N}$ aussi. □

*Exercice 7.1.5.* — Soit A un anneau, M un A-module et S une partie multiplicative de A. Si M est un A-module de type fini, alors $\mathrm{S}^{-1}\mathrm{M}$ est un $\mathrm{S}^{-1}\mathrm{A}$-module de type fini.

THÉORÈME 7.1.6 (Nakayama). — *Soit* M *un* A*-module de type fini et soit* I *un idéal de* A *tel que* $\mathrm{M} = \mathrm{IM}$*. Alors, il existe* $a \in \mathrm{I}$ *tel que* $(1+a)\mathrm{M} = 0$.

COROLLAIRE 7.1.7. — *Soit* A *un anneau et soit* I *un idéal de* A *contenu dans le radical de Jacobson. Soit* M *un* A*-module de type fini et soit* N *un sous-module de* M*. Si* $\mathrm{M} = \mathrm{N} + \mathrm{IM}$*, alors* $\mathrm{M} = \mathrm{N}$.

*Démonstration.* — On applique le théorème de Nakayama au A-module $\mathrm{M}/\mathrm{N}$. Il est de type fini et vérifie en outre $\mathrm{M}/\mathrm{N} = \mathrm{I}(\mathrm{M}/\mathrm{N})$. (Si $x \in \mathrm{M}/\mathrm{N}$, soit $m \in \mathrm{M}$ tel que $x = \mathrm{cl}(m)$. Comme $\mathrm{M} = \mathrm{N} + \mathrm{IM}$, il existe $n \in \mathrm{N}$, des $a_i \in \mathrm{I}$ et $m_i \in \mathrm{M}$ tels que $m = n + \sum a_i m_i$. Alors, $\mathrm{cl}(m) = \sum a_i \,\mathrm{cl}(m_i) \in \mathrm{I}(\mathrm{M}/\mathrm{N})$.) D'après le théorème 7.1.6, il existe $a \in \mathrm{I}$ tel que $(1+a)(\mathrm{M}/\mathrm{N}) = 0$.

Or, comme I est contenu dans tout idéal maximal de A, $1+a$ n'appartient à aucun idéal maximal, donc est inversible (voir aussi l'exercice 4.3.10). Il en résulte que $\mathrm{M}/\mathrm{N} = 0$, c'est-à-dire $\mathrm{M} = \mathrm{N}$. □

Un cas particulier important est le suivant.

COROLLAIRE 7.1.8. — *Soit* A *un anneau local*[1], *d'idéal maximal* $\mathfrak{m}$. *Soit* M *un* A*-module de type fini et soit* N *un sous-module de* M *tel que* $M = N + \mathfrak{m}M$. *Alors,* $M = N$.

*Démonstration.* — En effet, dans ce cas, $\mathfrak{m}$ est le radical de Jacobson de A. □

*Démonstration du théorème de Nakayama.* — Nous démontrons ce théorème par récurrence sur le nombre d'éléments d'une partie génératrice de M. Si M est engendré par 0 élément, $M = 0$ et on peut prendre $a = 0$. Soit maintenant $n \geq 1$ et supposons le lemme démontré pour tout A-module engendré par strictement moins de $n$ éléments. Soit M un A-module tel que $M = IM$ et qui est engendré par $n$ éléments. Soit $S \subset M$ de cardinal $n$ tel que $M = \langle S \rangle$. Soit $x \in S$ et posons $S' = S \setminus \{x\}$ de sorte que $S'$ a strictement moins de $n$ éléments.

Soit $N = M/Ax$ le quotient de M par le sous-module de M engendré par $x$. Ainsi, N est engendré par les classes des éléments de $S'$. Comme $M = IM$, on a $N = IN$. Par récurrence, il existe $a \in I$ tel que $(1 + a)N = 0$. Cela signifie que $(1 + a)M \subset Ax$.

Comme $x \in M = IM$, on peut écrire

$$x = bx + \sum_{s' \in S'} c_{s'} s'$$

où $b$ et les $b_{s'}$ sont dans I. Alors,

$$(1 - b)(1 + a)x = (1 + a)\left(\sum_{s'} b_{s'} s'\right) = \sum_{s' \in S'} b_{s'}(1 + a)s'$$

Pour tout $s'$, on a $(1 + a)s' \in Ax$, d'où $c_{s'} \in A$ tel que $(1 + a)s' = c_{s'}x$. On constate alors que

$$(1 - b)(1 + a)x = \left(\sum_{s' \in S'} b_{s'} c_{s'}\right) x = b'x \qquad \text{avec } b' \in I.$$

Finalement, si l'on pose $a' = a - b - ab - b'$, on a $(1 + a')x = 0$. Par suite, on a

$$(1 + a)(1 + a')M \subset (1 + a')Ax = 0$$

et $(1 + a)(1 + a') = 1 + (a + a' + aa')$ annule M, ce qu'il fallait démontrer puisque $a + a' + aa' \in I$. □

Voici une application « amusante » du théorème de Nakayama.

PROPOSITION 7.1.9. — *Soit* A *un anneau, soit* M *un* A*-module de type fini et soit* $u \in \mathrm{End}_A(M)$ *un endomorphisme surjectif. Alors, u est un isomorphisme.*

[1] Rappelons, cf. page 54, que cela signifie que A possède un unique idéal maximal.

*Démonstration.* — Munissons M d'une structure de A[X]-module en posant, si $\mathrm{P} = \sum_{k=0}^{n} a_k \mathrm{X}^k \in \mathrm{A}[\mathrm{X}]$ et $m \in \mathrm{M}$,

$$\mathrm{P} \cdot \mathrm{M} = \mathrm{P}(u)(m) = \sum_{k=0}^{n} a_k u^k(m).$$

En tant que A[X]-module, M est *a fortiori* de type fini. De plus, comme $u$ est surjectif, on a $\mathrm{M} = u(\mathrm{M}) = \mathrm{X} \cdot \mathrm{M}$, d'où $\mathrm{M} = (\mathrm{X})\mathrm{M}$. D'après le théorème de Nakayama, il existe $\mathrm{P} = \mathrm{XQ} \in (\mathrm{X})$ tel que $(1 + \mathrm{P}) \cdot \mathrm{M} = 0$. Par suite, pour tout $m \in \mathrm{M}$, $m + \mathrm{Q}(u)(u(m))) = 0$ et l'homomorphisme $v\colon m \mapsto -\mathrm{Q}(u)(m)$ est un inverse à gauche de $u$. Comme $\mathrm{Q}(u) \circ u = u \circ \mathrm{Q}(u)$, $v$ est l'inverse de $u$ qui est donc un isomorphisme. □

Une démonstration fréquente du théorème de Nakayama repose sur le théorème de Cayley–Hamilton. Elle a l'avantage de fournir un élément explicite de $1 + \mathrm{I}$ qui annule M.

*Autre démonstration du théorème de Nakayama.* — Soit $(m_1, \ldots, m_r)$ une famille de $r$ éléments qui engendre M. Comme $\mathrm{M} = \mathrm{IM}$, il existe une famille $(a_{ij})_{1 \leq i,j \leq r}$ d'éléments de I telle que pour tout $i$,

$$m_i = \sum_{j=1}^{r} a_{ij} m_j,$$

Autrement dit, si A désigne la matrice des $a_{ij}$, la matrice $\mathrm{I}_r - \mathrm{A}$ annule le vecteur colonne $(m_1; \ldots; m_r)$ de $\mathrm{M}^r$. (Une matrice $r \times r$ d'éléments de A opère sur $\mathrm{M}^r$ avec les formules habituelles.) Soit B la matrice transposée de la matrice des cofacteurs de $\mathrm{I}_r - \mathrm{A}$. C'est une matrice $r \times r$ à coefficients dans A telle que

$$\mathrm{B} \cdot (\mathrm{I}_r - \mathrm{A}) = (\mathrm{I}_r - \mathrm{A})\mathrm{B} = \det(\mathrm{I}_r - \mathrm{A})\mathrm{I}_r.$$

Par suite, la matrice $\det(\mathrm{I}_r - \mathrm{A})\mathrm{I}_r$ annule le vecteur colonne $(m_1; \ldots; m_r)$ de $\mathrm{M}^r$, autrement dit, $\det(\mathrm{I}_r - \mathrm{A})$ annule $m_1$, …, $m_r$. Comme $(m_1; \ldots; m_r)$ engendre M, $\det(\mathrm{I}_r - \mathrm{A})\mathrm{M} = 0$.

Il reste à remarquer que la définition du déterminant de $\mathrm{I}_r - \mathrm{A}$

$$\det(\mathrm{I}_r - \mathrm{A}) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_\sigma \prod_{i=1}^{n} (\delta_{i\sigma(i)} - a_{i\sigma(i)})$$

montre qu'il est de la forme $1 + a$ avec $a \in \mathrm{I}$. Le théorème est donc démontré. □

## 7.2. Modules noethériens. Généralités

PROPOSITION 7.2.1. — *Soit* A *un anneau et soit* M *un* A*-module. Les propriétés suivantes sont équivalentes :*

(1) *tout sous-module de* M *est de type fini ;*
(2) *toute suite croissante de sous-modules de* M *est stationnaire ;*
(3) *toute famille de sous-modules de* M *admet un élément maximal.*

DÉFINITION 7.2.2. — *Un* A*-module qui vérifie les propriétés ci-dessus est dit* noethérien. *Si* A *est un* A*-module noethérien, on dit que* A *est un* anneau noethérien.

*Remarque 7.2.3.* — Les sous-A-modules d'un anneau A sont ses idéaux. Ainsi, un anneau A est noethérien si et seulement si l'une des propriétés (équivalentes) ci-dessous est satisfaite :

(1) tout idéal de A est de type fini ;
(2) toute suite croissante d'idéaux de A est stationnaire.

*Exemple 7.2.4.* — Un anneau principal est noethérien. Relire la démonstration du théorème 5.2.6 selon lequel un anneau principal est factoriel. Un point crucial pour la démonstration de l'existence d'une décomposition en facteurs premiers réside dans le fait que toute suite croissante d'idéaux (principaux) est stationnaire.

*Démonstration de la proposition.* — a) Supposons que tout sous-module de M est de type fini et considérons une suite croissante $(M_n)_{n\in\mathbf{N}}$ de sous-modules de M. Soit $N = \bigcup M_n$ la réunion des $M_n$. Comme la réunion est croissante, N est un sous-module de A. Par hypothèse, il est de type fini : il existe $S \subset N$, S fini, tel que $N = \langle S\rangle$. Pour tout $s \in S$, il existe un entier $n_s \in \mathbf{N}$ tel que $s \in M_n$ pour $n \geq n_s$. Posons $\nu = \max(n_s)$, de sorte que $S \subset M_\nu$. Par suite, $N = \langle S\rangle$ est contenu dans $M_\nu$. Finalement, la suite d'inclusions $M_\nu \subset M_n \subset N \subset M_\nu$ pour $n \geq \nu$ montre que pour $n \geq \nu$, $M_n = M_\nu$. La suite est ainsi stationnaire.

b) Supposons que toute suite croissante de sous-modules de M est stationnaire et soit $(M_i)_{i\in I}$ une famille de sous-modules de M. Supposons par l'absurde qu'elle n'admette pas d'élément maximal. Choisissons $i_1 \in I$ ; ainsi, $M_{i_1}$ n'est pas maximal dans la famille $(M_i)$. Il existe alors $i_2 \in I$ tel que $M_{i_1} \subsetneq M_{i_2}$. Mais $M_{i_2}$ n'est pas non plus maximal, d'où l'existence de $i_3 \in I$, etc. On obtient ainsi une suite strictement croissante de sous-modules de M,

$$M_{i_1} \subsetneq M_{i_2} \subsetneq \dots$$

et une telle suite n'étant par définition pas stationnaire, on a une contradiction. (*Cette partie de la démonstration n'a rien à voir avec les modules, elle est valide dans tout ensemble ordonné.*)

c) Supposons que toute famille de sous-modules de M admet un élément maximal et montrons que tout sous-module de M est de type fini. Soit ainsi N un sous-module de M et considérons l'ensemble $\mathscr{S}_N$ des sous-modules de N qui sont de type fini. Par hypothèse, il admet un élément maximal ; soit $N'$ un tel

sous-module. Par définition, $N' \subset N$, $N'$ est de type fini et aucun sous-module de N qui contient strictement $N'$ n'est de type fini. Supposons par l'absurde que $N' \neq N$. Il existe ainsi $m \in N \setminus N'$. Le sous-module $N'' = N' + Am$ de M est de type fini et est contenu dans N. Comme $m \notin N'$, $N'' \neq N'$. Par suite, $N'' \in \mathscr{S}_N$, ce qui est absurde, $N'$ étant maximal dans $\mathscr{S}_N$. Donc $N' = N$ et N est de type fini. □

PROPOSITION 7.2.5. — *Soit* A *un anneau, soit* M *un* A*-module,* N *un sous-module de* A. *Alors,* M *est un* A*-module noethérien si et seulement si* N *et* M/N *sont des* A*-modules noethériens.*

*Démonstration.* — Supposons que M est un A-module noethérien. Comme tout sous-module de N est aussi un sous-module de M, tout sous-module de N est de type fini, donc N est noethérien. Si $\mathscr{P}$ est un sous-module de M/N, son image réciproque $\mathrm{cl}^{-1}(\mathscr{P})$ par l'homomorphisme canonique $\mathrm{cl}\colon M \to M/N$ est un sous-module de type fini de M. Comme $\mathscr{P} = \mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{P}))$, $\mathscr{P}$ est l'image d'un module de type fini, donc est de type fini. Ainsi, M/N est noethérien.

Supposons que N et M/N sont des A-modules noethériens. Soit $(P_n)$ une suite croissante de sous-modules de M. Posons $Q_n = P_n \cap N$. Par définition, les suites croissantes $(\mathrm{cl}(P_n))$ et $(P_n \cap N)$ de sous-modules de M/N (resp. de N) sont stationnaires. Fixons donc $\nu$ tel que si $n \geq \nu$,

$$\mathrm{cl}(P_n) = \mathrm{cl}(P_\nu) \quad \text{et} \quad P_n \cap N = P_\nu \cap N.$$

Nous allons montrer que pour $n \geq \nu$, $P_n = P_\nu$, ce qui établira que la suite $(P_n)$ est stationnaire.

Fixons donc $n \geq \nu$ et soit $p \in P_n$. On a $\mathrm{cl}(p) \in \mathrm{cl}(P_n) = \mathrm{cl}(P_\nu)$, si bien qu'il existe $p' \in P_\nu$ tel que $\mathrm{cl}(p) = \mathrm{cl}(p')$. Alors, $p - p'$ appartient à $P_n$ et vérifie $\mathrm{cl}(p - p') = 0$, d'où $p - p' \in P_n \cap N$. Par suite, $p - p' \in P_\nu \cap N$ et $p = p' + (p - p')$ appartient à $P_\nu$. Ainsi, $P_n \subset P_\nu$, d'où l'égalité. $\mathrm{cl}(P_n) = \mathrm{cl}(P_\nu)$ si $n \geq \nu$. □

COROLLAIRE 7.2.6. — *Produits, puissances de modules noethériens sont des modules noethériens.*

PROPOSITION 7.2.7. — *Soit* A *un anneau et soit* S *une partie multiplicative de* A. *Si* M *est un* A*-module noethérien,* $S^{-1}M$ *est un* $S^{-1}A$*-module noethérien.*

*Démonstration.* — Soit $\mathscr{N}$ un sous-$S^{-1}A$-module de $S^{-1}A$. D'après la proposition 6.5.10, il existe un sous-module N de M tel que $\mathscr{N} = S^{-1}N$. Comme M est un A-module noethérien, N est de type fini et par suite, $\mathscr{N}$ est de type fini. Ainsi, $S^{-1}M$ est un $S^{-1}A$-module noethérien. □

COROLLAIRE 7.2.8. — *Soit* A *un anneau noethérien.*

*Si* I *est un idéal de* A, *l'anneau quotient* A/I *est noethérien. Si* S *est une partie multiplicative de* A, *l'anneau localisé* $S^{-1}A$ *est noethérien.*

*Démonstration.* — D'après la proposition 7.2.5, A/I est un A-module noethérien. Mais un sous-A-module de A/I n'est autre qu'un idéal de A/I. Par suite, A/I est un A/I-module noethérien. C'est donc un anneau noethérien.

*Autre démonstration.* — Soit $\mathscr{J}$ un idéal de A/I. Par la surjection canonique $\mathrm{cl}\colon \mathrm{A} \to \mathrm{A/I}$, il lui correspond un idéal $\mathrm{J} = \mathrm{cl}^{-1}(\mathscr{J})$ de A qui contient I. Puisque A est un anneau noethérien, J est de type fini, $\mathrm{J} = (a_1, \dots, a_r)$. Alors, $\mathscr{J} = \mathrm{cl}(\mathrm{J}) = (\mathrm{cl}(a_1), \dots, \mathrm{cl}(a_r))$ est de type fini.

D'après la proposition 7.2.7, $\mathrm{S}^{-1}\mathrm{A}$ est un $\mathrm{S}^{-1}\mathrm{A}$-module noethérien. Par définition, c'est donc un anneau noethérien. □

PROPOSITION 7.2.9. — *Soit* A *un anneau,* M *un* A*-module de type fini. Alors, pour tout module noethérien* N, $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})$ *est un* A*-module noethérien.*

*Démonstration.* — Comme M est de type fini, on peut considérer une famille finie $(m_1, \dots, m_n)$ d'éléments de M qui l'engendrent. On a alors un homomorphisme canonique

$$\theta\colon \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N}) \to \mathrm{N}^n, \qquad \varphi \mapsto \theta(\varphi) = (\varphi(m_1), \dots, \varphi(m_n)).$$

C'est effectivement un homomorphisme car pour $\varphi$ et $\psi$ dans $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})$ et $a$ et $b$ dans A, on a

$$\begin{aligned}\theta(a\varphi + b\psi) &= ((a\varphi + b\psi)(m_1), \dots, (a\varphi + b\psi)(m_n)) \\ &= (a\varphi(m_1) + b\psi(m_1), \dots, a\varphi(m_n) + b\psi(m_n)) \\ &= a(\varphi(m_1), \dots, \varphi(m_n)) + b(\psi(m_1, \dots, \psi(m_n)) \\ &= a\theta(\varphi) + b\theta(\psi).\end{aligned}$$

Il est injectif car si un homomorphisme de M dans N est nul en tous les $m_i$, il s'annule en toute combinaison linéaire des $m_i$ donc sur M.

Ainsi, $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})$ est isomorphe à un sous-module de $\mathrm{N}^n$. Comme N est un A-module noethérien, $\mathrm{N}^n$ aussi et $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})$ est un A-module noethérien. □

COROLLAIRE 7.2.10. — *Soit* A *un anneau noethérien. Si* M *et* N *sont deux* A*-modules de type fini,* $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})$ *est un* A*-module de type fini.*

## 7.3. Algèbres de polynômes

Le théorème suivant a été démontré par D. Hilbert lorsque $\mathrm{A} = \mathbf{Z}$.

THÉORÈME 7.3.1 (Hilbert). — *Si* A *est un anneau noethérien, l'anneau* A[X] *est noethérien.*

*Démonstration.* — Soit I un idéal de A[X]. Si $n \geq 0$, soit $I_n$ l'ensemble des coefficients du terme de degré $n$ des polynômes de I qui sont de degré $\leq n$. Alors, $I_n$ est un idéal de A. En effet, si $x$ et $y \in I_n$, il existe P et Q dans I de degrés $\leq n$ dont les coefficients de $X^n$ sont $x$ et $y$ respectivement. Alors, si $a$ et $b \in A$, le coefficient de $X^n$ dans le polynôme $aP + bQ$ est $ax + by$, et $aP + bQ$ est un polynôme de O de degré $\leq n$. De plus, comme le polynôme nul appartient à I, $0 \in I_n$.

Remarquons que la suite $(I_n)$ est stationnaire : si $P \in I$ est de degré $\leq n$, $XP \in I$ est de degré $\leq n+1$ le coefficient de $X^{n+1}$ dans XP est celui de $X^n$ dans P. Ainsi, $I_n \subset I_{n+1}$.

Comme A est noethérien, la suite $(I_n)_n$ est stationnaire. Soit $\nu \in$

l'existence d'un (unique) homomorphisme de A-algèbres $\varphi\colon \mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_r] \to \mathrm{B}$ tel que $\varphi(\mathrm{X}_i) = b_i$ pour tout $i \in \{1;\dots;r\}$. Comme $\mathrm{B} = \mathrm{A}[\mathrm{S}]$, $\varphi$ est surjectif. Son noyau est un idéal I de $\mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_r]$ et B est isomorphe à un quotient de l'anneau $\mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_r]$.

Par suite, B est noethérien. □

PROPOSITION 7.3.5. — *Soit k un anneau,* A *une k-algèbre de type fini et* B *une* A*-algèbre de type fini. Alors,* B *est une k-algèbre de type fini.*

*Démonstration.* — Soit $(a_1,\dots,a_r)$ une famille d'éléments de A telle que $\mathrm{A} = k[a_1,\dots,a_r]$ et soit $(b_1,\dots,b_s)$ une famille d'éléments de B telle que $\mathrm{B} = \mathrm{A}[b_1,\dots,b_s]$.[(2)] Montrons alors que $\mathrm{B} = k[a_1,\dots,a_r,b_1,\dots,b_s]$. Il suffit de montrer que tout élément $b \in \mathrm{B}$ est un polynôme à coefficients dans $k$ en les $a_j$ et $b_j$. Or, il existe $\mathrm{P} \in \mathrm{A}[\mathrm{Y}_1,\dots,\mathrm{Y}_s]$ tel que $b = \mathrm{P}(b_1,\dots,b_s)$. Écrivons

$$\mathrm{P} = \sum_{m\in\mathbf{N}^s} p_m \mathrm{Y}_1^{m_1}\dots\mathrm{Y}_s^{m_s},$$

où les $p_m$ sont des éléments de A. Pour tout multi-indice $m$, soit $\mathrm{P}_m \in k[\mathrm{X}_1,\dots,\mathrm{X}_r]$ tel que $p_m = \mathrm{P}_m(a_1,\dots,a_r)$. Alors, on a

$$\begin{aligned} b &= \mathrm{P}(b_1,\dots,b_r)\\ &= \sum_m p_m b_1^{m_1}\dots b_s^{m_s}\\ &= \sum_m \mathrm{P}_m(a_1,\dots,a_r) b_1^{m_1}\dots b_s^{m_s}\\ &= \mathrm{Q}(a_1,\dots,a_r,b_1,\dots,b_s) \end{aligned}$$

où Q est le polynôme de $\mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_r,\mathrm{Y}_1,\dots,\mathrm{Y}_s]$ défini par

$$\mathrm{Q}(\mathrm{X}_1,\dots,\mathrm{X}_r,\mathrm{Y}_1,\dots,\mathrm{Y}_s) = \sum_m \mathrm{P}_m(\mathrm{X}_1,\dots,\mathrm{X}_r)\mathrm{Y}_1^{m_1}\dots\mathrm{Y}_s^{m_s}.$$

La proposition est donc démontrée. □

## 7.4. Un théorème de Hilbert

Pour motiver ce paragraphe, donnons d'abord un exemple important.

DÉFINITION 7.4.1. — *Soit k un anneau. Les* polynômes symétriques élémentaires *de* $k[\mathrm{X}_1,\dots,\mathrm{X}_n]$ *sont les polynômes :*

$$\mathrm{S}_r(\mathrm{X}) = \sum_{1\le i_1<\dots<i_r\le} \mathrm{X}_{i_1}\mathrm{X}_{i_2}\dots\mathrm{X}_{i_r}, \qquad 1 \le r \le n.$$

(2) *Stricto sensu,* on devrait écrire des homomorphismes $f\colon k \to \mathrm{A}$ et $g\colon \mathrm{A} \to \mathrm{B}$, noter $f(x)a$ si $x \in k$ et $a \in \mathrm{A}$, etc. Conformément à la convention annoncée page 16 on omet ces homomorphismes de la notation.

Autrement dit, les $S_r$ vérifient la relation

$$(T - X_1) \dots (T - X_n) = T^n - S_1(X)T^{n-1} + \cdots + (-1)^n S_n.$$

Il est évident que les polynômes symétriques élémentaires sont *symétriques*, un polynôme $P \in k[X_1, \dots, X_n]$ étant dit symétrique si pour tout $\sigma \in \mathfrak{S}_n$,

$$P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n).$$

THÉORÈME 7.4.2. — *Soit $k$ un anneau et soit $P \in k[X_1, \dots, X_n]$ un polynôme symétrique. Alors, il existe un unique polynôme $Q \in k[Y_1, \dots, X_n]$ tel que*

$$P(X_1, \dots, X_n) = Q(S_1(X), \dots, S_n(X)).$$

De manière un peu imprécise, *toute fonction symétrique des racines d'un polynôme peut s'exprimer à l'aide des fonctions symétriques élémentaires des racines.*

*Démonstration.* — Remarquons que pour tout $i$, $S_i$ est un polynôme homogène de degré $i$. Convenons d'appeler poids d'un monôme $Y_1^{p_1} \dots Y_n^{p_n}$ l'entier $p_1 + 2p_2 + \cdots + np_n$ et poids d'un polynôme $Q \in k[Y]$ le maximum des poids des monômes qui constituent Q. Ainsi, si Q est de poids $\leq d$, le polynôme $Q(S_1(X), \dots, S_n(X))$ est de degré $\leq d$.

Nous allons démontrer l'existence d'un polynôme Q par récurrence sur $n$, puis par récurrence sur le degré de P. Nous allons de plus montrer que Q est de poids $\leq \deg P$. Si $n = 1$, on a $X_1 = S_1$ et le résultat est clair. Supposons le vérifié dans le cas de $n - 1$ variables.

Le résultat est vrai si P est de degré $d = 0$. Supposons qu'il est vérifié en degré $< d$. Considérons alors le polynôme

$$P(X_1, \dots, X_{n-1}, 0) \in k[X_1, \dots, X_{n-1}].$$

Il est symétrique, si bien qu'il existe $Q_1 \in k[Y_1, \dots, Y_{n-1}]$ de poids $\leq \deg P$ tel que

$$P(X_1, \dots, X_{n-1}, 0) = Q_1(S_1(X_1, \dots, X_{n-1}), \dots, S_{n-1}(X_1, \dots, X_{n-1})).$$

Le polynôme

$$P_1(X_1, \dots, X_n) = P(X_1, \dots, X_n) - Q_1(S_1(X_1, \dots, X_n), \dots, S_{n-1}(X_1, \dots, X_n))$$

est symétrique, de degré $\leq d$ et vérifie $P_1(X_1, \dots, X_{n-1}, 0) = 0$. Il est donc multiple de $X_n$. Comme il est symétrique, il est multiple de $X_i$ pour tout $i$. Alors, $P_1$ est multiple de $X_1 \dots X_n$. (Tout monôme $X_1^{p_1} \dots X_n^{p_n}$ qui intervient dans $P_1$ est multiple de $X_i$ pour tout $i$, donc chaque $p_i \geq 1$.) On peut écrire

$$P_1(X_1, \dots, X_n) = (X_1 \dots X_n)P_2(X_1, \dots, X_n)$$

et, $P_1$ étant symétrique, $P_2$ l'est aussi. Comme il est de degré $< d$, il existe par récurrence un polynôme $Q_2 \in k[Y_1, \dots, Y_n]$ de poids $< d$ tel que

$$P_2(X_1, \dots, X_n) = Q_2(S_1, \dots, S_n).$$

Par conséquent,

$$P(X_1, \dots, X_n) = Q_1(S_1, \dots, S_n) + Q_2(S_1, \dots, S_n)$$

et il suffit de poser $Q = Q_1 + Q_2$.

Montrons maintenant l'unicité. Pour cela, il suffit de montrer que si $Q \in k[Y_1, \dots, Y_n]$ vérifie $Q(S_1, \dots, S_n) = 0$, alors $Q = 0$. On raisonne par récurrence sur $n$, puis sur le degré de Q.

Développons Q dans $k[Y_1, \dots, Y_{n-1}][Y_n]$ :

$$Q(Y_1, \dots, Y_n) = Q_d(Y_1, \dots, Y_{n-1})Y_n^d + \cdots + Q_0(Y_1, \dots, Y_{n-1})$$

et

$$\begin{aligned} 0 = Q(S_1, \dots, S_n) \\ &= Q_d(S_1(X_1, \dots, X_n), \dots, S_{n-1}(X_1, \dots, X_n))S_n^d + \dots \\ &\qquad + Q_0(S_1(X_1, \dots, X_n), \dots, S_{n-1}(X_1, \dots, X_n)). \end{aligned}$$

Si l'on substitue $X_n = 0$ dans cette dernière relation, $S_n = 0$ et on obtient la relation

$$0 = Q_0(S_1(X_1, \dots, X_{n-1}), \dots, S_{n-1}(X_1, \dots, X_{n-1})).$$

Par récurrence, sur $n$, $Q_0 = 0$.

Alors, le polynôme

$$R(Y_1, \dots, Y_n) = Q_d(Y_1, \dots, Y_{n-1})Y_n^{d-1} + \cdots + Q_1(Y_1, \dots, Y_{n-1})$$

vérifie $R(S_1, \dots, S_n) = 0$. (On utilise ici le fait que $S_n$ est simplifiable dans $k[X_1, \dots, X_n]$.) Comme il est de degré $< \deg Q$, on a $R = 0$. Par suite, $Q = 0$. □

PROPOSITION 7.4.3 (Reformulation). — *Soit $k$ un anneau, soit $A$ l'anneau $k[X_1, \dots, X_n]$ et considérons l'action du groupe symétrique $\mathfrak{S}_n$ sur $A$ par permutation des variables :*

$$\sigma(P) = P(X_{\sigma^{-1}(1)}, \dots, X_{\sigma^{-1}(n)}).$$

*Alors, l'homomorphisme naturel :*

$$k[Y_1, \dots, Y_n] \to A^{\mathfrak{S}_n}, \qquad Y_i \mapsto S_i(X)$$

*est un isomorphisme. En particulier, la k-algèbre des polynômes symétriques est engendrée par les polynômes symétriques élémentaires, donc est de type fini.*

Le théorème de Hilbert que nous allons démontrer maintenant est une généralisation de cette reformulation : il affirme que *les invariants d'une k-algèbre de type fini sous l'action d'un groupe fini forment encore une k-algèbre de type fini.* C'est pour démontrer ce théorème que Hilbert a introduit la notion d'anneau noethérien et démontré que les anneaux de polynômes sur un corps sont noethériens !

THÉORÈME 7.4.4 (Hilbert, 1893). — *Soit $k$ un corps et soit* A *une $k$-algèbre de type fini et* G *un groupe fini d'automorphismes de* A. *Alors, l'ensemble* $\mathrm{A}^{\mathrm{G}}$ *des $a \in \mathrm{A}$ tels que pour tout $g \in \mathrm{G}$, $g(a) = a$, est une sous-$k$-algèbre de type fini de* A.

La démonstration du théorème 7.4.4 se fait en trois étapes.

LEMME 7.4.5. — $\mathrm{A}^{\mathrm{G}}$ *est une sous-$k$-algèbre de* A.

*Démonstration.* — Il faut démontrer que
– si $a$ et $b$ sont dans $\mathrm{A}^{\mathrm{G}}$, $a+b$, et $ab$ aussi ;
– si $a$ appartient à $\mathrm{A}^{\mathrm{G}}$ et $\lambda \in k$, $\lambda a$ aussi.
Or, si $g \in \mathrm{G}$, $g$ est un automorphisme de $k$-algèbres de A, donc $g(a+b) = g(a)+g(b) = a+b$, et $g(ab) = g(a)g(b) = ab$, si bien que $a+b$ et $ab$ appartiennent à $\mathrm{A}^{\mathrm{G}}$. De plus, $g(\lambda a) = \lambda g(a) = \lambda a$, si bien que $\lambda a \in \mathrm{A}^{\mathrm{G}}$. □

LEMME 7.4.6. — *Sous les hypothèses du théorème 7.4.4,* A *est un $\mathrm{A}^{\mathrm{G}}$-module de type fini.*

*Démonstration.* — Comme A est une $k$-algèbre de type fini, on peut choisir des éléments $a_1, \ldots, a_r \in \mathrm{A}$ tels que $\mathrm{A} = k[a_1, \ldots, a_r]$.

Fixons $i \in \{1; \ldots; r\}$ et considérons le polynôme de A[X],

$$\mathrm{P}_i(\mathrm{X}) = \prod_{g \in \mathrm{G}} (\mathrm{X} - g(a_i)).$$

Par suite, si $h \in \mathrm{G}$,

$$h(\mathrm{P}_i(\mathrm{X})) = \prod_{g \in \mathrm{G}} (\mathrm{X} - h(g(a_i))) = \prod_{g \in \mathrm{G}} (\mathrm{X} - g(a_i)) = \mathrm{P}_i(\mathrm{X})$$

et les coefficients de $\mathrm{P}_i$ sont invariants par $h$. Ainsi, $\mathrm{P}_i$ est à coefficients dans $\mathrm{A}^{\mathrm{G}}$. Écrivons ainsi

$$\mathrm{P}_i(\mathrm{X}) = \mathrm{X}^n + b_1\mathrm{X}^{n-1} + \cdots + b_n$$

où les $b_j$ appartiennent à $\mathrm{A}^{\mathrm{G}}$. Comme $\mathrm{P}_i(a_i) = 0$, il en résulte que, notant N le cardinal de G, $a_i^{\mathrm{N}}$ appartient au sous-$\mathrm{A}^{\mathrm{G}}$-module de A engendré par 1, …, $a_i^{\mathrm{N}-1}$.

Montrons maintenant que A est engendré comme $\mathrm{A}^{\mathrm{G}}$-module par les $\mathrm{N}^r$ produits $\prod_{i=1}^{r} a_i^{n_i}$, où pour tout $i$, $0 \leq n_i \leq \mathrm{N}-1$. Notons $\mathrm{A}'$ le sous-module engendré par ces éléments. Comme A est engendré comme $k$-module (donc *a fortiori* comme $\mathrm{A}^{\mathrm{G}}$-module) par tous les produits $\prod_{i=1}^{r} a_i^{n_i}$ avec $n_i \geq 0$, il suffit de montrer qu'un tel produit appartient à $\mathrm{A}'$. Soit ainsi $\mathrm{X}^{n_i} = \mathrm{Q}_j(\mathrm{X})\mathrm{P}_i(\mathrm{X}) + \mathrm{R}_i(\mathrm{X})$ la

division euclidienne dans $A^G[X]$ de $X^{n_i}$ par $P_i$, de sorte que $R_i$ est un polynôme à coefficients dans $A^G$ de degré $< N$. On a donc, en évaluant en $X = a_i$, $a_i^{n_i} = R_i(a_i)$, puis

$$\prod_{i=1}^{r} a_i^{n_i} = \prod_{i=1}^{r} R_i(a_i).$$

Si l'on développe cette dernière expression, on constate qu'elle appartient à $A'$. □

LEMME 7.4.7 (Artin–Tate). — *Soit $k \subset B \subset A$ trois anneaux. On suppose que $k$ est un anneau noethérien, que A est une $k$-algèbre de type fini et un A-module de type fini. Alors,* B *est une $k$-algèbre de type fini.*

*Démonstration.* — Soit $(x_1, \dots, x_r)$ une famille finie de générateurs de A comme $k$-algèbre et $(a_1, \dots, a_n)$ une famille finie de générateurs de A comme B-module. Ainsi, tout élément de A s'écrit comme un polynôme en les $x_i$ et comme combinaison linéaire des $a_j$. Appliquant cette remarque aux $x_i$ et aux produits $x_i x_j$, il existe en particulier des éléments $\lambda_{i\ell}$ et $\mu_{ij\ell}$ dans B tels que pour tout $1 \leq i \leq r$, que $x_i = \sum_{\ell=1}^{n} \lambda_{i\ell} a_\ell$, et pour tous $1 \leq i, j \leq r$, $a_i a_j = \sum_{\ell=1}^{n} \mu_{ij\ell} a_\ell$.

Soit $B_0$ la sous-$k$-algèbre de B engendrée par les $\lambda_{i\ell}$ et les $\mu_{ij\ell}$. C'est une $k$-algèbre de type fini, donc un anneau noethérien.

Soit alors $A_0$ le sous-$B_0$-module de A engendré par les $a_\ell$. Remarquons que $A_0$ est une $k$-algèbre. En effet, puisque les produits $a_i a_j$ sont par construction dans $A_0$, $A_0$ est stable par multiplication. Toujours par construction, les $x_i$ appartiennent à $A_0$. Ainsi, $A_0 = A$ et A est un $B_0$-module de type fini. Comme $B_0$ est un anneau noethérien, A est un $B_0$-module noethérien.

Par suite, tout sous-$B_0$-module de A est de type fini. En particulier, B est un $B_0$-module de type fini, et donc *a fortiori*, une $B_0$-algèbre de type fini.

Comme $B_0$ est une $k$-algèbre de type fini, B est aussi une $k$-algèbre de type fini. Le lemme est démontré. □

## 7.5. Idéaux premiers minimaux

DÉFINITION 7.5.1. — *Soit* A *un anneau. On dit qu'un idéal premier* $\mathfrak{p}$ *de* A *est minimal si* A *n'a pas d'idéal premier strictement contenu dans* $\mathfrak{p}$.

*Plus généralement, un idéal premier minimal contenant un idéal* I *de* A *est un élément minimal de l'ensemble des idéaux premiers de* A *qui contiennent* I.

THÉORÈME 7.5.2. — *Soit* A *un anneau. Pour tout idéal* I *de* A *distinct de* A*, il existe un idéal premier minimal contenant* I.

*Démonstration.* — On démontre le résultat lorsque $I = 0$. Le cas général en découle puisque la bijection entre idéaux de A contenant I et idéaux de A/I respecte à la fois les idéaux premiers et l'inclusion.

Soit donc $\mathscr{P}$ l'ensemble des idéaux premiers de A. Il est non vide car $A \neq 0$. Montrons que $\mathscr{P}$ muni de l'ordre opposé à celui défini par l'inclusion est un ensemble inductif. Il faut donc montrer que pour toute famille totalement ordonnée $(\mathfrak{p}_i)$ d'idéaux premiers de A, il existe un idéal premier $\mathfrak{p}$ contenu dans l'intersection $J = \bigcap \mathfrak{p}_i$. Or, J est premier ! Soit en effet $a$ et $b$ sont deux éléments de A tels que $ab \in J$ mais $a \notin J$. Soit $i$ tel que $a \notin \mathfrak{p}_i$. Si $j$ est tel que $j \leq i$, comme $\mathfrak{p}_j \subset \mathfrak{p}_i$, $a$ n'appartient pas à $mathfrak{p}_j$ ; comme $\mathfrak{p}_j$ est premier et comme $ab$ appartient à $\mathfrak{p}_j$, $b$ appartient à $\mathfrak{p}_j$. Si $j \geq i$, $b$ appartenant à $\mathfrak{p}_i$ appartient aussi à $\mathfrak{p}_j$. Par suite, $b$ appartient à J.

D'après le lemme de Zorn, $\mathscr{P}$ admet donc un élément minimal, lequel est un idéal premier minimal de A. □

THÉORÈME 7.5.3. — *Soit* A *un anneau noethérien. Si* I *est un idéal de* A*, l'ensemble des idéaux premiers de* A *contenant* I *n'a qu'un nombre fini d'éléments minimaux.*

*En particulier,* A *lui-même n'a qu'un nombre fini d'idéaux premiers minimaux.*

*Démonstration.* — Soit $\mathfrak{C}$ l'ensemble des idéaux de A qui ne satisfont pas à la conclusion du théorème. Si par l'absurde $\mathfrak{C}$ n'est pas vide, le fait que A soit noethérien garantit que $\mathfrak{C}$ admet un élément maximal I. C'est un idéal I de A vérifiant les deux propriétés suivantes :

– l'ensemble $\mathscr{R}$ des idéaux premiers de A qui contiennent I a un nombre infini d'éléments minimaux ;

– pour tout idéal J contenant I, distinct de I, l'ensemble $\mathscr{R}$ des idéaux premiers de A qui contiennent J n'a qu'un nombre fini d'éléments minimaux.

Si I était premier, I serait l'unique élément minimal de $\mathscr{R}$, ce qui contredit l'hypothèse que $\mathscr{R}$ admet une infinité d'éléments minimaux. Donc I n'est pas premier et il existe deux éléments $f$ et $g$ dans $A \setminus I$ tels que $fg \in I$.

Soit $\mathfrak{p}$ un idéal premier contenant I. Comme $fg \in I \subset \mathfrak{p}$, ou bien $f$ ou bien $g$ appartient à $\mathfrak{p}$ et par conséquent, $\mathfrak{p}$ contient $I + (f)$ ou $I + (g)$. Par suite, les éléments minimaux de $\mathscr{R}$ sont des éléments minimaux dans $\mathscr{R}_{I+(f)}$ ou dans $\mathscr{R}_{I+(g)}$ et l'un de ces deux ensemble admet par suite une infinité d'éléments minimaux, autrement dit, $I + (f)$ ou $I + (g)$ appartient à $\mathfrak{C}$. Or, par hypothèse, $f \notin I$ et $g \notin I$, si bien que $I + (f) \supsetneq I$ et $I + (g) \supsetneq I$. Ceci contredit le fait que I était maximal dans $\mathfrak{C}$. Ainsi, $\mathfrak{C}$ est vide et le théorème est démontré. □

Dans la suite de ce paragraphe, nous allons donner une traduction géométrique de cet énoncé lorsque $A = \mathbf{C}[X_1, \ldots, X_n]$.

DÉFINITION 7.5.4. — *Un ensemble algébrique* $V \subset \mathbf{C}^n$ *est dit* irréductible *s'il n'est pas réunion de deux ensembles algébriques distincts de* V.

PROPOSITION 7.5.5. — *Un ensemble algébrique* $V \subset \mathbf{C}^n$ *est irréductible si et seulement si son idéal* $\mathscr{I}(V)$ *est un idéal premier de* $\mathbf{C}[X_1, \ldots, X_n]$.

*Démonstration.* — Supposons que V est irréductible et montrons que $\mathscr{I}(V)$ est un idéal premier. Soit $f$ et $g$ deux éléments de $\mathbf{C}[X_1, \ldots, X_r]$ tels que $fg \in \mathscr{I}(V)$. On a ainsi $V \subset \mathscr{Z}(fg) = \mathscr{Z}(f) \cup \mathscr{Z}(g)$, d'où

$$V = (\mathscr{Z}(f) \cap V) \cup (\mathscr{Z}(g) \cap V).$$

Puisque V est irréductible, l'un de ces deux facteurs est égal à V. Supposons pour fixer les notations qu'il s'agit du premier. Alors, $V \subset \mathscr{Z}(f)$, donc $f \in \mathscr{I}(V)$. Ainsi, $\mathscr{I}(V)$ est un idéal premier de $\mathbf{C}[X_1, \ldots, X_n]$.

Supposons réciproquement que $\mathscr{I}(V)$ est un idéal premier et soit $V_1$, $V_2$ deux ensembles algébriques de $\mathbf{C}^n$ tels que $V = V_1 \cup V_2$, d'où $\mathscr{I}(V) = \mathscr{I}(V_1) \cap \mathscr{I}(V_2)$. Si $V_1 \subsetneq V$, on a $\mathscr{I}(V) \subsetneq \mathscr{I}(V_1)$ et il existe $f \in \mathscr{I}(V_1)$ tel que $f \notin \mathscr{I}(V)$. Alors, si $g \in \mathscr{I}(V_2)$, $fg$ appartient à la fois à $\mathscr{I}(V_1)$ et à $\mathscr{I}(V_2)$, donc $fg \in \mathscr{I}(V)$. Comme $\mathscr{I}(V)$ est supposé être premier et $f \notin \mathscr{I}(V)$, on a $g \in \mathscr{I}(V_2)$. Nous avons donc prouvé que $\mathscr{I}(V_2) \subset \mathscr{I}(V)$, d'où l'inclusion $V \subset V_2$. Comme $V_2 \subset V$, on a $V = V_2$. Cela prouve que V est un ensemble algébrique irréductible. □

L'interprétation géométrique du théorème 7.5.3 est alors la suivante.

THÉORÈME 7.5.6. — *Tout ensemble algébrique de* $\mathbf{C}^n$ *est réunion d'un nombre fini d'ensembles algébriques irréductibles.*

*Démonstration.* — Soit V un ensemble algébrique de $\mathbf{C}^n$. Un ensemble algébrique irréductible W est contenu dans V si et seulement si sont idéal $\mathscr{I}(W)$ est un idéal premier qui contient $\mathscr{I}(V)$. Réciproquement, un idéal premier contenant $\mathscr{I}(V)$ est de la forme $\mathscr{I}(W)$ pour un ensemble algébrique irréductible W contenu dans V.

Comme $\mathscr{I}(V)$ est un idéal radiciel, $\mathscr{I}(V)$ est l'intersection des idéaux premiers qui le contiennent, d'où l'existence d'une famille finie d'ensembles algébriques irréductibles $W_1$, …, $W_r$ tels que

$$\mathscr{I}(V) = \mathscr{I}(W_1) \cap \cdots \cap \mathscr{I}(W_r).$$

On a donc

$$\mathscr{I}(W_1 \cup \cdots \cup W_r) = \mathscr{I}(W_1) \cap \cdots \cap \mathscr{I}(W_r) = \mathscr{I}(V)$$

et par suite,

$$V = W_1 \cup \cdots \cup W_r.$$

□

## 7.6. Exercices

*Exercice 7.6.1.* — Soit A un anneau, M un A-module de type fini et $\varphi : \mathrm{M} \longrightarrow \mathrm{A}^n$ un morphisme surjectif de A-modules.

**a)** Montrer que $\varphi$ admet un inverse à droite.

**b)** Montrer que $\mathrm{M} \simeq \mathrm{Ker}\,\varphi \oplus \mathrm{Im}\,\psi$.

**c)** Montrer que $\mathrm{Ker}\,\varphi$ est de type fini.

*Exercice 7.6.2.* — Soient A un anneau, M un A-module, N un A-module de type fini et $u : \mathrm{M} \longrightarrow \mathrm{N}$ un homomorphisme de A-modules. Soit $\mathfrak{R}$ le radical de Jacobson de A (intersection de tous les idéaux maximaux).

**a)** Montrer que $u$ induit un homomorphisme $v : \mathrm{M}/\mathfrak{R} \cdot \mathrm{M} \longrightarrow \mathrm{N}/\mathfrak{R} \cdot \mathrm{N}$.

**b)** Remarquer que si I est un idéal de A et si $\mathrm{N}' \subset \mathrm{M}'$ sont deux A-modules alors $\mathrm{I} \cdot (\mathrm{M}'/\mathrm{N}') = (\mathrm{I} \cdot \mathrm{M}' + \mathrm{N}')/\mathrm{N}'$.

**c)** On suppose que $v$ est surjectif. Calculer $\mathrm{Im}(u) + \mathfrak{R}\mathrm{N}$ et en déduire que $u$ est surjectif.

*Exercice 7.6.3.* — Soit A un anneau et I un idéal de type fini de A tel que $\mathrm{I} = \mathrm{I}^2$. Montrer qu'il existe $e \in \mathrm{A}$ tel que $e^2 = e$ et $\mathrm{I} = (e)$. (*Utiliser le lemme de Nakayama pour trouver* $a \in \mathrm{I}$ *tel que* $(1 + a)\mathrm{I} = 0$.)

*Exercice 7.6.4.* — Soit A un anneau. Si A[X] est noethérien, A est-il nécessairement noethérien ?

*Exercice 7.6.5.* — Soit $\mathscr{E}$ une partie de $\mathbf{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et $\mathscr{V}$ l'ensemble des $n$-uplets $(x_1, \ldots, x_n) \in \mathbf{C}^n$ tels que pour tout $\mathrm{P} \in \mathscr{E}$, $\mathrm{P}(x_1, \ldots, x_n) = 0$. Montrer qu'il existe une partie finie $\{\mathrm{P}_1, \ldots, \mathrm{P}_r\} \subset \mathscr{E}$ telle que $\mathscr{V}$ soit défini par les équations $\mathrm{P}_i(x_1, \ldots, x_n) = 0$ (pour $1 \leq i \leq r$).

*Exercice 7.6.6.* — Soit A un anneau et $\mathrm{I}_1 \subset \mathrm{I}_2 \subset \ldots$ une suite croissante d'idéaux de type fini. Soit $\mathrm{I} = \bigcup \mathrm{I}_n$. Montrer que I est de type fini si et seulement si la suite $(\mathrm{I}_n)$ est stationnaire.

*Exercice 7.6.7.* — Soit A un anneau et I, J deux idéaux de A tels que $\mathrm{I} \cap \mathrm{J} = (0)$. Montrer que A est noethérien si et seulement si A/I et A/J sont noethériens.

*Exercice 7.6.8* (Exemples d'anneaux non noethériens). — Montrer que les anneaux suivants ne sont pas noethériens.

**a)** $k[\mathrm{X}_1, \mathrm{X}_2, \ldots, \mathrm{X}_n, \ldots]$ ;

**b)** $\mathscr{C}^0(\mathbf{R}, \mathbf{R})$ ;

**c)** $\mathscr{C}^\infty(\mathbf{R}, \mathbf{R})$. Montrer néanmoins que l'idéal des fonctions nulles en l'origine est principal.

**d)** le sous-module de $\mathbf{C}[\mathrm{X}, \mathrm{Y}]$ engendré par $\mathbf{C}$ et l'idéal (X) est un sous-anneau de $\mathbf{C}[\mathrm{X}, \mathrm{Y}]$. Il n'est pas noethérien.

*Exercice 7.6.9.* — Soit $\mathscr{F}$ l'ensemble des polynômes $P \in \mathbf{Q}[X]$ tel que pour tout $n \in \mathbf{Z}$, $P(n) \in \mathbf{Z}$.

**a)** Montrer que $\mathscr{F}$ est une sous $\mathbf{Z}$-algèbre de $\mathbf{Q}[X]$.

**b)** Montrer qu'une fonction $P : \mathbf{Z} \to \mathbf{Z}$ appartient à $\mathscr{F}$ si et seulement si $P(0) \in \mathbf{Z}$ et la fonction $n \mapsto P(n+1) - P(n) \in \mathscr{F}$.

**c)** Montrer que les polynômes $1, X, X(X-1)/2, \ldots, X(X-1)\ldots(X-p+1)/p!, \ldots$ forment une base de $\mathscr{F}$ comme $\mathbf{Z}$-module.

**d)** Montrer que $\mathscr{F}$ n'est pas noethérien.

*Exercice 7.6.10.* — Soit M un A-module noethérien et $I = (0 : M)$ l'annulateur de M dans A.

Montrer que A/I est un anneau noethérien.

*Exercice 7.6.11.* — Soit M un A-module noethérien et $\varphi : M \to M$ un endomorphisme de M. Montrer qu'il existe un entier $n \geq 1$ tel que

$$\operatorname{Ker} \varphi^n \cap \operatorname{Im} \varphi^n = (0).$$

*Exercice 7.6.12.* — Soit A un anneau et M un A-module de type fini. On définit pour tout idéal maximal $\mathfrak{m}$ de A,

$$d(\mathfrak{m}) = \dim_{A/\mathfrak{m}} M/\mathfrak{m}M.$$

**a)** Soit $\mathfrak{m}$ un idéal maximal de M, $d = d(\mathfrak{m})$. Montrer qu'il existe $a \in A \setminus \mathfrak{m}$ tel que si $S = \{1, a, a^2, \ldots\}$, $S^{-1}M$ soit engendré par $d$ éléments.

**b)** Si $\mathfrak{m}'$ est un idéal maximal de A ne contenant pas $a$, montrer que $d(\mathfrak{m}') \leq d$.

## 7.7. Solutions

*Solution de l'exercice 7.6.1.* — **a)** Notons $(e_1, \ldots, e_n)$ la base standard de $A^n$. Comme $\varphi$ est surjectif, il existe pour tout $i \in \{1, \ldots, n\}$ un élément $m_i \in M$ tel que $\varphi(m_i) = e_i$. Définissons alors un homomorphisme de A-modules $\psi : A^n \to M$ par $\psi(e_i) = m_i$. Ainsi, $\varphi(\psi(e_i)) = e_i$ pour tout $i$, si bien que $\varphi \circ \psi = \mathrm{Id}_{A^n}$. Autrement dit, $\psi$ est un inverse à droite de $\varphi$.

**b)** On vérifie que l'homomorphisme de A-modules $\theta : \operatorname{Ker} \varphi \oplus A^n \to M$ donné par $\theta(m \oplus e) = m + \psi(e)$ est un isomorphisme. Si en effet $\theta(m \oplus e) = 0$, soit $m + \psi(e) = 0$, on a $\varphi(m + \psi(e)) = \varphi(m) + \varphi(\psi(e)) = e = 0$, puis $\psi(e) = 0$, et enfin $m = 0$, d'où l'injectivité. Quant à la surjectivité, si $m \in M$, posont $m_0 = m - \psi(\varphi(m))$. Alors,

$$\begin{aligned} \varphi(m_0) &= \varphi(m) - \varphi(\psi(\varphi(m))) \\ &= \varphi(m) - (\varphi \circ \psi)(\varphi(m)) \\ &= \varphi(m) - \varphi(m) = 0, \end{aligned}$$

ce qui signifie que $m_0 \in \operatorname{Ker}\varphi$. Alors, $m = \theta(m_0 \oplus \varphi(m)) \in \operatorname{Im}\theta$.

**c)** Soient $(f_i)_{1\le i\le \mu}$ des générateurs de M. On écrit pour tout $i$, $f_i = \theta(m_i \oplus \psi(v_i))$, avec $m_i \in \operatorname{Ker}\varphi$ et $v_i \in \mathrm{A}^n$. Prouvons que les $(m_i)$ engendrent $\operatorname{Ker}\varphi$. En effet, soit $m \in \operatorname{Ker}\varphi$. Comme les $(f_i)$ engendrent M, on peut écrire

$$\begin{aligned} m &= \sum_{i=1}^{\mu} a_i f_i = \sum_{i=1}^{\mu} a_i(m_i + \psi(v_i)) \\ &= \sum_{i=1}^{\mu} a_i m_i + \psi\Big(\sum_{i=1}^{\mu} a_i v_i\Big) \\ &= \theta\Big(\big(\sum_{i=1}^{\mu} a_i m_i\big) \oplus \big(\sum_{i=1}^{\mu} a_i v_i\big)\Big). \end{aligned}$$

Par unicité, on a donc $\sum_{i=1}^{\mu} a_i v_i = 0$ et ainsi, $m = \sum_{i=1}^{\mu} a_i m_i$ est engendré par les $m_i$.

On peut aussi remarquer que $\operatorname{Ker}\varphi \simeq \mathrm{M}/\operatorname{Im}\psi$ est un quotient d'un module de type fini, donc est de type fini.

*Solution de l'exercice 7.6.2.* — **a)** Il faut montrer que l'homomorphisme composé $\mathrm{M} \xrightarrow{u} \mathrm{N} \to \mathrm{N}/\mathfrak{R}\cdot\mathrm{N}$ passe au quotient par $\mathfrak{R}\cdot\mathrm{M}$. Ce dernier module est engendré par les produits $am$, où $a \in \mathfrak{R}$ et $m \in \mathrm{M}$. L'image d'un tel produit est égale à $\mathrm{cl}(u(am)) = \mathrm{cl}(au(m)) = 0$ car $a \in \mathfrak{R}$ et $u(m) \in \mathrm{N}$, donc $au(m) \in \mathfrak{R}\cdot\mathrm{N}$.

**b)** Considérons l'application (A-linéaire) $\varphi : \mathrm{I}\cdot(\mathrm{M}'/\mathrm{N}') \to (\mathrm{I}\cdot\mathrm{M}' + \mathrm{N}')/\mathrm{N}'$ telle que $\varphi(\sum a_i\,\mathrm{cl}(m_i)) = \mathrm{cl}(\sum a_i m_i) \in (\mathrm{I}\cdot\mathrm{M}'+\mathrm{N}')/\mathrm{N}'$. Elle est bien définie, car si $m = \sum a_i\,\mathrm{cl}(m_i) = 0$ dans $\mathrm{M}'/\mathrm{N}'$, c'est-à-dire si $\sum a_i m_i \in \mathrm{N}'$, alors $\varphi(m) = 0$. D'autre part, si $\varphi(m) = 0$, on en déduit que $\sum a_i m_i \in \mathrm{N}'$, et donc que $m = 0$. Ainsi, $\varphi$ est injective. Finalement, considérons un élément $m = \sum \alpha_i m_i + n \in (\mathrm{I}\cdot\mathrm{M}' + \mathrm{N}')$. On a $\mathrm{cl}(m) = \mathrm{cl}(\sum \alpha_i m_i) = \varphi(\sum a_i\,\mathrm{cl}(m_i))$, si bien que $\varphi$ est surjective.

**c)** On a $\operatorname{Im}(u) + \mathfrak{R}\mathrm{N} \subset \mathrm{N}$. Montrons en fait l'égalité. Si $n \in \mathrm{N}$, il existe, $v$ étant surjectif, $m \in \mathrm{M}$ tel que $u(m) - n \in \mathfrak{R}\mathrm{N}$. Par suite, $n \in \operatorname{Im}(u) + \mathfrak{R}\mathrm{N}$ et donc $\mathrm{N} = \operatorname{Im}(u) + \mathfrak{R}\mathrm{N}$.

Alors, $\mathfrak{R}\cdot(\mathrm{N}/\operatorname{Im}u) = (\mathfrak{R}\mathrm{N} + \operatorname{Im}u)/(\operatorname{Im}u) = \mathrm{N}/\operatorname{Im}u$. On constate que $\mathrm{P} = \mathrm{N}/\operatorname{Im}u$ est un A-module de type fini tel que $\mathfrak{R}\mathrm{P} = \mathrm{P}$. D'après le lemme de Nakayama, $\mathrm{P} = 0$. Par suite, $\mathrm{N} = \operatorname{Im}u$.

*Solution de l'exercice 7.6.3.* — On a $\mathrm{I} = \mathrm{I}\cdot\mathrm{I}$. Comme I est un A-module de type fini, il existe en vertu du lemme de Nakayama un élément $a \in \mathrm{I}$ tel que $(1+a)\mathrm{I} = 0$. Posons $e = -a$. Comme $e \in \mathrm{I}$, $(1-e)e = 0$ et $e = e^2$. Par ailleurs, si $x \in \mathrm{I}$, $(1-e)x = 0$, d'où $x = ex \in (e)$. Par suite, $\mathrm{I} = (e)$.

*Solution de l'exercice 7.6.4.* — Oui. Soit en effet I un idéal de A, et soit $\mathrm{I}\cdot\mathrm{A}[\mathrm{X}]$ l'idéal engendré par I dans A[X]. Comme A[X] est noethérien, $\mathrm{I}\cdot\mathrm{A}[\mathrm{X}]$ est

engendré par un nombre fini de polynômes $P_1, \dots, P_r$. Soit alors $a \in I$. Comme $a \in I \cdot A[X]$, il existe des polynômes $Q_j \in A[X]$ tels que

$$a = \sum_{i=1}^{r} Q_j(X) P_i(X),$$

d'où

$$a = \sum_{i=1}^{r} Q_j(0) P_i(0),$$

ce qui prouve que I est engendré par les $P_i(0)$. Ainsi, I est de type fini.

En fait, tout quotient d'un anneau noethérien est noethérien, et $A \simeq A[X]/(X)$.

*Solution de l'exercice 7.6.5.* — Supposons le résultat faux, c'est-à-dire que pour toute partie finie $\{P_1, \dots, P_r\} \subset \mathscr{E}$, l'ensemble des $x \in \mathbf{C}^n$ tels que $P_1(x) = \cdots = P_r(x) = 0$ contienne strictement $\mathscr{V}$.

On construit alors par récurrence une suite $(P_i)_{i \geq 1}$ d'éléments de $\mathscr{E}$ de la façon suivante. On choisit un élément $P_1 \in \mathscr{E}$. Alors, l'ensemble $\mathscr{V}_1$ des $x \in \mathbf{C}^n$ tels que $P_1(x) = 0$ est distinct de $\mathscr{V}$. Il existe donc $P_2 \in \mathscr{E}$ et $x \in \mathscr{V}_1$ tel que $P_2(x) \neq 0$ Ainsi l'ensemble $\mathscr{V}_2$ des $x \in \mathbf{C}^n$ tels que $P_1(x) = P_2(x) = 0$ est strictement inclus dans $\mathscr{V}_1$, mais il contient strictement $\mathscr{V}$, d'où un polynôme $\mathscr{V}_3 \in \mathscr{E}$, etc.

La suite $(P_1) \subset (P_1, P_2) \subset (P_1, P_2, P_3) \subset \dots$ d'idéaux de $\mathbf{C}[X_1, \dots, X_n]$ est stationnaire. Il existe ainsi $n \geq 1$ tel que $P_{n+1} \in (P_1, \dots, P_n)$. Mais alors, si $x \in \mathscr{V}_n$, $P_{n+1}(x)$ est nécessairement nul, ce qui est une contradiction.

*Solution de l'exercice 7.6.6.* — Supposons la suite stationnaire. Alors, $I = I_n$ est de type fini.

Supposons réciproquement que I est de type fini. Soient $(a_i)$ des générateurs de I, en nombre fini. On peut trouver pour tout $i$ un entier $n_i$ tel que $a_i \in I_{n_i}$, et en posant $N = \max(n_i)$, on a $a_i \in I_N$ pour tout $i$. Alors, $I_N$ contient les générateurs de I, donc $I_N$ contient I. Comme $I_N \subset I$, on a $I = I_N$ et la suite est stationnaire.

*Solution de l'exercice 7.6.7.* — Si A est noethérien, A/I et A/J sont des quotients de l'anneau A, donc des anneaux noethériens.

Réciproquement, supposons que A/I et A/J soient des anneaux noethériens. Puisque $I \cap J = (0)$, l'homomorphisme composé $I \to A \to A/J$ est injectif et identifie I à un sous-A-module de A/J. Par suite, I est un A-module noethérien. Comme A/I est un anneau noethérien, donc un A/I-module noethérien, donc un A-module noethérien, la suite exacte

$$0 \to I \to A \to A/I \to 0$$

implique alors que A est un A-module noethérien, et par conséquent un anneau noethérien.

*Solution de l'exercice 7.6.8.* — **a)** On a une suite croissante d'idéaux

$$(X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, X_2, \ldots, X_n) \subset \ldots$$

dont on va prouver qu'elle n'est pas stationnaire. Si c'était le cas, on aurait un entier $n$ tel que $X_{n+1} \in (X_1, X_2, \ldots, X_n)$. Cela signifie qu'il existe des polynômes $P_i$ (pour $1 \leq i \leq n$) tels que $X_{n+1} = \sum X_i P_i$. Les $P_i$ ne font intervenir qu'un nombre fini de variables, disons les variables $X_j$ pour $j \leq D$. Alors, on peut évaluer la relation au point $(x_1, \ldots, x_D)$ tel que $x_j = 0$ pour tout $j \neq n+1$, et $x_{n+1} = 1$. On trouve $1 = 0$, d'où une contradiction.

**b)** Soit I l'idéal des fonctions nulles en 0. Il n'est pas de type fini. Soit en effet $(f_1, \ldots, f_n)$ est une famille finie de fonctions continues nulles en 0. Or, tout élément $f$ de l'idéal engendré par les $f_i$ vérifie

$$|f(x)| \leq \text{constante} \times \max |f_i(x)|$$

dans un voisinage de 0. Or, la fonction

$$f = \sqrt{\max |f_i|}$$

est continue, nulle en zéro et ne vérifie aucune inégalité de ce type.

**c)** Soit $I_n$ l'idéal des fonctions nulles dans $[-1/n; 1/n]$. On a ainsi une suite croissante d'idéaux qui n'est manifestement pas stationnaire.

Si $f \in \mathscr{C}^\infty$ vérifie $f(0) = 0$, un exercice du cours d'analyse de DEUG (ou de Licence...) montre qu'il existe une fonction $g : \mathbf{R} \to \mathbf{R}$ de classe $\mathscr{C}^\infty$ telle que $f(x) = xg(x)$. Autrement dit, l'idéal des fonctions nulles en l'origine est engendré par la fonction $x$.

**d)** On considère l'ensemble des sommes $\sum a_{i,j} X^i Y^j$ qui ne contiennent pas de monôme en puissance de Y. C'est un sous-anneau de $\mathbf{C}[X,Y]$ car si P et Q ne font pas intervenir de monôme $Y^\alpha$, PQ non plus.

Alors, considérons l'idéal $(X, XY, XY^2, \ldots)$. Supposons qu'il soit de type fini. On aurait alors $XY^n = \sum_{k<n} a_k XY^k$, avec $a_k \in A \subset \mathbf{C}[X,Y]$. Il existe forcément un entier $k$ et un monôme non nul $X^i Y^j$ de $a_k$ tels que $X^{i+1}Y^{j+k} = XY^n$, d'où $i = 0$ et $j + k = n$. Cela implique $j > 1$ et donc $a_k$ contient un monôme qui est une puissance de Y. C'est absurde.

*Solution de l'exercice 7.6.9.* — **a)** Si P et Q sont deux polyômes tels que $P(\mathbf{Z}) \subset \mathbf{Z}$, alors PQ vérifie aussi $P(n)Q(n) \in \mathbf{Z}$ pour tout $n \in \mathbf{Z}$, de même que $aP + bQ$ pour tous $a$ et $b \in \mathbf{Z}$.

**b)** Comme $n \mapsto P(n+1) - P(n)$ est une fonction polynômiale, la condition est évidemment nécessaire.

Réciproquement, soit $Q \in \mathbf{Q}[X]$ tel que pour tout $n$, $Q(n) = P(n+1) - P(n)$. Soit $d$ le degré de Q et $\Delta : \mathbf{Q}_{d+1}[X] \to \mathbf{Q}_d[X]$ l'application linéaire qui associe à un polynôme A de degré $\leq d+1$ le polynôme $A(X+1) - A(X)$. Si $A = c_r X^r + \ldots$,

on a $\Delta(A) = rc_r X^{r-1} + \dots$, si bien que $\operatorname{Ker}\Delta = \mathbf{Q}$. On a alors $\dim \operatorname{Im}\Delta = \dim \mathbf{Q}_{d+1}[X] - \dim \operatorname{Ker}\Delta = d + 2 - 1 = d + 1$, et donc $\operatorname{Im}\Delta = \mathbf{Q}_d[X]$. Il existe ainsi un polynôme $A \in \mathbf{Q}_{d+1}[X]$ tel que $A(X+1) - A(X) = Q(X)$.

Alors, la fonction $\varphi : n \mapsto P(n) - A(n)$ vérifie $\varphi(n+1) - \varphi(n) = 0$ pour tout $n$. On a ainsi $P(n) = A(n) + \varphi(0)$ pour tout $n \in \mathbf{Z}$. Comme $\varphi(0) = P(0) - A(0) \in \mathbf{Q}$, la fonction P est bien la restriction à $\mathbf{Z}$ d'un polynôme à coefficients rationnels.

**c)** Notons $P_d = X(X-1)\dots(X-d+1)/d!$. La famille $P_0, P_1, \dots$ forme une base de $\mathbf{Q}[X]$ comme $\mathbf{Q}$-espace vectoriels. Si $\Delta$ est l'endomorphisme de $\mathbf{Q}[X]$ défini par $\Delta(P) = P(X+1) - P(X)$, on a

$$\begin{aligned}\Delta(P_d) &= \frac{1}{d!}\left((X+1)X\dots(X+2-d) - X(X-1)\dots(X+1-d)\right)\\ &= \frac{1}{d!}X\dots(X+2-d)\left((X+1) - (X+1-d)\right)\\ &= P_{d-1}.\end{aligned}$$

Enfin, remarquons aussi que si $P = c_0P_0 + \dots$, on a $P(0) = 0$.

Il résulte de la question précédente que si $P = c_0P_0 + \dots$, alors

$$P \in \mathscr{F} \qquad \Leftrightarrow \qquad c_0 \in \mathbf{Z} \quad \text{et} \quad c_1P_0 + \dots \in \mathscr{F}.$$

Par récurrence, $P \in \mathscr{F}$ si et seulement si tous les $c_d$ sont des entiers. Un élément de $\mathscr{F}$ est donc combinaison linéaire des $P_d$, et ce de manière unique. Les polynômes $P_d$ forment donc bien une base de $\mathscr{F}$ comme $\mathbf{Z}$-module.

**d)** Si $d+1$ est un nombre premier, montrons que le polynôme $P_{d+1}$ n'appartient pas à l'idéal $(P_1, \dots, P_d)$. Supposons par l'absurde que

$$P_{d+1} = Q_1P_1 + \dots + P_dQ_d$$

pour des polynômes $Q_i \in \mathscr{F}$. On a en particulier

$$\begin{aligned}1 &= P_{d+1}(d+1)\\ &= Q_1(d+1)P_1(d+1) + \dots + Q_d(d+1)P_d(d+1).\end{aligned}$$

Or, quand $i < d+1$, $d+1$ étant premier,

$$P_i(d+1) = \frac{(d+1)d\dots(d+2-i)}{i!} \in (d+1)\mathbf{Z}.$$

Il en résulte que $1 \in (d+1)\mathbf{Z}$, ce qui est absurde.

La suite d'idéaux

$$(P_1) \subset (P_1, P_2) \subset (P_1, P_2, P_3) \subset \dots$$

n'est donc pas stationnaire. L'anneau $\mathscr{F}$ n'est pas noethérien.

*Solution de l'exercice 7.6.10.* — Soient $m_1, \dots, m_n$ des générateurs de M comme A-module. Considérons l'homomorphisme de A-modules

$$\mathrm{A} \to \mathrm{M}^n, \quad a \mapsto (am_1, \dots, am_n).$$

Son noyau contient I, mais réciproquement, si $am_i = 0$ pour tout $i$, $am = 0$ pour tout $m \in \mathrm{M}$ puisque les $m_i$ engendrent M. Donc son noyau est égal à I et le théorème de factorisation nous permet d'en déduire que A/I est isomorphe à un sous-A-module de $\mathrm{M}^n$.

Or, $\mathrm{M}^n$ est noethérien. Tous ses sous-modules sont noethériens, donc A/I est noethérien.

*Solution de l'exercice 7.6.11.* — La suite des modules $\operatorname{Ker}\varphi^n$ est croissante, donc stationnaire. Il existe ainsi $n$ tel que $\operatorname{Ker}\varphi^n = \operatorname{Ker}\varphi^{n+1} = \dots$

Si $x \in \operatorname{Ker}\varphi^n \cap \operatorname{Im}\varphi^n$, on a alors $x = \varphi^n(y)$, avec $y \in \mathrm{M}$, mais aussi $\varphi^n(x) = \varphi^{2n}(y) = 0$. Donc $y \in \operatorname{Ker}\varphi^{2n} = \operatorname{Ker}\varphi^n$. Par suite, $\varphi^n(y) = 0$ et $x = 0$.

*Solution de l'exercice 7.6.12.* — **a)** Soient $x_1, \dots, x_d$ des éléments de M dont les images engendrent $\mathrm{M}/\mathfrak{m}\mathrm{M}$ comme $\mathrm{A}/\mathfrak{m}$-module. D'après le lemme de Nakayama, les $x_i$ engendrent $\mathrm{M}_\mathfrak{m}$ comme $\mathrm{A}_\mathfrak{m}$-module. Soit $\mathrm{N} \subset \mathrm{M}$ le sous-module engendré par les $x_i$.

Soient maintenant des générateurs $m_j$ (pour $1 \leq j \leq n$) de M. Comme les $x_i$ engendrent l'image de $m_j$ dans $\mathrm{M}_\mathfrak{m}$, il existe des $b_{i,j} \notin \mathfrak{m}$, et $a_j \notin \mathfrak{m}$ tels que

$$a_j m_j = \sum_{i=1}^{d} b_{i,j} x_i,$$

autrement dit, $a_j m_j \in \mathrm{N}$. Posons $a = a_1 \dots a_n$. On a $bm_j \in \mathrm{N}$ pour tout $j$, si bien que l'image de $m_j$ dans $\mathrm{S}^{-1}\mathrm{M}$ appartient à $\mathrm{S}^{-1}\mathrm{N}$ si $\mathrm{S} = \{1, a, a^2, \dots\}$. Comme $\mathrm{S}^{-1}\mathrm{M}$ est engendré par les $m_j$, $\mathrm{S}^{-1}\mathrm{M} = \mathrm{S}^{-1}\mathrm{N}$ est donc engendré par $d$ éléments.

**b)** Comme $\mathfrak{m}'$ ne contient pas $a$,

$$\mathrm{A}/\mathfrak{m}' = \mathrm{S}^{-1}\mathrm{A}/\mathrm{S}^{-1}\mathfrak{m}'$$

et

$$\mathrm{M}/\mathfrak{m}'\mathrm{M} = \mathrm{S}^{-1}\mathrm{M}/\mathfrak{m}'\mathrm{S}^{-1}\mathrm{M}$$

est un quotient d'un $\mathrm{S}^{-1}\mathrm{A}$-module engendré par $d$ éléments, donc est engendré comme $\mathrm{S}^{-1}\mathrm{A}$-module par $d$ éléments, et aussi comme $\mathrm{A}/\mathfrak{m}'$-espace vectoriel, puisque cette structure est héritée de la structure de $\mathrm{S}^{-1}\mathrm{A}$-module. Par suite,

$$d(\mathfrak{m}') \leq d = d(\mathfrak{m}).$$

Remarque. — Cela signifie que la fonction $\mathfrak{m} \mapsto d(\mathfrak{m})$ est semi-continue supérieurement pour la topologie de Zariski sur l'ensemble des idéaux maximaux de A.

# 8 Modules de type fini sur un anneau principal

*La théorie des modules sur un anneau arbitraire est compliquée. Lorsque l'anneau est un corps, on retrouve la théorie des espaces vectoriels, laquelle est plus simple notamment grâce à l'existence de bases et de supplémentaires.*
*Dans le cas d'un anneau principal, on peut donner une description relativement précise et explicite des modules de type fini. On verra que ceux-ci, dès qu'ils sont sans torsion, sont automatiquement libres.*
*En outre, appliquée aux cas de l'anneau des entiers et de l'anneau des polynômes à coefficients dans un corps, on obtiendra des renseignements concernant dans un cas les groupes abéliens de type fini et dans l'autre les classes de similitude de matrices.*

## 8.1. Sous-modules d'un module libre

On commence ce paragraphe par quelques rappels.

LEMME 8.1.1. — *Soit* A *un anneau intègre, soit* M *un* A*-module et soit* $m$ *un élément de* M. *Le sous-module* $(m)$ *de* M *engendré par* M *est libre si et seulement si* $m = 0$ *ou si* $\mathrm{Ann}(m) = (0)$.

*Démonstration.* — Si $m = 0$, $(m) = (0)$ est libre, de base l'ensemble vide (!). Supposons maintenant $m \neq 0$. Par définition, la partie $\{m\}$ est génératrice. Elle est libre puisque si $am = 0$, on a $a \in \mathrm{Ann}(m)$, donc $a = 0$.

Réciproquement, supposons que $(m)$ est un A-module libre. S'il est nul, $m = 0$. Sinon, soit $\mathscr{B}$ une base de $(m)$. Montrons que $\mathscr{B}$ est de cardinal exactement 1. Sinon, soit $m'$ et $m''$ deux éléments distincts de $\mathscr{B}$. On peut donc écrire $m' = am$ et $m'' = bm$ pour deux éléments $a$ et $b$ de A, non nuls. On a alors $bm' - am'' = 0$, ce qui prouve, la famille $\{m'; m''\} \subset \mathscr{B}$ étant libre, que $a = b = 0$, d'où une contradiction. Ainsi, $\mathscr{B}$ a exactement un élément ; soit donc $m' = am$ une base de $(m)$. On peut en particulier écrire $m = bm'$, d'où $m' = abm'$ et $(1 - ab)m' = 0$.

Puisque $m'$ est une base de $(m)$, $1 = ab$ et $a$ est inversible. Ainsi, $m$ est aussi une base de $(m)$. Si maintenant $a \in \mathrm{Ann}(m)$, on a $am = 0$. Puisque la partie $\{m\}$ est libre, $a = 0$ et $\mathrm{Ann}(m) = (0)$, ainsi qu'il fallait démontrer. □

DÉFINITION 8.1.2. — *Soit* A *un anneau et soit* M *un* A*-module. On dit qu'un élément* $m \in \mathrm{M}$ *est de* torsion *s'il existe* $a \in \mathrm{A}$, $a \neq 0$, *tel que* $am = 0$.

*On dit que* M *est* de torsion *si tout élément de* M *est de torsion et qu'il est* sans torsion *si* 0 *est le seul élément de* M *qui soit de torsion.*

PROPOSITION 8.1.3. — *Soit* A *un anneau* intègre *et soit* M *un* A*-module. Soit* $\mathrm{M}_{\mathrm{tor}}$ *l'ensemble des éléments de* M *qui sont de torsion. Alors,* $\mathrm{M}_{\mathrm{tor}}$ *est un sous-module de* M.

*De plus,* $\mathrm{M}/\mathrm{M}_{\mathrm{tor}}$ *est sans torsion.*

*Démonstration.* — L'élément $0 \in \mathrm{M}$ vérifie $1 \cdot 0 = 0$, donc est de torsion puisque $1 \neq 0$ dans A. Soit $m$ et $n$ deux éléments de $\mathrm{M}_{\mathrm{tor}}$ et choisissons $a$ et $b$ non nuls dans A tels que $am = bn = 0$. On a alors $ab(m+n) = abm + abn = b(am) + a(bn) = 0$ et comme A est intègre, $ab \neq 0$. Ainsi, $m + n$ est de torsion. Enfin, soit $m$ un élément de torsion dans M et soit $a \in \mathrm{A}$ tel que $am = 0$. Pour tout $x \in \mathrm{A}$, $a(xm) = x(am) = 0$ donc $xm$ est de torsion.

Ains, $\mathrm{M}_{\mathrm{tor}}$ est un sous-A-module de M.

Notons $\mathrm{cl} : \mathrm{M} \to \mathrm{M}/\mathrm{M}_{\mathrm{tor}}$ l'homomorphisme canonique et soit $m \in \mathrm{M}$ tel que $\mathrm{cl}(m)$ est de torsion dans $\mathrm{M}/\mathrm{M}_{\mathrm{tor}}$. Soit ainsi $a \in \mathrm{A}$, $a \neq 0$ tel que $a\,\mathrm{cl}(m) = 0$. Puisque $\mathrm{cl}(am) = a\,\mathrm{cl}(m) = 0$, on a ainsi $am \in \mathrm{M}_{\mathrm{tor}}$. Par suite, il existe $b \in \mathrm{A}$, $b \neq 0$ tel que $b(am) = 0$. Puisque A est intègre, $ab \neq 0$ et $m$ est de torsion, d'où $m \in \mathrm{M}_{\mathrm{tor}}$ et $\mathrm{cl}(m) = 0$. On a donc $(\mathrm{M}/\mathrm{M}_{\mathrm{tor}})_{\mathrm{tor}} = 0$. □

On rappelle aussi le résultat suivant, démontré à l'exercice 6.6.13.

LEMME 8.1.4. — *Soit* A *un anneau et soit* $f : \mathrm{M} \to \mathrm{N}$ *un homomorphisme de* A*-modules. On suppose que* $\mathrm{Ker}\, f$ *et* $\mathrm{Im}\, f$ *sont des* A*-modules libres de rangs* $p$ *et* $q$. *Alors,* M *est un* A*-module libre de rang* $p + q$.

Donnons maintenant une première version du théorème de structure des sous-modules d'un module libre sur un anneau principal.

PROPOSITION 8.1.5. — *Soit* A *un anneau principal, soit* $n$ *un entier soit* M *un sous-*A*-module du module libre* $\mathrm{A}^n$. *Alors* M *est libre de rang inférieur ou égal à* $n$.

*Démonstration.* — La démonstration se fait par récurrence sur $n$. Un sous-module M de A est un idéal I de A. Si $\mathrm{I} = 0$, M est libre de rang 0. Sinon, comme A est principal, il existe $a \in \mathrm{A}$, $a \neq 0$, tel que $\mathrm{I} = (a)$ et puisque A est intègre, $\{a\}$ est une base de $\mathrm{I} = \mathrm{M}$, donc M est libre de rang 1.

Supposons le résultat vrai en rang $< n$, c'est-à-dire que tout sous-module de $A^{n-1}$ est libre de rang $\leq n-1$. Soit M un sous-module de $A^n$, considérons l'homomorphisme $f\colon A^n \to A$ tel que $f(a_1,\dots,a_n) = a_n$ et soit $g = f|_M$ la restriction de $f$ à M.

L'image de $g$ est un sous-module de A donc est libre de rang $\leq 1$. Le noyau de $f$ est égal à l'ensemble des $(a_1,\dots,a_n)$ tels que $a_n = 0$. Il s'identifie ainsi à $A^{n-1}$ et $\operatorname{Ker} g$ s'identifie donc à un sous-module de $A^{n-1}$. Par récurrence, $\operatorname{Ker} g$ est libre de rang $\leq n-1$. D'après le lemme précédent, M est libre de rang $\leq 1 + (n-1) = n$. □

Le théorème que nous démontrons maintenant s'établit de manière semblable, mais nécessite un peu plus de soin.

THÉORÈME 8.1.6. — *Soit* A *un anneau principal. Soit* M *un* A*-module libre de rang* $m$ *et soit* P *un sous-module de* M. *Il existe alors un entier* $p \in \{0;1;\dots;m\}$, *une base* $(e_1,\dots,e_m)$ *de* M *et des éléments* $a_1,\dots,a_r$ *non nuls dans* A *tels que :*

– *pour tout* $i \in \{1;\dots;r-1\}$, $a_i$ *divise* $a_{i+1}$ ;

– *la famille* $\{a_1e_1;\dots;a_re_r\}$ *est une base de* P.

*Démonstration.* — Pour motiver cette démonstration, commençons par une remarque. Soit $\varphi \in M^\vee$ une forme linéaire sur M. Si $(e_1,\dots,e_n)$ et $(a_1,\dots,a_r)$ sont comme dans le théorème, $\varphi$ est déterminée par les images $\varphi(e_i)$ de la base fixée. De plus, si $m \in P$, on peut écrire $m = x_1a_1e_1 + \cdots + x_ra_re_r$ avec des $x_i$ dans A et la relation

$$\varphi(m) = x_1a_1\varphi(e_1) + \cdots + x_ra_r\varphi(e_r)$$

montre que $\varphi(m)$ est multiple de $a_1$, d'où $\varphi(P) \subset (a_1)$. Réciproquement, la forme linéaire $\varphi$ définie par $\varphi(e_1) = 1$ et $\varphi(e_i) = 0$ pour $i > 1$ est telle que $\varphi(P) = (a_1)$. On va ainsi être amené à considérer des idéaux maximaux parmi les idéaux $\varphi(P)$, $\varphi$ parcourant les formes linéaires sur M.

Démontrons maintenant le théorème. La démonstration est encore par récurrence sur $n$. Si $n = 1$, on a $M = (a_1)$. Supposons maintenant le théorème démontré en rang $\leq n-1$.

On peut supposer $M \neq 0$ (sinon, on pose $r = 0$).

a) Soit $\mathscr{I}$ l'ensemble des idéaux de A de la forme $\varphi(P)$, lorsque $\varphi$ parcourt l'ensemble des formes linéaires sur M. Comme A est noethérien, $\mathscr{I}$ admet des éléments maximaux. Considérons un tel élément maximal. Il est de la forme $\varphi(P) = (a_1)$ pour un certain $a_1 \in A$, $a_1 \neq 0$ et $\varphi \in M^\vee$. Il existe en particulier $e \in P$ tel que $\varphi(e) = a_1$.

b) Soit $f$ une autre forme linéaire sur M et montrons que $a_1$ divise $f(e)$. Notons en effet $d = \operatorname{pgcd}(a_1, f(e))$, il existerait $x$ et $y$ dans A tel que $xa_1 + yf(e) = d$. Posons $\varphi' = x\varphi + yf \in M^*$. On a donc $\varphi'(e) = (x\varphi + yf)(e) = d$, d'où $\varphi'(e) \supset (d)$.

Puisque $(d) \supset (a_1)$, l'hypothèse de maximalité sur $\varphi$ montre que $(d) = (a_1)$ et donc $a_1$ divise $f(e)$.

En particulier, choisissons une base $(\varepsilon_1, \dots, \varepsilon_n)$ de M. Appliqué aux $n$ formes linéaires de coordonnées sur M (la base duale), on obtient que $a_1$ divise toutes les coordonnées de $e$. Ainsi, il existe un élément $e_1 \in \mathrm{M}$ tel que $e = a_1 e_1$.

c) Appliquons l'hypothèse de récurrence à $\mathrm{P}' = \operatorname{Ker}\varphi|_{\mathrm{P}} = \operatorname{Ker}\varphi \cap \mathrm{P}$. Notons $\mathrm{M}' = \operatorname{Ker}\varphi$ ; d'après la proposition précédente, M est libre de rang $\leq n-1$ (en fait de rang exactement $n-1$, car M est de rang $\leq \operatorname{rang}\mathrm{M}' + \operatorname{rang}\operatorname{Im}\varphi$). Il existe ainsi une base $(e_2, \dots, e_n)$ de $\operatorname{Ker}\varphi$, des éléments $a_2, \dots, a_r$ non nuls dans A de sorte que $a_i$ divise $a_{i+1}$ pour $i \geq 2$ et que $(a_2 e_2, \dots, a_r e_r)$ soit une base de $\mathrm{P}'$. De plus, $\varphi(e_1)$ est une base de $\varphi(\mathrm{M})$ et $\varphi(a_1 e_1)$ est une base de $\varphi(\mathrm{P})$. D'après le lemme 8.1.4 $(e_1, \dots, e_n)$ est une base de M et $(a_1, \dots, a_r)$ est une base de P.

d) Démontrons que $a_1$ divise $a_2$. Soit $\psi$ la forme linéaire sur M définie par $\psi(x_1 e_1 + \cdots + x_n e_n) = x_1 + x_2$. Si $m \in \mathrm{P}$, on peut écrire $m = x_1 a_1 e_1 + \cdots + x_r a_r e_r$, d'où $\psi(m) = x_1 a_1 + x_2 a_2 \in (a_1, a_2) = (d)$ ; de plus, choisissant $x$ et $y$ dans A tels que $d = x a_1 + y a_2$, on constate que $\psi(a_1 x e_1 + a_2 y e_2) = d$ et donc $\psi(\mathrm{P}) = (d)$. Par maximalité de $(a_1)$, $(a_1) = (d)$ et $a_1$ divise $a_2$. □

*Remarque 8.1.7.* — L'entier $r$ est le rang de P, bien défini d'après le théorème 6.3.7. On verra plus loin que les idéaux $(a_1) \supset (a_2) \supset \cdots \supset (a_r)$ sont uniquement déterminés par P.

*Exemple 8.1.8.* — Soit M l'ensemble des $(x_1, x_2, x_3) \in \mathbf{Z}^3$ tels que $x_1 + x_2 + x_3$ est pair. Alors, M est un sous-module libre de $\mathbf{Z}^3$ de rang 3. Les trois vecteurs $e_1 = (1,1,0)$ , $e_2 = (1,0,1)$ et $e_3 = (0,0,1)$ forment une base de $\mathbf{Z}^3$ telle que $(e_1, e_2, 2e_3)$ soit une base de M.

*Démonstration.* — Je laisse en exercice le soin de vérifier que M est un sous-$\mathbf{Z}$-module de $\mathbf{Z}^3$. D'après le théorème 8.1.6, M est donc libre de rang $\leq 3$. Pour montrer qu'il est de rang 3, il suffit d'exhiber trois vecteurs de M linéairement indépendants, par exemple $(2,0,0)$, $(0,2,0)$ et $(0,0,2)$.

Pour établir la seconde partie, suivons le fil de la démonstration. Il existe des éléments de M dont les coordonnées sont premières entre elles, par exemple $e_1 = (1,1,0)$ et $e_2 = (1,0,1)$. Alors, on constate que

$$(x, y, z) = y e_1 + z e_2 + (x - y - z)(1,0,0).$$

Posons $e_3 = (1,0,0)$. Il en résulte que $(e_1, e_2, e_3)$ est une base de $\mathbf{Z}^3$ et qu'un vecteur $m = x_1 e_1 + x_2 e_2 + x_3 e_3$ appartient à M si et seulement si la coordonnée $x_3$ est paire. (Remarquer que $x - y - z$ et $x + y + z$ ont même parité.) Par suite, $(e_1, e_2, 2e_3)$ engendre M. Comme ils sont linéairement indépendants, ils en forment une base. □

## 8.2. Modules de type fini

THÉORÈME 8.2.1. — , *Soit* A *un anneau principal et soit* M *un* A*-module de type fini. Il existe alors un unique entier* $r \geq 0$ *et une unique famille d'éléments* $(d_1, \dots d_r)$ *non inversibles tels que* $(d_1) \supset (d_2) \supset \cdots \supset (d_r)$ *et*

$$\mathrm{M} \simeq (\mathrm{A}/(d_1)) \oplus (\mathrm{A}/(d_2)) \oplus \cdots \oplus (\mathrm{A}/(d_r)).$$

DÉFINITION 8.2.2. — *On dit que les éléments* $(d_1, \dots, d_r)$ *sont les facteurs invariants de* M.

COROLLAIRE 8.2.3. — *Si* A *est un anneau principal et si* M *est un* A*-module de type fini* sans torsion*, alors* M *est libre.*

*Démonstration.* — En effet, dans un isomorphisme $\mathrm{M} \simeq \bigoplus_{i=1}^{r} (\mathrm{A}/(d_i))$, l'élément $(\mathrm{cl}(1), 0, \dots)$ est de torsion dès que $d_1 \neq 0$, et n'est pas nul si $d_1$ n'est pas inversible, ce qu'on peut supposer. Donc $d_1 = 0$ et par suite tous les $d_i$ sont nuls. On a ainsi $\mathrm{M} \simeq \mathrm{A}^r$. □

COROLLAIRE 8.2.4. — *Si* A *est un anneau principal et si* M *est un* A*-module de type fini, alors* M *est la somme directe du sous-module de torsion* $\mathrm{M}_{\mathrm{tor}}$ *et d'un* A*-module libre de type fini.*

*Démonstration.* — Fixons un isomorphisme $\mathrm{M} \simeq \bigoplus_{i=1}^{r} (\mathrm{A}/(d_i))$, dans lequel les $d_i$ sont supposés non inversibles (sinon, le facteur $\mathrm{A}/(d_i)$ est nul). Supposons que $d_s \neq 0$ mais que $d_{s+1} = \cdots = d_r = 0$. Un élément $(\mathrm{cl}(a_1), \dots, \mathrm{cl}(a_r))$ est de torsion si et seulement si $a_{s+1} = \cdots = a_r = 0$. On écrit ainsi

$$\mathrm{M} \simeq \bigoplus_{i=1}^{s} (\mathrm{A}/(d_i)) \oplus \mathrm{A}^{s-r},$$

ce qui écrit M comme la somme directe du module de torsion $\bigoplus_{i=1}^{s} (\mathrm{A}/(d_i))$ (car annulé par $d_s$) et du module libre $\mathrm{A}^{s-r}$. □

*Remarque 8.2.5.* — Soit $(d_1, \dots, d_r)$ les facteurs invariants d'un module de type fini M sur un anneau principal. Alors, M est de torsion si et seulement si aucun $d_i$ n'est nul, tandis que M est sans torsion si et seulement si tous ses $d_i$ sont nuls.

*Démonstration du théorème.* — Soit $(m_1, \dots, m_r)$ une famille finie d'éléments de M qui l'engendrent comme A-module. Considérons l'homomorphisme canonique $\varphi\colon \mathrm{A}^r \mapsto \mathrm{M}$ défini par $\varphi(a_1, \dots, a_r) = a_1 m_1 + \dots a_r m_r$. Il est surjectif par définition et son noyau est un sous-module P de $\mathrm{A}^r$.

Considérons alors une base $(e_1, \dots, e_r)$ de $A^r$ et des éléments $(d_1, \dots, d_r)$ de A comme dans le théorème des facteurs invariants (théorème 8.1.6), de sorte que $(d_1 e_1, \dots, d_s e_s)$ est une base de P pour un certain entier $s \in \{0; \dots; r\}$.

Considérons maintenant l'homomorphisme

$$\psi : A^r \to M, \qquad \psi(a_1, \dots, a_r) = \varphi(a_1 e_1 + \cdots + a_r e_r).$$

Comme les $e_i$ forment une base de $A^r$, ile engendrent $A^r$ et $\psi$ est surjectif. Son noyau est l'ensemble des familles $(a_1, \dots, a_r)$ telles que $a_1 e_1 + \cdots + a_r e_r$ appartient au noyau de $\varphi$, c'est-à-dire P. C'est donc l'ensemble des $(a_1, \dots, a_r)$ tels que $a_1$ est multiple de $d_1$, …, $a_r$ est multiple de $d_r$. Ainsi, on constate que M est isomorphe au quotient

$$A^r/((d_1) \oplus \cdots \oplus (d_r)) = (A/(d_1)) \oplus \cdots \oplus (A/(d_r)).$$

L'unicité sera démontrée plus loin (théorème 8.2.8). □

*Décomposition primaire des modules de torsion.* — Soit A un anneau principal et M un A-module de type fini *de torsion*. Pour tout élément irréductible $p$ dans A, définissons

$$M_p = \{m \in M ; \exists r \geq 0, \quad p^r m = 0\}.$$

C'est un sous-module de M : il contient 0, et, s'il contient $m$ et $n$, soit $r$ et $s$ des entiers tels que $p^r m = 0$ et $p^s n = 0$. Alors, on a $p^{\max(r,s)}(am + bn) = 0$ pour tous $a$ et $b$ dans A, donc $M_p$ contient $am + bn$.

Soit $(d_1, \dots, d_r)$ la suite des facteurs invariants de M et pour tout $i \in \{1; \dots; r\}$, notons $d_i = u_i \prod_p p^{n_{p,i}}$ la décomposition en facteurs irréductibles de $d_i$ (avec $u_i \in A^\times$).

Proposition 8.2.6. — *On a les relations*

$$A/(d_i) \simeq \bigoplus_p A/(p^{n_{p,i}}) \quad \textit{et} \quad M_p \simeq \bigoplus_{i=1}^{r} A/(p^{n_{p,i}}).$$

*Par suite,* $M = \bigoplus_p M_p$ .

*Démonstration.* — Comme les idéaux $(p^{n_{p,i}})$ ($i$ étant fixé) sont deux à deux comaximaux, la première formule n'est autre que le théorème chinois (théorème 3.1.6).

Remarquons maintenant que l'on a

$$M \simeq \bigoplus_{i=1}^{r} \left( \bigoplus_p A/(p^{n_{p,i}}) \right) \simeq \bigoplus_p \left( \bigoplus_{i=1}^{r} A/(p^{n_{p,i}}) \right).$$

Ainsi, il suffit de démontrer que dans cet isomorphisme, $M_q$ s'identifie pour tout irréductible $q$ au sous-module $\bigoplus_{i=1}^{r} A/(q^{n_{q,i}})$ du second membre. La formule précédente implique alors que $M = \bigoplus_p M_p$.

Fixons un élément irréductible $q$ et soit $m$ un élément de M. Notons $(m_{p,i})$ ses composantes dans l'isomorphisme ci-dessus et soit $a_{p,i}$ un élément de A tel que $m_{p,i} = \mathrm{cl}(a_{p,i})$.

Supposons que $m \in M_q$. Soit $s \in \mathbf{N}$ tel que $q^s m = 0$. Alors, pour tout $p$ et tout $i$, $p^{n_{p,i}}$ divise $q^s a_{p,i}$. Si $q \neq p$, cela implique que $p^{n_{p,i}}$ divise $a_{p,i}$ (lemme de Gauß) et donc $m_{p,i} = 0$. Par suite, $m$ appartient à $\bigoplus_{i=1}^{r} A/(q^{n_{q,i}})$

Réciproquement, un tel élément est annulé par $q^n$ où $n = \max(n_{q,1}, \ldots, n_{q,r})$. La proposition est donc démontrée. □

Nous allons utiliser cette description pour établir l'unicite des facteurs invariants dans le théorème 8.1.6.

Lemme 8.2.7. — *Soit* A *un anneau principal, p un élément irréductible de* A *et d un élément de* A. *Posons* $M = A/(d)$. *et définisson pour tout* $n \geq 0$, *un* A*-module* $M_n = p^n M/p^{n+1} M$. *Alors,* $M_n$ *est isomorphe à* $A/(p)$ *si* $p^{n+1}$ *divise d et est nul sinon.*

*Démonstration.* — Considérons l'homomorphisme

$$\varphi : A \to p^n M \to M_n, \qquad a \mapsto \mathrm{cl}(p^n \,\mathrm{cl}(a)).$$

Comme tout élément de $p^n M$ est de la forme $p^n \,\mathrm{cl}(a)$ pour $a \in A$, et comme l'homomorphisme canonique $M \to M_n$ est surjectif, l'homomorphisme $\varphi$ est surjectif. On va montrer que le noyau de $\varphi$ est égal à $(p)$ si $p^{n+1}$ divise $d$ et qu'il est égal à A sinon.

Un élément $a \in A$ appartient alors au noyau de $\varphi$ si et seulement s'il existe $b \in A$ tel que $p^n \,\mathrm{cl}(a) = p^{n+1} \,\mathrm{cl}(b)$ dans $A/(d)$, donc si et seulement s'il existe $b \in A$ et $c \in A$ tels que $p^n a - p^{n+1} b = cd$. Ainsi, $a \in \mathrm{Ker}\,\varphi$ si et seulement si $p^n a$ appartient à l'idéal $(d, p^{n+1})$. Écrivons $d = p^r e$ où $p$ ne divise pas $e$ et $r \geq 0$. Alors, $(d, p^{n+1}) = (p^s)$ avec $s = \min(n+1, r)$.

Si $r \leq n$, $s = \min(n+1, r) \leq n$ et tout élément de $a$ est tel que $p^n a$ est multiple de $p^s$, d'où $\mathrm{Ker}\,\varphi = A$ et $M_n = (0)$. Dans l'autre cas, si $r \geq n+1$, $s = n+1$ et un élément $a$ vérifie $p^n a \in (p^{n+1})$ si et seulement si $a \in (p)$ (car A est intègre). Ainsi, $\mathrm{Ker}\,\varphi = (p)$ et $M_n \simeq A/(p)$. □

Théorème 8.2.8 (Unicité des facteurs invariants). — *Soit* A *un anneau principal,* $(d_1, \ldots, d_r)$ *et* $(e_1, \ldots, e_s)$ *deux suites d'élements non inversibles de* A *tels que*

– *pour tout i,* $d_i$ *divise* $d_{i+1}$ *et* $e_i$ *divise* $e_{i+1}$ ;

– $\bigoplus_{i=1}^{r} \mathrm{A}/(d_i)$ *est isomorphe à* $\bigoplus_{j=1}^{s} \mathrm{A}/(d_s)$.

*Alors,* $r = s$ *et pour tout* $i$*, les idéaux* $(d_i)$ *et* $(e_i)$ *sont égaux.*

*Démonstration.* — Pour simplifier les notations par la suite, rajoutons des éléments inversibles au début de la liste des $d_i$ si $r < s$ ou de la liste des $e_j$ si $r > s$. On préserve ainsi les relations de divisibilité et $r$ et $s$ sont égaux — de force. Si on a rajouté un élément inversible au début de la liste des $d_i$, la relation $(d_1) = (e_1)$ impliquera que $e_1$ est aussi inversible, ce qui est absurde. Ainsi, on n'aura rien rajouté et $r$ était bien égal à $s$.

Notons M le module $\bigoplus_{i=1}^{r} \mathrm{A}/(d_i)$. Posons pour tout $i$ et tout $j$,

$$n_{p,i} = \sup\{n \in \mathbf{N}\,;\, p^n \mid d_i\}, \qquad m_{p,j} = \sup\{n \in \mathbf{N}\,;\, p^n \mid e_j.$$

Si $d_i$ est non nul, cela revient à dire que la décomposition en facteurs premiers de $d_i$ s'écrit

$$d_i = u_i \prod_p p^{n_{p,i}}.$$

Si $d_i = 0$, on a $n_{p,i} = +\infty$. Les relations de divisibilité sur les $d_i$ se traduisent en les inégalités $n_{p,1} \leq n_{p,2} \leq \cdots \leq n_{p,r}$ et $m_{p,1} \leq m_{p,2} \leq \cdots \leq m_{p,r}$

Fixons un élément irréductible $p$ de A. Alors, $p^n\mathrm{M}/p^{n+1}\mathrm{M}$ est un A-module isomorphe à $(\mathrm{A}/p)^t$, où $t$ est le plus grand entier tel que $p^{n+1}$ divise $d_{r-t+1}$. De plus, comme A est un anneau principal, l'idéal $(p)$ est maximal, donc $p^n\mathrm{M}/p^{n+1}\mathrm{M}$ est naturellement un $\mathrm{A}/p$-espace vectoriel. Sa dimension est ainsi égale au plus grand entier $t$ tel que $p^{n+1}$ divise $d_{r-t+1}$. Par suite, pour tout $k \geq 0$,

$$n_{p,r-t+1} \geq k+1 \Leftrightarrow \dim_{\mathrm{A}/p}(p^n\mathrm{M}/p^{n+1}\mathrm{M}) \geq t \Leftrightarrow m_{p,r-t+1} \geq k+1.$$

Ainsi, $n_{p,t} = m_{p,t}$ pour tout $t$.

Comme $p$ est arbitraire, on a $n_{p,t} = m_{p,t}$ pour tout $t$ et tout irréductible $p$. Par suite, pour tout $t$, on a l'égalité d'idéaux $(d_t) = (e_t)$. □

*Exercice 8.2.9.* — Calculer les facteurs invariants des modules $(\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$ et $(\mathbf{Z}/6\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z})$.

*Solution.* — Comme 3 et 5 sont premiers entre eux, $(\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$ est isomorphe à $\mathbf{Z}/15\mathbf{Z}$. Il n'a qu'un facteur invariant, égal à 15.

Les entiers 6 et 4 ne sont pas premiers entre eux, mais on a $6 = 2 \cdot 3$ et 2 et 3 sont premiers entre eux, d'où

$$(\mathbf{Z}/6\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z}) \simeq (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z}).$$

Comme 3 et 4 sont premiers entre eux, on peut les regrouper et

$$(\mathbf{Z}/6\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z}) \simeq (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/12\mathbf{Z})$$

dont les facteurs invariants sont $(2; 12)$. □

Dans le but de fournir une seconde démonstration de l'unicité, reformulons le théorème des facteurs invariants en termes de matrices.

PROPOSITION 8.2.10. — *Soit* A *un anneau principal et soit* $M \in \mathrm{Mat}_{r,n}(A)$ *une matrice à r colonnes et n lignes à coefficients dans* A *dont les colonnes sont linéairement indépendantes. Alors, il existe deux matrices* $P \in \mathrm{GL}_n(A)$ *et* $Q \in \mathrm{GL}_r(A)$, *des éléments non nuls* $d_1, \ldots, d_r$ *de* A *tels que* $d_1 \mid d_2 \cdots \mid d_r$ *de sorte que*

$$PMQ = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \\ & 0 & \end{pmatrix}.$$

*Démonstration.* — Considérons le sous-module V de $A^n$ engendré par les vecteurs colonnes $(v_1, \ldots, v_r)$ de M. Par définition, il est libre de rang $r$. Notons $(\varepsilon_1, \ldots, \varepsilon_n)$ la base canonique de $A^n$. Ainsi, M est la matrice de l'injection $V \to A^n$ dans les bases $(v_1, \ldots, v_r)$ et $(\varepsilon_1, \ldots, \varepsilon_n)$.

D'après le théorème des facteurs invariants, il existe une base $(e_1, \ldots, e_n)$ de $A^n$ et des éléments $(d_1, \ldots, d_r)$ de A tels que $(d_1e_1, \ldots, d_re_r)$ soit une base de V et tels que $d_1 \mid d_2 \mid \cdots \mid d_r$.

Soit alors P la matrice de passage de la base $(e_1, \ldots, e_n)$ à la base $(\varepsilon_1, \ldots, \varepsilon_n)$ dans $A^n$ et soit Q la matrice de passage de la base $(v_1, \ldots, v_r)$ à la base $(d_1e_1, \ldots, d_re_r)$ dans V. Alors, PMQ est la matrice de l'injection $V \to A^n$ dans les bases $(d_1e_1, \ldots, d_re_r)$ sur V et $(e_1, \ldots, e_n)$ sur $A^n$. Elle est exactement comme indiqué dans l'énoncé de la proposition. □

COROLLAIRE 8.2.11. — *Avec les notations précédentes, pour tout* $s \in \{1; \ldots; r\}$, *l'idéal* $(d_1 \ldots d_s)$ *est l'idéal engendré par les mineurs* $s \times s$ *de la matrice* M.

*Démonstration.* — Remarquons que la formule est vérifiée si M est diagonale $(d_1, \ldots, d_r)$ comme dans la conclusion du théorème. Le corollaire sera démontré dès que l'on établit que cet idéal engendré par les mineurs de taille donnée de M est inchangé lorsqu'on multiplie M par une matrice inversible à droite ou à gauche.

Soit ainsi $I \subset \{1; \ldots; n\}$ et $J \subset \{1; \ldots; r\}$ deux parties de cardinal $s$ et soit P un élément de $\mathrm{Mat}_n(A)$. Les colonnes de PM sont des combinaisons linéaires des colonnes de M. Par suite, la $n$-linéarité des déterminants montre que le mineur (I,J) de PM est une combinaison linéaire des mineurs de rang $s$ dans M. Ainsi, l'idéal $\mathscr{I}_{PM}$ engendré par les mineurs de rang $s$ de M est contenu dans l'idéal $\mathscr{I}_M$. Si P est inversible, on a l'inclusion

$$\mathscr{I}_M = \mathscr{I}_{P^{-1}PM} \subset \mathscr{I}_{PM},$$

d'où finalement l'égalité.

L'argument lorsqu'on multiplie M par une matrice de $\mathrm{GL}_r(\mathrm{A})$ à droite est identique en échangeant lignes et colonnes. □

## 8.3. Exemples

Pour nous, les deux exemples fondamentaux d'anneaux principaux sont $\mathbf{Z}$ et $k[\mathrm{X}]$, $k$ étant un corps commutatif.

Rappelons qu'un $\mathbf{Z}$-module de type fini n'est rien d'autre qu'un groupe abélien fini. Il résulte alors du théorème des facteurs invariants le théorème suivant.

THÉORÈME 8.3.1. — *Si* G *est un groupe abélien de type fini, il existe un unique entier* $r \geq 0$ *et une unique famille d'entiers strictement positifs* $(d_1; \ldots; d_s)$ *telle que* $d_1$ *divise* $d_2 \ldots$ *qui divise* $d_s$ *et telle que*

$$\mathrm{G} \simeq \mathbf{Z}^r \oplus (\mathbf{Z}/d_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/d_s\mathbf{Z}).$$

*8.3.2. Matrices et modules sur l'anneau des polynômes.* — Soit $k$ un corps. On va s'intéresser maintenant à certains $k[\mathrm{X}]$-modules. Pour commencer, rappelons quelques résultats de l'exercice 6.6.7. Soit V un $k$-espace vectoriel et $u$ un endomorphisme de V. On définit alors une structure de $k[\mathrm{X}]$-module sur V en posant pour tout polynôme $\mathrm{P} \in k[\mathrm{X}]$ et tout $v \in \mathrm{V}$, $\mathrm{P} \cdot v = \mathrm{P}(u)(v)$. Si $\mathrm{P} = \sum_{n=0}^{d} a_n \mathrm{X}^n$, on a ainsi

$$\mathrm{P} \cdot v = \sum_{n=0}^{d} a_n u^n(v).$$

On note $\mathrm{V}_u$ le $k[\mathrm{X}]$-module ainsi obtenu.

Si V′ est un autre $k$-espace vectoriel et $u'$ un endormorphisme de V′, un homomorphisme (de $k[\mathrm{X}]$-modules) de $\mathrm{V}_u$ dans $\mathrm{V}'_{u'}$ est la donnée d'une application $k$-linéaire $f : \mathrm{V} \to \mathrm{V}'$ telle que $f \circ u = u' \circ f$.

En particulier, si $\mathrm{V}' = \mathrm{V}$, les $k[\mathrm{X}]$-modules $\mathrm{V}_u$ et $\mathrm{V}_{u'}$ sont isomorphes si et seulement si il existe $f \in \mathrm{GL}(\mathrm{V})$ telle que $u = f^{-1}u'f$, c'est-à-dire si $u$ et $u'$ sont *conjugués*. (En termes de matrices, on dit *semblables*.)

DÉFINITION 8.3.3. — *Un* $k[\mathrm{X}]$*-module* M *est dit cyclique s'il existe un polynôme* $\mathrm{P} \in k[\mathrm{X}]$ *non nul tel que* $\mathrm{M} \simeq k[\mathrm{X}]/(\mathrm{P})$.

LEMME 8.3.4. — *Si* V *est un* $k$*-espace vectoriel,* $u$ *un endormorphisme de* V*, le* $k[\mathrm{X}]$*-module* $\mathrm{V}_u$ *est cyclique si et seulement si il existe un vecteur* $v \in \mathrm{V}$ *et un entier* $n \geq 1$ *tels que la famille* $(v, u(v), \ldots, u^{n-1}(v))$ *soit une base de* V.

*Démonstration.* — Commençons la démonstration par une remarque. Si P est un polynôme non nul, le $k[\mathrm{X}]$-module cyclique $k[\mathrm{X}]/(\mathrm{P})$ est de dimension finie

comme $k$-espace vectoriel, dimension d'ailleurs égale au degré de P. De plus, si $n = \deg \mathrm{P}$, les éléments $\mathrm{cl}(1)$, $\mathrm{cl}(\mathrm{X})$, …, $\mathrm{cl}(\mathrm{X}^{n-1})$ en forment une base.

Soit maintenant V un $k$-espace vectoriel et $u$ un endormorphisme de V. Si $\mathrm{V}_u$ est cyclique, l'image de X par un isomorphisme $k[\mathrm{X}]/(\mathrm{P}) \simeq \mathrm{V}_u$ est un élément $v$ de V tel que $(v, u(v), \ldots, u^{n-1}(v))$ soit une base de V. Réciproquement, si $v \in \mathrm{V}$ est un vecteur tel que la famille $(v, u(v), \ldots, u^{n-1}(v))$ soit une base de V, écrivons $u^n(v) = \sum_{p=0}^{n-1} a_p u^p(v)$ dans cette base. Alors l'homomorphisme $\varphi\colon k[\mathrm{X}] \to \mathrm{V}$, $\mathrm{P} \mapsto \mathrm{P}(u)(v)$ est surjectif et un polynôme P est dans le noyau si et seulement s'il est multiple du polynôme $\Pi = (\mathrm{X}^n - \sum_{p=0}^{n-1} a_p \mathrm{X}^p)$. En effet, la division euclidienne de P par $\Pi$ est un polynôme R de degré $< n$. Si $\mathrm{R} \neq 0$ mais si son image par $\varphi$ est nul, on obtient une relation de dépendance linéaire non triviale entre $(v, \ldots, u^{n-1}(v))$, ce qui est absurde. □

*Remarque 8.3.5.* — Si $\mathrm{V}_u$ est un endomorphisme cyclique, la matrice de $u$ dans la base $(v, \ldots, u^{n-1}(v))$ est égale à

$$\begin{pmatrix} 0 & & & a_0 \\ 1 & 0 & & a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 \quad 0 & a_{n-1} \end{pmatrix},$$

c'est-à-dire à la matrice compagnon $\mathrm{C}_\Pi$ du polynôme $\Pi = \mathrm{X}^n - a_{n-1}\mathrm{X}^{n-1} - \cdots - a_1\mathrm{X} - a_0$. De plus, $\Pi$ est le polynôme minimal et le polynôme caractéristique de cette matrice.

Les rappels qui précèdent et le théorème 8.2.1 établissent le théorème suivant.

THÉORÈME 8.3.6. — *Soit $k$ un corps. Soit V un $k$-espace vectoriel de dimension finie et $u$ un endomorphisme de V. Il existe alors une unique famille $(\mathrm{P}_1, \ldots, \mathrm{P}_r)$ de polynômes unitaires (non constants) dans $k[\mathrm{X}]$ tels que $\mathrm{P}_1$ divise…qui divise $\mathrm{P}_r$ et telle que la matrice de $u$ soit semblable à la matrice diagonale par blocs*

$$\begin{pmatrix} \mathrm{C}_{\mathrm{P}_1} & & & \\ & \mathrm{C}_{\mathrm{P}_2} & & \\ & & \ddots & \\ & & & \mathrm{C}_{\mathrm{P}_r} \end{pmatrix}.$$

Les polynômes $(\mathrm{P}_1, \ldots, \mathrm{P}_r)$ sont appelés facteurs invariants de $u$. On constate sur l'expression matricielle ci-dessus $\mathrm{P}_r$ est le polynôme minimal de $u$, tandis que $\mathrm{P}_1 \ldots \mathrm{P}_r$ est son polynôme caractéristique.

COROLLAIRE 8.3.7. — *En particulier deux endomorphismes $u$ et $u'$ sont semblables s'ils ont même famille de facteurs invariants.*

*Exercice 8.3.8* (Décomposition de Jordan). — Soit $k$ un corps algébriquement clos. Soit V un $k$-espace vectoriel de dimension finie et $u$ un endomorphisme de V. Montrer que V possède une base dans laquelle la matrice de $u$ est diagonale par blocs, chaque bloc étant un « bloc de Jordan » de la forme

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}$$

(*Utiliser la décomposition du $k[X]$-module $V_u$ fournie par la proposition 8.2.6.*)

Toute la théorie qui précède a un corollaire amusant, facile, mais non trivial si on évite la théorie des facteurs invariants.

COROLLAIRE 8.3.9. — *Soit K un corps et $k \subset K$ un sous-corps. Soit A et B deux matrices de $\mathrm{Mat}_n(k)$ qui soient semblables en tant que matrices de $\mathrm{Mat}_n(K)$, c'est-à-dire qu'il existe $P \in \mathrm{GL}_n(K)$ telle que $B = P^{-1}AP$. Alors, A et B sont semblables sur $k$ : il existe Q dans $\mathrm{GL}_n(k)$ telle que $B = Q^{-1}AQ$.*

*Démonstration.* — Notons $(P_1, \dots, P_r)$ la famille des facteurs invariants de A en tant que matrice à coefficients dans $k$. Il existe donc une base de $V = k^n$ dans laquelle la matrice de A est une diagonale-blocs de matrices compagnons de polynômes caractéristiques $(P_1, \dots, P_r)$. La même matrice de changement de base fournit une base de $K^n$ dans laquelle la matrice de A est la même diagonale par blocs. En particulier, les facteurs invariants de A en tant que matrice à coefficients dans K sont aussi les $P_i$.

Soit maintenant $(Q_1, \dots, Q_s)$ la famille des facteurs invariants de B en tant que matrice à coefficients dans $k$, ou dans K, puisque c'est la même chose. Puisque A et B sont semblables en tant que matrices à coefficients dans K, on a les égalités $r = s$ et $P_1 = Q_1$, …, $P_r = Q_r$. Par suite A et B sont semblables en tant que matrices à coefficients dans $k$. □

*8.3.10. Calcul des facteurs invariants d'une matrice.* — Nous allons utiliser le corollaire 8.2.11 pour calculer les facteurs invariants d'une matrice.

PROPOSITION 8.3.11. — *Soit $k$ un corps et soit A une matrice de $M_n(k)$. Pour tout entier $r$ compris entre 1 et $n$, soit $\Delta_r \in k[X]$ le pgcd des mineurs d'ordre $r$ de la matrice $XI_n - A$. Alors, il existe des polynômes $P_1, \dots, P_n$ dans $k[X]$ tels que*

$$P_1 = \Delta_1, \quad P_1P_2 = \Delta_2, \quad \dots, P_1 \dots P_n = \Delta_n.$$

*Pour tout $r$, $\mathrm{P}_r$ divise $\mathrm{P}_{r+1}$ et si $r$ est le plus petit entier tel que $\mathrm{P}_r \neq 1$, les facteurs invariants de* A *sont les* $(\mathrm{P}_{r+1}, \ldots, \mathrm{P}_n)$.

*Démonstration.* — Posons $\mathrm{A} = k[\mathrm{X}]$. Pour déduire cette proposition du corollaire 8.2.11, Il suffit de remarquer que, notant $(e_1, \ldots, e_n)$ la base canonique de $\mathrm{A}^n$, l'homomorphisme

$$\varphi \colon \mathrm{A}^n \to \mathrm{A}^n, \qquad e_i \mapsto \mathrm{X}e_i - u(e_i)$$

a pour matrice $\mathrm{XI}_n - \mathrm{A}$ et que $(k^n)_{\mathrm{A}}$ est isomorphe à $\mathrm{A}^n / \operatorname{Im}\varphi$. □

## 8.4. Exercices

*Exercice 8.4.1.* — Soient A un anneau principal et L, M deux A-modules de type fini. Montrer que $\mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{M})$ est un A-module de type fini.

*Exercice 8.4.2.* — Soit A un anneau principal et M un A-module de type fini.

**a)** Justifier l'existence d'éléments $m_i$ (pour $1 \leq i \leq s$) de M d'annulateurs $(d_i)$, avec $d_1 | \ldots | d_s$, tel que

$$\mathrm{M} = \bigoplus_{i=1}^{s} \mathrm{A}m_i.$$

**b)** Soit $i \in \{1, \ldots, s\}$. Montrer qu'il existe $u_i \in \mathrm{End}_{\mathrm{A}}(\mathrm{M})$ tel que

$$u_i(m_1) = \cdots = u_i(m_{s-1}) = 0, \quad u_i(m_s) = m_i.$$

**c)** Soit $u \in \mathrm{End}_{\mathrm{A}}(\mathrm{M})$ qui commute à tout autre élément de $\mathrm{End}_{\mathrm{A}}(\mathrm{M})$. Montrer qu'il existe $a \in \mathrm{A}$ tel que $u(m) = am$ pour tout $m$.

**d)** Soit $u : \mathrm{M} \to \mathrm{M}$ une application additive telle que pour tout $v \in \mathrm{End}_{\mathrm{A}}(\mathrm{M})$, $u \circ v = v \circ u$. Montrer que $u$ est une homothétie $m \mapsto am$, pour $a \in \mathrm{A}$.

**e)** Soit K un corps commutatif, E un K-espace vectoriel de dimension finie sur K et $u \in \mathrm{End}_{\mathrm{K}}(\mathrm{E})$. Montrer que tout endomorphisme de E qui commute à tout endomorphisme commutant à $u$ est un polynôme en $u$. (*On pourra utiliser la structure de* $\mathrm{K}[\mathrm{X}]$*-module sur* E *définie par* $u$.)

*Exercice 8.4.3.* — Dans $\mathrm{M}_n(\mathbf{Z})$, on définit la relation $\mathrm{A} \sim \mathrm{B}$ si et seulement s'il existe P et Q dans $\mathrm{GL}_n(\mathrm{Z})$ tels que $\mathrm{AP} = \mathrm{QB}$.

**a)** Montrer que c'est une relation d'équivalence.

**b)** Montrer que l'ensemble des matrices de la forme $\mathrm{diag}(d_1, \ldots, d_n)$, où les $d_i$ sont des entiers positifs vérifiant $d_1 | d_2 | \ldots | d_n$ est un système de représentants des classes d'équivalences.

**c)** Généraliser les questions précédentes au cas d'un anneau principal quelconque.

**d)** Retrouver un résultat du cours de DEUG lorsque A est un corps.

*Exercice 8.4.4.* — Soit A un anneau principal et L un A-module libre de rang fini. Soit M un sous-**Z**-module de L. Montrer qu'il possède un supplémentaire dans L si et seulement si L/M est sans-torsion.

*Exercice 8.4.5.* — Soit M un module libre de type fini sur un anneau principal A.

**a)** Soit $m \in \mathrm{M}$ non nul. Montrer que les propriétés suivantes sont équivalentes :
(1) $m$ fait partie d'une base ;
(2) il existe $f \in \mathrm{M}^*$ tel que $f(m) = 1$ ;
(3) les coordonnées de $m$ dans *toute* base de M sont premières entre elles ;
(4) les coordonnées de $m$ dans *une* base de M sont premières entre elles ;
(5) si $m = am'$ avec $a \in \mathrm{A}$, alors $a \in \mathrm{A}^\times$ ;
(6) si $am = a'm'$ avec $a \in \mathrm{A}$, $a' \in \mathrm{A}$ et $a \neq 0$, alors $a$ est multiple de $a'$.
On dit qu'un tel vecteur est primitif.

**b)** Montrer que tout vecteur est multiple d'un vecteur primitif.

**c)** *Exemple :* $\mathrm{A} = \mathbf{Z}$, $\mathrm{M} = \mathbf{Z}^4$, $m = (126, 210, 168, 504)$.

*Exercice 8.4.6.* — Soit M une matrice à $n$ lignes et $p$ colonnes ($p \leq n$) dont les coefficients sont dans un anneau principal A.

Montrer qu'on peut compléter M en une matrice $\mathrm{P} \in \mathrm{GL}(n, \mathrm{A})$ si et seulement si le pgcd des mineurs d'ordre $p$ de A est égal à 1.

*Exercice 8.4.7.* — Soit A un anneau principal, K son corps des fractions.

**a)** Soit $x$ un élément non nul de $\mathrm{K}^n$. Montrer qu'il existe une matrice de $\mathrm{GL}_n(\mathrm{A})$ dont la colonne est proportionnelle à $x$.

**b)** Démontrer que toute matrice carrée d'ordre $n$ à coefficients dans K est produit d'une matrice de $\mathrm{GL}_n(\mathrm{A})$ et d'une matrice triangulaire de $\mathrm{M}_n(\mathrm{K})$. (Raisonner par récurrence.)

**c)** *Application numérique :* $\mathrm{A} = \mathbf{Z}$ et

$$\mathrm{M} = \begin{pmatrix} 1/2 & 1 & -1/4 \\ 2/5 & 2 & 2/3 \\ 3/4 & 1/7 & -1 \end{pmatrix}.$$

*Exercice 8.4.8.* — Soit A un anneau principal et M un A-module de type fini. On note $(d_1, \ldots, d_r)$ les facteurs invariants de M.

Montrer que toute famille génératrice d'éléments de M a au moins $r$ éléments.

*Exercice 8.4.9.* — **a)** Soit G un groupe abélien fini. Soit $n$ le plus petit entier $\geq 1$ tel que $n\mathrm{G} = 0$. Montrer qu'il existe $g \in \mathrm{G}$ d'ordre $n$, c'est-à-dire tel que $n$ est le plus petit entier $\geq 1$ tel que $ng = 0$.

**b)** Soit K un corps commutatif et soit G un sous-groupe fini de $\mathrm{K}^*$. Montrer que G est cyclique.

En particulier, le groupe multiplicatif d'un corps fini est cyclique.

## 8.5. Solutions

*Solution de l'exercice 8.4.1.* — Comme A est principal, tout A-module de type fini est somme directe de A-modules égaux à A ou à $A/aA$. De plus,

$$\mathrm{Hom}(L \oplus L', M) = \mathrm{Hom}(L, M) \oplus \mathrm{Hom}(L', M).$$

Par récurrence, il suffit ainsi de traiter le cas où $L = A$ et le cas où $L = A/a$ avec $a \in A$ non nul. Dans le premier cas, $\mathrm{Hom}_A(L, M) = \mathrm{Hom}_A(A, M) = M$ est un A-module de type fini. Dans le second cas,

$$\mathrm{Hom}_A(L, M) = \mathrm{Hom}_A(A/a, M) = \{m \in M\,;\, ax = 0\} = M_a$$

est l'ensemble des éléments de M qui sont annulés par $a$. C'est un sous-A-module de M. Comme A est principal, il est noethérien et $M_a$ est de type fini.

*Solution de l'exercice 8.4.2.* — **a)** C'est exactement le théorème de structure des modules de type fini sur un anneau principal.

**b)** D'après la question précédente, M est le quotient de $A^s$ par le sous-module $(d_1) \oplus \cdots \oplus (d_s)$. Si la base canonique de $A^s$ est notée $(e_1, \ldots, e_s)$, il suffit donc de prouver que l'homomorphisme $u : A^s \to M$ tel que $u(e_j) = 0$ pour $j < s$ et $u(e_s) = m_i$ a un noyau qui contient $(d_1) \oplus \cdots \oplus (d_s)$. Or, soit $x = (a_1, \ldots, a_s) \in A^s$, avec $a_i \in (d_i)$ pour tout $i$ ; on a donc $u(x) = a_s m_i = 0$ car $a_s$ est multiple de $d_s$, donc de $d_i$ et $d_i m_i = 0$.

**c)** Soit $u$ un élément du centre de $\mathrm{End}_A(M)$. Soient $(a_{i,j})$ des éléments de A tels que pour tout $i$,

$$u(m_i) = \sum_{j=1}^{s} a_{i,j} m_j.$$

Si $i \in \{1, \ldots, s\}$, on a en particulier $u \circ u_i = u_i \circ u$. On en déduit que

$$\begin{aligned} u(m_i) &= u(u_i(m_s)) = u_i(u(m_s)) \\ &= u_i(\textstyle\sum a_{s,j} m_j) = u_i(a_{s,s} m_s) \\ &= a_{s,s} m_i. \end{aligned}$$

Autrement dit, en posant $a = a_{s,s}$, on a $u(m_i) = a m_i$ pour tout $i$, d'où le résultat puisque $u$ est un endomorphisme de M.

**d)** Maintenant, on suppose juste que $u$ est additif. Soit $\lambda \in A$ et $\mu : M \to M$ la multiplication par $\lambda$. On a

$$u(\lambda m) = u(\mu(m)) = \mu(u(m)) = \lambda u(m),$$

autrement dit, $u$ est un homomorphisme de A-modules. D'après la question précédente, $u$ est une homothétie.

**e)** Considérons E comme un K[X]-module en posant $P(X) \cdot m = P(u)(m)$. Les endomorphismes de E comme K[X]-module sont les K-endomorphismes tels que $P(u) \circ v = v \circ P(u)$, autrement dit, ce sont les endomorphismes de E qui commutent à $u$. Soit $v$ un K-endomorphisme de E qui commute à tout endomorphisme de E qui commute à $u$, cela signifie donc que $v$ commute à tout K[X]-endomorphisme de E. De plus, $v$ étant K-linéaire, il est a fortiori additif. D'après la question précédente, $v$ est une homothétie : il existe $P \in K[X]$ tel que $v(m) = P(X) \cdot m = P(u)(m)$. Autrement dit, $v$ est un polynôme en $u$.

*Solution de l'exercice 8.4.3.* — **a)** Elle est réflexive : avec $P = Q = I$, on a $AI = IA$, donc $A \sim A$. Elle est symétrique : si $A \sim B$, soit $AP = QB$, alors $BP^{-1} = Q^{-1}Q$, donc $B \sim A$. Elle est transitive : si $A \sim B$, soit $AP = QB$ et $B \sim C$, soit $BR = SC$, on a $C = S^{-1}BR = S^{-1}Q^{-1}APR$, d'où $(QS)C = A(PR)$, et donc $A \sim C$.

C'est donc une relation d'équivalence.

**b)** Soit $A \in M_n(\mathbf{Z})$. L'image de $\mathbf{Z}^n$ par A est un sous-$\mathbf{Z}$-module de $\mathbf{Z}^n$. Les facteurs invariants de $\mathbf{Z}^n/A(\mathbf{Z}^n)$ ne dépendent que de la classe d'équivalence de A pour la relation introduite dans l'exercice. En effet, si $A \sim B$, soit $AP = QB$, alors

$$\begin{aligned}\mathbf{Z}^n/B(\mathbf{Z}^n) &\simeq Q(\mathbf{Z}^n)/QB(\mathbf{Z}^n) = \mathbf{Z}^n/QB(\mathbf{Z}^n)\\ &= \mathbf{Z}^n/AP(Z^n) = \mathbf{Z}^n/A(\mathbf{Z}^n)\end{aligned}$$

car $Q(\mathbf{Z}^n) = \mathbf{Z}^n$ et $P(\mathbf{Z}^n) = \mathbf{Z}^n$.

D'après le théorème de structure, il existe une base $(f_1, \dots, f_n)$ de $\mathbf{Z}^n$ et des entiers $d_1, \dots, d_n$ avec $d_1 | \dots | d_n$ tels que $A(\mathbf{Z}^n)$ soit engendré par les $d_i f_i$. On peut bien sûr supposer $d_i \geq 0$ pour tout $i$. Soit P la matrice de la famille $(f_i)$ dans la base canonique $(e_i)$, on a ainsi $P(e_i) = f_i$, et soit $\Delta$ la matrice $\mathrm{diag}(d_1, \dots, d_n)$. Ainsi, A et $P\Delta$ ont même image. Comme cette image est un sous-$\mathbf{Z}$-module de $\mathbf{Z}^n$, il est libre, et on a des isomorphismes

$$\mathbf{Z}^n \simeq A(\mathbf{Z}^n) \oplus \mathrm{Ker}\, A, \quad \mathbf{Z}^n \simeq P\Delta(\mathbf{Z}^n) \oplus \mathrm{Ker}(\mathbf{P}\Delta).$$

Enfin, les noyaux de A et $P\Delta$ ont nécessairement même rang, donc son isomorphes. Il existe ainsi un isomorphisme $Q : \mathbf{Z}^n \to \mathbf{Z}^n$ tel que $AQ = P\Delta$. Finalement, on a $A \sim \Delta$.

**c)** La même démonstration s'applique mot pour mot au cas d'un anneau principal quelconque. Pour fixer le choix des facteurs invariants, il suffit de choisir un élement irréductible dans chaque classe et de prendre les $d_i$ parmi les produits de ces éléments irréductibles, et 0.

**d)** Si A est un corps, on a $d_i = 1$ ou 0. La relation d'équivalence est étudiée en DEUG sous le nom de « matrices équivalentes » et on y démontre en général que deux matrices sont équivalentes si et seulement si elles ont même rang.

*Solution de l'exercice 8.4.4.* — La condition est nécessaire car un supplémentaire de M dans L est à la fois sans torsion et isomorphe à L/M. Inversement, si L/M est sans-torsion, le théorème de structure permet d'affirmer que L/M est un A-module libre. Choisissons-en une base $(\mathrm{cl}(\ell_1), \dots, \mathrm{cl}(\ell_r))$ avec des $\ell_i \in \mathrm{L}$ et soit N le sous-module de L engendré par les $\ell_i$. L'homomorphisme canonique $\mathrm{L} \to \mathrm{L/M}$ induit un homomorphisme surjectif $\mathrm{N} \to \mathrm{L/M}$, mais aussi injectif car si $\mathrm{cl}(\sum a_i \ell_i) = 0$, tous les $a_i$ sont nuls, les $\mathrm{cl}(\ell_i)$ formant une base de L/M. Donc $\mathrm{L} \simeq \mathrm{M} \oplus \mathrm{N}$.

*Solution de l'exercice 8.4.5.* — **a)** (1)⇒ (2). — Supposons que $m$ fait partie d'une base. Si $(e_1, e_2, \dots, e_n)$ est une base de M, avec $m = e_1$, soit $f$ l'applciation linéaire telle que $a_1 e_1 + \cdots + a_n e_n \mapsto a_1$. On a ainsi $f(m) = f(e_1) = 1$.

(2)⇒ (3). — Soit $f \in \mathrm{M}^*$ telle que $f(m) = 1$. Soit $(e_1, \dots, e_n)$ une base de M et écrivons $m = a_1 e_1 + \cdots + a_n e_n$. Alors,

$$1 = f(m) = a_1 f(e_1) + \cdots + a_n f(e_n)$$

ce qui montre que les $a_i$ sont premiers entre eux.

(3)⇒ (4). — C'est évident (car un module libre possède une base).

(4)⇒ (5). — Soit $(e_1, \dots, e_n)$ une base de M dans laquelle les coordonnées $(a_1, \dots, a_n)$ de $m$ soient premières entre elles. Soit $m' \in \mathrm{M}$ et $a \in \mathrm{A}$ tels que $m = am'$. Notons $(a'_1, \dots, a'_n)$ les coordonnées de $m'$ dans cette base. Ainsi, pour tout $i$ on a $a_i = aa'_i$ et l'idéal $(a_1, \dots, a_n) = \mathrm{A}$ est contenu dans l'idéal $(a)$. Par suite, $a$ est inversible.

(5)⇒ (6). — Supposons que $am = a'm'$. Comme $a \neq 0$, $a'$ est non nul. Soit $d$ le pgcd de $a$ et $a'$ et écrivons $a = db$, $a' = db'$, on a donc $d(bm - b'm') = 0$ et comme M est libre, donc sans torsion, $bm = b'm'$, ce qui permet de supposer que $b$ et $b'$ premiers entre eux.

Soit alors $u$ et $v$ des éléments de A tels que $bu + b'v = 1$. On a

$$m = (bu + b'v)m = bum + b'vm = b'um' + b'vm = b'(vm + um').$$

Par hypothèse, $b'$ est inversible, ce qui prouve que $a'$ divise $a$, ou encore que $a$ est multiple de $a'$.

(6)⇒ (1). — En vertu de l'exercice 8.4.4, il suffit de montrer que le A-module M/A$m$ est sans torsion. Soit $m' \in \mathrm{M}$ tel que $\mathrm{cl}(m')$ est un élément de torsion dans M/A$m$. Cela signifie qu'il existe $b \in \mathrm{A}$, $b \neq 0$, tel que $b\,\mathrm{cl}(m') = 0$, c'est-à-dire $bm' \in \mathrm{A}m$. Autrement dit, il existe $a$ et $b$ dans A, *non nuls*, tels que $bm' = am$. Par hypothèse, $a$ est multiple de $b$. Si on écrit $a = bc$, on obtient $b(cm - m') = 0$ et comme M est sans torsion, $m' = cm \in \mathrm{A}m$ et donc $\mathrm{cl}(m') = 0$.

**b)** Soit $(e_1, \dots, e_n)$ une base de M et $(a_1, \dots, a_n)$ un vecteur non nul de M. Soit $d$ le pgcd des $a_i$ et écrivons $a_i = db_i$ pour tout $i$. Alors, le vecteur $(b_1, \dots, b_n)$ est primitif.

**c)** On a

$$126 = 2 \cdot 3^2 \cdot 7, \quad 210 = 2 \cdot 3 \cdot 5 \cdot 7, \quad 168 = 2^3 \cdot 3 \cdot 7 \quad \text{et} \quad 504 = 2^3 \cdot 3^2 \cdot 7.$$

Par suite, le pgcd de ces entiers est égal à $2 \cdot 3 \cdot 7 = 42$ si bien que le vecteur $(126; 210; 168; 504)$ est égal à 42 fois le vecteur $(3; 5; 4; 12)$.

*Solution de l'exercice 8.4.6.* — Soit $V \subset A^n$ l'image de l'homomorphisme $A^p \to A^n$ de matrice M. Notons pour tout $r \leq p$, $\Delta_r$ le pgcd des mineurs d'ordre $r$ de A. Comme $\Delta_p = 1$, les $p$ vecteurs colonnes de M sont linéairement indépendants donc forment une base du A-module V qu'ils engendrent. D'après l'exercice 8.4.4, il suffit ainsi de montrer que le A-module $A^n/V$ est sans torsion, voire libre.

Or, d'après le corollaire 8.2.11 du cours, $A^n/V$ est un A-module de type fini isomorphe à une somme directe $\bigoplus_{i=1}^{p} A/(d_i) \oplus A^{n-p}$ telle que les facteurs invariants $d_1, \ldots, d_p$ vérifient pour tout $r \leq p$ la relation $\Delta_r = d_1 \ldots d_r$ (à un élément inversible près). Si $\Delta_p = 1$, tous les $d_i$ sont 1 et $A^n/V \simeq A^{n-p}$ est donc un A-module libre.

*Solution de l'exercice 8.4.7.* — **a)** Il existe une matrice de $GL_n(A)$ de première colonne $v_1 = (a_1, \ldots, a_n)$ fixée si et seulement si on peut compléter cette colonne en une base de $A^n$, c'est-à-dire si $A^n/Av_1$ est un A-module libre. D'après l'exercice 8.4.4, il faut et il suffit que le A-module $A^n/Av_1$ soit sans torsion, c'est-à-dire que les coordonnées de $v_1$ soient premières entre elles.

Pour répondre à la question, il suffit maintenant de remarquer que tout élément non nul de $K^n$ s'écrit $x = \lambda v_1$ avec $\lambda \in K$ et $v_1 \in A^n$ à coordonnées premières entre elles.

*Autre méthode :* choisir $\alpha \in A \setminus \{0\}$ tel que $x' = \alpha x$ appartient à $A^n$ et appliquer le théorème de structure au sous-module $Ax' \subset A^n$.

**b)** Soit M une matrice carée d'ordre $n$ à coefficients dans K. Si la première colonne de M n'est pas nulle, il existe d'après la première question un élément non nul $\lambda \in K$ et une matrice carrée $U_1 \in GL_n(A)$ telle que $U_1^{-1}M$ ait $(\lambda, 0, \ldots, 0)$ pour première colonne. Posons $M_1 = U_1^{-1}M$. Si la première colonne de M est nulle, on pose $U_1 = I_n$ et $M_1 = M$.

On écrit alors $M_1$ par blocs

$$M_1 = \begin{pmatrix} \lambda & L_1' \\ 0 & M' \end{pmatrix}$$

où $M'$ est une matrice $(n-1) \times (n-1)$. Par récurrence, on peut écrire $M' = U'T'$ avec $T' \in M_{n-1}(k)$ triangulaire supérieure et $U' \in GL_{n-1}(A)$. Posons par blocs

$$U = \begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix},$$

de sorte que

$$T = U^{-1}M_1 = \begin{pmatrix} \lambda & L_1' \\ 0 & T' \end{pmatrix}$$

est triangulaire supérieure. Finalement, $M = U_1M_1 = U_1UT$ est le produit d'une matrice de $GL_n(A)$ est d'une matrice triangulaire supérieure de $M_n(k)$.

**c)** On a

$$M = \frac{1}{420}\begin{pmatrix} 210 & 420 & -105 \\ 168 & 840 & 280 \\ 315 & 60 & -420 \end{pmatrix}.$$

La première colonne est égale à

$$\frac{1}{20}\begin{pmatrix} 10 \\ 8 \\ 15 \end{pmatrix}$$

et la matrice

$$U_1 = \begin{pmatrix} 10 & 0 & 1 \\ 8 & 1 & 0 \\ 15 & 2 & 0 \end{pmatrix}$$

appartient à $GL_3(\mathbf{Z})$ (remarquer que les deux derniers coefficients 8 et 15 sont premiers entre eux !). Son inverse est

$$U_1^{-1} = \begin{pmatrix} 0 & 2 & -1 \\ 0 & -15 & 8 \\ 1 & -20 & 10 \end{pmatrix}.$$

On a

$$420U_1^{-1}M = \begin{pmatrix} 21 & 1620 & 980 \\ 0 & -12\,120 & -7\,560 \\ 0 & -15\,780 & -9\,905 \end{pmatrix}.$$

Les deux coefficients 12 120 et 15 780 ont pour pgcd 60. Une fois divisés par 60, ils deviennent 202 et 263 et une relation de Bézout est

$$-202 \times 69 + 263 \times 53 = 1.$$

On pose alors

$$U_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -202 & 53 \\ 0 & -263 & 69 \end{pmatrix}$$

d'où

$$420U_2^{-1}U_1^{-1}M = \begin{pmatrix} 21 & 1\,620 & 980 \\ 0 & 60 & 3\,325 \\ 0 & 0 & 12\,530 \end{pmatrix}.$$

Finalement, on a $M = UT$ avec

$$U = U_2U_1 = \begin{pmatrix} 10 & -263 & 69 \\ 8 & -202 & 53 \\ 15 & -404 & 106 \end{pmatrix}$$

et

$$T = \begin{pmatrix} 1/20 & 27/7 & 7/3 \\ 0 & 1/7 & 95/12 \\ 0 & 0 & 179/60 \end{pmatrix}.$$

*Solution de l'exercice 8.4.8.* — Soit $(m_1, \dots, m_s)$ une famille génératrice dans M. On dispose ainsi d'un homomorphisme surjectif

$$\varphi\colon A^s \to M, \qquad \varphi(a_1, \dots, a_s) = a_1m_1 + \cdots + a_sm_s.$$

Soit N le noyau de $\varphi$, de sorte que $M \simeq A^s/N$. D'après le théorème de structure des sous-modules d'un module libre sur un anneau principal (théorème 8.1.6), il existe une base $(e_1, \dots, e_s)$ de $A^s$, un entier $\sigma \leq s$ et des éléments $(\delta_1, \dots, \delta_\sigma)$ de A tels que $(\delta_1e_1, \dots, \delta_\sigma e_\sigma)$ soit une base de N. Soit $i \in \{1; \dots; \sigma\}$ tel que $\delta_1, \dots, \delta_{i-1}$ soient inversibles mais $\delta_i$ n'est pas inversible. Par suite,

$$A^n/N \simeq (A/\delta_i) \oplus \cdots \oplus (A/\delta_\sigma) \oplus A^{s-\sigma}.$$

Le théorème 8.2.8 implique alors que $r = (s-i+1) + (s-\sigma) = s-i+1$. Comme $i \geq 1$, on a $r \leq s$, ainsi qu'il fallait démontrer.

*Solution de l'exercice 8.4.9.* — **a)** Soit $(d_1, \dots, d_r)$ la suite des facteurs invariants de G de sorte que $G = (\mathbf{Z}/d_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/d_r\mathbf{Z})$. Alors, $n = d_r$. En effet, puisque pour tout $i$, $d_i$ divise $d_r$, on a $d_rG = 0$. Mais d'autre part, la classe de l'élément $(0, \dots, 1) \in \mathbf{Z}^r$ n'est annulée par aucun entier $m \in \{1; \dots; d_{r-1}\}$.

La classe de cet élément est précisément d'ordre $d_r$.

**b)** Soit $n$ l'ordre de G. D'après la question précédente, G contient un élément d'ordre $g$, c'est-à-dire une racine primitive $n^{\text{e}}$ de l'unité et $\operatorname{card} G \geq \operatorname{card}\langle g\rangle = n$.

Tout élément de G vérifie $g^n = 1$. (Contrairement à la question 1), on note multiplicativement la loi de groupe de G.) Mais l'équation polynômiale $X^n - 1 = 0$ a au plus $n$ solutions dans K. Comme les $n$ éléments du sous-groupe engendré par G sont solutions, $G = \langle g\rangle$, donc G est cyclique.

# 9 Corps et algèbres

## 9.1. Éléments entiers, algébriques

DÉFINITION 9.1.1. — *Soit* A *un anneau et* B *une* A*-algèbre. On dit qu'un élément* $b \in \mathrm{B}$ *est* algébrique *sur* A *s'il existe un polynôme non nul* $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ *tel que* $\mathrm{P}(b) = 0$.

*On dit qu'un élément* $b \in \mathrm{B}$ *est* entier *sur* A *s'il existe un polynôme unitaire (non nul)* $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ *tel que* $\mathrm{P}(b) = 0$.

Une relation non triviale de la forme $a_n b^n + \cdots + a_1 b + a_0 = 0$ est appelée *relation de dépendance algébrique* pour $b$, resp. *intégrale* si $a_n = 1$.

*Exemple 9.1.2.* — Les nombres complexes $z = \exp(2i\pi/n)$, $u = (-1 + \sqrt{5})/2$ sont algébriques sur $\mathbf{Z}$. (Ils vérifient les relations $z^n = 1$ et $u^2 + u + 1 = 0$.)

*Exemple 9.1.3.* — Un nombre rationnel $x \in \mathbf{Q}$ n'est entier sur $\mathbf{Z}$ que s'il est un élément de $\mathbf{Z}$.

*Démonstration.* — En effet, soit $\mathrm{P} = \mathrm{X}^n + a_1 \mathrm{X}^{n-1} + \cdots + a_n$ un polynôme unitaire à coefficients entiers tel que $\mathrm{P}(x) = 0$. Écrivons $x = a/b$ avec $a$ et $b$ entiers premiers entre eux. Alors, on peut multiplier par $b^n$ la relation $\mathrm{P}(b) = 0$, d'où

$$a^n + a_1 a^{n-1} b + \cdots + a_{n-1} a b^{n-1} + a_n b^n = 0.$$

Par suite, $a^n = -b(a_1 a^{n-1} + \cdots + a_n b^{n-1})$ est multiple de $b$. Comme $b$ est premier avec $a$, il est premier avec $a^n$ si bien que $b$ est inversible : $b = \pm 1$. On a donc $x \in \mathbf{Z}$. □

*Remarque 9.1.4.* — Soit A un anneau et B une A-algèbre. Si $b \in \mathrm{B}$ est algébrique sur A, soit $\mathrm{P} = a_n \mathrm{X}^n + \cdots + a_0$ un polynôme non nul à coefficients dans A tel que $\mathrm{P}(b) = 0$. On peut supposer $a_n \neq 0$ et $a_n b$ est entier sur A. En effet, en multipliant la relation $\mathrm{P}(b) = 0$ par $a_n^{n-1}$, on obtient

$$(a_n b)^n + a_{n-1}(a_n b)^{n-1} + \cdots + a_0 a_n^{n-1} = 0,$$

ce qui est une relation de dépendance intégrale pour $a_n b$.

Réciproquement, s'il existe $a \in \mathrm{A}$ non nilpotent tel que $ab$ est entier sur A, alors $b$ est algébrique sur A. En effet, d'une relation de dépendance intégrale

$$(ab)^n + c_{n-1}(ab)^{n-1} + \cdots + c_0 = 0$$

pour $ab$, on déduit une relation de dépendance algébrique

$$a^n b^n + a^{n-1} c_{n-1} b^{n-1} + \cdots + a c_1 b + c_0 = 0$$

pour $b$. Cette relation est non triviale puisque, $a$ n'étant pas nilpotent $a^n \neq 0$.

En particulier, si A est un corps, un élément $b$ de B est entier sur A si et seulement s'il est algébrique sur A.

Si B est une A-algèbre, le théorème suivant fournit une caractérisation très utile des éléments de B qui sont entiers sur A.

THÉORÈME 9.1.5. — *Soit* A *un anneau et soit* B *une* A*-algèbre. Soit $b$ un élément de* B *et notons* $\mathrm{A}[b]$ *la sous-*A*-algèbre* $\mathrm{A}[b]$ *engendrée par $b$ dans* A. *Les propositions suivantes sont équivalentes :*

(1) *$b$ est entier sur* A *;*

(2) $\mathrm{A}[b]$ *est un* A*-module de type fini ;*

(3) *il existe un* $\mathrm{A}[b]$*-module qui est d'annulateur nul et de type fini en tant que* A*-module.*

*Démonstration.* — (1)⇒(2). — Soit $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ un polynôme unitaire tel que $\mathrm{P}(b) = 0$. Notons $\mathrm{P} = \mathrm{X}^n + a_1\mathrm{X}^{n-1} + \cdots + a_n$ et montrons alors que la famille $(1, b, \ldots, b^{n-1})$ engendre $\mathrm{A}[b]$ comme A-module. Par définition, un élément de $\mathrm{A}[b]$ est de la forme $\mathrm{Q}(b)$ pour P un polynôme à coefficients dans A. Comme P est unitaire, on peut effectuer la division euclidienne de Q par P : $\mathrm{Q} = \mathrm{PQ}_1 + \mathrm{R}$, où $\mathrm{R} \in \mathrm{A}[\mathrm{X}]$ est un polynôme de degré $< n$. Alors, $\mathrm{Q}(b) = \mathrm{P}(b)\mathrm{Q}_1(b) + \mathrm{R}(b) = \mathrm{R}(b)$, donc est combinaison linéaire à coefficients dans A de $(1, \ldots, b^{n-1})$, ce qu'on voulait démontrer.

(2)⇒(3). — Il suffit de poser $\mathrm{M} = \mathrm{A}[b]$. En effet, si $x \in \mathrm{A}[b]$ est un élément de l'annulateur de M, on a $x\mathrm{M} = 0$ et en particulier, puisque $1_\mathrm{B} \in \mathrm{A}[b]$, $x1 = x = 0$.

(3)⇒(1). — Soit $(m_1; \ldots; m_r)$ une famille finie d'éléments de M qui l'engendre. Pour tout $i \in \{1; \ldots; r\}$, $bm_i$ est un élément de M qu'on peut écrire $\sum_{j=1}^{r} a_{ij} m_j$ pour des $a_{ij}$ dans A. Soit T la matrice des $(a_{ij})$. Par définition, la matrice $b\mathrm{I}_r - \mathrm{T} \in \mathrm{Mat}_r(\mathrm{A}[b])$ anule le vecteur colonne $(m_1; \ldots; m_r)$. En multipliant cette relation à gauche par la matrice transposée des cofacteurs de $b\mathrm{I}_r - \mathrm{T}$, on obtient la relation

$$\det(b\mathrm{I}_r - \mathrm{T})\mathrm{I}_r \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = 0$$

c'est-à-dire $\det(b\mathrm{I}_r - \mathrm{T})m_i = 0$ pour tout $i \in \{1; \ldots; r\}$. Comme les $m_i$ engendrent M, $\det(b\mathrm{I}_r - \mathrm{T})$ annule M. Par suite, $\det(b\mathrm{I}_r - \mathrm{T}) = 0$ dans $\mathrm{A}[b]$. (C'est une variante

de la démonstration du théorème de Cayley–Hamilton.) Enfin, rappelons que le polynôme caractéristique de la matrice T est un polynôme unitaire à coefficients dans A et que l'on a $P(b) = \det(bI_r - T)$. Ainsi, $P(b) = 0$ est la relation de dépendance intégrale cherchée. □

COROLLAIRE 9.1.6. — *Soit* A *un anneau et soit* B *une* A*-algèbre. Si* $b$ *et* $c$ *sont deux éléments de* B *entiers sur* A*, tout élément de* $A[b, c]$ *est entier sur* A.

*En particulier,* $b + c$ *et* $bc$ *sont entiers sur* A.

*Démonstration.* — Notons P et Q des polynômes unitaires à coefficients dans A tels que $P(b) = Q(c) = 0$. Soit $A[b, c]$ la sous-A-algèbre de B engendrée par $b$ et $c$ ; c'est l'ensemble des expressions de la forme $R(b, c)$ pour $R \in A[X, Y]$. Une division euclidienne de R par P(X) dans A[Y][X] fournit une expression

$$R(X, Y) = P(X)R'(X, Y) + \sum_{k<\deg P} R_k(Y)X^k.$$

Une autre division euclidienne, par Q(Y) maintenant permet d'écrire $R_k(Y) = Q(Y)R'_k(Y) + S_k(Y)$ où $S_k \in A[Y]$ est de degré $< \deg Q$. Ainsi,

$$R(X, Y) = P(X)R'(X, Y) + Q(Y) \sum_{k<\deg P} R'_k(Y)X^k + \sum_{k<\deg P} S_k(Y)X^k$$

et

$$R(b, c) = \sum_{k<\deg P} S_k(c)b^k$$

est une combinaison linéaire des $\deg P \deg Q$ éléments $b^k c^\ell$ pour $0 \leq k < \deg P$ et $0 \leq \ell < \deg Q$. Ainsi, $A[b, c]$ est un A-module de type fini. Comme il contient 1, son annulateur en tant que $A[b, c]$-module est nul.

Soit $x \in A[b, c]$. On peut ne considérer $A[b, c]$ que comme $A[x]$-module, mais son annulateur en tant que $A[x]$-module est a fortiori réduit à (0).. D'après le théorème précédent, $x$ est entier sur A. □

*Exercice 9.1.7.* — Écrire des relations de dépendance intégrale sur **Z** pour les éléments $\sqrt{2} + \sqrt{3}$ et $\sqrt{5}(1 + \sqrt{3})$.

DÉFINITION 9.1.8. — *Soit* A *un anneau et* B *une* A*-algèbre.*

*L'ensemble des éléments de* B *qui sont entiers sur* A *est une sous-*A*-algèbre de* B*. On l'appelle* clôture intégrale de A dans B.

LEMME 9.1.9. — *Soit* K *un corps et soit* A *une* K*-algèbre intègre, Si* $x \in A \setminus \{0\}$ *est algébrique sur* K*, alors* $x$ *est inversible dans* A *et* $1/x$ *est algébrique sur* K.

*Démonstration.* — Comme K est un corps, être algébrique sur K ou être entier sur K sont deux propriétés équivalentes. Soit donc $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un polynôme unitaire dans K[X] de degré minimal tel que $P(x) = 0$. Si $a_0 = 0$,

on peut écrire factoriser P par X, $P = XQ$. Comme $x \neq 0$, $Q(x) = 0$ ce qui contredit l'hypothèse que P est de degré minimal. Alors,

$$0 = P(x) = x\left(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1\right) + a_0 = xy + a_0,$$

où on a noté $y = x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1$. Comme $a_0 \neq 0$, $a_0$ est inversible. Enfin, l'existence d'un élément $y \in K[x]$ tel que $xy = -a_0$ est inversible implique que $x$ est inversible dans $K[x]$, d'inverse $-y/a_0$. Comme $K[x]$ est un K-module de type fini (c'est-à-dire un K-espace vectoriel de dimension finie), $1/x$ est entier sur K, donc algébrique sur K. □

*Exercice 9.1.10* (Autre démonstration). — Remarquer que $K[x]$ est un K-espace vectoriel de dimension finie. Considérer l'endomorphisme $\mu_x$ de $K[x]$ défini par $\mu_(y) = xy$ pour tout $y \in K[x]$. Montrer qu'il est injectif. En déduire qu'il est surjectif et que $x$ est inversible dans $K[x]$.

*Exercice 9.1.11.* — Soit L un corps et $K \subset L$ un sous-corps de L. Montrer qu'un élément $x \in L$ est algébrique sur K si et seulement si la K-algèbre $K[x]$ engendrée par $x$ dans L est un corps.

Définition 9.1.12. — *Soit* K *un corps et* A *une* K*-algèbre intègre. L'ensemble des éléments de* A *qui sont algébriques sur* K *est un corps contenu dans* A. *On l'appelle* clôture algébrique de K dans A.

Définition 9.1.13. — *Soit* K *un corps et* A *une* K*-algèbre intègre. Soit* $a \in A$ *un élément algébrique. L'ensemble des polynômes* $P \in K[X]$ *tels que* $P(a) = 0$ *est un idéal premier de* K[X]. *Le* polynôme minimal *de a en est l'unique générateur unitaire.*

C'est aussi le polynôme unitaire P de plus petit degré tel que $P(a) = 0$. On remarquera que c'est un polynôme irréductible.

## 9.2. Extensions entières, algébriques

Définition 9.2.1. — *On dit qu'une extension d'anneaux* $A \subset B$ *est* entière *si tout élément de* B *est entier sur* A.

*On dit qu'une extension de corps* $K \subset L$ *est* algébrique *si tout élément de* L *est algébrique sur* K.

Définition 9.2.2. — *On dit qu'une extension d'anneaux* $A \subset B$ *est* finie *si* B *est un* A*-module de type fini.*

*De même, une extension de corps* $K \subset L$ *est dite* finie *si* L *est un* K*-espace vectoriel de dimension finie.*

PROPOSITION 9.2.3. — *Une extension finie d'anneaux est entière. Une extension finie de corps est algébrique.*

*Réciproquement, si* $A \subset B$ *est une extension entière de type fini, alors c'est une extension finie.*

*Démonstration.* — Soit $A \subset B$ une extension finie d'anneaux. Pour tout $b \in B$, B est un $A[b]$-module dont l'annulateur est nul et qui est un A-module de type fini. D'après le théorème 9.1.5, $b$ est entier sur A. Tout élément de B étant entier sur A, l'extension $A \subset B$ est entière.

Le cas d'une exetnsion de corps est analogue.

Soit $(b_1; \ldots; b_m)$ une famille finie d'éléments de B qui engendre B comme A-algèbre. Comme B est entière sur A, il existe un entier N tel que pour tout $i$, $b_i^N$ soit une combinaison linéaire à coefficients dans A des $b_i^n$ pour $0 \leq n < N$. Alors, tout polynôme en les $b_i$ est combinaison linéaire des $m^N$ produits $b_1^{n_1} \ldots b_m^{n_m}$ pour des $n_i \in \{0; \ldots; N-1\}$. Autrement dit, B est engendré comme A-module par ces $m^N$-produits, donc est un A-module de type fini, ce qu'il fallait démontrer. □

DÉFINITION 9.2.4. — *Soit* $K \subset L$ *une extension finie. Le* degré *de* L *sur* K*, noté* $[L : K]$ *est la dimension de* L *comme* K*-espace vectoriel.*

PROPOSITION 9.2.5. — *Soit* $K \subset L$ *et* $L \subset M$ *deux extensions finies. Alors,* $K \subset M$ *est une extension finie et on a la relation*

$$[M : K] = [M : L]\,[L : K].$$

*Démonstration.* — Posons $m = [M : L]$ et soit $(y_1; \ldots; y_m)$ une base de M comme L-espace vectoriel. Soit $n = [L : K]$ et soit $(x_1; \ldots; x_n)$ une base de L en tant que K-espace vectoriel. Montrons alors que la famille des $(x_i y_j)$ est une base de M comme K-espace vectoriel. Par suite, l'extension $K \subset M$ sera finie de degré $mn = [M : L]\,[L : K]$.

Soit $a$ un élément de M, on peut l'écrire $\sum_{i=1}^{m} a_i y_i$ où $a_i \in L$. De même, chacun des $a_i$ s'écrit $\sum_{j=1}^{n} a_{i,j} x_j$ pour des $a_{i,j} \in K$. Ainsi,

$$a = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} x_j y_i.$$

Ceci prouve que la famille $(x_i y_j)$ engendre M en tant que K-espace vectoriel.

Soit maintenant $0 = \sum_{i,j} a_{i,j} x_j y_i$ une relation de dépendance linéaire avec des $a_{i,j} \in \mathrm{K}$. On l'écrit

$$\sum_i \left( \sum_j a_{i,j} x_j \right) y_i = 0.$$

Les éléments $a_i = \sum_j a_{i,j} x_j$ appartiennent à L et comme $(y_1; \ldots; y_m)$ est une base de M comme L-espace vectoriel, $a_i = 0$ pour tout $i$. Comme $(x_1; \ldots; x_n)$ est une base de L comme K-espace vectoriel, $a_{i,j} = 0$ pour tout $i$ et tout $j$. Ceci prouve que la famille $(x_i y_j)$ est libre.

Étant libre et génératrive, la famille $(x_i y_j)$ est une base de M comme K-espace vectoriel. □

*Exercice 9.2.6.* — Si $\mathrm{A} \subset \mathrm{B}$ et $\mathrm{B} \subset \mathrm{C}$ sont deux extensions d'anneaux finies, l'extension $\mathrm{A} \subset \mathrm{C}$ est finie. (*Reprendre la partie de la démonstration précédente qui établit que les $x_i y_j$ engendrent* M *comme* K*-espace vectoriel.*)

Corollaire 9.2.7. — *Si* $\mathrm{A} \subset \mathrm{B}$ *et* $\mathrm{B} \subset \mathrm{C}$ *sont deux extensions d'anneaux entières, l'extension* $\mathrm{A} \subset \mathrm{C}$ *est entière.*

*Démonstration.* — Soit $c \in \mathrm{C}$ ; il vérifie ainsi une relation de dépendance intégrale $c^n + b_{n-1} c^{n-1} + \cdots + b_0 = 0$ à coefficients dans B. Par suite, $c$ est entier sur la A-algèbre $\mathrm{B}_1 = \mathrm{A}[b_0; \ldots; b_{n-1}]$ engendrée dans B par les $b_i$. Ainsi, l'extension $\mathrm{B}_1 \subset \mathrm{B}_1[c]$ est finie. Comme les $b_i$ sont entiers sur A, $\mathrm{B}_1$ est entier sur A et étant de type fini, $\mathrm{B}_1$ est finie sur A.

Par suite, l'extension $\mathrm{A} \subset \mathrm{B}_1 \subset \mathrm{B}_1[c]$ est finie. Cela implique que $c$ est entier sur A. Comme $c$ est quelconque, l'extension $\mathrm{A} \subset \mathrm{C}$ est entière. □

*Exercice 9.2.8.* — Soit $\mathrm{A} \subset \mathrm{B}$ une extension entière.

a) Si S est une partie multiplicative de A, $\mathrm{S}^{-1}\mathrm{A} \subset \mathrm{S}^{-1}\mathrm{B}$ est entière.

b) Si I est un idéal de B, l'extension $\mathrm{A}/(\mathrm{I} \cap \mathrm{A}) \subset \mathrm{B}/\mathrm{I}$ est entière.

Définition 9.2.9. — *Soit* A *un anneau intègre et soit* K *son corps des fractions. On dit que* A *est* intégralement clos *si la clôture intgrale de* A *dans* K *est égale à* A*, autrement dit si les éléments de* A *sont les seuls éléments de* K *qui sont entiers sur* A.

Nous avons vu dans l'exemple 9.1.3 que **Z** est intégralement clos. Plus généralement, on a le théorème suivant.

Théorème 9.2.10. — *a) Un anneau factoriel est intégralement clos.*

*b) Si* A *est un anneau intégralement clos,* A[X] *est intégralement clos.*

La démonstration est laissée en exercice. Pour le a), il suffit essentiellement de recopier la démonstration que **Z** est intégralement clos. Le b) est un cas

particulier de l'exercice 9.4.7 (avec les notations de cet exercice, prendre pour B le corps des fractions de A).

PROPOSITION 9.2.11. — *Soit* A *un anneau intégralement clos. Pour toute partie multiplicative* $S \subset A$ *(ne contenant pas* 0*), l'anneau* $S^{-1}A$ *est intégralement clos.*

*Démonstration.* — Si K désigne le corps des fractions de A, on a une inclusion $A \subset S^{-1}A \subset K$ et K est aussi le corps des fractions de $S^{-1}A$. Soit $x \in K$ un élément entier sur $S^{-1}A$ et choisissons une relation de dépendance intégrale

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

où les $a_i$ sont dans $S^{-1}A$. Soit $s \in S$ un dénominateur commun aux $a_i$, de sorte que pour tout $i$, $b_i = sa_i \in A$. On a alors, multipliant la relation précédente par $s^n$,

$$(sx)^n + b_{n-1}(sx)^{n-1} + \cdots + b_1 s^{n-1}(sx) + b_0 s^{n-1} = 0,$$

ce qui prouve que $sx$ est entier sur A. Comme A est intégralement clos, $sx \in A$, puis $x = (sx)/s$ appartient à $S^{-1}A$. Par conséquent, $S^{-1}A$ est intégralement clos. □

## 9.3. Construction d'extensions algébriques

LEMME 9.3.1. — *Soit* K *un corps et soit* $P \in K[X]$ *un polynôme irréductible. Alors, la* K*-algèbre* $L = K[X]/(P)$ *est une extension algébrique finie de* K *et l'élément* $x = \mathrm{cl}(X)$ *est racine de* P *dans* L.

*Démonstration.* — Comme P est irréductible et comme l'anneau K[X] est principal, l'idéal (P) est un idéal maximal de K[X]. Ainsi, L est un corps. Si P est de degré $n$, L est un K-espace vectoriel de dimension $n$. C'est donc une extension algébrique finie de K.

Enfin, on a $P(\mathrm{cl}(X)) = \mathrm{cl}(P(X)) = 0$. □

DÉFINITION 9.3.2. — *Si* K *est un corps et* $P \in K[X]$ *un polynôme irréductible, l'extension* $L = K[X]/(P)$ *de* K *est appelée* corps de rupture *du polynôme* P.

PROPOSITION 9.3.3. — *Soit* K *un corps et* $P \in K[X]$ *un polynôme non constant. Il existe une extension algébrique finie* $K \subset L$ *telle que* P *a une racine dans* L.

*Démonstration.* — Si P a une racine dans K, on pose L = K. Sinon, soit Q un facteur irréductible de P et posons $L = K[X]/(Q)$. D'après le lemme précédent, Q a une racine dans L. *A fortiori,* P a une racine dans L. □

COROLLAIRE 9.3.4. — *Soit* K *un corps et soit* $P \in K[X]$ *un polynôme non constant. Il existe une extension algébrique finie* $K \subset L$ *telle que* P *soit scindé dans* L.

*Démonstration.* — On démontre ceci par récurrence sur le degré de P. Le résultat est vrai pour $\deg P = 1$, car alors P est déjà scindé sur K.

D'après la proposition précédente, il existe une extension finie $K \subset L$ telle que P admette une racine $x$ dans L. En tant que polynôme de $L[X]$, P est donc multiple de $X - x$. Soit $Q = P(X)/(X - x)$ le quotient. C'est un polynôme de $L[X]$ de degré $< \deg P$. Par récurrence, il existe une extension algébrique finie $L \subset M$ telle que Q soit scindé sur M.

Ainsi, M est une extension algébrique finie de K et P est scindé sur M. □

COROLLAIRE 9.3.5. — *Soit* K *un corps. Les propositions suivantes sont équivalentes :*

(1) K *n'admet pas d'extension algébrique* $K \subset L$ *avec* $L \neq K$ *;*
(2) *les polynômes irréductibles de* $K[X]$ *sont les polynômes de degré* 1 *;*
(3) *tout polynôme non constant à coefficients dans* K *possède une racine dans* K *;*
(4) *tout polynôme à coefficients dans* K *est scindé.*

DÉFINITION 9.3.6. — *Si un corps* K *vérifie les propriétés équivalentes du corollaire ci-dessus, on dit que* K *est* algébriquement clos.

*Preuve du corollaire 9.3.5.* — (1)⇒(2). — C'est la construction du lemme 9.3.1 : si $\Pi \in K[X]$ est un polynôme irréductible de degré $n \geq 2$, le corps de rupture L de $\Pi$ est une extension algébrique de K de degré $n$, donc $K \neq L$. Ceci contredit l'hypothèse que K n'admet pas d'extension algébrique distincte de K.

(2)⇒(3). — Soit P un polynôme non constant et $\Pi$ un facteur irréductible de P. Ainsi, $\Pi$ est de degré 1 et il possède une racine dans K. *A fortiori,* P admet une racine dans K.

(3)⇒(4). — Soit $P \in K[X]$ un polynôme. Si $\deg P = 0$, P est scindé. Supposons que $\deg P \geq 1$ et que tout polynôme de degré $< \deg P$ soit scindé. Alors, P possède une racine $a$ dans K. Le polynôme $P(X)$ est multiple de $(X - a)$ ; soit $Q(X) = P(X)/(X - a)$ le quotient. Par récurrence, Q est scindé dans K et $P(X) = (X - a)Q(X)$ est donc scindé.

(4)⇒(1). — Soit $K \subset L$ une extension algébrique et soit $x$ un élément de L. Il est algébrique sur K donc il existe un polynôme non constant $P \in K[X]$ tel que $P(x) = 0$. Comme P est scindé, on peut écrire $P = c\prod_{i=1}^{n}(X - a_i)$ pour des $a_i \in K$ et $c \neq 0$. Par suite, $P(x) = c\prod_{i=1}^{n}(x - a_i) = 0$. Comme L est un corps, il existe $i$ tel que $x - a_i = 0$, d'où $x = a_i \in K$. Par suite, $L = K$. □

THÉORÈME 9.3.7 (Théorème de d'Alembert–Gauß). — *Le corps* $\mathbf{C}$ *des nombres complexes est algébriquement clos.*

Toutes les démonstrations de ce théorème reposent à un point ou à un autre sur un argument de nature analytique, essentiellement le fait que $\mathbf{R}$ est

complet. Nous donnons une démonstration courte mais faisant appel à des résultats d'analyse complexe. Une démonstration d'apparence plus algébrique est proposée dans l'exercice 9.4.1.

*Démonstration.* — Soit $P \in \mathbf{C}[X]$ un polynôme non constant dont on veut prouver qu'il admet une racine dans $\mathbf{C}$. On peut supposer que P est unitaire et on écrit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Soit $M = \max(|a_0|, \ldots, |a_{n-1}|)$ et posons $R = 1+2M$. Alors, si $z \in \mathbf{C}$ vérifie $|z| \geq R$, on a

$$\begin{aligned} |P(z)| &= \left|z^n + a_{n-1}z^{n-1} + \cdots + a_0\right| \geq |z^n| - \left|a_{n-1}z^{n-1}\right| - \cdots - |a_0| \\ &\geq R^n - M\frac{R^n - 1}{R - 1} = R^n\Big(1 - \frac{M}{R-1}\Big) + \frac{M}{R-1} \geq \frac{1}{2}R^n. \end{aligned}$$

Ainsi, $\lim\limits_{|z|\to+\infty} |P(z)| = +\infty$.

Raisonnons par l'absurde et supposons que P n'a pas de racine dans $\mathbf{C}$. On peut alors considérer la fonction $\varphi\colon \mathbf{C} \to \mathbf{C}$ définie par $z \mapsto 1/P(z)$. Elle est holomorphe sur $\mathbf{C}$ et tend vers 0 lorsque $|z|$ tend vers $+\infty$. Par conséquent, elle est bornée sur $\mathbf{C}$. Le théorème de Liouville implique que $\varphi$ est constante, ce qui est absurde. □

Définition 9.3.8. — *Soit* K *un corps. Une clôture algébrique est une extension algébrique* $K \subset \Omega$ *telle que* $\Omega$ *soit algébriquement clos.*

Le fait de connaître *un* exemple de corps algébriquement clos nous en donne automatiquement d'autres.

Proposition 9.3.9. — *Soit* K *un corps et* E *une extension algébriquement close de* K. *Soit* $\Omega$ *la clôture algébrique de* K *dans* E *(ensemble des éléments de* E *qui sont algébriques sur* K*). Alors,* $\Omega$ *est une clôture algébrique de* K.

En particulier, l'ensemble $\overline{\mathbf{Q}}$ des nombres algébriques (nombres complexes qui sont algébriques sur $\mathbf{Q}$) est une clôture algébrique de $\overline{\mathbf{Q}}$.

*Démonstration.* — Comme $\Omega$ est algébrique sur K, il suffit de démontrer que $\Omega$ est algébriquement clos, et donc que tout polynôme non constant $P \in \Omega[X]$ admet une racine dans $\Omega$.

On peut supposer que P est unitaire et écrire

$$P = X^n + a_1X^{n-1} + \cdots + a_n$$

où les $a_i$ sont des éléments de $\Omega$. Par définition, les $a_i$ sont algébriques sur K et l'extension $L = K[a_1, \ldots, a_n]$ engendrée par les $a_i$ dans L est une extension algébrique finie de K.

Comme E est algébriquement clos, le polynôme P admet une racine $\xi$ dans E. La relation $P(\xi) = 0$ avec $P \in L[x]$ montre que $\xi$ est algébrique sur L. Par suite, $\xi$ est algébrique sur K, autrement dit, $\xi \in \Omega$. □

THÉORÈME 9.3.10 (Steinitz). — *Tout corps a une clôture algébrique.*

LEMME 9.3.11. — *Soit* K *un corps et soit* $\mathscr{P}$ *une famille de polynômes non constants de* K[X]. *Il existe alors une extension algébrique* L *de* K *telle que tout polynôme de* $\mathscr{P}$ *a une racine dans* L.

*Démonstration.* — Si $\mathscr{P}$ est fini, on peut démontrer l'existence de L par récurrence à l'aide de la proposition 9.3.3.

Soit $A = K[(X_P)_{P\in\mathscr{P}}]$ la K-algèbre de polynômes engendrée par une infinité de variables, une variable $X_P$ pour chaque polynôme $P \in \mathscr{P}$. Soit I l'idéal de A engendré par les $P(X_P)$, lorsque P parcourt $\mathscr{P}$. Montrons que $I \neq A$. Sinon, il existe une relation de la forme $1 = \sum_{P\in\mathscr{P}} Q_P(X)P(X_P)$. C'est une somme finie qui ne fait intervenir qu'un nombre fini de variables $X_P$ et qu'on peut ainsi récrire

$$1 = Q_1(X)P_1(X_1) + \cdots + Q_r(X)P_r(X_r)$$

D'après le corollaire 9.3.4 il existe une extension algébrique $K \subset K_1$ dans laquelle le polynôme $P_1 \dots P_r$ est scindé, d'où pour tout $i$ une racine $a_i$ de $P_i$ dans L. On spécialise la relation précédente au point $X_1 = a_1, \dots, X_r = a_r$, d'où la relation

$$1 = Q_1(a)P_1(a_1) + \cdots + Q_r(a)P_r(a_r) = 0,$$

ce qui est absurde.

D'après le théorème de Krull sur l'existence d'idéaux maximaux (théorème 4.1.10), il existe un idéal maximal $\mathfrak{m}$ de A qui contient I. Définissons $\Omega$ comme le corps $A/\mathfrak{m}$. Pour tout $P \in \mathscr{P}$, on a $P(X_P) \in I$, donc $P(X_P) \in \mathfrak{m}$, si bien que $\mathrm{cl}(P(X_P)) = P(\mathrm{cl}(x_P)) = 0$ dans $A/\mathfrak{m}$. Ainsi, $\mathrm{cl}(x_P)$ est une racine de P dans $\Omega$.

De plus, comme A est engendrée comme K-algèbre par les $x_P$, $\Omega$ est engendrée en tant que K-algèbre par les $\mathrm{cl}(x_P)$. Ceux-ci étant algébriques sur K, $\Omega$ est algébrique sur K. □

*Démonstration du théorème.* — Posons $E_0 = K$ et construisons une suite de corps $(E_n)_n$ algébriques sur K de la façon suivante. Si $E_n$ est construit, on définit $E_{n+1}$ comme une extension de $E_n$ telle que tout polynôme non constant de $E_n[X]$ admet une racine dans $E_{n+1}$. L'existence d'un tel corps $E_{n+1}$ est affirmée par le lemme 9.3.11. Comme $E_{n+1}$ est algébrique sur $E_n$, on voit par récurrence que pour tout $n$, $E_n$ est algébrique sur K.

On obtient de la sorte une suite de corps

$$K = E_0 \subset E_1 \subset \dots$$

et soit $\Omega$ la réunion des $E_n$ pour $n \geq 0$. C'est un corps qui contient K. (Un élément de $\Omega$ est un élément d'un certain $E_n$, l'addition ou la multiplication de deux éléments $x$ et $y$ de $\Omega$ se fait dans tout corps $E_n$ dans lequel $x$ et $y$ « habitent ».)

Comme tout élément de $\Omega$ appartient à l'un des $E_n$, $\Omega$ est algébrique sur K. Montrons enfin que $\Omega$ est algébriquement clos. Soit $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ un polynôme non constant à coefficients dans $\Omega$. Il existe un entier $m \geq 0$ tel que tous les coefficients de P appartiennent à $E_m$, de sorte que $P \in E_m[X]$. Par construction, P admet donc une racine dans $E_{m+1}$, donc dans $\Omega$.

Puisque tout polynôme non constant de $\Omega[X]$ a une racine dans $\Omega$, la proposition 9.3.5 montre que $\Omega$ est algébriquement clos. □

## 9.4. Exercices

*Exercice 9.4.1.* — Le but de l'exercice est de démontrer que le corps **C** des nombres complexes est algébriquement clos.

Si $P = a_n X^n + \cdots + a_0 \in \mathbf{C}[X]$ est un polynôme à coefficients complexes, on note $\bar{P}$ le polynôme conjugué défini par $\bar{P} = \bar{a}_n X^n + \cdots + \bar{a}_0$. On fixe aussi une clôture algébrique $\Omega$ de **C**.

**a)** Montrer que tout nombre complexe a une racine carrée dans **C**. En déduire que toute équation du second degré à coefficients dans **C** a ses racines dans **C**.

Dans les questions suivantes, on démontre que tout polynôme P de $\mathbf{R}[X]$ a une racine dans **C**. Si le degré de P s'écrit $d = 2^n m$ avec $m$ impair, on raisonne par récurrence sur l'entier $n$.

**b)** Cas $n = 0$. — Soit $P \in \mathbf{R}[X]$ un polynôme de degré impair. Montrer qu'il a une racine dans **R**.

Soit P un polynôme irréductible de $\mathbf{R}[X]$ dont le degré $d = 2^n m$ est pair $(n \geq 1)$.

**c)** Montrer que P a $d$ racines distinctes $x_1, \ldots, x_d$ dans $\Omega$.

Montrer que pour tout $c \in \mathbf{R}$, il existe un polynôme $P_c \in \mathbf{R}[X]$ dont les racines sont les $x_j + x_k + c x_j x_k$, avec $1 \leq j < k \leq d$. (*Utiliser le théorème sur les polynômes symétriques élémentaires.*)

**d)** En utilisant l'hypothèse de récurrence, montrer que pour tout $c \in \mathbf{R}$, $P_c$ a une racine dans **C**. En choisissant convenablement plusieurs valeurs de $c$, montrer qu'il existe deux indices distincts $j$ et $k$ tels que $x_j + x_k$ et $x_j x_k$ sont dans **C**. En déduire que $x_j$ et $x_k$ sont des éléments de **C**.

**e)** Montrer que tout polynôme non constant dans $\mathbf{C}[X]$ a une racine dans **C**.

*Exercice 9.4.2.* — **a)** Soit A un anneau et P un polynôme unitaire de A[X] de degré $d > 0$. Montrer que l'anneau $B = A[X]/(P)$ contient un sous anneau isomorphe à A, auquel on l'identifie.

**b)** Montrer que B est entier sur A, et qu'il existe $a \in B$ tel que $P(a) = 0$.

**c)** Montrer qu'il existe un anneau C contenant A, entier sur A et des éléments $a_1, \dots, a_d \in C$ tels que $P = \prod_{i=1}^{d} (X - a_i)$.

*Exercice 9.4.3.* — Soient $A \subset B$ deux anneaux, $x$ un élément inversible de B et soit $y \in A[x] \cap A[x^{-1}]$. Montrer qu'il existe un entier $n$ tel que le A-module $M = A + Ax + \cdots + Ax^n$ soit stable pour la multiplication par $y$. En déduire que $y$ est entier sur A.

*Exercice 9.4.4.* — Soit A un anneau intègre et K son corps des fractions.

**a)** Soit $x \in K$ qui est entier sur A. Montrer qu'il existe $a \in A \setminus \{0\}$ tel que pour tout $n \geq 0$, $ax^n \in A$.

**b)** On suppose que A est noethérien. Réciproquement, soit $a \in A \setminus \{0\}$ et $x \in K$ tels que pour tout $n$, $ax^n \in A$. Montrer que $x$ est entier sur A.

*Exercice 9.4.5.* — Quels sont les entiers $d$ tels que $\mathbf{Z}[\sqrt{d}]$ soit intégralement clos ?

*Exercice 9.4.6.* — **a)** Soit A un anneau intègre et $t \in A$ tel que $A/tA$ est réduit (n'a pas d'élément nilpotent autre que 0). On suppose que $A_t$ est intégralement clos. Montrer que A est intégralement clos.

**b)** Montrer que l'anneau $A = \mathbf{C}[X, Y, Z]/(XZ - Y(Y + 1))$ est intégralement clos. (Introduire la classe de X dans A.)

*Exercice 9.4.7.* — Soient $A \subset B$ deux anneaux tels que A est intégralement fermé dans B.

**a)** Soient P et Q deux polynômes unitaires de B[X] tels que $PQ \in A[X]$. Montrer que P et Q sont dans A[X]. (*Utiliser l'exercice 9.4.2 pour introduire un anneau* $C \supset B$ *tel que* $P = \prod_{i=1}^{m} (X - a_i)$ *et* $Q = \prod_{i=1}^{n} (X - b_i)$ *où* $a_1, \dots, a_m, b_1, \dots, b_n \in C$.)

**b)** Montrer que A[X] est intégralement fermé dans B[X]. (*Si* $P \in B[X]$ *est entier sur* A[X], *considérer le polynôme unitaire* $Q = X^r + P$ *avec r suffisament grand.*)

## 9.5. Solutions

*Solution de l'exercice 9.4.1.* — **a)** Soit $z = a + ib$ un nombre complexe. Une racine carrée de $z$ est un nombre complexe $u = x + iy$ tel que $u^2 = z$, d'où les équations

$$x^2 - y^2 = a \quad \text{et} \quad 2xy = b.$$

Si $b = 0$, soit $a \geq 0$ auquel cas on choisit $u = \sqrt{a}$, soit $a \leq 0$ auquel cas on choisit $u = \mathrm{i}\sqrt{-a}$. Supposons donc $b \neq 0$. En multipliant la première relation par $4x^2$, on obtient $4x^4 - 4x^2y^2 = 4ax^2$, d'où $(2x^2) - 2a(2x^2) - b^2 = 0$. C'est une équation à coefficients réels de discriminant réduit $a^2 + b^2 \geq 0$. Elle a une racine positive $\frac{1}{2}\left(a + \sqrt{a^2 + b^2}\right)$. Il suffit maintenant de poser

$$x = \frac{1}{2}\sqrt{a + \sqrt{a^2 + b^2}}$$

puis, remarquant que $x > 0$, $y = b/2x$.

Si $\mathrm{P} = a\mathrm{X}^2 + 2b\mathrm{X} + c$ est un polynôme de $\mathbf{C}[\mathrm{X}]$ de degré 2, la méthode de résolution des équations du second degré montre qu'il a ses racines dans $\mathbf{C}$ si et seulement son discriminant réduit $b^2 - ac$ est un carré dans $\mathbf{C}$. D'après le début de la question, c'est effectivement le cas.

**b)** Quitte à diviser P par son coefficient dominant, on peut supposer qu'il est unitaire. Alors, lorsque $x$ tend vers $+\infty$, $\mathrm{P}(x)$ tend vers $+\infty$ tandis que P a pour limite $-\infty$ en $-\infty$. D'après le théorème des valeurs intermédiaires, P s'annule dans $\mathbf{R}$.

**c)** Comme $\Omega$ est algébriquement clos, P est scindé dans $\Omega$. Puisque P est irréductible dans $\mathbf{R}[\mathrm{X}]$ et comme $\mathrm{P}' \neq 0$, on a $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = 1$ dans $\mathbf{R}[\mathrm{X}]$. Cela implique qu'il existe A et B dans $\mathbf{R}[\mathrm{X}]$ tels que $\mathrm{AP} + \mathrm{BP}' = 1$. Par suite, si $x$ est une racine de P dans $\Omega$, on a $\mathrm{B}(x)\mathrm{P}'(x) = 1$ et donc $\mathrm{P}'(x) \neq 0$. Cela montre que P n'a pas de racines multiples dans $\Omega$ puisque les racines multiples d'un polynôme sont aussi des racines du polynôme dérivé.

Notons

$$\mathrm{P}(\mathrm{X}) = a_d \prod_{j=1}^{d} (\mathrm{X} - x_j) = \sum_{j=0}^{d} a_j \mathrm{X}^j.$$

Posons $z_{ij} = x_j + x_k + cx_jx_k$. Considérons le polynôme à coefficients dans $\mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_d]$ :

$$\mathrm{Q}(\mathrm{T}) = \prod_{1 \leq j < k \leq d} (\mathrm{T} - \mathrm{X}_j - \mathrm{X}_k - c\mathrm{X}_j\mathrm{X}_k).$$

Il est de degré $\mathrm{D} = d(d-1)/2 = 2^{n-1}m(2^n m - 1)$ et est symétrique en les $\mathrm{X}_i$. Si on l'écrit

$$\mathrm{Q}(\mathrm{T}) = \sum_{j=0}^{\mathrm{D}} \mathrm{Q}_j(\mathrm{X}_1, \ldots, \mathrm{X}_d)\mathrm{T}^j$$

les polynômes $\mathrm{Q}_j$ sont donc symétriques et il existe pour tout $j$ un unique polynôme $\mathrm{R}_j \in \mathbf{Z}[\mathrm{Y}_1, \ldots, \mathrm{Y}_d]$ tel que $\mathrm{Q}_j(\mathrm{X}) = \mathrm{R}_j(\mathrm{S}_1(\mathrm{X}), \ldots, \mathrm{S}_d(\mathrm{X}))$.

Spécialisons les $X_j$ en les éléments $x_j \in \Omega$. On a ainsi $S_j(x_1, \dots, x_d) = (-1)^j a_{d-j}/a_d$ ; c'est donc un réel, que nous notons $\sigma_j$. Il en résulte une expression

$$P_c(T) = \prod_{1 \leq j < k \leq d} (T - z_{jk}) = \sum_{j=0}^{D} R_j(\sigma_1, \dots, \sigma_d) T^j.$$

Par suite, les $z_{jk}$ sont bien les zéros d'un polynôme à coefficients réels.

**d)** Ce polynôme est de degré $D = 2^{n-1}m(2^n m - 1)$ dont l'exposant de 2 est $n - 1$. Par récurrence, il a donc une racine dans **C** et il existe un couple $(j, k)$ tel que $x_j + x_k + c x_j x_k \in \mathbf{C}$.

Comme **R** est infini et comme il n'y a qu'un nombre fini de couples $(j, k)$ possibles, on peut trouver deux réels $c$ et $c'$ tels que

$$z = x_j + x_k + c x_j x_k \quad \text{et} \quad z' = x_j + x_k + c' x_j x_k$$

appartiennent à **C**. Comme

$$x_j + x_k = \frac{c'z - cz'}{c' - c} \quad \text{et} \quad x_j x_k = \frac{z - z'}{c - c'},$$

il en résulte que $x_j + x_k$ et $x_j x_k$ appartiennent à **C**. Le polynôme $(T - x_j)(T - x_k)$ appartient ainsi à $\mathbf{C}[X]$. Il est de degré 2. D'après la première question, ses racines appartiennent à **C**.

En particulier, P a une racine dans **C**.

**e)** Les questions précédentes permettent d'établir par récurrence que *tout polynôme non constant à coefficients réels a une racine dans* **C**.

Soit maintenant P un polynôme non constant de $\mathbf{C}[X]$ et posons $Q = P\bar{P}$ : si $P(X) = a_d X^d + \cdots + a_0$,

$$Q(X)\,(a_d X^d + \cdots + a_0)\,(\bar{a}_d X^d + \cdots + \bar{a}_0).$$

C'est un polynôme de $\mathbf{C}[X]$ tel que $\bar{Q}(X) = \bar{P}(X)P(X) = Q(X)$. Il est donc à coefficients réels. Par suite, il a une racine $z$ dans **C**.

Si $z$ n'est pas une racine de P, c'est une racine de $\bar{P}$. Alors, $P(\bar{z}) = \overline{\bar{P}(z)} = 0$, si bien que $\bar{z}$ est une racine de P.

Tout polynôme non constant à coefficients dans **C** a une racine dans **C** : **C** est algébriquement clos.

*Solution de l'exercice 9.4.2.* — **a)** Il suffit de montrer que l'homomorphisme naturel $A \to B$ défini par $a \mapsto \mathrm{cl}(a)$ est injectif. Or, si $a$ est un polynôme constant non nul et multiple de P, écrivons $a = P(X)Q(X)$. Soit $q_r X^r$ le monôme de plus grand degré dans Q. Comme P est unitaire de degré $d > 0$, le monôme de plus grand degré dans PQ est égal à $q_r X^{r+d}$. Mais $r + d > 0$ et le polynôme constant $a$ est de degré 0. Cette contradiction montre que l'homomorphisme naturel $A \to B$ est injectif et identifie ainsi A à son image dans B.

**b)** Si Q est un polynôme de A[X], on peut effectuer la division euclidienne de Q par P dans A[X]. Ainsi, on constate que cl(Q) est égal à la classe d'un polynôme de degré $< d$. Autrement dit, cl(1), ..., cl($X^{d-1}$) engendrent B comme A-module si bien que B est un A-module de type fini. D'après la proposition 9.2.3, l'extension $A \subset B$ est entière.

**c)** On démontre ce résultat par récurrence sur le degré $d$ de P, sachant qu'il est trivial si $d \leq 1$. Supposons le vérifié en degré $< d$.

Par construction, P a une racine $a_1$ dans l'extension entière $A \subset B = A[X]/(P)$. On peut effectuer la division euclidienne de P par $X - a_1$ dans B[X], d'où une expression $P = (X - a_1)Q + b_1$ avec $b_1 \in B$. En spécialisant en $X = a_1$, on trouve $b_1 = P(a_1) = 0$. Il existe alors une extension $B \subset C$ et des éléments $a_2, \ldots, a_d \in C$ tels que $Q(X) = (X - a_2) \ldots (X - a_d)$. Ainsi, $P(X) = (X - a_1) \ldots (X - a_d)$.

*Solution de l'exercice 9.4.3.* — Soient P et Q deux polynômes de A[X] tels que $y = P(x) = Q(1/x)$. Si $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$, on en déduit

$$\begin{aligned} y = P(x) &= \sum_{k=0}^{n} a_k x^k \\ &= \sum_{k=0}^{m} b_k x^{-k} = x^{-m} \sum_{k=0}^{m} b_k x^{m-k} = x^{-m} R(x), \end{aligned}$$

où R est de degré $\leq m$. Posons $N = m + n$ et $M = A + Ax + \cdots + Ax^N$. Soit $a \in M$, on écrit $a = a_1 + a_2$, où les puissances de $x$ qui interviennent dans $a_1$ sont $< m$, et celles qui interviennent dans $a_2$ sont $\geq m$. Alors, $ya_1 = P(x)a_1$ appartient à N car il ne fait intervenir que des puissances de $x$ qui sont $< m + n = N$. De même, $ya_2 = (x^{-m}a_2)R(x)$ s'écrit comme un polynôme en $x$ de degré $\leq N - m + m = N$. Ainsi, $ya = ya_1 + ya_2$ appartient à M.

Ainsi, $y = y \cdot 1$ appartient à M, et $A[y] \subset M$. Comme M est de type fini, le théorème 8.5 du cours implique que $y$ est entier sur A.

*Solution de l'exercice 9.4.4.* — **a)** Comme $x$ est entier sur A, il existe $n \geq 0$ tel que $A[x] \subset A + Ax + \cdots + Ax^n$. Soit $a \in A \setminus \{0\}$ tel que $ax^m \in A$ si $0 \leq m \leq n$. On constate que $aA[x] \subset A$ et donc $ax^m \in A$ pour tout entier $m \geq 0$.

**b)** Soit I l'idéal de A engendré par les $ax^n$ pour $n \geq 0$. Comme A est noethérien, c'est un A-module de type fini ; Il est stable par multiplication par $x$. De plus, l'élément non nul $a \in I$ n'est annulé par aucun élément non nul de $A[x]$. Autrement dit, I est un $A[x]$-module fidèle qui est de type fini comme A-module. On sait que cela implique que $x$ est entier sur A.

*Solution de l'exercice 9.4.5.* — Si $\sqrt{d} \in \mathbf{Z}$, $\mathbf{Z}[\sqrt{d}] = \mathbf{Z}$ est intégralement clos. On suppose donc dans la suite que $d$ n'est pas un carré parfait.

Le polynôme minimal de $x = a + b\sqrt{d}$ est égal à

$$(\mathrm{X} - a)^2 - b^2 d = \mathrm{X}^2 - 2a\mathrm{X} + a^2 - b^2 d.$$

L'élément $x$ est donc entier sur $\mathbf{Z}$ si et seulement si $2a \in \mathbf{Z}$ et $a^2 - b^2 d \in \mathbf{Z}$.

Si on peut écrire $d = d'e^2$ avec $e > 1$, alors on constate que $\sqrt{d'} = \sqrt{d}/e$ est entier sur $\mathbf{Z}$ mais n'appartient pas à $\mathbf{Z}[\sqrt{d}]$. L'anneau $\mathbf{Z}[\sqrt{d}]$ n'est alors pas intégralement clos.

On suppose dans la suite que $d$ est sans facteurs carrés. Nous allons en fait calculer la clôture intégrale de $\mathbf{Z}$ dans le corps $\mathbf{Q}(\sqrt{d})$.

Si $x = a + b\sqrt{d}$ est entier sur $\mathbf{Z}$, on voit que nécessairement

$$4b^2 d = 4(b^2 d - a^2) + (2a)^2 \in \mathbf{Z}.$$

Comme $d$ est sans facteurs carrés, cela implique que $2b \in \mathbf{Z}$. Si R est la clôture intégrale de $\mathbf{Z}$ dans $\mathbf{Q}[\sqrt{d}]$, on a ainsi une inclusion

$$\mathbf{Z}[\sqrt{d}] \subset \mathrm{R} \subset \frac{1}{2}\mathbf{Z}[\sqrt{d}].$$

Des représentants du $\mathbf{Z}$-module $\mathrm{R}/\mathbf{Z}[\sqrt{d}]$ sont donc contenus dans l'ensemble $\{0, 1/2, \sqrt{d}/2, (1+\sqrt{d})/2\}$. Comme $1/2$ et $(\sqrt{d})/2$ ne sont pas entiers sur $\mathbf{Z}$,

Ensuite, $(1+\sqrt{d})/2$ est entier sur $\mathbf{Z}$ si et seulement si $1 - d \in 4\mathbf{Z}$, c'est-à-dire $d \equiv 1 \pmod 4$. il en résulte que $\mathrm{R} = \mathbf{Z}[\sqrt{d}]$ si et seulement si $d \not\equiv 1 \pmod 4$ et que si $s \equiv 1 \pmod 4$, $\mathrm{R} = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$.

*Solution de l'exercice 9.4.6.* — **a)** Soit K le corps des fractions de A et soit $x \in \mathrm{K}$ qui est entier sur A. Comme $x$ est entier sur $\mathrm{A}_t$ et comme $\mathrm{A}_t$ est supposé intégralement clos, $x \in \mathrm{A}_t$. Soit $n \geq 0$ minimal tel que $a = xt^n \in \mathrm{A}$. Montrons que $n = 0$. Considérons pour cela une équation de dépendance intégrale

$$x^d + a_1 x^{d-1} + \cdots + a_d = 0.$$

Multiplions cette égalité par $t^{nd}$. On obtient

$$a^d + a_1 t^n a^{d-1} + \cdots + a_d t^{nd} = 0.$$

Supposons par l'absurde que $n \geq 1$. On en déduit que $t$ divise $a^d$, donc $a^d = 0 \pmod t$. Comme $\mathrm{A}/t$ est réduit, $a = 0 \pmod t$ et il existe $b \in \mathrm{A}$ tel que $a = bt$. Alors, $xt^{n-1} = b \in \mathrm{A}$ ce qui contredit l'hypothèse que $n$ était minimal.

**b)** Le polynôme $\mathrm{XZ} - \mathrm{Y}(\mathrm{Y}+1)$ est irréductible car de degré 1 en X et non multiple de Z. Comme l'anneau $\mathbf{C}[\mathrm{X},\mathrm{Y},\mathrm{Z}]$ est factoriel, A est un anneau intègre.

D'autre part,

$$\mathrm{A}/(x) = \mathbf{C}[\mathrm{X},\mathrm{Y},\mathrm{Z}]/(\mathrm{XZ} - \mathrm{Y}(\mathrm{Y}+1), \mathrm{X}) = \mathbf{C}[\mathrm{Y},\mathrm{Z}]/(\mathrm{Y}(\mathrm{Y}+1)) = \mathbf{C}[\mathrm{Z}] \times \mathbf{C}[\mathrm{Z}]$$

n'a pas d'éléments nilpotents. De plus,

$$\begin{aligned} A_x &= \mathbf{C}[X,Y,Z,X^{-1}]/(XZ - Y(Y+1)) = \mathbf{C}[X,X^{-1},Y,Z]/(Z - Y(Y+1)X^{-1}) \\ &= \mathbf{C}[X,X^{-1},Y] \end{aligned}$$

est un localisé de l'anneau $\mathbf{C}[X,Y]$. Comme cet anneau est factoriel, il est intégralement clos et $A_x$ est intégralement clos.

La première question montre alors que A est intégralement clos.

*Solution de l'exercice 9.4.7.* — **a)** Notons $P = X^m + \sum_{i=1}^{m}(-1)^i p_i X^{m-i}$ et $Q = X^n + \sum_{i=1}^{n}(-1)^i q_i X^{n-i}$. Soit C l'anneau

$$C = B[a_1,\dots,a_m,b_1,\dots,b_n]/I$$

où I est l'idéal engendré par les éléments

$$\sum_{\sigma\in F_k^m} a_{\sigma(1)}\dots a_{\sigma(k)} - p_k$$

et

$$\sum_{\sigma\in F-k^n} b_{\sigma(1)}\dots b_{\sigma(k)} - q_k.$$

(On a noté $F_k^m$ l'ensemble des applications injectives $\{1,\dots,k\} \to \{1,\dots,m\}$.) Dans C, on a ainsi $P(X) = \prod_{i=1^m}(X - a_i)$ et $Q(X) = \prod_{i=1}^{n}(X - b_i)$. De plus, les $a_i$ et $b_j$ sont solutions d'une équation polynômiale unitaire (donnée respectivement par P et Q), donc sont entiers sur B. Cela implique que C est une B-algèbre engendrée par des éléments entiers sur B donc que C est entière sur B.

Puisque $PQ \in A[X]$, les $a_i$ et $b_j$ sont entiers sur A. Par suite, les $p_k$ et $q_k$, étant les fonctions symétriques élémentaires des $a_i$ (resp. des $b_j$), sont entiers sur A pour tout $k$. Comme ce sont des éléments de B est que A est intégralement fermé dans B, ils appartiennent à A si bien que $P \in A[X]$ et $Q \in A[X]$, ainsi qu'il fallait démontrer.

**b)** Soit $P \in B[X]$ un polynôme qui est entier sur A[X] et considérons une relation de dépendance intégrale

$$P^d + R_1 P^{d-1} + \dots + R_d = 0,$$

avec $R_i \in A[X]$. On pose $Q = X^r - P$ avec $r > \deg P$ (de sorte que Q est unitaire) et on récrit cette égalité

$$(-Q + X^r)^d + R_1(-Q + X^r)^{d-1} + \dots + R_d = 0.$$

Développons ; on trouve une égalité

$$\sum_{k=0}^{d} Q^k (-1)^k \sum_{i=k}^{d} R_{d-i}\binom{i}{k} X^{r(i-k)} = 0$$

dans laquelle $R_0 = 1$ que l'on récrit

$$\sum_{k=0}^{d} S_k Q^k = 0$$

avec $S_k \in A[X]$. On a $S_d = 1$ et

$$S_0 = \sum_{i=0}^{d} R_{d-i} X^{ri} = X^r d + \dots$$

donc $S_0$ est unitaire si $r > \max(\deg R_i)$. L'égalité

$$Q(-Q^{d-1} - S_{d-1}Q^{d-2} - \cdots - S_1) = S_0$$

et la question précédente impliquent alors que $Q \in A[X]$. Par suite, $P = X^r - Q \in A[X]$, ce qui prouve que $A[X]$ est intégralement fermé dans $B[X]$.

# 10 Algèbre homologique

*Ce chapitre expose quelques rudiments d'algèbre homologique. Issue de la topologie algébrique où elle a des applications frappantes (le théorème de Brouwer par exemple), le formalisme algébrique qui la sous-tend a ensuite essaimé dans de nombreux domaines des mathématiques. C'est aujourd'hui en outil fondamental en algèbre commutative, en géométrie algébrique, en topologie et elle a même des applications en robotique !*

## 10.1. Suites exactes

La notion de suite exacte permet de résumer dans un diagramme simple à écrire de nombreuses propriétés algébriques.

Définition 10.1.1. — *Soit* A *un anneau. Une* suite exacte *de* A*-modules est un diagramme*

$$\mathrm{M}_0 \xrightarrow{f_1} \mathrm{M}_1 \xrightarrow{f_2} \mathrm{M}_2 \to \cdots \to \mathrm{M}_{n-1} \xrightarrow{f_n} \mathrm{M}_n$$

*où pour tout* $i \in \{2; \ldots; n\}$, $\operatorname{Ker} f_i = \operatorname{Im} f_{i-1}$.

En particulier, on a $f_i \circ f_{i-1} = 0$ pour tout $i \in \{2; \ldots; n\}$. Un cas particulier très important est fournie par les suites de 5 modules, les deux extrémités étant nulles. On parle alors de *suite exacte courte*.

Proposition 10.1.2. — *Une suite de* A*-modules*

$$0 \to \mathrm{N} \xrightarrow{i} \mathrm{M} \xrightarrow{p} \mathrm{P} \to 0$$

*est exacte si et seulement si :*

- *$i$ est injectif ;*
- $\operatorname{Ker} p = \operatorname{Im} i$ *;*
- *$p$ est surjectif.*

*Alors, $i$ induit un isomorphisme de* N *sur le sous-*A*-module* $i(\mathrm{N})$ *de* M *et $p$ induit un isomorphisme* $\mathrm{M}/i(\mathrm{N}) \simeq \mathrm{P}$.

*Démonstration.* — Il suffit d'écrire toutes les conditions. L'image de la flèche $0 \to \mathrm{N}$ est 0, c'est aussi le noyau de $i$, donc $i$ est injectif. Ensuite, $\operatorname{Im} i = \operatorname{Ker} p$. Enfin, l'image de $p$ est égale au noyau de l'homomorphisme $\mathrm{P} \to 0$, c'est-à-dire P, donc $p$ est surjectif. Le reste de la proposition provient du théorème de factorisation. □

DÉFINITION 10.1.3. — *Un complexe est un diagramme*

$$\mathrm{M}_0 \xrightarrow{f_1} \mathrm{M}_1 \xrightarrow{f_2} \mathrm{M}_2 \to \cdots \to \mathrm{M}_{n-1} \xrightarrow{f_n} \mathrm{M}_n$$

*où pour tout* $i \in \{2; \ldots; n\}$, $f_i \circ f_{i-1} = 0$.

DÉFINITION 10.1.4. — *Soit* A *un anneau et* $f\colon \mathrm{M} \to \mathrm{N}$ *un homomorphisme de* A*-modules. Le* A*-module quotient* $\mathrm{N}/f(\mathrm{M})$ *est appelé* conoyau *de* $f$. *On le note* $\operatorname{Coker} f$.

*Remarque 10.1.5.* — On a $\operatorname{Coker} f = 0$ si et seulement si $f$ est surjectif. Ainsi, un homomorphisme $f\colon \mathrm{M} \to \mathrm{N}$ est un isomorphisme si et seulement si $\operatorname{Ker} f = 0$ et $\operatorname{Coker} f = 0$.

THÉORÈME 10.1.6 (Lemme du serpent). — *Considérons un diagramme d'homomorphismes de* A*-modules*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{N} & \xrightarrow{i} & \mathrm{M} & \xrightarrow{p} & \mathrm{P} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & \mathrm{N}' & \xrightarrow{i'} & \mathrm{M}' & \xrightarrow{p'} & \mathrm{P}' & \longrightarrow & 0 \end{array}$$

*dans lequel les deux lignes sont supposées exactes et les deux carrés commutatifs :* $i' \circ f = f \circ i$ *et* $p' \circ g = h \circ p$. *Il existe alors un homomorphisme canonique* $\partial\colon \operatorname{Ker} h \to \operatorname{Coker} f$ *tel que l'on ait une suite exacte*

$$0 \to \operatorname{Ker} f \xrightarrow{i_*} \operatorname{Ker} g \xrightarrow{p_*} \operatorname{Ker} h \xrightarrow{\partial} \operatorname{Coker} f \xrightarrow{i'_*} \operatorname{Coker} g \xrightarrow{p'_*} \operatorname{Coker} h \to 0.$$

*Démonstration.* — a) On a $i(\operatorname{Ker} f) \subset \operatorname{Ker} g$ et $p(\operatorname{Ker} g) \subset \operatorname{Ker} h$. En effet, si $x \in \mathrm{N}$ vérifie $f(x) = 0$, alors $g(i(x)) = (g \circ i)(x) = (i' \circ f)(x) = i'(f(x)) = 0$, donc $i(x) \in \operatorname{Ker} g$. De même, si $y \in \operatorname{Ker} g$, on a $h(p(y)) = (h \circ p)(y) = (p' \circ g)(y) = p'(g(y)) = 0$, donc $p(y) \in \operatorname{Ker} h$.

On a ainsi des homomorphismes $i_*\colon \operatorname{Ker} f \to \operatorname{Ker} g$ et $p_*\colon \operatorname{Ker} g \to \operatorname{Ker} h$.

b) On a $i'(\operatorname{Im} f) \subset \operatorname{Im} g$ et $p'(\operatorname{Im} g) \subset \operatorname{Im} h$. En effet, si $x' \in \operatorname{Im} f$, soit $x \in \mathrm{N}$ tel que $x' = f(x)$. Alors, $i'(x') = (i' \circ f)(x) = (g \circ i)(x) = g(i(x))$, ce qui prouve que $i'(x')$ appartient à $\operatorname{Im} g$.

De même, si $y' \in \operatorname{Im} g$, soit $y \in \mathrm{M}$ tel que $y' = g(y)$. On a alors $p'(y') = (p' \circ g)(y) = (h \circ p)(y) = h(p(y))$ donc $p'(y')$ appartient à $\operatorname{Im} h$.

Il en résulte que le noyau de l'homomorphismes composé

$$\mathrm{N}' \xrightarrow{i'} \mathrm{M}' \to \mathrm{M}'/\operatorname{Im} g = \operatorname{Coker}(g)$$

contient $\mathrm{Im}(f)$, d'où par passage au quotient un homomorphisme canonique $i'_*$: $\mathrm{Coker}(f) = \mathrm{N}'/\mathrm{Im}(f) \to \mathrm{Coker}(g)$. De même, on en déduit un homomorphisme $p'_*$: $\mathrm{Coker}(g) \to \mathrm{Coker}(h)$, induit par $p'$.

c) L'homomorphisme $i_*$ est injectif : si $i_*(x) = 0$, $i(x) = 0$ donc $x = 0$.

Comme $p_*$ est la restriction à $\mathrm{Ker}\, g$ de $p$ et comme $p \circ i = 0$, on a $p_* \circ i_* = 0$ donc $\mathrm{Im}\, i_* \subset \mathrm{Ker}\, p_*$. Réciproquement, soit $y \in \mathrm{Ker}\, p_*$. On a donc $y \in \mathrm{Ker}\, g$ et $p(y) = 0$. Comme la première ligne du diagramme est exacte, $y \in \mathrm{Im}\, i$. Soit ainsi $x \in \mathrm{N}$ tel que $y = i(x)$. On a $0 = g(y) = g(i(x)) = (g \circ i)(x) = (i' \circ f)(x) = i'(f(x))$. Comme $i'$ est injectif, $f(x) = 0$ et $x \in \mathrm{Ker}\, f$. Par suite, $y = i(x) \in i(\mathrm{Ker}\, f) = i_*(\mathrm{Ker}\, f)$.

d) L'homomorphisme $p'_*$ est surjectif : si $\zeta' \in \mathrm{Coker}\, h$, on peut écrire $\zeta' = \mathrm{cl}(z')$ avec $z' \in \mathrm{P}'$. Comme $p'$ est surjectif, il existe $y' \in \mathrm{M}'$ tel que $z' = p'(y')$. Alors, par définition de $p'_*$, on a $\zeta' = p'_*(\mathrm{cl}(y'))$, si bien que $\zeta' \in \mathrm{Im}\, p'_*$.

On a $p'_* \circ i'_* = 0$. En effet, par définition de $i'_*$, si $x' \in \mathrm{N}'$, $i'_*(\mathrm{cl}(x')) = \mathrm{cl}(i'(x'))$, d'où

$$p'_*(i'_*(\mathrm{cl}(x')) = p'_*(\mathrm{cl}(i'(x'))) = \mathrm{cl}(p'(i'(x'))) = 0.$$

Réciproquement, si $p'_*(\mathrm{cl}(y')) = 0$, on a $\mathrm{cl}(p'(y')) = 0$, d'où $p'(y') \in \mathrm{Im}\, h$. On écrit $p'(y') = h(z)$ avec $z \in \mathrm{P}$. Comme $p$ est surjectif, il existe $y \in \mathrm{M}$ tel que $z = p(y)$ et $p'(y') = h(p(z)) = p'(g(z))$. Ainsi, $y' - g(z)$ appartient à $\mathrm{Ker}\, p'$, donc est de la forme $i'(x')$ pour $x' \in \mathrm{N}'$. Finalement,

$$\mathrm{cl}(y') = \mathrm{cl}(g(z) + i'(x')) = \mathrm{cl}(i'(x')) = i'_*(x'),$$

d'où $\mathrm{Ker}\, p'_* = \mathrm{Im}\, i'_*$.

e) Nous allons maintenant construire l'homomorphisme $\partial$. La restriction à $p^{-1}(\mathrm{Ker}\, h) = \mathrm{Ker}(h \circ p)$ de $g$ fournit un homomorphisme $\mathrm{Ker}(h \circ p) \to \mathrm{M}$ dont l'image est contenue dans le noyau de $p'$ (si $h(p(y)) = 0$, $p'(g(y)) = 0$). Puisque $\mathrm{Ker}\, p' = \mathrm{Im}\, i'$ et comme $i'$: $\mathrm{N}' \to \mathrm{Im}\, i'$ est un isomorphisme, il en résulte un homomorphisme canonique $p^{-1}(\mathrm{Ker}\, h) \to \mathrm{N}'$ que l'on compose ensuite avec la surjection canonique $\mathrm{N}' \to \mathrm{Coker}(f)$, d'où un homomorphisme $\gamma$: $p^{-1}(\mathrm{Ker}\, h) \to \mathrm{Coker}(f)$.

Si $y = i(x) \in i(\mathrm{N})$, on a $g(y) = i'(f(x))$, donc $\gamma(y) = \mathrm{cl}(f(x)) = 0$. Ainsi, $\mathrm{Ker}\, \gamma$ contient $i(\mathrm{N})$, d'où par passage au quotient un homomorphisme bien défini

$$\partial\colon\ \mathrm{Ker}\, h = p^{-1}(\mathrm{Ker}\, h)/p^{-1}(0) = p^{-1}(\mathrm{Ker}\, h)/i(\mathrm{N}) \xrightarrow{\gamma} \mathrm{Coker}(f).$$

Concrètement, l'image d'un élément $z$ de $\mathrm{Ker}\, h$ par l'homomorphisme $\partial$ est obtenue de la façon suivante. Comme $p$ est surjectif, il existe $y \in \mathrm{M}$ tel que $z = p(y)$. Alors, $0 = h(z) = h(p(y)) = p'(g(y))$, donc $g(y) \in \mathrm{Ker}\, p' = \mathrm{Im}\, i'$. Il existe ainsi $x' \in \mathrm{N}'$ tel que $g(y) = i'(x')$. Alors, $\partial(z)$ est la classe de $x'$ dans $\mathrm{Coker}(f) = \mathrm{N}'/\mathrm{Im}\, f$.

f) Montrons que $\mathrm{Im}\, p_* = \mathrm{Ker}\, \partial$.

Soit $z \in \operatorname{Im} p_*$, d'où $y \in \operatorname{Ker} g$ tel que $p(y) = z$. Autrement dit, $g(y) = 0$ et avec les notations du paragraphe précédent, $x' = 0$, d'où $\partial(z) = 0$ et $z \in_k er\partial$.

Réciproquement, si $z \in \operatorname{Ker} \partial$, on a $x' \in \operatorname{Im} f$, donc $x' = f(x)$ pour un certain $x \in \mathrm{N}$ et $g(y) = i'(x') = g(i(x))$. On a donc $y - i(x) \in \operatorname{Ker} g$. Par suite, $z = p(y) = p(y - i(x)) \in p(\operatorname{Ker} g) = \operatorname{Im} p_*$.

g) Enfin, montrons que $\operatorname{Im} \partial = \operatorname{Ker} i'_*$.

Soit $z \in \mathrm{N}$; avec les mêmes notations, $i'(\partial(z)) = i'(\mathrm{cl}(x')) = \mathrm{cl}(i'(x')) = \mathrm{cl}(g(y)) = 0$, donc $\partial(z) \in \operatorname{Ker} i'_*$ et $\operatorname{Im} \partial \subset \operatorname{Ker} i'_*$.

Réciproquement, soit $\xi' \in \operatorname{Ker} i'_*$. On peut écrire $\xi' = \mathrm{cl}(x')$. On a alors $i'_*(\xi') = \mathrm{cl}(i'(x'))$. Par suite, $i'(x') \in \operatorname{Im} g$. Si $i'(x') = g(y)$ avec $y \in \mathrm{M}$, on a par définition $\partial(p(y)) = \mathrm{cl}(x') = \xi'$ si bien que $\operatorname{Ker} i'_* \subset \operatorname{Im} \partial$.

Le théorème est donc démontré. □

Corollaire 10.1.7. — *a) Si $f$ et $h$ sont injectives, $g$ aussi. Si $f$ et $h$ sont surjectives, $g$ aussi.*

*b) Si $f$ est surjective et $g$ injective, $h$ est injective Si $g$ est surjective et $h$ injective, $f$ est surjective..*

*Démonstration.* — a) Si $f$ et $h$ sont injectives, la suite exacte du diagramme du serpent commence par $0 \to 0 \xrightarrow{i_*} \operatorname{Ker} g \xrightarrow{p_*} 0$. Nécessairement, $\operatorname{Ker} g = 0$. Si $f$ et $h$ sont surjectives, elle se termine par $0 \xrightarrow{i'_*} \operatorname{Coker} g \xrightarrow{p'_*} 0$, donc $\operatorname{Coker} g = 0$ et $f$ est injective.

b) Si $f$ est surjective et $g$ injective, on a $\operatorname{Ker} g = 0$ et $\operatorname{Coker} f = 0$. Par suite, le milieu de la suite exacte s'écrit $0 \xrightarrow{p_*} \operatorname{Ker} h \xrightarrow{\partial} 0$, donc $h$ est injective. Enfin, si $g$ est surjective et $h$ injective, on a $\operatorname{Ker} h = 0$, $\operatorname{Coker} g = 0$, d'où une suite exacte $0 \xrightarrow{\partial} \operatorname{Coker} f \xrightarrow{i'_*} 0$, donc $f$ est surjective. □

*Exercice 10.1.8.* — Démontrer directement le corollaire précédent.

## 10.2. Suites exactes scindées. Modules projectifs et injectifs

Lemme 10.2.1. — *Soit* A *un anneau. et considérons une suite exacte courte de* A*-modules*

$$0 \to \mathrm{N} \xrightarrow{i} \mathrm{M} \xrightarrow{p} \mathrm{P} \to 0.$$

*Les propriétés suivantes sont équivalentes :*

(1) *il existe* $q : \mathrm{P} \to \mathrm{M}$ *tel que* $p \circ q = \mathrm{Id}_\mathrm{P}$ *(p a un inverse à droite) ;*

(2) *il existe* $j : \mathrm{M} \to \mathrm{N}$ *tel que* $j \circ i = \mathrm{Id}_\mathrm{N}$ *(i a un inverse à gauche) ;*

(3) $i(\mathrm{N})$ *a un supplémentaire dans* M.

Définition 10.2.2. — *Une suite exacte courte qui vérifie les conditions du lemme 10.2.1 précédent est dite* scindée.

*Démonstration.* — (1)⇒(3). — Soit $Q = q(P)$ l'image de $q$ dans M et montrons que Q est un supplémentaire de $i(N)$. Tout d'abord, si $m = i(x) + q(y)$, pour $x \in N$ et $y \in P$, on a $p(m) = p(i(x)) + p(q(y)) = y$. Ainsi, si $m = i(x) + q(y) = 0$, alors $y = p(m) = 0$ puis $i(x) = 0$ — donc aussi $x = 0$ puisque $i$ est injectif. Cela montre que $i(N)$ et Q sont en somme directe. De plus, si $m \in M$, posons $y = p(m)$. Alors, $p(m - q(y)) = p(m) - p(q(p(m))) = p(m) - p(m) = 0$, donc $m - q(y) \in i(N)$. Cela montre que $M = i(N) + Q$. Ainsi, $M = i(N) \oplus Q$ et Q est un supplémentaire de $i(N)$ dans M.

(3)⇒(1). — Soit Q un supplémentaire de $i(N)$ dans M. Considérons l'homomorphisme $p' : Q \to P$ obtenu par restriction à Q de $p$. On a $\operatorname{Ker} p' = \operatorname{Ker} p \cap Q = i(N) \cap Q = 0$ puisque Q et $i(N)$ sont en somme directe. Donc $p'$ est injectif. De plus, si $x \in P$, soit $y \in M$ tel que $x = p(y)$. On peut écrire $y = i(z) + z'$ avec $z \in N$ et $z' \in Q$. Alors, $x = p(i(z)) + p(z') = p(z')$ et $p'$ est surjectif. Par suite, $p'$ est un isomorphisme et l'homomorphisme réciproque $q : P \to Q$ vérifie bien $p \circ q = \mathrm{Id}_P$.

(2)⇒(3).— Soit Q le noyau de $j$. Si $x \in Q \cap i(N)$, on peut écrire $x = i(y)$ avec $y \in N$ et $0 = j(x) = j(i(y)) = y$, donc $y = 0$ et $x = 0$. Ainsi, Q et $i(N)$ sont en somme directe. De plus, si $x \in M$, posons $y = x - i(j(x))$. Alors, $j(y) = j(x) - j(i(j(x)) = 0$ donc $y \in Q$. Ceci prouve que $Q + i(N) = M$. Ainsi, $M = Q \oplus i(N)$.

(3)⇒(2). — Soit Q un supplémentaire de $i(N)$ dans M. Considérons l'application $j : M \to N$ qui associe à $m = x + i(y)$ avec $x \in Q$ et $y \in N$ l'élément $y \in N$. Elle est bien définie car $i$ est injectif. De plus, c'est un homomorphisme. Enfin, un élément $i(y) \in i(N)$ se décompose $i(y) = 0 + i(y)$, donc $j(i(y)) = y$ et $j \circ i = \mathrm{Id}_N$. □

*Remarque 10.2.3.* — Comme tout sous-espace vectoriel d'un espace vectoriel possède un supplémentaire, toute suite exacte de modules sur un corps est scindée.

Définition 10.2.4. — *On dit qu'un* A*-module* P *est* projectif *si toute suite exacte courte*

$$0 \to N \to M \to P \to 0$$

*est scindée.*

Autrement dit, P est projectif si et seulement si tout homomorphisme surjectif $f : M \to P$ admet un inverse à droite.

Théorème 10.2.5. — *Soit* P *un* A*-module. Les propriétés suivantes sont équivalentes :*

(1) P *est projectif ;*

(2) P *est un facteur direct d'un* A*-module libre ;*

(3) *pour tout homomorphisme surjectif* $p : M \to N$ *et tout homomorphisme* $f : P \to N$, *il existe un homomorphisme* $g : P \to M$ *tel que* $f = p \circ g$.

Rappelons qu'un facteur direct d'un module est un sous-module qui possède un supplémentaire. D'autre part, l'énoncé (3) du théorème est souvent pris comme définition des modules projectifs.

*Démonstration.* — (1)⇒(2). — Supposons que P est projectif. Soit S une famille génératrice dans P et soit $L = A^{(S)}$ le A-module libre de base S. On a un homomorphisme canonique $p\colon L \to P$ tel que $e_s$ (vecteur de $A^{(S)}$ dont toutes les coordonnées valent 0 sauf la coordonnée $s$ qui vaut 1) a pour image $s$. Soit N le noyau de $p$, d'où une suite exacte courte $0 \to N \to L \to P \to 0$. Comme P est supposé projectif, N admet un supplémentaire Q dans L. Dans la démonstration du lemme 10.2.1, on a montré que la restriction à Q de l'homomorphisme $p$ est un isomorphisme $Q \simeq P$. Par suite, P est (isomorphe à) un facteur direct du A-module libre L.

(2)⇒(3). — Supposons maintenant qu'il existe un A-module libre L contenant P et un sous-module Q de L tel que $P \oplus Q = L$. Fixons une base S de L.

Soit $p\colon M \to N$ un homomorphisme surjectif et $f\colon P \to N$ un homomorphisme quelconque. On veut montrer qu'il existe $g\colon P \to M$ tel que $p \circ g = f$.

On définit un homomorphisme $\varphi\colon L \to N$ par $\varphi(x+y) = f(p)$ si $x \in P$ et $y \in Q$. Par construction, la restriction de $\varphi$ à P est égale à $f$. Pour tout $s \in S$, soit alors $m_s$ un élément de M tel que $p(m_s) = \varphi(s)$ (il en existe car $p$ est surjectif). Alors, la propriété universelle des modules libres implique qu'il existe un unique homomorphisme $\gamma\colon L \to M$ tel que $\gamma(s) = m_s$. Pour tout $s \in S$, on a alors $p \circ \gamma(s) = p(m_s) = \varphi(s)$, donc S formant une base de L, $p \circ \gamma = \varphi$. Soit $g$ la restriction de $\varphi$ à P. Elle vérifie $p \circ g = \varphi|_P = f$.

(3)⇒(1). — Soit $p\colon M \to P$ un homomorphisme surjectif. On applique l'hypothèse de (3) avec $N = P$ et $f = \mathrm{Id}_P$. Il existe alors $g\colon P \to M$ tel que $p \circ g = \mathrm{Id}_P$, autrement dit $p$ a un inverse à droite. Cela prouve que P est un module projectif. □

En particulier, les modules libres sont projectifs.

*Exercice 10.2.6.* — a) Soit P un A-module projectif. Si P est de type fini, montrer qu'il existe un A-module libre de type fini L dont P est un facteur direct.

b) On suppose que A est un anneau principal. Montrer que tout A-module projectif de type fini est libre.

DÉFINITION 10.2.7. — *On dit qu'un* A*-module* I *est injectif si tout homomorphisme injectif* $i\colon I \to M$ *admet un inverse à gauche.*

Ceci revient bien sûr à dire que toute suite exacte courte

$$0 \to I \to M \to N \to 0$$

est scindée. C'est en quelque sorte la définition duale de celle des modules projectif. Comme le fait remarquer Matsumura dans [5], il n'y a pas de notion duale des modules libres, si bien que l'on n'a pas de caractérisation des modules injectifs complètement analogue à celle fournie par le théorème 10.2.5 pour les modules projectifs.

THÉORÈME 10.2.8. — *Soit* I *un* A*-module. Les conditions suivantes sont équivalentes.*

(1) I *est injectif ;*

(2) *pour tout idéal* $\mathfrak{a}$ *de* A *et tout homomorphisme injectif* $f\colon \mathfrak{a} \to \mathrm{I}$*, il existe un homomorphisme* $g\colon \mathrm{A} \to \mathrm{I}$ *tel que* $f = g|_{\mathfrak{a}}$ *;*

(3) *pour tout homomorphisme injectif* $i\colon \mathrm{M} \to \mathrm{N}$ *et tout homomorphisme* $f\colon \mathrm{M} \to \mathrm{I}$*, il existe un homomorphisme* $g\colon \mathrm{N} \to \mathrm{I}$ *tel que* $f = g \circ i$*.*

Là encore, c'est souvent la troisième de ces conditions qui est prise comme définition des modules injectifs.

*Démonstration.* — (3)⇒(2). — Il suffit de poser $\mathrm{M} = \mathfrak{a}$ et $\mathrm{N} = \mathrm{A}$.

(3)⇒(1). — Si $i\colon \mathrm{I} \to \mathrm{M}$ est injectif, appliquons l'hypothèse (3) à l'homomorphisme identique $\mathrm{I} \to \mathrm{I}$. On obtient un homomorphisme $g\colon \mathrm{M} \to \mathrm{I}$ tel que $g \circ i = \mathrm{Id}_{\mathrm{I}}$. Ainsi, I est injectif.

(1)⇒(3). — Soit $i\colon \mathrm{M} \to \mathrm{N}$ un homomorphisme injectif et $f\colon \mathrm{M} \to \mathrm{I}$ un homomorphisme. On veut montrer qu'il existe $g\colon \mathrm{N} \to \mathrm{I}$ tel que $f = g \circ i$.

Soit $\mathrm{P} \subset \mathrm{N} \times \mathrm{I}$ le sous-module image de l'homomorphisme $\mathrm{M} \to \mathrm{N} \times \mathrm{I}$ tel que $m \mapsto (i(m), -f(m))$ et soit $\varphi\colon \mathrm{I} \to \mathrm{N} \times \mathrm{I} \to (\mathrm{N} \times \mathrm{I})/\mathrm{P}$ l'homomorphisme composé tel que $x \mapsto \mathrm{cl}(0, x)$. Si $\varphi(x) = 0$, il existe $m \in \mathrm{M}$ tel que $(0, x) = (i(m), -f(m))$. Comme $i$ est injectif, $m = 0$ et $x = 0$. Ainsi, $\varphi$ est injectif.

Par hypothèse, il existe un homomorphisme $\psi\colon (\mathrm{N} \times \mathrm{I})/\mathrm{P} \to \mathrm{I}$ tel que $\psi \circ \varphi = \mathrm{Id}_{\mathrm{I}}$. Soit alors $g\colon \mathrm{N} \to \mathrm{I}$ l'homomorphisme défini par $g(x) = \psi(\mathrm{cl}(x, 0))$. Si $x \in \mathrm{M}$, on a

$$g(i(x)) = \psi(\mathrm{cl}(i(x), 0)) = \psi(\mathrm{cl}(0, f(x))) = \psi(\varphi(f(x))) = f(x).$$

Ainsi, $g \circ i = f$, ce qu'il fallait démontrer.

(2)⇒(1). — Soit $i\colon \mathrm{I} \to \mathrm{M}$ un homomorphisme injectif. On veut prouver qu'il existe $f\colon \mathrm{M} \to \mathrm{I}$ qui est un inverse à gauche de $i$, c'est-à-dire tel que $f \circ i = \mathrm{Id}_{\mathrm{I}}$.

Soit $\mathscr{F}$ l'ensemble des couples $(\mathrm{N}, f_{\mathrm{N}})$ où N est un sous-module de M contenant I et $f_{\mathrm{N}}$ un homomorphisme $\mathrm{N} \to \mathrm{I}$ vérifiant $f_{\mathrm{N}} \circ i = \mathrm{Id}_{\mathrm{I}}$. Comme $i$ est injectif, c'est un isomorphisme $\mathrm{I} \to i(\mathrm{I})$ et l'isomorphisme réciproque définit un élément $(i(\mathrm{I}), i^{-1})$ de $\mathscr{F}$. Par conséquent, $\mathscr{F}$ n'est pas vide.

On définit un ordre $\prec$ sur $\mathscr{F}$ en posant

$$(\mathrm{N}, f_{\mathrm{N}}) \prec (\mathrm{N}', f_{\mathrm{N}'}) \qquad \Leftrightarrow \qquad \mathrm{N} \subset \mathrm{N}' \quad \text{et} \quad f_{\mathrm{N}'}|_{\mathrm{N}} = f_{\mathrm{N}}.$$

Muni de cette relation d'ordre, $\mathscr{F}$ est inductif. En effet, si $(N_\alpha, f_\alpha)$ est une famille totalement ordonnée dans $\mathscr{F}$, la réunion $N = \bigcup N_\alpha$ est un sous-module de M et on peut définir $f_N : N \to I$ en posant, si $\alpha$ est tel que $x \in N_\alpha$, $f_N(x) = f_{N_\alpha}(x)$. Si $x \in N_\alpha$ et $x \in N_\beta$, on peut supposer, quitte à échanger $\alpha$ et $\beta$, que $(N_\alpha, f_{N_\alpha}) \prec (N_\beta, f_{N_\beta})$. Alors, $N_\alpha \subset N_\beta$ et $f_{N_\beta}|_{N_\alpha}$, d'où $f_{N_\beta}(x) = f_{N_\alpha}(x)$, ce qui prouve que $f_N$ est bien défini.

D'après le lemme de Zorn, $\mathscr{F}$ admet un élément maximal $(N, f_N)$. Supposons par l'absurde que $N \neq M$. Soit alors $m \in M \setminus N$ et soit $\mathfrak{a} = (N : m)$ l'ensemble des $a \in A$ tels que $am \in N$. Notons $N' = N + Am$. C'est un sous-module de M qui contient strictement N.

Soit $\varphi : \mathfrak{a} \to I$ l'homomorphisme défini par $a \mapsto f_N(am)$ si $a \in \mathfrak{a}$. Par l'hypothèse (2), il existe un homomorphisme $\psi : A \to I$ tel que $\psi(a) = f_N(am)$ si $a \in \mathfrak{a}$.

On définit alors un homomorphisme $g : N' \to I$ en posant, si $x \in N$ et $a \in A$, $g(x + am) = f_N(x) - \psi(a)$. C'est une application bien définie : si $x + am = x' + a'm$, $(a' - a)m = x - x'$ appartient à N, donc $a' - a \in \mathfrak{a}$ et

$$\begin{aligned}\big(f_N(x') - \psi(a')\big) - \big(f_N(x) - \psi(a)\big) &= f_N(x' - x) - \psi(a' - a)\\ &= f_N(x' - x) - f_N((a' - a)m) = 0.\end{aligned}$$

Il est facile de vérifier que c'est un homomorphisme. De plus, on a $g|_N = f_N$, donc aussi $g \circ i = \mathrm{Id}_I$, si bien que le couple $(N', g)$ définit un élément de $\mathscr{F}$. Mais ceci contredit l'hypothèse que N était maximal.

Par suite, un élément maximal de $\mathscr{F}$ est de la forme $(M, f_M)$ où $f_M : M \to I$ est un homomorphisme tel que $f_M \circ i = \mathrm{Id}_I$.

Ceci clôt la démonstration du théorème. □

COROLLAIRE 10.2.9. — *Soit* A *un anneau principal et* M *un* A*-module. Alors,* M *est injectif si et seulement si pour tout* $a \in A$, $a \neq 0$, *l'homomorphisme* $\mu_a : M \to M$, $x \mapsto ax$ *est surjectif.*

*Démonstration.* — Supposons que M est injectif et soit $a \in A$, $a \neq 0$. Soit $x \in M$ et considérons l'homomorphisme $(a) \to M$ défini par $ab \mapsto bx$ (c'est là qu'on utilise que $a \neq 0$, le fait que $a$ soit simplifiable suffirait). Comme M est injectif, la propriété (2) du théorème 10.2.8 montre qu'il existe un homomorphisme $f : A \to M$ tel que $f(ab) = bx$ si $b \in A$. Alors, $f(1)$ est un élément de M tel que $af(1) = f(a) = x$. Ainsi, l'homomorphisme $\mu_a$ est surjectif.

Réciproquement, supposons que cette propriété est satisfaite. Soit $\mathfrak{a}$ un idéal de A et $f : \mathfrak{a} \to M$ un homomorphisme. Comme A est principal, il existe $a \in A$ tel que $\mathfrak{a} = (a)$. Si $a = 0$, tout homomorphisme $g : A \to M$ convient, par exemple l'homomorphisme nul. Supposons maintenant que $a \neq 0$. Alors, pour tout $b \in A$, $f(ab) = bf(a)$. Par hypothèse, il existe $x \in M$ tel que $ax = f(a)$. Alors, l'homomorphisme $g : A \to M$ tel que $g(b) = bx$ pour tout $b \in A$ vérifie

$g(ab) = abx = bf(a) = f(ab)$ pour tout $b \in \mathrm{A}$. Ainsi, la restriction de $g$ à l'idéal $(a)$ est bien égale à $f$. Ceci prouve que M est injectif. □

*Exemple 10.2.10.* — Le **Z**-module $\mathbf{Q}/\mathbf{Z}$ est un **Z**-module injectif.

## 10.3. Foncteurs exacts

Rappelons qu'un foncteur $F$ de la catégorie des A-modules dans elle-même est une « application » qui associe à tout module M un module $F(\mathrm{M})$ et à tout homomorphisme $f\colon \mathrm{M} \to \mathrm{N}$ un homomorphisme $F(f)\colon F(\mathrm{M}) \to F(\mathrm{N})$ de sorte que l'application $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M},\mathrm{N}) \to \mathrm{Hom}_{\mathrm{A}}(F(\mathrm{M}),F(\mathrm{N}))$ est un homomorphisme de A-algèbres (non commutatives) :

– on a $F(\mathrm{Id}_{\mathrm{M}}) = \mathrm{Id}_{F(\mathrm{M})}$ pour tout module M ;

– l'application $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M},\mathrm{N}) \to \mathrm{Hom}_{\mathrm{A}}(F(\mathrm{M}),F(\mathrm{N}))$ est un homomorphisme de A-modules ;

– pour tout couple d'endomorphisme $f\colon \mathrm{M} \to \mathrm{N}$ et $g\colon \mathrm{N} \to \mathrm{P}$, $F(g \circ f) = F(g) \circ F(f)$.

Un tel foncteur est aussi appelé *foncteur covariant*.

Un foncteur *contravariant* est une application du même genre mais qui renverse le sens des flèches : à un homomorphisme $f\colon \mathrm{M} \to \mathrm{N}$ est associé un homomorphisme $F(f)\colon F(\mathrm{N}) \to F(\mathrm{M})$ et l'on a $F(f \circ g) = F(g) \circ F(f)$.

*Exemple 10.3.1* (Foncteurs Hom). — Soit P un A-module fixé. Pour tout A-module M, considérons le A-module $\mathrm{Hom}_{\mathrm{A}}(\mathrm{P},\mathrm{M})$. Si $f\colon \mathrm{M} \to \mathrm{N}$ est un homomorphisme, on considère l'homomorphisme $\mathrm{Hom}_{\mathrm{A}}(\mathrm{P},\mathrm{M}) \to \mathrm{Hom}_{\mathrm{A}}(\mathrm{P},\mathrm{N})$ tel que $\varphi \mapsto f \circ \varphi$. Cela définit un foncteur $\mathrm{Hom}_{\mathrm{A}}(\mathrm{P},\bullet)$.

Si on considère en revanche les A-modules $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M},\mathrm{P})$ et pour $f\colon \mathrm{M} \to \mathrm{N}$ l'homomorphisme $\mathrm{Hom}_{\mathrm{A}}(\mathrm{N},\mathrm{P}) \to \mathrm{Hom}_{\mathrm{A}}(\mathrm{M},\mathrm{P})$ défini par $\varphi \mapsto \varphi \circ f$, on définit un foncteur contravariant $\mathrm{Hom}_{\mathrm{A}}(\bullet,\mathrm{P})$.

*Remarque 10.3.2.* — Considérons $f\colon \mathrm{M} \to \mathrm{N}$ et $g\colon \mathrm{N} \to \mathrm{P}$ deux homomorphismes tels que $g \circ f = 0$, de sorte que le diagramme $\mathrm{M} \xrightarrow{f} \mathrm{N} \xrightarrow{g} \mathrm{P}$ est un complexe. Alors, pour tout foncteur covariant $F$, on a $F(g) \circ F(f) = F(g \circ f) = F(0) = 0$ si bien que le diagramme $F(\mathrm{M}) \xrightarrow{F(f)} F(\mathrm{N}) \xrightarrow{F(g)} F(\mathrm{P})$ est encore un complexe.

Une remarque analogue vaut bien entendu pour les foncteurs contravariants.

Définition 10.3.3. — *Un foncteur covariant $F$ est dit* exact à gauche *si pour toute suite exacte*

$$0 \to \mathrm{M} \to \mathrm{N} \to \mathrm{P},$$

*la suite*

$$0 \to F(\mathrm{M}) \to F(\mathrm{N}) \to F(\mathrm{P})$$

*est exacte.*

*On dit qu'il est* exact à droite *si pour toute suite exacte*

$$\mathrm{M} \to \mathrm{N} \to \mathrm{P} \to 0,$$

*la suite*

$$F(\mathrm{M}) \to F(\mathrm{N}) \to F(\mathrm{P}) \to 0$$

*est exacte.*

*On dit enfin qu'il est* exact *s'il est à la fois exact à droite et à gauche.*

Pour un foncteur contravariant, on a une notion analogue : un foncteur contravariant $F$ est dit *exact à droite* si pour toute suite exacte $0 \to \mathrm{M} \to \mathrm{N} \to \mathrm{P}$, la suite $F(\mathrm{P}) \to F(\mathrm{N}) \to F(\mathrm{M}) \to 0$ est exacte. Il est *exact à gauche* si pour toute suite exacte $\mathrm{M} \to \mathrm{N} \to \mathrm{P} \to 0$, la suite $0 \to F(\mathrm{P}) \to F(\mathrm{N}) \to F(\mathrm{M})$ est exacte. Il est enfin *exact* s'il est à la fois exact à droite et exact à gauche.

Proposition 10.3.4. — *Soit* A *un anneau et soit* L *un* A*-module.*

*a) Le foncteur* $\mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \bullet)$ *est exact à gauche. Il est exact si et seulement si* L *est un* A*-module projectif.*

*b) Le foncteur* $\mathrm{Hom}_{\mathrm{A}}(\bullet, \mathrm{P})$ *est exact à gauche. Il est exact si et seulement si* L *est un* A*-module injectif.*

*Démonstration.* — a) Considérons une suite exacte

$$0 \to \mathrm{M} \xrightarrow{f} \mathrm{N} \xrightarrow{g} \mathrm{P}$$

et soit

$$0 \to \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{M}) \xrightarrow{f\circ} \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{N}) \xrightarrow{g\circ} \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{P})$$

le complexe obtenu en lui appliquant le foncteur $\mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \bullet)$. Nous devons montrer que cette suite est exacte.

*Exactitude en* $\mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{M})$. Si $\varphi \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{M})$ vérifie $f \circ \varphi = 0$, cela signifie que pour tout $x \in \mathrm{L}$, $f(\varphi(x)) = 0$. Comme $f$ est injectif, $\varphi(x) = 0$ et $\varphi = 0$.

*Exactitude en* $\mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{N})$. On doit montrer que pour tout homomorphisme $\varphi \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{N})$ tel que $g \circ \varphi = 0$, il existe $\psi \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{M})$ tel que $\varphi = f \circ \psi$. Or, si $x \in \mathrm{L}$, $g(\varphi(x)) = 0$. Par suite, $\varphi(x) \in \mathrm{Ker}\, g = \mathrm{Im}\, f$. Ainsi, $\varphi$ est un homomorphisme $\mathrm{L} \to f(\mathrm{M})$. Comme $f\colon \mathrm{M} \to f(\mathrm{M})$ est un isomorphisme, on peut poser $\psi = f^{-1} \circ \varphi$. Alors, $f \circ \psi = \varphi$.

a′) Le foncteur $\mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \bullet)$ est exact à droite si pour toute suite exacte

$$0 \to \mathrm{M} \xrightarrow{f} \mathrm{N} \xrightarrow{g} \mathrm{P} \to 0,$$

la suite

$$0 \to \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{M}) \xrightarrow{f\circ} \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{N}) \xrightarrow{g\circ} \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{P}) \to 0$$

est exacte. Seule l'exactitude en $\mathrm{Hom}_A(L,P)$ n'a pas été vérifiée. Cela revient à dire que pour tout homomorphisme $\varphi\colon L \to P$, il existe un homomorphisme $\psi\colon L \to N$ tel que $\varphi = g \circ \psi$. D'après le théorème 10.2.5, cette condition signifie exactement que L est un A-module projectif.

b) Considérons une suite exacte

$$M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

et soit

$$0 \to \mathrm{Hom}_A(P,L) \xrightarrow{\circ g} \mathrm{Hom}_A(N,L) \xrightarrow{\circ f} \mathrm{Hom}_A(M,L)$$

le complexe obtenu en luis appliquant le foncteur contravariant $\mathrm{Hom}_A(\bullet, L)$. Nous devons montrer que cette suite est exacte.

*Exactitude en* $\mathrm{Hom}_A(P,L)$. Soit $\varphi \in \mathrm{Hom}_A(P,L)$ tel que $\varphi \circ g = 0$. Cela implique que le noyau de $\varphi$ contient $g(N) = P$, donc $\varphi = 0$.

*Exactitude en* $\mathrm{Hom}_A(N,L)$. Soit $\varphi \in \mathrm{Hom}_A(N,L)$ tel que $\varphi \circ f = 0$. On cherche $\psi \in \mathrm{Hom}_A(P,L)$ tel que $\varphi = \psi \circ g$. Or, dire que $\varphi \circ f = 0$ signifie exactement que $\mathrm{Ker}\,\varphi$ contient $\mathrm{Im}\, f$. Par passage au quotient, on en déduit un unique homomorphisme $\psi_0\colon N/\mathrm{Im}\, f \to L$ tel que $\varphi(x) = \psi_0(\mathrm{cl}(x))$ pour tout $x \in N$. Par définition d'une suite exacte, $g$ définit un isomorphisme $N/\mathrm{Im}\, f \to P$, on peut ainsi définir $\psi$ comme la composition

$$\psi_0 \circ g^{-1}\colon P \xrightarrow{\sim} N/\mathrm{Im}\, f \xrightarrow{\psi_0} L.$$

b′) Il faut démontrer que L est un A-module injectif si et seulement si le foncteur $\mathrm{Hom}_A(L,\bullet)$ envoie une suite exacte sur une suite exacte. Seule reste à vérifier l'exactitude au dernier cran, c'est-à-dire que si $f\colon M \to N$ est injectif, l'homomorphisme $\circ f\colon \mathrm{Hom}_A(N,L) \to \mathrm{Hom}_A(M,L)$ est surjectif. Il faut ainsi démontrer que pour tout homomorphisme $\varphi\colon M \to L$, il existe un homomorphisme $\psi\colon N \to L$ tel que $\psi \circ f = \varphi$. D'après le théorème 10.2.8, cette condition est vérifiée si et seulement si L est injectif. □

*10.3.5. Foncteur de localisation.* — Soit A un anneau et soit S une partie multiplicative de A. Si M est un A-module, on sait depuis le chapitre 6 lui associer un $S^{-1}A$-module $S^{-1}M$. De plus, si $f\colon M \to N$ est un homomorphisme de A-modules, on dispose, *cf.* la proposition 6.5.5 d'un (unique) homomorphisme $S^{-1}f\colon S^{-1}M \to S^{-1}N$ tel que $(S^{-1}f)(m/s) = f(m)/s$ pour tout $m \in M$ et tout $s \in S$. De plus, $S^{-1}(f \circ g) = S^{-1}f \circ S^{-1}g$. Ainsi, la localisation est un foncteur de la catégorie de A-modules dans celle des $S^{-1}A$-modules. On le considère ici seulement comme un foncteur sur la catégorie des A-modules.

Proposition 10.3.6 (Exactitude de la localisation). — *Soit* A *un anneau et soit* S *une partie multiplicative de* A. *Le foncteur de localisation par rapport à* S *est un foncteur*

*exact : si* $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ *est une suite exacte de* A*-modules, la suite* $0 \to S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P \to 0$ *est encore exacte.*

*Démonstration.* — Identifions M à un sous-module de N via $f$ et P au quotient N/M via $g$. D'après la proposition 6.5.8, l'homomorphisme $S^{-1}f$ est injectif et le quotient $S^{-1}N/S^{-1}M$ s'identifie à $S^{-1}(N/M) = S^{-1}P$ par l'application de $S^{-1}N$ dans $S^{-1}P$ donnée par

$$\mathrm{cl}(n/s) \mapsto \mathrm{cl}(n)/s = \mathrm{cl}(g(n))/s = (S^{-1}g)(n/s).$$

□

## 10.4. Modules différentiels. Homologie et cohomologie

Définition 10.4.1. — *Soit* A *un anneau. Un* A*-module différentiel est un couple* $(M, d)$ *formé d'un* A*-module* M *et d'un endomorphisme appelé* différentielle $d\colon M \to M$ *tel que* $d^2 = 0$.

*Un morphisme de modules différentiels* $f\colon (M, d_M) \to (N, d_N)$ *est un homomorphisme* $f\colon M \to N$ *tel que* $d_N \circ f = f \circ d_M$.

Définition 10.4.2. — *Si* $(M, d)$ *est un* A*-module différentiel, on définit trois* A*-modules :*

- *le module des cycles :* $Z(M) = \operatorname{Ker} d$ *;*
- *le module des bords :* $B(M) = \operatorname{Im} d$ *;*
- *le module d'homologie de* M *:* $H(M) = Z(M)/B(M) = \operatorname{Ker}(d)/\operatorname{Im}(d)$.

Lemme 10.4.3. — *Un homomorphisme de modules différentiels* $f\colon (M, d_M) \to (N, d_N)$ *induit des homomorphismes* $Z(M) \to Z(N)$, $B(M) \to B(N)$ *d'où un homomorphisme* $H(f)\colon H(M) \to H(N)$.

*Démonstration.* — Comme $f \circ d_M = d_N \circ f$, si $d_M(x) = 0$, alors $d_N(f(x)) = f(d_M(x)) = 0$, donc l'image de $\operatorname{Ker} d_M$ par $f$ est contenue dans $\operatorname{Ker} d_N$ : $f(Z(M)) \subset Z(N)$.

De même, $f(B(M)) \subset B(N)$ puisque $f(d_M(x)) = d_N(f(x))$ pour tout $x \in M$.

Il en résulte par passage au quotient un homomorphisme canonique $H(f)\colon H(M) = Z(M)/B(M) \to Z(N)/B(N) = H(N)$. □

Définition 10.4.4. — *Un* A*-module différentiel gradué est un module différentiel* $(M, d)$ *tel que*

- M *est la somme directe d'une famille* $(M_n)_{n\in\mathbf{Z}}$ *(*M *est* gradué*);*
- *il existe un entier* $r$ *tel que l'endomorphisme* $d$ *est de* degré $r$ *: pour tout* $n \in \mathbf{Z}$*, on a* $d(M_n) \subset M_{n+r}$.

*Dans ce cas, on note* $Z_n(M) = Z(M) \cap M_n$, $B_n(M) = B(M) \cap M_n$ *et* $H_n(M) = Z_n(M)/B_n(M)$.

LEMME 10.4.5. — *Soit* $(M, d)$ *un* A*-module différentiel gradué. On a alors les égalités*

$$Z(M) = \bigoplus_n Z_n(M), \quad B(M) = \bigoplus_n B_n(M) \quad \textit{et} \quad H(M) = \bigoplus_{n\in\mathbf{Z}} H_n(M).$$

*Autrement dit, cycles, bords et homologie de* M *sont automatiquement gradués.*

*Démonstration.* — Comme $Z_n(M)$ est un sous-module de $M_n$ et comme les $M_n$ sont en somme directe, les modules $Z_n(M)$ sont aussi en somme directe. D'autre part, si $x \in Z(M)$, on peut écrire $x = \sum x_n$ où pour tout $n$, $x_n \in M_n$. Alors, $0 = \partial(x) = \sum \partial(x_n)$. Si $r$ est le degré de l'homomorphisme $\partial$, on a donc que pour tout $x$, $\partial(x_n)$ appartient à $M_{n+r}$. Comme les $M_n$ sont en somme directe, $\partial(x_n) = 0$ pour tout $n$ et $x \in \sum Z_n(M)$.

De même, les $B_n(M)$ sont en somme directe. Si $x \in B(M)$, écrivons $x = \partial(y)$ avec $y \in M$. On peut écrire $y = \sum_n y_n$ avec $y_n \in M_n$ pour tout $n$. Alors, $x = \partial(y) = \sum_n \partial(y_n)$. Pour tout $n$, $\partial(y_n) \in M_{n+r} \cap \operatorname{Im}\partial = B_{n+r}(M)$. si bien que $x$ appartient à $\sum_n B_n(M)$. Comme chacun des $Z_n(M)$ est contenu dans $M_n$, la somme est nécessairement directe.

Enfin, on a

$$\begin{aligned} H(M) = Z(M)/B(M) &= \left(\bigoplus_n Z_n(M)\right) / \left(\bigoplus_n B_n(M)\right) \\ &= \bigoplus_n (Z_n(M)/B_n(M)) = \bigoplus_n H_n(M). \end{aligned}$$

□

*Remarque 10.4.6.* — Considérons un complexe de A-modules

$$\ldots \xrightarrow{d_{n-1}} M_{n-1} \xrightarrow{d_n} M_n \xrightarrow{d_{n+1}} M_{n+1} \to \ldots$$

Définissons alors $M = \bigoplus M_n$ et soit $d \in \operatorname{End}(M)$ l'endomorphisme défini par les $d_n$ : si $x \in M_{n-1}$, $d(x) = d_n(x)$.

Alors, $(M, d)$ est un A-module différentiel gradué dont la différentielle est de degré 1. De plus, $H_n(M) = \operatorname{Ker} d_{n+1}/\operatorname{Im} d_n$. La tradition veut qu'on note plutôt $H^n(M)$ et qu'on appelle ces modules *modules de cohomologie* du complexe.

*10.4.7. Complexe de de Rham d'un ouvert de* $\mathbf{R}^2$. — Soit U un ouvert de $\mathbf{R}^2$. Si $0 \leq p \leq 2$, soit $\Omega^p(U)$ le $\mathbf{R}$-espace vectoriel des formes différentielles de degré $p$ sur U. Pour $p = 0$, $\Omega^0(U)$ est l'espace vectoriel des fonctions $\mathscr{C}^\infty$ sur U. Pour $p = 1$, une forme différentielle $\omega$ de degré 1 s'écrit

$$\omega = A(x, y)\, dx + B(x, y)\, dy$$

où A et B sont des fonctions $\mathscr{C}^\infty$. Enfin, une forme différentielle $\alpha$ de degré 2 s'écrit

$$\alpha = \mathrm{A}(x,y)\,\mathrm{d}x \wedge \mathrm{d}y.$$

On a un homomorphisme « différentielle extérieure » défini ainsi :

$$d\colon \Omega^0(\mathrm{U}) \to \Omega^1(\mathrm{U}) \qquad f \mapsto \frac{\partial f}{\partial x}\,\mathrm{d}x + \frac{\partial f}{\partial y}\,\mathrm{d}y$$

$$d\colon \Omega^1(\mathrm{U}) \to \Omega^2(\mathrm{U}) \qquad \mathrm{A}(x,y)\,\mathrm{d}x + \mathrm{B}(x,y)\,\mathrm{d}y \mapsto \left(\frac{\partial \mathrm{B}(x,y)}{\partial x} - \frac{\partial \mathrm{A}(x,y)}{\partial y}\right)\mathrm{d}x \wedge \mathrm{d}y$$

et $d$ est nul sur $\Omega^2(\mathrm{U})$.

On constate que $d \circ d = 0$. Le seul calcul nécessaire est celui de $d^2(f)$ pour $f \in \Omega^0(\mathrm{U})$ et

$$d^2(f) = d\left(\frac{\partial f}{\partial x}\,\mathrm{d}x + \frac{\partial f}{\partial y}\,\mathrm{d}y\right) = \left(\frac{\partial^2 f}{\partial x \partial y} - \frac{\partial^2 f}{\partial y \partial x}\right)\mathrm{d}x \wedge \mathrm{d}y$$

et le théorème de Schwarz implique que $d^2(f) = 0$.

On a ainsi défini un complexe, appelé *complexe de de Rham de* U :

$$0 \to \Omega^0(\mathrm{U}) \xrightarrow{d} \Omega^1(\mathrm{U}) \xrightarrow{d} \Omega^2(\mathrm{U}) \to 0.$$

On peut alors calculer ses groupes de cohomologie, notés $\mathrm{H}^i_{\mathrm{DR}}(\mathrm{U})$ Un théorème fondamental de de Rham affirme que ce sont des espaces vectoriels de même dimension que les espaces de cohomologie fournis par la théorie singulière.

Calculons $\mathrm{H}^0(\Omega^\bullet)$. Si $f \in \mathrm{Z}^0(\Omega^\bullet)$, $f$ est une fonction $\mathscr{C}^\infty$ sur U telle que $df = 0$, c'est-à-dire $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0$. Ainsi, $f$ est constante sur chaque composante connexe de U Comme $\mathrm{B}^0 = 0$, on a $\mathrm{H}^0_{\mathrm{DR}}(\mathrm{U}) = \mathbf{R}^{\pi_0(\mathrm{U})}$, $\pi_0(\mathrm{U})$ désignant le nombre de composantes connexes de U.

Si U est simplement connexe (par exemple, U contractible, ou U étoilé, ou simplement $\mathrm{U} = \mathbf{R}^2$), le lemme de Poincaré affirme qu'une forme différentielle $\omega$ sur U telle que $d\omega = 0$ (on dit que $\omega$ est fermée) est exacte : il existe $f$ telle que $\omega = df$. (Vous avez peut-être rencontré la formulation plus commune en physique ou en calcul différentiel élémentaire : *un champ de vecteurs dont le rotationnel est nul est un gradient.*)

On peut le démontrer très simplement dans le cas où U est étoilé, disons par rapport à l'origine $0 \in \mathbf{R}^2$. Si $\omega = \mathrm{A}(x,y)\,\mathrm{d}x + \mathrm{B}(x,y)\,\mathrm{d}y = 0$ vérifie $d\omega = 0$, posons

$$f(x,y) = \int_0^1 \left(x\mathrm{A}(tx,ty) + y\mathrm{B}(tx,ty)\right)\,\mathrm{d}t.$$

Alors — voir un cours d'intégration — $f$ est de classe $\mathscr{C}^\infty$ sur U et on obtient $\partial f/\partial x$ et $\partial f/\partial y$ en dérivant sous le signe somme. On obtient :

$$\frac{\partial f}{\partial x}(x,y) = \int_0^1 \left( \mathrm{A}(tx,ty) + tx\frac{\partial \mathrm{A}}{\partial x}(tx,ty) + ty\frac{\partial \mathrm{B}}{\partial x}(tx,ty) \right) \mathrm{d}t.$$

Comme $d\omega = 0$, $\frac{\partial \mathrm{B}}{\partial x} = \frac{\partial \mathrm{A}}{\partial y}$ si bien que

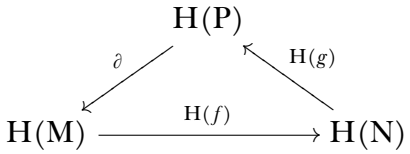
$$\begin{aligned}\frac{\partial f}{\partial x}(x,y) &= \int_0^1 \left( \mathrm{A}(tx,ty) + tx\frac{\partial \mathrm{A}}{\partial y}(tx,ty) + ty\frac{\partial \mathrm{B}}{\partial x}(tx,ty) \right) \mathrm{d}t. \\ &= \int_0^1 \left( \mathrm{A}(tx,ty) + t\frac{d}{dt}(\mathrm{A}(tx,ty)) \right) \mathrm{d}t. \\ &= \int_0^1 \frac{d}{dt}(t\mathrm{A}(tx,ty)) = [t\mathrm{A}(tx,ty)]_0^1 \\ &= \mathrm{A}(x,y).\end{aligned}$$

De même, on démontre que $\frac{\partial f}{\partial y}(x,y) = \mathrm{B}(x,y)$ si bien que $df = \omega$.

THÉORÈME 10.4.8. — *Soit* A *un anneau et soit* $0 \to \mathrm{M} \xrightarrow{f} \mathrm{N} \xrightarrow{g} \mathrm{P} \to 0$ *une suite exacte de modules différentiels. Cela signifie que cette suite est une suite exacte de* A*-modules ainsi que les deux égalités*

$$d_\mathrm{N} \circ f = f \circ d_\mathrm{M} \quad \textit{et} \quad d_\mathrm{P} \circ g = g \circ d_\mathrm{N}.$$

*Il existe alors un homomorphisme* $\partial\colon \mathrm{H}(\mathrm{P}) \to \mathrm{H}(\mathrm{M})$ *tel que l'on ait un « triangle exact » :*




*Ceci signifie les trois égalité :*

$$\operatorname{Ker}\partial = \operatorname{Im}\mathrm{H}(g), \quad \operatorname{Ker}\mathrm{H}(g) = \operatorname{Im}\mathrm{H}(f), \quad \operatorname{Ker}\mathrm{H}(f) = \operatorname{Im}\partial.$$

*Démonstration.* — a) Montrons que $\operatorname{Ker}\mathrm{H}(g) = \operatorname{Im}\mathrm{H}(f)$. Comme $g \circ f = 0$, on a $\mathrm{H}(g) \circ \mathrm{H}(f) = \mathrm{H}(g \circ f) = 0$ et $\operatorname{Im}\mathrm{H}(f) \subset \operatorname{Ker}\mathrm{H}(g)$. Réciproquement, soit $\xi \in \operatorname{Ker}\mathrm{H}(g)$. On peut écrire $\xi = \mathrm{cl}(x)$ avec $x \in \operatorname{Ker} d_\mathrm{N}$. Alors, $\mathrm{H}(g)(\xi) = \mathrm{cl}(g(x))$, si bien qu'il existe $y \in \mathrm{P}$ tel que $g(x) = d_\mathrm{P}(y)$. Puisque l'homomorphisme $g\colon \mathrm{N} \to \mathrm{P}$ est surjectif, il existe $z \in \mathrm{N}$ tel que $y = g(z)$. Alors, $g(x) = d_\mathrm{P}(y) = d_\mathrm{P}(g(z)) = g(d_\mathrm{N}(z))$ si bien que $x - d_\mathrm{N}(z)$ appartient à $\operatorname{Ker} g = \operatorname{Im} f$. Soit $t \in \mathrm{M}$ tel que $x - d_\mathrm{N}(z) = f(t)$. On a alors $\xi = \mathrm{cl}(x) = \mathrm{cl}(d_\mathrm{N}(z) + f(t)) = \mathrm{cl}(f(t)) = \mathrm{H}(f)(\mathrm{cl}(t))$. Par suite, $\operatorname{Ker}\mathrm{H}(g) \subset \operatorname{Im}\mathrm{H}(f)$, d'où l'égalité.

b) Consruisons ensuite l'homomorphisme $\partial$. Soit $\xi \in \mathrm{H}(\mathrm{P})$. Écrivons $\xi = \mathrm{cl}(x)$ avec $x \in \operatorname{Ker} d_\mathrm{P}$. Comme $g$ est surjectif, il existe $y \in \mathrm{M}$ tel que $x = g(y)$. Alors, $0 = d_\mathrm{P}(x) = d_\mathrm{P}(g(y)) = g(d_\mathrm{N}(y))$ si bien qu'il existe $z \in \mathrm{M}$ tel que $d_\mathrm{N}(y) = f(z)$.

On a $f(d_{\mathrm{M}}z) = d_{\mathrm{N}}(f(z)) = d_{\mathrm{N}}d_{\mathrm{N}}(y) = 0$ puisque $d_{\mathrm{N}}^2$. Comme $f$ est injectif, $d_{\mathrm{M}}z = 0$. Posons ainsi $\partial(\xi) = \mathrm{cl}(z) \in \mathrm{H}(\mathrm{M})$.

Il faut vérifier que cette application est bien définie. Or, $z \in \mathrm{M}$ a été choisi de sorte que soient vérifiées les relations $f(z) = d_{\mathrm{N}}(y)$, $x = g(y)$ et $\xi = \mathrm{cl}(x)$. Si on a fait d'autres choix : $\xi = \mathrm{cl}(x')$, $x' = g(y')$ et $f(z') = d_{\mathrm{N}}(y')$, alors :

– il existe $x'' \in \mathrm{P}$ tel que $x = x' + d_{\mathrm{P}}x''$. Choisissons aussi $y'' \in \mathrm{N}$ tel que $x'' = g(y'')$ ;

– $g(y'-y) = x'-x = d_{\mathrm{P}}(x'') = d_{\mathrm{P}}(g(y'')) = g(d_{\mathrm{N}}(y''))$, si bien qu'il existe $z'' \in \mathrm{M}$ tel que $y'-y = d_{\mathrm{N}}(y'') + f(z'')$ ;

– alors, $f(z'-z) = d_{\mathrm{N}}(y') - d_{\mathrm{N}}(y) = d_{\mathrm{N}}(d_{\mathrm{N}}(y'')+f(z'')) = d_{\mathrm{N}}(f(z'')) = f(d_{\mathrm{M}}(z''))$. Comme $f$ est injectif, $z'-z = d_{\mathrm{M}}(z'')$ et $\mathrm{cl}(z') = \mathrm{cl}(z)$ dans $\mathrm{H}(\mathrm{M})$.

Enfin, $\partial$ est un homomorphisme : si on a fait les choix $(x_1, y_1, z_1)$ pour $\xi_1$ et $(x_2, y_2, z_2)$ pour $\xi_2$, on peut faire les choix $(a_1x_1+a_2x_2, a_1y_1+a_2y_2, a_1z_1+a_2z_2)$ pour $a_1\xi_1 + a_2\xi_2$, si bien que $\partial(a_1\xi_1 + a_2\xi_2) = a_1\partial(\xi_1) + a_2\partial(\xi_2)$.

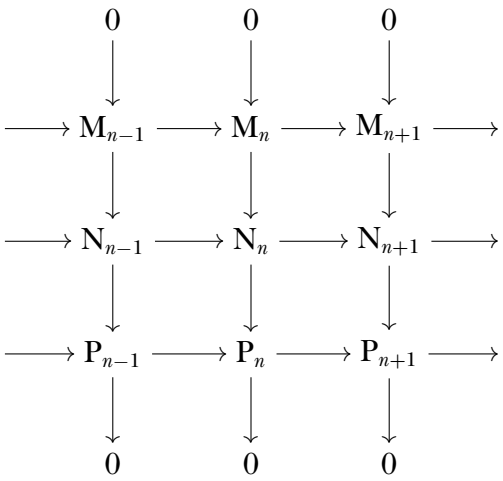
c) Montrons que $\mathrm{Ker}\,\mathrm{H}(f) = \mathrm{Im}\,\partial$. Si $\xi = \mathrm{cl}(x)$ vérifie $\mathrm{H}(f)(\xi) = 0$, on a $f(x) \in \mathrm{Im}\,d_{\mathrm{N}}$. Par suite, soit $y \in \mathrm{N}$ tel que $f(x) = d_{\mathrm{N}}(y)$. Il en résulte par définition de l'homomorphisme $\partial$ que $\partial(\mathrm{cl}(g(y))) = \mathrm{cl}(x) = \xi$, soit $\mathrm{Ker}\,\mathrm{H}(f) \subset \mathrm{Im}\,\partial$.

Réciproquement, si $\mathrm{cl}(z) = \partial(\mathrm{cl}(x))$, on a $\mathrm{H}(f)(\mathrm{cl}(z)) = \mathrm{cl}(f(z))$ donc est égal avec les notations du b) à $\mathrm{cl}(d_{\mathrm{N}}(y)) = 0$.

d) Montrons que $\mathrm{Im}\,\mathrm{H}(g) = \mathrm{Ker}\,\partial$. Si $\partial(\xi) = 0$, soit $(x, y, z)$ un système de choix comme au b) de sorte que $\partial(\xi) = \mathrm{cl}(z)$. On a donc $z \in \mathrm{Im}\,d_{\mathrm{M}}$. Soit $z' \in \mathrm{M}$ tel que $z = d_{\mathrm{M}}(z')$. Alors, $f(z) = f(d_{\mathrm{M}}(z')) = d_{\mathrm{N}}(f(z')) = d_{\mathrm{N}}^2(y) = 0$ donc, $f$ étant injectif, $z = 0$. Par suite, $d_{\mathrm{N}}(y) = f(z) = 0$. La classe de $y$ dans $\mathrm{H}(\mathrm{N})$ vérifie ainsi $\mathrm{H}(g)(\mathrm{cl}(y)) = \mathrm{cl}(g(y)) = \mathrm{cl}(x) = \xi$, ce qui prouve que $\xi \in \mathrm{Im}\,\mathrm{H}(g)$.

Réciproquement, soit $\xi = \mathrm{cl}(g(y))$ un élément de $\mathrm{Im}\,\mathrm{H}(g)$ avec $y \in \mathrm{Ker}\,d_{\mathrm{N}}$. Par définition, $\partial(\xi) = \mathrm{cl}(z)$ où $z$ est l'unique élément de M tel que $f(z) = d_{\mathrm{N}}(y) = 0$, donc $z = 0$ et $\partial(\xi) = 0$. □

COROLLAIRE 10.4.9. — *Considérons une suite exacte de complexes, c'est-à-dire un diagramme commutatif*



*dans lequel les colonnes sont des suites exactes. Alors, il existe pour tout $n$ un homomorphisme $\partial^n : \mathrm{H}^n(\mathrm{P}) \to \mathrm{H}^{n+1}(\mathrm{M})$ tel que l'on ait une suite exacte*

$$\cdots \to \mathrm{H}^n(\mathrm{M}) \to \mathrm{H}^n(\mathrm{N}) \to \mathrm{H}^n(\mathrm{P}) \xrightarrow{\partial^n} \mathrm{H}^{n+1}(\mathrm{M}) \to \dots$$

La démonstration est laissée en exercice. Il faut essentiellement juste vérifier qu'avec les notations du théorème, l'homomorphisme $\partial$ est de degré 1, c'est-à-dire que pour tout $n$, $\partial(\mathrm{H}^n(\mathrm{P})) \subset \mathrm{H}^{n+1}(\mathrm{M})$.

## 10.5. Exercices

*Exercice 10.5.1.* — **a)** Soit $\mathrm{M}_0 \xrightarrow{f_0} \mathrm{M}_1 \xrightarrow{f_1} \dots \xrightarrow{f_{n-1}} \mathrm{M}_n$ un complexe. Montrer que ce complexe est une suite exacte si et seulement si pour tout $i$ les suites $(0) \to \operatorname{Ker} f_i \to \mathrm{M}_i \xrightarrow{f_i} \operatorname{Ker} f_{i+1} \to (0)$ sont exactes.

**b)** On suppose que A est un corps $k$ et que les $\mathrm{M}_i$ sont des $k$-espaces vectoriels de dimension finie. Soit $0 \to \mathrm{M}_1 \xrightarrow{f_1} \mathrm{M}_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} \mathrm{M}_n \to 0$ une suite exacte. Montrer que $\sum_{i=1}^{n} (-1)^i \dim \mathrm{M}_i = 0$.

*Exercice 10.5.2.* — Soit A un anneau, soit M un A-module et soit $(a, b)$ deux éléments de A.

**a)** Montrer que les applications $d_1 : \mathrm{M} \to \mathrm{M} \times \mathrm{M}$ et $d_2 : \mathrm{M} \times \mathrm{M} \to \mathrm{M}$ définies par

$$d_1(x) = (ax, bx) \quad \text{et} \quad d_2(x, y) = by - ax$$

définissent un complexe $\mathrm{M}^\bullet$ :

$$0 \to \mathrm{M} \xrightarrow{d_1} \mathrm{M} \times \mathrm{M} \xrightarrow{d_2} \to 0.$$

**b)** Montrer que $\mathrm{H}^0(\mathrm{M}^\bullet) = \{x \in \mathrm{M}\,;\, ax = by = 0\}$ et que $\mathrm{H}^2(\mathrm{M}^\bullet) = \mathrm{M}/(a\mathrm{M} + b\mathrm{M})$.

**c)** On suppose que la multiplication par $a$ dans M est injective. Montrer alors que la multiplication par $b$ dans $\mathrm{M}/a\mathrm{M}$ est injective si et seulement si $\mathrm{H}^1(\mathrm{M}^\bullet) = 0$.

*Exercice 10.5.3.* — Soit A un anneau et I un idéal de A

**a)** On suppose que l'homomorphisme canonique $\mathrm{cl}\colon \mathrm{A} \to \mathrm{A/I}$ n'admet un inverse à droite $f$. Montrer qu'il existe $a \in \mathrm{I}$ tel que $a = a^2$ et $\mathrm{I} = (a)$.

**b)** Si A est intègre montrer que A/I est un A-module projectif si et seulement si $\mathrm{I} = 0$ ou $\mathrm{I} = \mathrm{A}$.

*Exercice 10.5.4.* — Soit A un anneau et soit $0 \to \mathrm{M} \xrightarrow{f} \mathrm{N} \xrightarrow{g} \mathrm{P} \to 0$ une suite exacte scindée. Montrer que pour tout A-module X, cette suite induit des suites exactes scindées

$$0 \to \mathrm{Hom}(\mathrm{X}, \mathrm{M}) \xrightarrow{f\circ} \mathrm{Hom}(\mathrm{X}, \mathrm{N}) \xrightarrow{g\circ} \mathrm{Hom}(\mathrm{X}, \mathrm{P}) \to 0$$

et

$$0 \to \mathrm{Hom}(\mathrm{P}, \mathrm{X}) \xrightarrow{\circ g} \mathrm{Hom}(\mathrm{N}, \mathrm{X}) \xrightarrow{\circ f} \mathrm{Hom}(\mathrm{M}, \mathrm{X}) \to 0.$$

*Exercice 10.5.5.* — Soit A un anneau local noethérien. Notons $\mathfrak{m}$ son idéal maximal et $k$ le corps résiduel $\mathrm{A}/\mathfrak{m}$. Soit P un A-module projectif de type fini.

**a)** Montrer que $\mathrm{P}/\mathfrak{m}\mathrm{P}$ est un $k$-espace vectoriel de dimension finie.

Notons $d$ cette dimension. et considérons des éléments $e_1, \ldots, e_d \in \mathrm{P}$ tels que $(\mathrm{cl}(e_1), \ldots, \mathrm{cl}(e_d))$ soit une base de $\mathrm{P}/\mathfrak{m}\mathrm{P}$.

**b)** Montrer à l'aide du théorème de Nakayama que $(e_1, \ldots, e_d)$ engendrent P en tant que A-module. En déduire l'existence d'une suite exacte

$$0 \to \mathrm{M} \to \mathrm{A}^n \to \mathrm{P} \to 0.$$

**c)** En utilisant l'hypothèse que P est projectif, montrer que $\mathrm{A}^n \simeq \mathrm{P} \oplus \mathrm{M}$. En déduire que $\dim_k(\mathrm{M}/\mathfrak{m}\mathrm{M}) = 0$.

**d)** En appliquant de nouveau le théorème de Nakayama, montrer que $\mathrm{M} = 0$ et donc que P est un A-module libre.

*Exercice 10.5.6.* — Soit A un anneau et soit S une partie multiplicative de A.

**a)** Montrer que si on a un diagramme commutatif de A-modules

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{E} & \xrightarrow{f} & \mathrm{F} & \xrightarrow{g} & \mathrm{G} \\
 & & \downarrow{\scriptstyle \alpha_\mathrm{A}} & & \downarrow{\scriptstyle \alpha_\mathrm{F}} & & \downarrow{\scriptstyle \alpha_\mathrm{G}} \\
0 & \longrightarrow & \mathrm{E}' & \xrightarrow{f'} & \mathrm{F}' & \xrightarrow{g'} & \mathrm{G}'
\end{array}$$

dont les lignes sont exactes, avec $\alpha_\mathrm{F}$ et $\alpha_\mathrm{G}$ des isomorphismes, alors $\alpha_\mathrm{E}$ est un isomorphisme.

**b)** Soient M et N des A-modules. Définir un morphisme naturel de A-modules

$$\alpha_{M,N} : S^{-1}\mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$$

qui soit l'identité pour $M = A$.

**c)** Démontrer que si M est un A-module libre de type fini, $\alpha_{M,N}$ est un isomorphisme.

**d)** Montrer, à l'aide des questions précédentes, que si A est noethérien et M est un A-module de type fini, alors $\alpha_{M,N}$ est toujours un isomorphisme.

**e)** Donner un exemple pour lequel $\alpha_{M,N}$ n'est pas un isomorphisme.

## 10.6. Solutions

*Solution de l'exercice 10.5.1.* — **a)** Comme $\mathrm{Im}(f_i) \subset \mathrm{Ker}\, f_{i+1}$, on a une application $f_i : M_i \to \mathrm{Ker}(f_{i+1})$ bien définie, et un complexe $(0) \to \mathrm{Ker}\, f_i \to M_i \xrightarrow{f_i} \mathrm{Ker}\, f_{i+1} \to (0)$. Dire que ces suites sont exactes revient à dire que l'image de $f_i$ dans $\mathrm{Ker}\, f_{i+1}$ est égale à $\mathrm{Ker}\, f_{i+1}$, soit $\mathrm{Im}\, f_i = \mathrm{Ker}\, f_{i+1}$. Cela équivaut à l'exactitude du complexe.

**b)** Si $A = k$ est un corps, et si $(0) \to \mathrm{Ker}\, f_i \to M_i \xrightarrow{f_i} \mathrm{Ker}\, f_{i+1} \to (0)$ est exacte, on peut trouver un supplémentaire de $\mathrm{Ker}\, f_i$ dans $M_i$ qui sera isomorphe à $\mathrm{Ker}\, f_{i+1}$. Ainsi, pour tout $i \in \{1,\dots,n\}$, $\dim M_i = \dim \mathrm{Ker}\, f_i + \dim \mathrm{Ker}\, f_{i+1}$. (On a noté $f_{n+1} = 0$.) Par suite, on a

$$\begin{aligned}\sum_{i=1}^{n}(-1)^i \dim M_i &= \sum_{i=1}^{n}(-1)^i \dim \mathrm{Ker}\, f_i + \sum_{i=1}^{n}(-1)^i \dim \mathrm{Ker}\, f_{i+1} \\ &= \dim \mathrm{Ker}\, f_0 + (-1)^n \dim \mathrm{Ker}\, f_{n+1} = 0.\end{aligned}$$

*Solution de l'exercice 10.5.2.* — **a)** Pour tout $x \in M$, $d_2(d_1(x)) = d_2(ax, bx) = bax - abx = 0$ donc $d_2 \circ d_1 = 0$.

**b)** On a $B^0(M^\bullet) = \mathrm{Im}(0 \to M) = 0$. On a $Z^0(M^\bullet) = \mathrm{Ker}\, d_1$ donc est l'ensemble des $x \in M$ tels quye $ax = bx = 0$. Par suite, $H^0(M^\bullet) = \{x \in M\,;\, ax = bx = 0\}$.

On a $Z^2(M^\bullet) = \mathrm{Ker}(M \to 0) = M$ tandis que $B^2(M^\bullet) = \mathrm{Im}\, d_2$. C'est l'ensemble des $ax+by$ avec $x$ et $y \in M$, donc $B^2(M^\bullet) = aM+bM$. Ainsi, $H^2(M^\bullet) = M/(aM+bM)$.

**c)** Supposons que la multiplication par $b$ dans $M/aM$ est injective. Soit $(x,y) \in Z^1(M^\bullet) = \mathrm{Ker}\, d_2$. On a donc $by = ax$. Dans $M/aM$, $b\,\mathrm{cl}(y) = 0$, si bien que $\mathrm{cl}(y) = 0$. Il existe ainsi $y' \in M$ tel que $y = ay'$. Alors, $a(x-by') = 0$ et puisque la multiplication par $a$ dans M est injective, $x = by'$. Ainsi, $(x,y) = (by', ay') = d_1(y')$. On a donc prouvé que $(x,y) \in B^1(M^\bullet)$, d'où $H^1(M^\bullet) = 0$.

Supposons maintenant que $H^1(M^\bullet) = 0$. Soit $x \in M$ tel que $b\,\mathrm{cl}(x) = 0$ dans $M/aM$, c'est-à-dire $bx \in aM$. Il existe alors $y \in M$ tel que $bx = ay$ et $(x,y) \in \mathrm{Ker}\, d_2$. Comme $H^1(M^\bullet) = 0$, $\mathrm{Ker}\, d_2 = Z^1(M^\bullet) = B^1(M^\bullet) = \mathrm{Im}\, d_1$ et il existe $z \in M$ tel que

$(x,y) = d_1(z) = (az, bz)$. Par suite, $x = az \in a\mathrm{M}$ et $\mathrm{cl}(x) = 0$ dans $\mathrm{M}/a\mathrm{M}$. Nous avons donc démontré que la multiplication par $b$ dans $\mathrm{M}/a\mathrm{M}$ est injective.

*Solution de l'exercice 10.5.3.* — **a)** Notons cl l'homomorphisme canonique $\mathrm{A} \to \mathrm{A}/\mathrm{I}$. Soit $f\colon \mathrm{A}/\mathrm{I} \to \mathrm{A}$ un homomorphisme tel que $\mathrm{cl} \circ f = \mathrm{Id}_{\mathrm{A}/\mathrm{I}}$. Notons $b = f(\mathrm{cl}(1))$. Comme $f$ est un inverse à droite de cl, $\mathrm{cl}(b) = \mathrm{cl}(f(\mathrm{cl}(1))) = \mathrm{cl}(1)$ et $b \in 1 + \mathrm{I}$. Notons $a = 1 - b \in \mathrm{I}$. Alors, pour tout $x \in \mathrm{A}$, $f(\mathrm{cl}(x)) = f(x\,\mathrm{cl}(1)) = x(1-a)$. Si $x \in \mathrm{I}$, on a $\mathrm{cl}(x) = 0$ si bien que $x(1-a) = 0$.

Comme $a \in \mathrm{I}$, $a(1-a) = 0$ et $a = a^2$. On a enfin $(a) \subset \mathrm{I}$. Réciproquement, si $x \in \mathrm{I}$, $x(1-a) = 0$, donc $x = ax \in (a)$. Ainsi, $\mathrm{I} = (a)$.

**b)** Si A est intègre, un élément $a \in \mathrm{A}$ tel que $a(1-a) = 0$ vérifie $a = 0$ ou $a = 1$. Ainsi, $\mathrm{I} = 0$ ou $\mathrm{I} = \mathrm{A}$.

*Solution de l'exercice 10.5.5.* — **a)** Le A-module $\mathrm{P}/\mathfrak{m}\mathrm{P}$ est annulé par $\mathfrak{m}$. Il est donc naturellement muni d'une structure de $\mathrm{A}/\mathfrak{m}$-module. Comme $\mathfrak{m}$ est un idéal maximal, $k = \mathrm{A}/\mathfrak{m}$ est un corps et $\mathrm{P}/\mathfrak{m}\mathrm{P}$ est un $k$-espace vectoriel.

Soit $(x_1, \dots, x_r)$ une famille génératrice finie dans P. Alors, les classes $(\mathrm{cl}(x_1), \dots, \mathrm{cl}(x_r))$ engendrent $\mathrm{P}/\mathfrak{m}\mathrm{P}$ comme A-module, donc aussi comme $k$-espace vectoriel. Par suite, $\mathrm{P}/\mathfrak{m}\mathrm{P}$ est un $k$-espace vectoriel de dimension finie.

**b)** Soit L le sous-module de P engendré par les $e_i$. Soit $p \in \mathrm{P}$. Comme les $\mathrm{cl}(e_i)$ forment une base de $\mathrm{P}/\mathfrak{m}\mathrm{P}$, il existe des $x_i \in k$ tels que $\mathrm{cl}(p) = \sum x_i\,\mathrm{cl}(e_i)$. Si $a_i \in \mathrm{A}$ vérifie $\mathrm{cl}(a_i) = x_i$, il en résulte que $p - \sum a_i e_i$ appartient à $\mathfrak{m}\mathrm{P}$. Ainsi, $\mathrm{P} = \mathrm{L} + \mathfrak{m}\mathrm{P}$.

D'après le théorème de Nakayama (corollaire 7.1.8), $\mathrm{P} = \mathrm{L}$.

Les $e_i$ définissent un homomorphisme $\mathrm{A}^d \to \mathrm{P}$. On vient de voir que cet homomorphisme est surjectif. Si M désigne son noyau, on a une suite exacte $0 \to \mathrm{M} \to \mathrm{A}^n \to \mathrm{P} \to 0$.

**c)** Comme P est projectif, cette suite exacte est scindée et $\mathrm{A}^n \simeq \mathrm{M} \oplus \mathrm{P}$. Alors, dans cet isomorphisme, $\mathfrak{m}^n$ s'identifie au sous-module $\mathfrak{m}\mathrm{M} \oplus \mathfrak{m}\mathrm{P}$. Ainsi, on a un isomorphisme de A-modules

$$(\mathrm{A}/\mathfrak{m})^n = \mathrm{A}^n/\mathfrak{m}^n = (\mathrm{M}/\mathfrak{m}\mathrm{M}) \oplus (\mathrm{P}/\mathfrak{m}\mathrm{P}).$$

et comme ces A-modules sont des $k$-espaces vectoriels, c'est un isomorphisme de $k$-espaces vectoriels.

L'égalité des dimensions implique alors

$$n = \dim_k k^n = \dim_k(\mathrm{M}/\mathfrak{m}\mathrm{M}) + \dim_k(\mathrm{P}/\mathfrak{m}\mathrm{P}) = \dim_k(\mathrm{M}/\mathfrak{m}\mathrm{M}) + n$$

donc $\dim_k(\mathrm{M}/\mathfrak{m}\mathrm{M}) = 0$.

**d)** Ainsi, $\mathrm{M}/\mathfrak{m}\mathrm{M}$ est l'espace vectoriel nul, donc $\mathrm{M} = \mathfrak{m}\mathrm{M}$. Comme A est noethérien et M un sous-module de $\mathrm{A}^n$, M est de type fini. Une nouvelle application

du lemme de Nakayama implique ainsi que $M = 0$. Par suite, l'homomorphisme $A^n \to P$ défini par les $e_i$ est injectif. C'est donc un isomorphisme.

*Solution de l'exercice 10.5.6.* — **a)** Si les homomorphismes $g$ et $g'$ étaient surjectifs, il suffirait d'appliquer le lemme du serpent établi dans le cours. On va redémontrer ici ce dont on a besoin.

*Montrons que $\alpha_E$ est injectif.* Soit en effet $x \in E$ tel que $\alpha_E(x) = 0$. On a alors $\alpha_F(f(x)) = f'(\alpha_E(x)) = 0$ et comme $\alpha_F$ est un isomorphisme, $f(x) = 0$. Comme $f$ est injectif, $x = 0$.

*Montrons que $\alpha_E$ est surjectif.* Soit $x' \in E'$. Comme $\alpha_F$ est un isomorphisme, il existe $y \in F$ tel que $\alpha_F(y) = f'(x') \in F'$. Alors, $\alpha_G(g(y)) = g'(\alpha_F(y)) = g'(f'(x')) = 0$. Comme $\alpha_G$ est injectif, $g(y) = 0$. Donc $y \in \operatorname{Ker} g = \operatorname{Im} f$ et il existe $x \in E$ tel que $y = f(x)$. Alors, $f'(x') = \alpha_F(y) = \alpha_F(f(x)) = f'(\alpha_E(x))$. Comme $f'$ est injectif, $x' = \alpha_E(x)$.

**b)** Soit $f\colon M \to N$ un homomorphisme de A-modules. Si l'on compose $f$ avec l'homomorphisme canonique $N \to S^{-1}N$, on en déduit un homomorphisme de A-modules $f_1\colon M \to S^{-1}N$ tel que $f_1(m) = f(m)/1$. Comme $S^{-1}N$ est un $S^{-1}A$-module, la propriété universelle de la localisation fournit un unique homomorphisme $\varphi\colon S^{-1}M \to S^{-1}N$ tel que $\varphi(m/1) = f_1(m) = f(m)/1$. On a ainsi construit un homomorphisme de A-modules

$$\operatorname{Hom}_A(M, N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N).$$

Comme le second membre est un $S^{-1}A$-module, on peut étendre cet homomorphisme de manière unique en un homomorphisme de $S^{-1}A$-modules

$$S^{-1} \operatorname{Hom}_A(M, N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N).$$

En particulier, si $M = A$, $f\colon A \to N$ est de la forme $a \mapsto af(1)$, ce qui identifie $\operatorname{Hom}_A(A, N)$ à N. L'homomorphisme $f_1$ vérifie $f_1(a) = af(1)/1$ et on consate que l'homomorphisme $\varphi'\colon S^{-1}A \to S^{-1}N$ donné par $a/s \mapsto (a/s)f(1)$ est un homomorphisme tel que $\varphi'(m/1) = (a/1)f(1) = af(1)/1$ donc $\varphi$ s'identifie à $f(1)/1$ dans $\operatorname{Hom}_{S^{-1}A}(S^{-1}A, S^{-1}N) = S^{-1}N$. Le morphisme $f \mapsto \varphi$ correspond donc au morphisme $n \mapsto n/1$ et l'unique façon d'étendre ce morphisme en un homomorphisme de $S^{-1}A$-modules est l'homomorphisme identique $S^{-1}N \to S^{-1}N$, donc $\alpha_{A,N}$ s'identifie à l'homomorphisme identique.

**c)** Supposons que M est un A-module libre de type fini. Soit $n$ le rang de M. Alors une base de M fournit des identifications

$$S^{-1} \operatorname{Hom}_A(M, N) \simeq S^{-1} \operatorname{Hom}_A(A^n, N) \simeq S^{-1}N^n$$

et

$$\operatorname{Hom}_A(S^{-1}M, S^{-1}N) \simeq (S^{-1}N)^n$$

par lesquelles $\alpha_{M,N}$ correspond à l'identité sur chaque facteur, donc est un isomorphisme.

**d)** Comme M est de type fini, il existe un A-module libre de type fini $M_1$ et une surjection $g\colon M_1 \to M$. Le noyau de $g$ est un sous-module du module de type fini $M_1$. Comme A est noethérien, $\operatorname{Ker} g$ est de type fini et il existe un A-module libre de type fini $M_2$ ainsi qu'une surjection $f\colon M_2 \to \operatorname{Ker} g$. Autrement dit, on a une suite exacte

$$M_2 \xrightarrow{f} M_1 \xrightarrow{g} M \to 0$$

d'où on déduit, le foncteur $\operatorname{Hom}_A(\bullet, N)$ étant exact à gauche, une suite exacte

$$0 \to \operatorname{Hom}_A(M,N) \xrightarrow{\circ g} \operatorname{Hom}_A(M_1,N) \xrightarrow{\circ f} \operatorname{Hom}_A(M_2,N).$$

Comme le foncteur de localisation en la partie multiplicative S est exact, on a aussi une suite exacte

$$0 \to S^{-1}\operatorname{Hom}_A(M,N) \xrightarrow{\circ g} S^{-1}\operatorname{Hom}_A(M_1,N) \xrightarrow{\circ f} S^{-1}\operatorname{Hom}_A(M_2,N).$$

Partant de nouveau de la suite exacte

$$M_2 \xrightarrow{f} M_1 \xrightarrow{g} M \to 0$$

et utilisant d'abord que la localisation est exacte puis l'exactitude à gauche du foncteur Hom, on en déduit une autre suite exacte

$$0 \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N) \xrightarrow{\circ g} \operatorname{Hom}_{S^{-1}A}(S^{-1}M_1, S^{-1}N) \xrightarrow{\circ f} \operatorname{Hom}_{S^{-1}A}(S^{-1}M_2, S^{-1}N).$$

En faisant intervenir les homomorphismes $\alpha_{M,N}$, $\alpha_{M_1,N}$ et $\alpha_{M_2,N}$, on se retrouve dans la situation de la première question. Il en résulte que $\alpha_{M,N}$ est un isomorphisme.

**e)** Prenons $A = \mathbf{Z}$, $M = \mathbf{Q}/\mathbf{Z}$ et $S = \mathbf{Z} \setminus \{0\}$. Alors, $S^{-1}M = 0$ puisque tout élément de M est de torsion. Par suite, $\operatorname{Hom}_{\mathbf{Z}}(S^{-1}M, S^{-1}N)$ est nul pour tout $\mathbf{Z}$-module N et le module d'arrivée de $\alpha_{M,N}$ aussi.

Prenons par exemple $M = N$. Alors, $\operatorname{Hom}_{\mathbf{Z}}(M,M)$ n'est pas nul : il contient $\mathrm{Id}_M$ De plus, pour tout $a \neq 0$, l'endomorphisme $a\,\mathrm{Id}_M$ de M n'est pas nul : par exemple $a(\mathrm{cl}(1/a)) = \mathrm{cl}(1) \neq 0$ Ainsi, $S^{-1}\operatorname{Hom}_{\mathbf{Z}}(M,M) \neq 0$ et $\alpha_{M,M}$ ne peut pas être un isomorphisme.

# 11 Produit tensoriel

*Dans ce chapitre, nous introduisons le produit tensoriel de modules et nous en donnons un certain nombre de propriétés. Malgré les apparences, il n'est pas si difficile que cela à comprendre. C'est une construction extrêmement importante car elle fournit un objet de nature linéaire (un module) qui permt de comprendre les applications bilinéaires. Ainsi, plutôt que la construction qui le définit, la propriété universelle qui le caractérise s'avère très pratique à manipuler.*

## 11.1. Définition

DÉFINITION 11.1.1. — *Soit* A *un anneau et soit* M, N, P *trois* A*-modules. Une* application bilinéaire *de* $\mathrm{M} \times \mathrm{N}$ *dans* P *est une application* $b\colon \mathrm{M} \times \mathrm{N} \to \mathrm{P}$ *vérifiant les propriétés suivantes :*

– *pour tout* $m \in \mathrm{M}$, *l'application* $b(m, \cdot)\colon \mathrm{N} \to \mathrm{P}$ *telle que* $n \mapsto b(m,n)$ *est un homomorphisme ;*

– *pour tout* $n \in \mathrm{N}$, *l'application* $b(\cdot, n)\colon \mathrm{M} \to \mathrm{P}$ *telle que* $m \mapsto b(m,n)$ *est un homomorphisme.*

Autrement dit, on demande que pour tous $a$, $b \in \mathrm{A}$, $m$, $m' \in \mathrm{M}$, $n$, $n' \in \mathrm{N}$, soient vérifiées les égalités

$$b(am + a'm', n) = ab(m,n) + a'b(m',n) \quad \text{et} \quad b(m, an + a'n') = ab(m,n) + a'b(m,n').$$

*Exercice 11.1.2.* — Soit A un anneau, soit M, M′, N, N′, P, P′ six A-modules. Soit $b\colon \mathrm{M} \times \mathrm{N} \to \mathrm{P}$ une application bilinéaire, et $f\colon \mathrm{M}' \to \mathrm{M}$, $g\colon \mathrm{N}' \to \mathrm{N}$, $h\colon \mathrm{P} \to \mathrm{P}'$ trois homomorphismes de modules. Alors, l'application $b'\colon \mathrm{M}' \times \mathrm{N}' \to \mathrm{P}'$ définie par $b'(m',n') = h(b(f(m'), g(n')))$ est une application bilinéaire.

La construction « produit tensoriel » fournit pour tout couple $(\mathrm{M}, \mathrm{N})$ de A-modules un A-module $\mathrm{M} \otimes_{\mathrm{A}} \mathrm{N}$ et une application bilinéaire $\mathrm{M} \times \mathrm{N} \to \mathrm{M} \otimes_{\mathrm{A}} \mathrm{N}$ telle

que toute application bilinéaire $M \times N \to P$ provienne d'un homomorphisme $M \otimes_A N \to P$.

*11.1.3. Construction.* — Considérons le A-module libre $L = A^{(M\times N)}$ de base $M\times N$. On note $e_{(m,n)}$ les vecteurs de la base. Soit R le sous-A-module de L engendré par les éléments suivants :

$$\begin{aligned} & ae_{(m,n)} - e_{(am,n)}, \\ & ae_{(m,n)} - a_{(m,an)}, \\ & e_{(m+m',n)} - e_{(m,n)} - e_{m',n} \\ \text{et} \quad & a_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}, \end{aligned}$$

lorsque $a \in A$, $m$ et $m'$ parcourent M, $n$ et $n'$ parcourent N. On définit alors le A-module $M \otimes_A N$ comme le quotient :

$$M \otimes_A N = L/R.$$

On note $m \otimes n$ la classe de $e_{(m,n)}$) dans $M \otimes_A N$.

En particulier, on a les relations suivantes dans $M \otimes_A N$ :

– $a(m \otimes n) = (am) \otimes n = m \otimes (an)$ ;

– $(m + m') \otimes n = m \otimes n + m' \otimes n$ ;

– $m \otimes (n + n') = m \otimes n + m \otimes n'$.

Un élément de $M \otimes_A N$ est appelé tenseur Un élément de $M \otimes_A N$ de la forme $m \otimes n$ pour $m \in M$ et $n \in N$ est appelé *tenseur décomposé*.

*Remarque 11.1.4.* — Le produit tensoriel de deux modules est engendré par les tenseurs décomposés.

THÉORÈME 11.1.5. — *Soit* A *un anneau et soit* M, N *deux* A*-modules.*

*L'application* $M \times N \to M \otimes_A N$ *définie par* $(m, n) \mapsto m \otimes n$ *est bilinéaire.*

*De plus, pour tout* A*-module* P *et toute application bilinéaire* $b\colon M \times N \to P$*, il existe un unique homomorphisme* $f\colon M \otimes_A N \to P$ *tel que pour tout* $(m, n) \in M \times N$*, on ait* $f(m \otimes n) = b(m, n)$.

*Démonstration.* — Si $a$, $a' \in A$, $m$, $m' \in M$ et $n \in N$, on a

$$(am + a'm') \otimes n = (am) \otimes n + (a'm') \otimes n = a(m \otimes n) + a'(m' \otimes n)$$

et

$$m \otimes (an + a'n') = m \otimes (an) + m' \otimes (a'n') = a(m \otimes n) + a'(m \otimes n').$$

Cela signifie bien que l'application $(m, n) \mapsto m \otimes n$ est bilinéaire.

Soit maintenant $b\colon M \times N \to P$ une application bilinéaire. S'il existe un homomorphisme $f\colon M \otimes_A N \to P$ tel que $f(m \otimes n) = b(m, n)$, $f$ est déterminé sur les tenseurs décomposés. Comme ceux-ci engendrent $M \otimes_A N$, un tel $f$ est unique. Pour construire $f$, nous allons revenir à la définition du produit tensoriel comme

quotient L/R, L étant le A-module libre de base $M \times N$ et R le sous-module des relations introduit plus haut. La propriété universelle des modules libres implique qu'il existe un unique homomorphisme $\varphi\colon A^{(M\times N)} \to P$ tel que $\varphi(e_{(m,n)} = b(m,n)$. Il faut alors montrer que le noyau de $\varphi$ contient R. On en déduira un unique homomorphisme $f\colon L/R \to P$ tel que $f(m \otimes n) = f(\mathrm{cl}(e_{(m,n)})) = b(m,n)$.

Comme le noyau de $\varphi$ est un sous-module de R, il suffit de vérifier qu'il contient la famille donnée de générateurs de R. Or, on a

$$\begin{aligned}
\varphi(ae_{m,n} - e_{am,n}) &= ab(m,n) - b(am,n) = 0\\
\varphi(ae_{m,n} - e_{m,an}) &= ab(m,n) - b(m,an) = 0\\
\varphi(e_{m+m',n} - e_{m,n} - e_{m',n}) &= b(m+m',n) - b(m,n) - b(m',n) = 0\\
\varphi(e_{m,n+n'} - e_{m,n} - e_{m,n'}) &= b(m,n+n') - b(m,n) - b(m,n') = 0
\end{aligned}$$

en raison de la bilinéarité de $b$. Par suite, $R \subset \mathrm{Ker}\,\varphi$ et il existe un homomorphisme $f$ tel que $f(m \otimes n) = b(m,n)$. □

Proposition 11.1.6 (Fonctorialité du produit tensoriel)

*Soit $f\colon M_1 \to M_2$ et $g\colon N_1 \to N_2$ deux homomorphismes de A-modules. Il existe alors un unique homomorphisme de A-modules*

$$f \otimes g\colon M_1 \otimes_A N_1 \to M_2 \otimes_A N_2$$

*tel que pour tout $m \in M_1$ et tout $n \in N_1$, on ait $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.*

*De plus, si $f'\colon M_2 \to M_3$ et $g'\colon N_2 \to N_3$ sont deux autres homomorphismes, alors $(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$.*

*Démonstration.* — D'après la propriété universelle (théorème 11.1.5), il suffit de montrer que l'application

$$M_1 \times N_1 \to M_2 \otimes_A N_2, \qquad (m,n) \mapsto f(m) \otimes g(n)$$

est bilinéaire. Or, si $m$ et $m'$ sont dans $M_1$, $n$ et $n'$ dans $M_2$, $a$ et $b$ dans A, on a

$$f(am+bm') \otimes g(n) = (af(m) + bf(m')) \otimes g(n) = a(f(m) \otimes g(n)) + b(f(m') \otimes g(n))$$

et

$$m \otimes g(an+bn') = m \otimes (ag(n) + bg(n')) = am \otimes g(n) + bm \otimes g(n')$$

d'où la bilinéarité requise pour l'existence d'un unique homomorphisme $f \otimes g$ tel que $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

Pour établir l'égalité $(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$, il suffit de remarquer que l'on a pour tout $(m,n) \in M_1 \otimes N_1$,

$$\begin{aligned}
(f' \circ f) \otimes (g' \circ g)(m \otimes n) &= (f' \circ f)(m) \otimes (g' \circ g)(n)) = f'(f(m)) \otimes g'(g(n))\\
&= (f' \otimes g')(f(m) \otimes g(n)) = (f' \otimes g')((f \otimes g)(m \otimes n))\\
&= ((f' \otimes g') \circ (f \otimes g))(m \otimes n).
\end{aligned}$$

Comme les tenseurs décomposés engendrent $M \otimes N$, l'égalité vaut pour tout élément de $M \otimes N$. □

## 11.2. Quelques propriétés

On démontre dans ce paragraphe quelques propriétés utiles du produit tensoriel. Leurs démonstrations sont un peu fastidieuses mais néanmoins faciles et les comprendre en détail permet de se familiariser avec cette notion.

PROPOSITION 11.2.1. — *Soit* A *un anneau et soit* M, N *deux* A*-modules. Il existe un unique homomorphisme de* A*-modules* $i\colon M \otimes_A N \to N \otimes_A M$ *tel que* $i(m \otimes n) = n \otimes m$. *C'est un isomorphisme.*

*Démonstration.* — L'application de $M \times N$ dans $N \otimes_A M$ qui à $(m, n)$ associe $n \otimes m$ est bilinéaire. Il existe par suite un unique homomorphisme $i\colon M \otimes_A N \to N \otimes_A M$ tel que pour tout $(m, n) \in M \times N$, $i(m \otimes n) = n \otimes m$.

De même, il existe un unique homomorphisme $j\colon N \otimes_A M \to M \otimes_A N$ tel que $j(n \otimes m) = m \otimes n$ pour tout $(m, n) \in M \times N$.

Alors, si $(m, n) \in M \times N$, $j \circ i(m \otimes n) = j(n \otimes m) = m \otimes n$. Comme les tenseurs décomposés dans $M \otimes N$ engendrent $M \otimes N$, $j \circ i = \mathrm{Id}_{M \otimes N}$. De même, $i \circ j = \mathrm{Id}_{N \otimes M}$. Par suite, $i$ et $j$ sont des isomorphismes. □

PROPOSITION 11.2.2. — *Soit* A *un anneau et soit* M, N, P *trois* A*-modules. Il existe un unique homomorphisme de* A*-modules* $\alpha\colon M \otimes_A (N \otimes_A P) \to (M \otimes_A N) \otimes_A P$ *tel que pour tout* $(m, n, p) \in M \times N \times P$, *on ait* $\alpha(m \otimes (n \otimes p)) = (m \otimes n) \otimes p$.

*De plus, c'est un isomorphisme.*

On pourra donc sans dommage oublier les parenthèses et écrire $M \otimes_A N \otimes_A P$.

*Démonstration.* — Si $m \in M$ est fixé, l'application qui associe au couple $(n, p) \in N \times P$ le tenseur $(m \otimes n) \otimes p$ est bilinéaire. Il existe ainsi un unique homomorphisme $\varphi_m$ de $N \otimes_A P$ dans $(M \otimes_A N) \otimes_A P$ par lequel $n \otimes p$ a pour image $(m \otimes n) \otimes p$. De plus, l'application $m \mapsto \varphi_m$ est linéaire : il faut vérifier que pour tous $m$, $m' \in M$ et tous $a$, $a' \in A$, $\varphi_{am+a'm'} = a\varphi_m + a'\varphi_{m'}$, c'est-à-dire que pour tout $v \in N \otimes_A P$,

$$\varphi_{am+a'm'}(v) = a\varphi_m(v) + a'\varphi_{m'}(v).$$

Pour démontrer que deux homomorphismes de $N \otimes_A P$ dans un module sont égaux, il est suffisant de vérifier qu'ils coïncident sur une partie génératrice de

$\mathrm{N} \otimes_{\mathrm{A}} \mathrm{P}$, en l'occurrence sur les tenseurs décomposés $n \otimes p$. Or, on a

$$\begin{aligned}\varphi_{am+a'm'}(n \otimes p) &= ((am + a'm') \otimes n) \otimes p \\ &= (am \otimes n + a'm' \otimes n) \otimes p \\ &= a(m \otimes n) \otimes p + a'(m' \otimes n) \otimes p \\ &= a\varphi_m(n \otimes p) + a'\varphi_{m'}(n \otimes p).\end{aligned}$$

Ainsi, l'application de $\mathrm{M} \times (\mathrm{N} \otimes_{\mathrm{A}} \mathrm{P})$ dans $(\mathrm{M} \otimes_{\mathrm{A}} \mathrm{N}) \otimes_{\mathrm{A}} \mathrm{P})$ qui à $(m, v)$ associe $\varphi_m(v)$ est bilinéaire, d'où un unique homomorphisme $\alpha\colon \mathrm{M} \otimes_{\mathrm{A}} (\mathrm{N} \otimes_{\mathrm{A}} \mathrm{P}) \to (\mathrm{M} \otimes_{\mathrm{A}} \mathrm{N}) \otimes_{\mathrm{A}} \mathrm{P})$ tel que $\alpha(m \otimes v) = \varphi_m(v)$ et donc $\alpha(m \otimes (n \otimes p)) = (m \otimes n) \otimes p$ pour tout $(m, n, p) \in \mathrm{M} \times \mathrm{N} \times \mathrm{P}$.

On construit de même un homomorphisme $\beta\colon (\mathrm{M} \otimes_{\mathrm{A}} \mathrm{N}) \otimes_{\mathrm{A}} \mathrm{P}) \to \mathrm{M} \otimes_{\mathrm{A}} (\mathrm{N} \otimes_{\mathrm{A}} \mathrm{P})$ tel que $\beta((m \otimes n) \otimes p) = m \otimes (n \otimes p)$. Comme $\alpha \circ \beta((m \otimes n) \otimes p) = \alpha(m \otimes (n \otimes p)) = (m \otimes n) \otimes p$, et comme ces tenseurs décomposés engendrent $(\mathrm{M} \otimes_{\mathrm{A}} \mathrm{N}) \otimes_{\mathrm{A}} \mathrm{P}$, $\alpha \circ \beta$ est l'identité de $(\mathrm{M} \otimes_{\mathrm{A}} \mathrm{N}) \otimes_{\mathrm{A}} \mathrm{P}$. De même, $\beta \circ \alpha$ est l'identité de $\mathrm{M} \otimes_{\mathrm{A}} (\mathrm{N} \otimes_{\mathrm{A}} \mathrm{P})$. Ce sont donc des isomorphismes. □

PROPOSITION 11.2.3. — *Soit* A *un anneau,* I *un idéal de* A *et* M *un* A*-module. Alors, il existe un unique homomorphisme de* A*-modules* $\mathrm{M} \otimes_{\mathrm{A}} (\mathrm{A}/\mathrm{I}) \to \mathrm{M}/\mathrm{IM}$ *tel que* $m \otimes \mathrm{cl}(1) \mapsto \mathrm{cl}(m)$. *C'est un isomorphisme.*

*En particulier,* $\mathrm{M} \otimes_{\mathrm{A}} \mathrm{A} \simeq \mathrm{M}$.

*Démonstration.* — Un tel homomorphisme doit associer à $m \otimes \mathrm{cl}(a) = am \otimes \mathrm{cl}(1)$ l'élément $a\,\mathrm{cl}(m) = \mathrm{cl}(am)$. Or, l'application de $\mathrm{M} \times (\mathrm{A}/\mathrm{I})$ dans $\mathrm{M}/\mathrm{IM}$ qui associe à $(m, \mathrm{cl}(a))$ la classe de $am$ est bien définie (si $\mathrm{cl}(a) = \mathrm{cl}(b)$, $a - b \in \mathrm{I}$ et $am - bm \in \mathrm{IM}$) et est bilinéaire. Il existe ainsi un unique homomorphisme $\varphi\colon \mathrm{M} \otimes_{\mathrm{A}} (\mathrm{A}/\mathrm{I}) \to \mathrm{M}/\mathrm{IM}$ tel que $\varphi(m \otimes \mathrm{cl}(1)) = \mathrm{cl}(m)$ pour tout $m \in \mathrm{M}$.

Considérons l'homomorphisme $\psi_0$ de M dans $\mathrm{M} \otimes_{\mathrm{A}} (\mathrm{A}/\mathrm{I})$ tel que $m \mapsto m \otimes \mathrm{cl}(1)$. Si $a \in \mathrm{I}$ et $m \in \mathrm{M}$, on a

$$\psi_0(am) = (am) \otimes \mathrm{cl}(1) = a(m \otimes \mathrm{cl}(1)) = m \otimes (a\,\mathrm{cl}(1)) = m \otimes \mathrm{cl}(a) = m \otimes 0 = 0$$

donc tout élément de la forme $am$ avec $a \in \mathrm{I}$ et $m \in \mathrm{M}$ est dans le noyau de $\psi_0$. Ces éléments engendrant IM, $\mathrm{IM} \subset \mathrm{Ker}\,\psi_0$, d'où par passage au quotient un unique homomorphisme de A-modules $\psi\colon \mathrm{M}/\mathrm{IM} \to \mathrm{M} \otimes_{\mathrm{A}} (\mathrm{A}/\mathrm{I})$ tel que $\psi(\mathrm{cl}(m)) = m \otimes \mathrm{cl}(1)$.

Si $m \in \mathrm{M}$, on a

$$\varphi(\psi(\mathrm{cl}(m))) = \varphi(m \otimes \mathrm{cl}(1)) = \mathrm{cl}(m)$$

tandis que si $m \in \mathrm{M}$ et $a \in \mathrm{A}$,

$$\psi(\varphi(m \otimes \mathrm{cl}(a))) = \psi(\mathrm{cl}(am)) = (am) \otimes \mathrm{cl}(1) = am \otimes \mathrm{cl}(1) = m \otimes \mathrm{cl}(a)$$

si bien que $\varphi \circ \psi = \mathrm{Id}_{\mathrm{M}/\mathrm{IM}}$ et $\psi \circ \varphi = \mathrm{Id}_{\mathrm{M} \otimes (\mathrm{A}/\mathrm{I})}$. Ce sont donc des isomorphismes. □

*Remarque 11.2.4.* — Soit un homomorphisme $f\colon \mathrm{M} \otimes_{\mathrm{A}} \mathrm{N} \to \mathrm{P}$

dont on veut prouver que c'est un isomorphisme. Il est en général assez facile de montrer qu'il est surjectif : souvent, on peut en effet construire les inverses d'assez d'éléments de P pour engendrer P. En revanche, il est plus difficile de montrer directement l'injectivité car il faudrait prouver que pour toute combinaison linéaire $\sum m_i \otimes n_i$ dont l'image est nulle, la combinaison linéaire $\sum m_i \otimes n_i$ est nulle, c'est-à-dire exprimer le vecteur $\sum e_{(m_i,n_i)}$ de $\mathrm{A}^{(\mathrm{M}\times\mathrm{N})}$ comme combinaison linéaire des relations élémentaires.

Il est utile de remarquer le fait suivant : si $f$ est un isomorphisme, tout élément de P a une unique image réciproque. Ainsi, dans la démonstration de la surjectivité, on a quasiment trouvé une formule pour l'inverse $g$ de $f$. Il faut alors juste vérifier que cette formule est bien vérifiée (typiquement, on connait l'image par $g$ de générateurs de P mais il faut s'assurer que les relations entre générateurs vont bien vers 0), puis que $f$ et $g$ sont inverses l'un de l'autre.

THÉORÈME 11.2.5. — *Soit* A *un anneau. Soit* $(\mathrm{M}_s)_{s\in\mathrm{S}}$ *une famille de* A*-modules et soit* P *un* A*-module. Pour* $s \in \mathrm{S}$*, notons* $i_s$ *et* $j_s$ *les homomorphismes canoniques* $\mathrm{M}_s \to \bigoplus_s \mathrm{M}_s$ *et* $\mathrm{M}_s \otimes \mathrm{P} \to \bigoplus(\mathrm{M}_s \otimes \mathrm{P})$.

*Alors, l'unique homomorphisme*

$$\alpha\colon \bigoplus_{s\in\mathrm{S}}(\mathrm{M}_s \otimes_{\mathrm{A}} \mathrm{P}) \to \left(\bigoplus_{s\in\mathrm{S}} \mathrm{M}_s\right) \otimes \mathrm{P}$$

*tel que pour tout* $s \in \mathrm{S}$, $\alpha \circ j_s = i_s \otimes \mathrm{Id}_{\mathrm{P}}$ *est un isomorphisme.*

*Démonstration.* — L'existence et l'unicité d'un tel homomorphisme $\alpha$ provient de la propriété universelle des sommes directes. Nous allons construire l'inverse de $\alpha$. Or, considérons l'application

$$(\bigoplus_s \mathrm{M}_s) \times \mathrm{P} \to \bigoplus_s (\mathrm{M}_s \otimes_{\mathrm{A}} \mathrm{P})$$

qui associe au couple $(\sum_{s\in\mathrm{S}} m_s, p)$ le tenseur $\sum_{s\in\mathrm{S}}(m_s \otimes p)$. Elle est bilinéaire (*exercice*) si bien qu'il existe un unique homomorphisme

$$\beta\colon \left(\bigoplus_{s\in\mathrm{S}} \mathrm{M}_s\right) \otimes \mathrm{P} \bigoplus_{s\in\mathrm{S}} (\mathrm{M}_s \otimes_{\mathrm{A}} \mathrm{P})$$

tel que $\beta((\sum_s m_s) \otimes p) = \sum_s (m_s \otimes p)$. De plus, $\beta \circ \alpha$ et $\alpha \circ \beta$ sont l'identité. □

COROLLAIRE 11.2.6. — *Soit* A *un anneau,* S *et* T *deux ensembles. Alors,* $\mathrm{A}^{(\mathrm{S})} \otimes_{\mathrm{A}} \mathrm{A}^{(\mathrm{T})} \simeq \mathrm{A}^{(\mathrm{S}\times\mathrm{T})}$.

*Le produit tensoriel de deux modules libres est libre.*

*Démonstration.* — On a en effet

$$\begin{aligned} \mathrm{A}^{(\mathrm{S})} \otimes_{\mathrm{A}} \mathrm{A}^{(\mathrm{T})} &= \left( \bigoplus_{s \in \mathrm{S}} \mathrm{A} \right) \otimes_{\mathrm{A}} \mathrm{A}^{(\mathrm{T})} = \bigoplus_{s \in \mathrm{S}} \left( \mathrm{A} \otimes_{\mathrm{A}} \mathrm{A}^{(\mathrm{T})} \right) \\ &= \bigoplus_{s \in \mathrm{S}} \mathrm{A}^{(\mathrm{T})} = \bigoplus_{\substack{s \in \mathrm{S} \\ t \in \mathrm{T}}} \mathrm{A} = \mathrm{A}^{(\mathrm{S} \times \mathrm{T})}. \end{aligned}$$

□

*Exercice 11.2.7.* — Si M est un A-module libre de base $(e_1, \ldots, e_m)$ et si N est un A-module libre de base $(f_1, \ldots, f_n)$, montrer que la famille $(e_i \otimes f_j)$ pour $1 \leq i \leq m$ et $1 \leq j \leq n$ est une base de $\mathrm{M} \otimes_{\mathrm{A}} \mathrm{N}$.

THÉORÈME 11.2.8 (Exactitude à droite du produit tensoriel)

*Soit* A *un anneau et soit* M *un* A*-module. Alors, pour toute suite exacte* $\mathrm{P}_1 \xrightarrow{f} \mathrm{P}_2 \xrightarrow{g} \mathrm{P}_3 \to 0$*, la suite*

$$\mathrm{M} \otimes_{\mathrm{A}} \mathrm{P}_1 \xrightarrow{\mathrm{Id}_{\mathrm{M}} \otimes f} \mathrm{M} \otimes_{\mathrm{A}} \mathrm{P}_2 \xrightarrow{\mathrm{Id}_{\mathrm{M}} \otimes g} \mathrm{M} \otimes_{\mathrm{A}} \mathrm{P}_3 \to 0$$

*est encore exacte.*

*Le foncteur « produit tensoriel par* M *»,* $\mathrm{P} \mapsto \mathrm{M} \otimes \mathrm{P}$*, est exact à droite.*

*Démonstration.* — *Exactitude en* $\mathrm{M} \otimes \mathrm{P}_3$. — On doit prouver que l'homomorphisme $\mathrm{Id}_{\mathrm{M}} \otimes g$ est surjectif. Or, si $m \in \mathrm{M}$ et $z \in \mathrm{P}_3$, soit $y \in \mathrm{P}_2$ tel que $g(y) = z$, ce qui est possible car $g$ est surjectif. Ainsi, l'image de $\mathrm{Id}_{\mathrm{M}} \otimes g$ contient les tenseurs décomposés de $\mathrm{M} \otimes \mathrm{P}_3$. Comme ceux-ci engendrent $\mathrm{M} \otimes_{\mathrm{A}} \mathrm{P}_3$, $\mathrm{Id}_{\mathrm{M}} \otimes g$ est surjectif.

*Exactitude en* $\mathrm{M} \otimes \mathrm{P}_2$. — L'inclusion $\operatorname{Im} \mathrm{Id}_{\mathrm{M}} \otimes f \subset \operatorname{Ker} \mathrm{Id}_{\mathrm{M}} \otimes g$ résulte du fait que $(\mathrm{Id}_{\mathrm{M}} \otimes g) \circ (\mathrm{Id}_{\mathrm{M}} \otimes f) = \mathrm{Id}_{\mathrm{M}} \otimes (g \circ f) = 0$. Dans l'autre sens, il est illusoire d'espérer démontrer directement que si $v \in \mathrm{M} \otimes_{\mathrm{A}} \mathrm{P}_2$ est tel que $(\mathrm{Id}_{\mathrm{M}} \otimes g)(v) = 0$, alors $v$ est dans l'image de $\mathrm{Id}_{\mathrm{M}} \otimes f$. (Relire la remarque 11.2.4. Mais que le lecteur incrédule ne se prive pas d'essayer !)

En raison de la surjectivité de $\mathrm{Id}_{\mathrm{M}} \otimes g$, le résultat à démontrer est équivalent au fait que $\mathrm{Id}_{\mathrm{M}} \otimes g$ induit un isomorphisme $g_0 \colon (\mathrm{M} \otimes \mathrm{P}_2) / \operatorname{Im}(\mathrm{Id}_{\mathrm{M}} \otimes f) \simeq \mathrm{M} \otimes \mathrm{P}_3$ et nous allons de fait construire une application réciproque. Définissons une application $h \colon \mathrm{M} \times \mathrm{P}_3 \to (\mathrm{M} \otimes \mathrm{P}_2) / \operatorname{Im}(\mathrm{Id}_{\mathrm{M}} \otimes f)$ comme suit : si $(m, z) \in \mathrm{M} \times \mathrm{P}_3$, soit $y \in \mathrm{P}_2$ tel que $g(y) = z$. L'élément $m \otimes y$ de $\mathrm{M} \otimes \mathrm{P}_2$ n'est bien défini mais si $y' \in \mathrm{P}_2$ vérifie $g(y') = z$, on a $y' - y \in \operatorname{Ker} g = \operatorname{Im} f$. Soit $x \in \mathrm{P}_1$ tel que $f(x) = y' - y$, alors

$$m \otimes y' - m \otimes y = m \otimes (y' - y) = m \otimes f(x) = (\mathrm{Id}_{\mathrm{M}} \otimes f)(m \otimes x),$$

si bien que la classe $\mathrm{cl}(m \otimes y)$ dans $(\mathrm{M} \otimes \mathrm{P}_2) / \operatorname{Im}(\mathrm{Id}_{\mathrm{M}} \otimes f)$ est, elle, bien définie. On définit $h(m, z)$ comme cette classe.

L'application $h$ est bilinéaire : si $z$ et $z'$ sont dans $\mathrm{P}_3$, si $g(y) = z$ et $g(y') = z'$, on a $g(ay + by') = az + bz'$ si bien que

$$\begin{aligned} h(m, az + bz') &= \mathrm{cl}(m \otimes (ay + by')) = a\,\mathrm{cl}(m \otimes y) + b\,\mathrm{cl}(m \otimes y') \\ &= ah(m, z) + bh(m, z') \end{aligned}$$

et

$$\begin{aligned} h(am + bm', z) &= \mathrm{cl}((am + bm') \otimes y) = a\,\mathrm{cl}(m \otimes y) + b\,\mathrm{cl}(m' \otimes y) \\ &= ah(m, z) + bh(m', z). \end{aligned}$$

Il existe ainsi un unique homomorphisme $h_0 \colon \mathrm{M} \otimes \mathrm{P}_3 \to (\mathrm{M} \otimes \mathrm{P}_2)/\operatorname{Im}(\mathrm{Id}_\mathrm{M} \otimes f)$ tel que $h_0(m \otimes g(y)) = \mathrm{cl}(m \otimes y)$ pour tout $m \in \mathrm{M}$ et tout $y \in \mathrm{P}_2$.

Alors, pour tout $m \in \mathrm{M}$ et tout $y \in \mathrm{P}_2$, on a

$$h_0 \circ g_0(\mathrm{cl}(m \otimes y)) = h_0(m \otimes g(y)) = \mathrm{cl}(m \otimes y).$$

Comme ces classes engendrent $(\mathrm{M} \otimes \mathrm{P}_2)/\operatorname{Im}(\mathrm{Id}_\mathrm{M} \otimes f)$, $h_0 \circ g_0 = \mathrm{Id}$. De même, si $m \in \mathrm{M}$, $z \in \mathrm{P}_3$ et si $y \in \mathrm{P}_2$ vérifie $g(y) = z$, on a

$$g_0 \circ h_0(m \otimes z) = g_0(\mathrm{cl}(m \otimes y)) = m \otimes g(y) = m \otimes z.$$

Il en résulte encore que $g_0 \circ h_0 = \mathrm{Id}$. Ainsi, $h_0$ et $g_0$ sont des isomorphismes réciproques l'un de l'autre. □

Définition 11.2.9. — *Soit* A *un anneau et* M *un* A*-module. On dit que* M *est plat si et seulement si le foncteur « produit tensoriel par* M *» est exact.*

Proposition 11.2.10. — *Si la suite exacte de* A*-modules*

$$0 \to \mathrm{P}_1 \xrightarrow{f} \mathrm{P}_2 \xrightarrow{g} \mathrm{P}_3 \to 0$$

*est scindée, alors pour tout* A*-module* M*, on a une suite exacte scindée*

$$0 \to \mathrm{M} \otimes_\mathrm{A} \mathrm{P}_1 \xrightarrow{\mathrm{Id}_\mathrm{M} \otimes f} \mathrm{M} \otimes_\mathrm{A} \mathrm{P}_2 \xrightarrow{\mathrm{Id}_\mathrm{M} \otimes g} \mathrm{M} \otimes_\mathrm{A} \mathrm{P}_3 \to 0$$

*Démonstration.* — Soit $h \colon \mathrm{P}_2 \to \mathrm{P}_1$ un inverse à gauche pour $f$ et considérons l'homomorphisme

$$\mathrm{Id}_\mathrm{M} \otimes h \colon \mathrm{M} \otimes_\mathrm{A} \mathrm{P}_2 \to \mathrm{M} \otimes_\mathrm{A} \mathrm{P}_1.$$

Il vérifie

$$(\mathrm{Id}_\mathrm{M} \otimes h) \circ (\mathrm{Id}_\mathrm{M} \otimes f) = \mathrm{Id}_\mathrm{M} \otimes (h \circ f) = \mathrm{Id}_\mathrm{M} \otimes \mathrm{Id}_{\mathrm{P}_1} = \mathrm{Id}$$

donc est un inverse à gauche de $\mathrm{Id}_\mathrm{M} \otimes f$.

Par suite, $\mathrm{Id}_\mathrm{M} \otimes f$ est injectif et l'on a bien une suite exacte scindée comme annoncé. □

## 11.3. Changement de base

Soit A un anneau, soit M et N deux A-modules. Si $\varphi$ est un endomorphisme de N, $\mathrm{Id}_M \otimes \varphi$ est un endomorphisme de $M \otimes_A N$. Un cas particulier important est celui où N est une A-algèbre B. Dans ce cas, pour tout $b \in B$, on dispose d'un endomorphisme A-linéaire $\mu_b$ de multiplication par $b$ dans B. Alors, $\mathrm{Id}_M \otimes \mu_b$ est un endomorphisme de $M \otimes_A B$, d'où une application $B \to \mathrm{End}_A(M \otimes_A B)$. Mais rappelons une remarque qu'on avait faite au chapitre 6 (remarque 6.1.4) : une structure de B-module sur un groupe abélien P est *équivalente* à la donnée d'un homomorphisme d'anneaux (non commutatifs) $B \to \mathrm{End}(M)$. Par cette remarque, $M \otimes_A B$ est donc muni d'une structure canonique de B-module.

THÉORÈME 11.3.1. — *Soit* A *un anneau,* B *une* A*-algèbre. Pour tout* A*-module* M*, il existe une unique structure de* B*-module sur* $M \otimes_A B$ *tel que pour tout* $b \in B$ *et tout* $m \in M$, $b(m \otimes 1) = m \otimes b$.

*De plus, si* $f : M \to N$ *est un homomorphisme de* A*-modules, l'homomorphisme canonique* $f \otimes \mathrm{Id}_B$ *est* B*-linéaire.*

En d'autres termes, la construction « produit tensoriel par B » est un *foncteur* de la catégorie des A-modules dans celle des B-modules. C'est le foncteur de changement de base de A à B.

*Démonstration.* — Les remarques qui précèdent l'énoncé du théorème prouvent effectivement l'existence d'une telle structure de B-module. Montrons l'unicité : il suffit de remarquer que la formule donnée détermine $bv$ pour tout tenseur $v \in M \otimes_A B$ et tout $b \in B$. Or, si $v = \sum m_i \otimes b_i$

$$\begin{aligned} bv &= b(\textstyle\sum m_i \otimes b_i) = \sum b(m_i \otimes b_i) = \sum b(b_i(m_i \otimes 1)) \\ &= \textstyle\sum (bb_i)(m_i \otimes 1) = \sum m_i \otimes (bb_i). \end{aligned}$$

Enfin, si $f : M \to N$ est un homomorphisme de A-modules, l'homomorphisme $f \otimes \mathrm{Id}_B$ est additif. Il reste à prouver qu'il est B-linéaire : si $v = \sum m_i \otimes b_i \in M \otimes_A B$ et si $b \in B$, on a

$$\begin{aligned} (f \otimes \mathrm{Id}_B)(bv) &= (f \otimes \mathrm{Id}_B)(b(\textstyle\sum m_i \otimes b_i)) = (f \otimes \mathrm{Id}_B)(\sum m_i \otimes (bb_i)) \\ &= \textstyle\sum f(m_i) \otimes (bb_i) = b(\sum f(m_i) \otimes b_i) \\ &= b(f \otimes \mathrm{Id}_B)(v). \end{aligned}$$

□

PROPOSITION 11.3.2. — *Soit* A *un anneau et* M *un* A*-module. Soit* B *une* A*-algèbre et* N *un* B*-module. Il existe une unique application* $\alpha : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_B(M \otimes_B, N)$ *telle que pour tout* $\varphi \in \mathrm{Hom}_A(M, N)$ *et tout* $m \in M$, $\alpha(\varphi)(m \otimes 1) = \varphi(m)$. *De plus,* $\alpha$ *est un isomorphisme de* A*-modules.*

Dans l'écriture $\mathrm{Hom}_A(M,N)$, N est considéré comme un A-module via le *foncteur d'oubli* de la structure de B-module. On dit ainsi que le foncteur de changement de base est *adjoint à gauche* au foncteur d'oubli et que le foncteur d'oubli est *adjoint à droite* au foncteur de changement de base.

*Démonstration.* — Justifions tout d'abord que $\alpha$ est bien défini. Si $\alpha(\varphi)$ est B-linéaire et vérifie $\alpha(\varphi)(m\otimes 1)=\varphi(m)$, on aura

$$\alpha(\varphi)(m\otimes b)=\alpha(\varphi)(b(m\otimes 1))=b\alpha(\varphi)(m\otimes 1)=b\varphi(m).$$

Remarquons alors que l'application $M\times B\to N$ qui à $(m,b)$ associe $b\varphi(m)$ est bilinéaire. Il existe ainsi un unique homomorphisme $M\otimes_A B\to N$ tel que $m\otimes b\mapsto b\varphi(m)$. Notons cet homomorphisme $\alpha(\varphi)$.

Alors, si $a$, $a'\in A$ et $\varphi$, $\varphi'\in\mathrm{Hom}_A(M,N)$, les homomorphismes $\alpha(a\varphi+a'\varphi')$ et $a\alpha(\varphi)+a'\alpha(\varphi')$ associent tous deux à $m\otimes 1$ l'élément $a\varphi(m)+a'\varphi'(m)$ de N. Ils sont donc égaux et $\alpha\colon\varphi\mapsto\alpha(\varphi)$ est ainsi A-linéaire.

Montrons enfin que c'est un isomorphisme. Nous allons pour cela construire l'isomorphisme réciproque. On associe tout simplement à $\psi\colon M\otimes_A B\to N$ l'homomorphisme $\beta(\psi)\colon M\to N$ composé de $\psi$ et de l'homomorphisme canonique $M\to M\otimes_A B$ qui à $m$ associe $m\otimes 1$. Autrement dit, $\beta(\psi)(m)=\psi(m\otimes 1)$.

On a alors pour tout $\psi\in\mathrm{Hom}_B(M\otimes_A B,N)$ et tout $m\in M$ l'égalité

$$\alpha(\beta(\psi))(m\otimes 1)=\beta(\psi)(m)=\psi(m\otimes 1)$$

si bien que $\alpha\circ\beta(\psi)=\psi$, tandis que pour tout $\varphi\in\mathrm{Hom}_A(M,N)$ et tout $m\in M$,

$$\beta(\alpha(\varphi))(m)=\alpha(\varphi)(m\otimes 1)=\varphi(m)$$

si bien que $\beta\circ\alpha(\varphi)=\varphi$. Ainsi, $\alpha$ et $\beta$ sont des isomorphismes réciproques l'un de l'autre. □

PROPOSITION 11.3.3. — *Soit* A *un anneau et soit* S *une partie multiplicative de* A. *Pour tout* A*-module* M, *il existe un homomorphisme canonique de* $S^{-1}A$*-modules* $M\otimes S^{-1}A\to S^{-1}M$ *tel que* $m\otimes 1\mapsto m/1$. *C'est un isomorphisme.*

Puisque le foncteur de localisation en toute partie multiplicative est exact (proposition 6.5.8), on en déduit immédiatement le fait suivant :

COROLLAIRE 11.3.4. — *Pour tout anneau* A *et toute partie multiplicative* S *de* A, *la* A*-algèbre* $S^{-1}A$ *est un* A*-module plat.*

*Démonstration de la proposition.* — Un tel homomorphisme $\alpha\colon M\otimes S^{-1}A\to S^{-1}M$ associe à $m\otimes(a/s)$ l'élément $am/s$ de $S^{-1}M$. Il est bien défini car l'application $M\times S^{-1}A\to S^{-1}M$ qui associe au couple $(m,a/s)$ l'élément $am/s$ est bilinéaire. (On aurait aussi pu appliquer l'isomorphisme d'adjonction à l'homomorphisme canonique $M\to S^{-1}M$.)

Pour voir que c'est un isomorphisme, nous construisons sa réciproque. Pour cela, on part de l'homomorphisme canonique $M \to M \otimes_A S^{-1}A$ tel que $m \mapsto m \otimes 1$. Comme $M \otimes_A S^{-1}A$ est un $S^{-1}A$-module, il existe d'après la propriété universelle de la localisation un unique homomorphisme $\beta\colon S^{-1}M \to M \otimes_A S^{-1}A$ tel que $m/1 \mapsto m \otimes 1$.

Alors, $\beta$ et $\alpha$ sont inverses l'un de l'autre. □

## 11.4. Adjonction et exactitude

Dans ce paragraphe, on profite de l'exemple fourni par le produit tensoriel pour donner un complément au chapitre d'algèbre homologique.

PROPOSITION 11.4.1. — *Soit* A *un anneau et soit*

$$M \to N \to P \to 0$$

*un complexe de* A*-modules. Alors, ce complexe est exact si et seulement si pour tout* A*-module* L*, la suite*

$$0 \to \mathrm{Hom}(P, L) \to \mathrm{Hom}(N, L) \to \mathrm{Hom}(M, L)$$

*est exacte.*

*Démonstration.* — Si l'on a une suite exacte $M \to N \to P \to 0$, le fait que le foncteur $\mathrm{Hom}(\bullet, L)$ soit exact à gauche implique que pour tout A-module L, la suite $0 \to \mathrm{Hom}(P, L) \to \mathrm{Hom}(N, L) \to \mathrm{Hom}(M, L)$ est exacte.

Réciproquement, notons $f\colon M \to N$ et $g\colon N \to P$ les homomorphismes intervenant dans le complexe $M \to N \to P \to 0$.

Montrons que $g$ est surjectif. Posons $L = P/g(N) = \mathrm{Coker}\, g$ et soit $\varphi \in \mathrm{Hom}(P, L)$ la surjection canonique. Son image dans $\mathrm{Hom}(N, L)$ par l'homomorphisme $\mathrm{Hom}(P, L) \to \mathrm{Hom}(N, L)$ induit par $g$ est égale à $\varphi \circ g$ donc est nulle puisque par construction $\mathrm{Ker}\, \varphi = \mathrm{Im}\, g$. Par hypothèse, l'homomorphisme $\circ g$ est injectif, d'où $\varphi = 0$. Ainsi, $\mathrm{Im}\, \varphi = L = 0$ et $g(N) = P$.

Montrons que $\mathrm{Ker}\, g = \mathrm{Im}\, f$. Par hypothèse, $g \circ f = 0$ donc $\mathrm{Im}\, f \subset \mathrm{Ker}\, g$. Posons $L = N/\mathrm{Im}\, f$ et soit $\varphi \in \mathrm{Hom}(N, L)$ l'homomorphisme canonique. Par construction, $\varphi \circ f = 0$, c'est-à-dire que $\varphi$ appartient au noyau de l'homomorphisme $\mathrm{Hom}(N, L) \to \mathrm{Hom}(M, L)$ induit par $f$. Par suite, $\varphi$ appartient à l'image de l'homomorphisme $\mathrm{Hom}(P, L) \to \mathrm{Hom}(N, L)$ induit par $g$ et il existe $\psi \in \mathrm{Hom}(P, L)$ tel que $\varphi = \psi \circ g$. Alors, si $x \in \mathrm{Ker}\, g$, $\varphi(x) = \psi(g(x)) = 0$ donc $x \in \mathrm{Im}\, f$. □

DÉFINITION 11.4.2. — *Soit* A *un anneau. Soit F et G deux foncteurs de la catégorie de* A*-modules dans elle-même, F étant contravariant et G covariant. On dit que G est un*

*adjoint à gauche de $F$ et que $F$ est un adjoint à droite de $G$ s'il existe pour tous* A*-modules* M *et* N *un isomorphisme*

$$\alpha_{M,N}\colon \mathrm{Hom}_A(G(M),N) \to \mathrm{Hom}_A(M,F(N))$$

*tel que pour tout couple d'homomorphismes $g\colon M \to M'$ et $f\colon N \to N'$, on ait un diagramme commutatif*

$$\begin{array}{ccc} \mathrm{Hom}_A(G(M'),N) & \xrightarrow{\alpha_{M',N}} & \mathrm{Hom}_A(M',F(N)) \\ \Big\downarrow{\scriptstyle f\circ\bullet\circ G(g)} & & \Big\downarrow{\scriptstyle F(f)\circ\bullet\circ g} \\ \mathrm{Hom}_A(G(M),N') & \xrightarrow{\alpha_{M,N}} & \mathrm{Hom}_A(M,N') \end{array}.$$

Proposition 11.4.3. — *Soit* A *un anneau. Un foncteur covariant $G$ qui est un adjoint à gauche est exact à droite.*

*Démonstration.* — Partons d'une suite exacte $M \to N \to P \to 0$. On doit prouver que son image $G(M) \to G(N) \to G(P) \to 0$ par le foncteur $G$ est encore exacte. Pour cela, il suffit d'après la proposition 11.4.1 de démontrer que pour tout A-module L, la suite

$$0 \to \mathrm{Hom}(G(P),L) \to \mathrm{Hom}(G(N),L) \to \mathrm{Hom}(G(M),L)$$

est exacte. Or, si $F$ est un foncteur donc $G$ est l'adjoint à gauche, cette suite s'identifie à la suite

$$0 \to \mathrm{Hom}(P,F(L)) \to \mathrm{Hom}(N,F(L)) \to \mathrm{Hom}(M,F(L)).$$

Comme on était parti d'une suite exacte $M \to N \to P \to 0$, la proposition 11.4.1 montre que cette suite est exacte, ce qu'on voulait démontrer. □

L'intérêt de ces généralités vient qu'on peut les appliquer au produit tensoriel pour démontrer son exactitude à droite de manière plus conceptuelle (mais plus abstraite aussi).

Théorème 11.4.4. — *Soit* A *un anneau et soit* P *un* A*-module. Le foncteur « produit tensoriel par* M *»,* $M \mapsto P \otimes_A M$ *est un adjoint à gauche du foncteur* $\mathrm{Hom}_A(P,\bullet)$.

*Démonstration.* — Pour tout couple $(M,N)$ de A-modules, il nous faut construire un isomorphisme $\alpha_{M,N}\colon \mathrm{Hom}_A(P\otimes_A M,N) \to \mathrm{Hom}_A(M,\mathrm{Hom}(P,N))$. Avant de donner une formule, interprétons les deux membres avec des mots. D'après la propriété universelle vérifiée par le produit tensoriel, $\mathrm{Hom}_A(P\otimes_A M,N)$ est l'ensemble des applications bilinéaires de $P\times M$ dans N. Or, une telle application bilinéaire $b$ est une application linéaire en chacune des variables. En particulier, pour tout $m$, elle induit une application linéaire $b(\cdot,m)$ de P dans N. Réciproquement, une famille d'applications linéaires $(b_m)_{m\in M}$ de P dans N telle

que l'application $m \mapsto b_m$ soit linéaire correspond exactement à une application bilinéaire de $P \times M$ dans M.

Si l'on veut, voici une formule. Si $b \in \mathrm{Hom}(M \otimes_A P, N)$, $\alpha_{M,N}(b)$ est l'application linéaire qui associe à $m \in M$ l'application linéaire $p \mapsto b(m \otimes p)$.

Enfin, si $g$ est un homomorphisme $M \to M'$ et $f$ un homomorphisme $N \to N'$, on doit comparer les deux homomorphismes

$$\mathrm{Hom}_A(M' \otimes P, N) \xrightarrow{\alpha_{M',N}} \mathrm{Hom}_A(M', \mathrm{Hom}_A(P, N)) \xrightarrow{f \circ \bullet \circ g} \mathrm{Hom}_A(M, \mathrm{Hom}_A(P, N'))$$

et

$$\mathrm{Hom}_A(M' \otimes P, N) \xrightarrow{f \circ \bullet \circ (g \otimes \mathrm{Id}_P)} \mathrm{Hom}_A(M \otimes P, N') \xrightarrow{\alpha_{M,N'}} \mathrm{Hom}_A(M, \mathrm{Hom}_A(P, N')).$$

Soit $b \in \mathrm{Hom}(M' \otimes P, N)$ et calculons ses images $\varphi_1(b)$ et $\varphi_2(b)$ par les deux lignes.

Tout d'abord, $\alpha_{M',N}(b)$ est l'application linéaire $M' \to \mathrm{Hom}_A(P, N)$ définie par $m' \mapsto \big(p \mapsto b(m' \otimes p)\big)$. Par suite, $\varphi_1(b)$ est l'application linéaire $M \to \mathrm{Hom}_A(P, N)$ définie par $m \mapsto \big(p \mapsto g(b(f(m) \otimes p))\big)$.

Ensuite, l'image de $b$ par l'homomorphisme $f \circ \bullet \circ (g \otimes \mathrm{Id}_P)$ est l'application de $M \otimes P$ dans $N'$ telle que $m \otimes p \mapsto g(b(f(m) \otimes p))$. Par suite, $\varphi_2(b)$ associe à $m \in M$ l'applicatin linéaire $p \mapsto g(b(f(m) \otimes p))$.

Les deux expressions $\varphi_1(b)$ et $\varphi_2(b)$ coïncident, ce qui achève la démonstration du fait que le foncteur produit tensoriel par P est l'adjoint à gauche du foncteur $\mathrm{Hom}(P, \bullet)$. □

Corollaire 11.4.5. — *Le foncteur produit tensoriel est exact à droite.*

*Exercice 11.4.6.* — Écrire les énoncés analogues à ceux de ce paragraphe en échangeant droite et gauche :

a) Donner un critère pour l'exactitude d'une suite $0 \to M \to N \to P$ en termes de suites de la forme $0 \to \mathrm{Hom}(L, M) \to \mathrm{Hom}(L, N) \to \mathrm{Hom}(L, P)$ lorsque L est un A-module quelconque.

b) Montrer qu'un foncteur qui est adjoint à droite est exact à gauche.

## 11.5. Exercices

*Exercice 11.5.1.* — Soient $m$ et $n$ deux entiers $\geq 1$ premiers entre eux. Montrer que

$$(\mathbf{Z}/m\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z}) = 0.$$

*Exercice 11.5.2.* — Soit X un espace topologique. Montrer

$$\mathscr{E}(X, \mathbf{R}) \otimes_{\mathbf{R}} \mathbf{C} \simeq \mathscr{E}(X, \mathbf{C}).$$

*Exercice 11.5.3.* — Soit M un A-module ; notons $\mathrm{M}^\vee = \mathrm{Hom}(\mathrm{M}, \mathrm{A})$.

**a)** Soit N un A-module. Montrer qu'il existe un unique homomorphisme de A-modules

$$\Phi : \mathrm{M}^\vee \otimes_\mathrm{A} \mathrm{N} \to \mathrm{Hom}_\mathrm{A}(\mathrm{M}, \mathrm{N})$$

qui associe à $\varphi \otimes n$ (pour $\varphi \in \mathrm{M}^\vee$ et $n \in \mathrm{N}$) l'homomorphisme $m \mapsto \varphi(m)n$.

**b)** Montrer que $\Phi$ est un isomorphisme si M est libre de type fini. Est-ce que $\Phi$ est un isomorphisme en général ?

**c)** Montrer qu'il existe un unique homomorphisme de A-modules

$$t : \mathrm{M}^\vee \otimes_\mathrm{A} \mathrm{M} \to \mathrm{A}$$

tel que $t(\varphi \otimes m) = \varphi(m)$.

On suppose que M est libre de rang fini et que $\mathrm{N} = \mathrm{M}$. Reconnaissez-vous l'homomorphisme

$$t \circ \Phi^{-1} : \mathrm{End}_\mathrm{A}(\mathrm{M}) \to \mathrm{A} \ ?$$

*Exercice 11.5.4.* — Soit M un $\mathbf{Z}$-module.

**a)** Montrer que $\mathrm{M} \otimes_\mathbf{Z} \mathbf{Q}$ est sans torsion.

**b)** Soit $\mathrm{S} = \mathbf{Z} \setminus \{0\}$. Montrer que $\mathrm{M} \otimes_\mathbf{Z} \mathbf{Q}$ est isomorphe à $\mathrm{S}^{-1}\mathrm{M}$.

**c)** Montrer que $\mathrm{M}_\mathrm{tor}$ est égal au noyau de l'homomorphisme naturel $\mathrm{M} \to \mathrm{M} \otimes_\mathbf{Z} \mathbf{Q}$.

*Exercice 11.5.5.* — Soit A un anneau local noethérien, notons $\mathfrak{m}$ son idéal maximal et $k = \mathrm{A}/\mathfrak{m}$ le corps résiduel.

Soient M et N deux A-modules de type fini, N étant en outre supposé libre sur A. Soit $f : \mathrm{M} \to \mathrm{N}$ un homomorphisme de A-modules tel que l'homomorphisme

$$\bar{f} : \mathrm{M} \otimes_\mathrm{A} k \to \mathrm{N} \otimes_\mathrm{A} k$$

soit un isomorphisme.

Montrer que $f$ est un isomorphisme.

*Exercice 11.5.6.* — Soit $p$ un nombre premier et A l'anneau $\mathbf{Z}/p^2\mathbf{Z}$. Soit M un A-module de type fini. Montrer que les conditions suivantes sont équivalentes :

(1) M est un A-module libre ;

(2) M est un A-module plat ;

(3) si $m \in \mathrm{M}$ vérifie $pm = 0$, il existe $m' \in \mathrm{M}$ tel que $m = pm'$.

*Exercice 11.5.7.* — Soient $k$ un anneau, A et B deux $k$-algèbres. Montrer que l'application

$$\big((a \otimes b), (a' \otimes b')\big) \mapsto (aa') \otimes (bb')$$

munit $\mathrm{A} \otimes_k \mathrm{B}$ d'une structure de $k$-algèbre.

*Exercice 11.5.8.* — Soient I et J deux idéaux de A. Montrer qu'il existe un isomorphisme de A-modules

$$(A/I) \otimes_A (A/J) \simeq A/(I+J).$$

Expliciter un tel isomorphisme qui est en outre un isomorphisme d'anneaux.

*Exercice 11.5.9.* — Soient M et N deux A-modules.

**a)** On suppose que M et N sont de type fini. Montrer que $M \otimes_A N$ est de type fini.

**b)** On suppose que M est un A-module noethérien et que N est de type fini. Montrer que $M \otimes_A N$ est noethérien.

**c)** On suppose que M est un A-module artinien et que N est de type fini. Montrer que $M \otimes_A N$ est artinien.

**d)** On suppose que M et N sont de longueur finie. Montrer que $M \otimes_A N$ est de longueur finie, et que

$$\ell_A(M \otimes_A N) \leq \ell_A(M)\ell_A(N).$$

*Exercice 11.5.10.* — Soit A un anneau local intègre de corps des fractions K et d'idéal maximal $\mathfrak{m}$. Soit M un A-module de type fini tel que

$$\dim_{A/\mathfrak{m}} M/\mathfrak{m}M = \dim_K M \otimes_A K.$$

Montrer que M est libre.

## 11.6. Solutions

*Solution de l'exercice 11.5.1.* — Un élément de $(\mathbf{Z}/m)\otimes(\mathbf{Z}/n)$ est somme de tenseurs $a \otimes b$, avec $a \in \mathbf{Z}/m$ et $b \in \mathbf{Z}/n$. Considérons un tel tenseur et montrons qu'il est nul. Soient $u$ et $v \in \mathbf{Z}$ tels que $um + vn = 1$. Alors,

$$\begin{aligned} a \otimes b &= 1(a \otimes b) \\ &= (um + vn)(a \otimes b) \\ &= um(a \otimes b) + vn(a \otimes b) \\ &= (uma) \otimes b + a \otimes (vnb) \\ &= 0 \otimes b + a \otimes 0 = 0. \end{aligned}$$

Par suite, tout élément de $(\mathbf{Z}/m) \otimes (\mathbf{Z}/n)$ est nul, donc

$$(\mathbf{Z}/m\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z}) = 0.$$

*Solution de l'exercice 11.5.2.* — L'application

$$\mathscr{E}(X, \mathbf{R}) \times \mathbf{C} \to \mathscr{E}(X, \mathbf{C})$$

définie par $(f,z) \mapsto zf$ est bilinéaire, d'où un homomorphisme

$$\mathscr{E}(X,\mathbf{R}) \otimes_{\mathbf{R}} \mathbf{C} \to \mathscr{E}(X,\mathbf{C}).$$

D'autre part, l'application

$$\mathscr{E}(X,\mathbf{C}) \to \mathscr{E}(X,\mathbf{R}) \otimes_{\mathbf{R}} \mathbf{C}$$

définie par

$$f \mapsto \Re(f) \otimes 1 + \Im(f) \otimes i$$

est linéaire, et est l'inverse de l'application précédente. On a donc un isomorphisme.

*Solution de l'exercice 11.5.3.* — **a)** L'application

$$M^\vee \times N \to \mathrm{Hom}_A(M,N)$$

qui envoie $(\varphi, n)$ sur l'homomorphisme $m \mapsto \varphi(m)n$ est A-bilinéaire. Il existe ainsi un unique homomorphisme $\Phi$ comme demandé.

**b)** Supposons que M est libre de rang $n$. Soit $(e_1,\dots,e_n)$ une base de M. On dispose alors de la base duale de $M^\vee$, $(\varphi_1,\dots,\varphi_n)$, définie par $\varphi_i(e_j) = 1$ si $i = j$ et $\varphi_i(e_j) = 0$ sinon.

Montrons que $\Phi$ est un isomorphisme. Alors, l'application

$$\begin{aligned}\Psi : \mathrm{Hom}_A(M,N) &\to M^\vee \otimes N \\ f &\mapsto \varphi_1 \otimes f(e_1) + \cdots + \varphi_n \otimes f(e_n)\end{aligned}$$

est un homomorphisme de A-modules. Si $f \in \mathrm{Hom}_A(M,N)$,

$$\begin{aligned}\Phi(\Psi(f))(e_i) &= \Phi(\sum_j \varphi_j \otimes f(e_j))(e_i) \\ &= \sum_j \varphi_j(e_i) f(e_j) = f(e_i),\end{aligned}$$

donc, les $e_i$ engendrant M, $\Phi(\Psi(f)) = f$. Réciproquement, si $\varphi \in M^\vee$ et $n \in N$,

$$\begin{aligned}\Psi(\Phi(\varphi \otimes n)) &= \Psi(m \mapsto \varphi(m)n) \\ &= \sum_i \varphi_i \otimes (\varphi(e_i)n) \\ &= (\sum_i \varphi(e_i)\varphi_i) \otimes n \\ &= \varphi \otimes n,\end{aligned}$$

donc, les $\varphi \otimes n$ engendrant $M^\vee \otimes N$, $\Psi \circ \Phi = \mathrm{Id}$. Par suite, $\Phi$ et $\Psi$ sont des isomorphismes réciproques l'un de l'autre.

**c)** L'application

$$M^\vee \times M, \quad (\varphi, m) \mapsto \varphi(m)$$

est bilinéaire, d'où l'existence et l'unicité de l'homomorphisme $t$.

Supposons maintenant que $M = N$ est libre de rang $n$. Soit $(e_1, \dots, e_n)$ une base de M, et notons $(\varphi_1, \dots, \varphi_n)$ la base duale. Alors, les $\varphi_i \otimes e_j$ forment une base de $M^\vee \otimes M$, l'endomorphisme correspondant de M étant donné dans la base $(e_i)$ par la matrice $E_{i,j}$ (des 0 partout sauf un 1 sur la $j^{\text{e}}$ ligne et la $i^{\text{e}}$ colonne. L'image de $E_{i,j}$ par $t \circ \Phi^{-1}$ est alors $\varphi_i(e_j) = 1$ si $i = j$, et 0 sinon. Par suite, l'image de la matrice $U = (a_{i,j})$ par $t \circ \Phi^{-1}$ est l'élément $\sum_i a_{i,i}$ de A. C'est la trace de U.

*Solution de l'exercice 11.5.4.* — **a)** La multiplication par $a \in \mathbf{Z}^*$ est un isomorphisme de $M \otimes_{\mathbf{Z}} \mathbf{Q}$. Son inverse est en effet donné par

$$m \otimes x \mapsto m \otimes (x/a)$$

qui est bien définie. Alors, si $am = 0$, on a nécessairement $m = 0$.

**b)** L'application $M \times \mathbf{Q} \to S^{-1}M$ donnée par $(m, a/b) \mapsto (am)/b$ est bilinéaire, donc définit un homomorphisme $f : M \otimes \mathbf{Q} \to S^{-1}M$.

D'autre part, on peut définir un homomorphisme dans l'autre sens $g : S^{-1}M \to M \otimes \mathbf{Q}$ par $g(m/b) = m \otimes (1/b)$. En effet, si $m/b = m'/b'$, c'est qu'il existe $a \in \mathbf{Z}^*$ tel que $ab'm = abm'$. Alors,

$$\begin{aligned} m \otimes (1/b) &= (amb') \otimes (1/abb') \\ &= (abm') \otimes (1/abb') \\ &= m' \otimes (1/b'). \end{aligned}$$

Enfin, $f(g(m/b)) = f(m \otimes (1/b)) = m/b$ et $g(f(m \otimes (a/b))) = g(am/b) = am \otimes (1/b) = m \otimes (a/b)$, si bien que $f \circ g = \mathrm{Id}$, $g \circ f = \mathrm{Id}$ et $f$ et $g$ sont des isomorphismes. Par conséquent

$$S^{-1}M \simeq M \otimes_{\mathbf{Z}} \mathbf{Q}.$$

**c)** L'homomorphisme naturel $\varphi : M \to M \otimes \mathbf{Q}$ est le composé de

$$M \to S^{-1}M \xrightarrow{g} M \otimes \mathbf{Q}.$$

On a vu que $g$ est un isomorphisme. Ainsi, le noyau de $\varphi$ est le noyau de $M \to S^{-1}M$. Or, si $m/1 = 0$, cela signifie qu'il existe $a \in \mathbf{Z}^*$ tel que $am = 0$, et donc que $m$ est de torsion. Ainsi, le noyau de $\varphi$ est le sous-module de torsion de M.

Remarque. — Tout l'exercice se généralise en remplaçant $\mathbf{Z}$ par un anneau intègre A et $\mathbf{Q}$ par le corps des fractions K de A.

*Solution de l'exercice 11.5.5.* — On identifie $M \otimes_A k$ à $M/\mathfrak{m}M$ et $N \otimes_A k$ à $N/\mathfrak{m}N$. Comme $\bar{f}$ est un isomorphisme, on a $N = \mathfrak{m}N + f(M)$. Comme N est de type fini sur A, le théorème de Nakayama implique que $N = f(M)$ : $f$ est surjectif.

Comme N est libre sur A, $f$ a un inverse à droite $g$, c'est-à-dire un homomorphisme $g\colon \mathrm{N} \to \mathrm{M}$ tel que $f \circ g = \mathrm{Id}_\mathrm{N}$. (Si l'on veut, on dit que tout module libre est projectif. Si on préfère un argument direct, on choisit une base $(e_1, \dots, e_n)$ de L et pour tout $n$ un élément $m_n \in \mathrm{M}$ tel que $f(m_n) = e_n$. Alors, on pose $g(\sum a_i e_i) = \sum a_i m_i$.)

L'homomorphisme induit $\bar{g}\colon \mathrm{N} \otimes_\mathrm{A} k \to \mathrm{M} \otimes_\mathrm{A} k$ est alors un inverse à gauche de $\bar{f}$. Comme l'inverse à gauche d'un isomorphisme d'espace vectoriels est égal à l'inverse, donc est un isomorphisme, $\bar{g}$ est un isomorphisme. Il est en particulier surjectif. Alors, $\mathrm{M} = \mathfrak{m}\mathrm{M} + g(\mathrm{N})$ et le théorème de Nakayama implique $\mathrm{M} = g(\mathrm{N})$. Donc $g$ est surjectif.

Montrons alors que $g \circ f = \mathrm{Id}_\mathrm{M}$. En effet, si $m \in \mathrm{M}$, choisissons $x \in \mathrm{N}$ tel que $g(x) = m$. On a alors $g(f(m)) = g(f(g(x))) = g(x)$ puisque $f \circ g = \mathrm{Id}_\mathrm{N}$, donc $g(f(m)) = m$. Ainsi, $f$ et $g$ sont des isomorphismes réciproques l'un de l'autre.

*Solution de l'exercice 11.5.6.* — (1)⇒(2).— Tout module libre est plat.

(2)⇒(3).— Considérons la suite exacte de A-modules

$$0 \to p(\mathbf{Z}/p^2\mathbf{Z}) \xrightarrow{i} (\mathbf{Z}/p^2\mathbf{Z}) \xrightarrow{p} p(\mathbf{Z}/p^2\mathbf{Z}) \to 0,$$

où la flèche $i$ est l'injection naturelle et la flèche $p$ la multiplication par $p$ dans $\mathrm{A} = \mathbf{Z}/p^2\mathbf{Z}$. Puisque M est plat, on obtient en la tensorisant par M une suite exacte

$$(*) \qquad 0 \to (p\mathrm{A}) \otimes_\mathrm{A} \mathrm{M} \xrightarrow{i} \mathrm{M} \xrightarrow{p} (pa) \otimes_\mathrm{A} \mathrm{M} \to 0.$$

Dans cette suite exacte, l'homomorphisme $i$ associe à $\sum(pa_j) \otimes m_j$ l'élément $\sum pa_j m_j$ de M. Puisqu'il est injectif, il définit donc un isomorphisme avec son image qui est $p\mathrm{M}$.

L'homomorphisme $p$ associe à $m \in \mathrm{M}$ l'élément $p \otimes m$ de $(p\mathrm{A}) \otimes_\mathrm{A} \mathrm{M}$. Alors, $i \circ p$ est l'homomorphisme $\mathrm{M} \to \mathrm{M}$ de multiplication par $p$. En identifiant $(p\mathrm{A}) \otimes_\mathrm{A} \mathrm{M}$ avec $p\mathrm{M}$ par l'isomorphisme $i$, la suite exacte $(*)$ devient ainsi

$$(**) \qquad 0 \to p\mathrm{M} \to \mathrm{M} \xrightarrow{p} p\mathrm{M} \to 0.$$

Alors, si $pm = 0$, $m$ appartient au noyau de $\mathrm{M} \xrightarrow{p} p\mathrm{M}$, donc à l'image de l'injection $p\mathrm{M} \to \mathrm{M}$ et il existe $m' \in \mathrm{M}$ tel que $m = pm'$.

(3)⇒(1). — Un $(\mathbf{Z}/p^2\mathbf{Z})$-module de type fini est un $\mathbf{Z}$-module de type fini annulé par $p^2$. Si $(d_1, \dots, d_r)$ sont les facteurs invariants de M, $d_r$ divise $p^2$, si bien que ces facteurs sont $p$ ou $p^2$.

Si M n'est pas libre, $d_1 = p$. L'élément $m = (\mathrm{cl}(1), 0, \dots, 0)$ est annulé par $p$ mais il n'appartient pas à $p\mathrm{M}$. (Si $m' = (\mathrm{cl}(a_1), \dots, \mathrm{cl}(a_r))$, $pm' = (p\,\mathrm{cl}(a_1), \dots, p\,\mathrm{cl}(a_r))$, on doit avoir $p\,\mathrm{cl}(a_1) = \mathrm{cl}(1)$ ce qui est impossible.) C'est une contradiction et M est un A-module libre.

*Solution de l'exercice 11.5.7.* — Une $k$-algèbre est d'abord un $k$-module. C'est bien le cas pour $A \otimes_k B$.

Elle est ensuite munie d'un produit. Il faut donc vérifier qu'il existe une application

$$(A \otimes_k B)^2 \to (A \otimes_k B)$$

bilinéaire telle que $(a \otimes b, a' \otimes b') \mapsto (aa') \otimes (bb')$. Pour cela, il suffit de vérifier que l'application

$$A \times B \times A \times B \to A \otimes_k B$$

telle que $(a, b, a', b') \mapsto (aa') \otimes (bb')$ est quadri-linéaire. Les bilinéarités par rapport aux deux premières variables d'une part et aux deux dernières variables d'autre part nous permettront d'en déduire une application bilinéaire. Or, c'est évident.

Enfin, il faut vérifier que cette application bilinéaire définit une structure d'anneau. La commutativité est claire sur les tenseurs décomposés, donc par linéarité, ce produit est commutatif. L'élément 0 est 0, l'unité est $1 \otimes 1$. (On a bien $(1 \otimes 1)(a \otimes b) = a \otimes b$ pour tout $a \in A$ et tout $b \in B$, donc par linéarité, $(1 \otimes 1)v = v$ pour tout $v \in A \otimes_k B$.) Enfin, on vérifie l'associativité sur les tenseurs décomposés :

$$\begin{aligned}\big((a \otimes b) \cdot (a' \otimes b')\big) \cdot (a'' \otimes b'') &= (aa' \otimes bb') \cdot (a'' \otimes b'') \\ &= (aa'a'') \otimes (bb'b'') \\ &= (a \otimes b) \cdot (a'a'' \otimes b'b'') \\ &= (a \otimes b) \cdot big\big((a' \otimes b') \cdot (a'' \otimes b'')\big).\end{aligned}$$

*Solution de l'exercice 11.5.8.* — D'après la proposition 11.2.3, on a

$$(A/I) \otimes (A/J) \simeq (A/I)/J(A/I) \simeq A/(I+J).$$

On laisse vérifier que

$$\mathrm{cl}(a) \otimes \mathrm{cl}(b) \mapsto \mathrm{cl}(ab)$$

et

$$\mathrm{cl}(a) \mapsto \mathrm{cl}(a) \otimes 1$$

définissent deux homomorphismes entre $(A/I) \otimes (A/J)$ et $A/(I+J)$ récoproques l'un de l'autre. Ce sont en outre des homomorphismes d'anneaux car $\mathrm{cl}(a) \cdot \mathrm{cl}(b) = \mathrm{cl}(ab)$ a pour image

$$\begin{aligned}\mathrm{cl}(ab) \otimes 1 &= (\mathrm{cl}(a) \cdot \mathrm{cl}(b)) \otimes (1 \cdot 1) \\ &= (\mathrm{cl}(a) \otimes 1) \cdot (\mathrm{cl}(b) \otimes 1)\end{aligned}$$

qui est le produit dans $(A/I) \otimes (A/J)$ des images de $\mathrm{cl}(a)$ et $\mathrm{cl}(b)$.

*Solution de l'exercice 11.5.9.* — **a)** Soient $(m_1,\dots,m_r)$ et $(n_1,\dots,n_s)$ des générateurs de M et N. On va prouver que les $m_i\otimes n_j$ engendrent $M\otimes_A N$. Comme $M\otimes N$ est engendré par les tenseurs décomposés, il suffit de prouver qu'un tel $m\otimes n$ est engendré par les $m_i\otimes n_j$. En effet, si $m=\sum a_i m_i$ et $n=\sum b_j n_j$, on a

$$m\otimes n=(\sum a_i m_i)\otimes(\sum b_j n_j)=\sum a_i b_j m_i\otimes n_j.$$

**b)** Comme N est de type fini, il existe $n\geq 1$ et un homomorphisme surjectif $A^n\to N$. Alors, l'homomorphisme

$$\mathrm{Id}_M\otimes p : M\otimes A^n=M^n\to M\otimes N$$

est surjectif. Comme M est noethérien, $M^n$ est noethérien, et $M\otimes N$ est noethérien comme quotient d'un module noethérien.

**c)** On change juste le mot « noethérien » par le mot « artinien » dans la question précédente.

**d)** Supposons M simple. Alors, $M=A/\mathfrak{m}$, pour un idéal maximal $\mathfrak{m}$ de A. Cela implique que $M\otimes N\simeq N/\mathfrak{m}N$ est un quotient de N, donc est de longueur finie $\leq \ell_A(N)$.

Raisonnons alors par récurrence sur la longueur de M. On vient de traiter le cas de longueur 1. Soit $M_1\subset M$ un sous-module de M tel que $M/M_1$ soit simple. Après tensorisation par M, la suite exacte

$$0\to M_1\to M\to (M/M_1)\to 0$$

fournit une suite exacte

$$M_1\otimes N\to M\otimes N\to (M/M_1)\otimes N\to 0.$$

Il en résulte que la longueur de $M\otimes N$ est inférieure ou égale à la somme des longueurs des extrémit'es. D'après le cas simple, la longueur de $(M/M_1)\otimes N$ est inférieure à $\ell(N)$, tandis que par récurrence, celle de $M_1\otimes N$ est inférieure à $\ell(M_1)\ell(N)$. On a ainsi

$$\ell_A(M\otimes N)\leq \ell(M_1)\ell(N)+\ell(N)=\ell(M)\ell(N)$$

puisque $\ell(M)=\ell(M_1)+1$.

*Solution de l'exercice 11.5.10.* — Soit $n=\dim_{A/\mathfrak{m}} M/\mathfrak{m}M$ et choisissons $e_1,\dots,e_n$ une base de cet espace vectoriel. Soit $m_i\in M$ dont $e_i$ est la classe et $\varphi : A^n\to M$ l'homomorphisme défini par $(a_1,\dots,a_n)\mapsto a_1m_1+\cdots+a_nm_n$.

Par construction, on a $\mathrm{Im}(\varphi)+\mathfrak{m}M=M$. Comme M est de type fini, le lemme de Nakayama implique que $\mathrm{Im}(\varphi)=M$. Donc $\varphi$ est surjective.

D'autre part, $\varphi_K : K^n\to M\otimes_A K$ est une application K-linéaire surjective de K-espaces vectoriels de même dimension. Elle est donc injective. Comme $\mathrm{Ker}\,\varphi\subset\mathrm{Ker}\,\varphi_K$, $\varphi$ est injective.

Par suite, $\varphi$ est un isomorphisme et $M\simeq A^n$.

# 12 Modules, II

## 12.1. Longueur

Définition 12.1.1. — *Soit* A *un anneau. On dit qu'un* A*-module non nul est simple si ses seuls sous-modules sont* 0 *et lui-même.*

*Exemples 12.1.2.* — a) Le module nul n'est pas simple.

b) Si A est un corps et M un A-espace vectoriel simple non nul. toute droite de M est égale à M, donc M est de dimension 1.

c) Soit A un anneau et I un idéal de A. Dans l'identification entre A-modules annulés par I et (A/I)-modules, sous-A-modules et sous-(A/I)-modules se correspondent. Par suite, un A-module annulé par I est simple si et seulement si il est simple en tant que (A/I)-module.

d) Si $\mathfrak{m}$ est un idéal maximal de A, A/$\mathfrak{m}$ est un (A/$\mathfrak{m}$)-espace vectoriel de dimension 1, donc est simple comme (A/$\mathfrak{m}$)-module, donc aussi comme A-module.

Proposition 12.1.3. — *Soit* A *est un anneau et* M *un* A*-module simple. Alors, l'annulateur de* M *est un idéal maximal de* A *et* $\mathrm{M} \simeq \mathrm{A}/\operatorname{Ann}(\mathrm{M})$.

*Démonstration.* — Soit $m$ un élément non nul de M et soit $f$ l'homomorphisme $\mathrm{A} \to \mathrm{M}$ défini par $f(a) = am$. Comme $m \neq 0$, $\operatorname{Im} f$ est un sous-module non nul de M. Puisque M est simple, $\operatorname{Im} f = \mathrm{M}$ et $f$ est surjectif. Ainsi, $\mathrm{M} \simeq \mathrm{A}/\operatorname{Ann}(m)$.

Montrons maintenant que $\operatorname{Ann}(m)$ est un idéal maximal de A. Tout idéal I de A contenant $\operatorname{Ann}(m)$ définit un sous-module $\mathrm{I}/\operatorname{Ann}(m)$ de $\mathrm{A}/\operatorname{Ann}(m)$, donc un sous-module de M (en l'occurrence le sous-module IM). Comme M est simple, ou bien $\mathrm{I} = \operatorname{Ann}(m)$ ou bien $\mathrm{I} = \mathrm{A}$, ce qui signifie que $\operatorname{Ann}(m)$ est un idéal maximal de A.

Enfin, tout élément de M étant multiple de $m$, $\operatorname{Ann}(m) \subset \operatorname{Ann}(\mathrm{M})$, d'où l'égalité et le fait que Ann(M) est un idéal maximal de A. □

DÉFINITION 12.1.4. — *Soit* A *un anneau. La longueur d'un* A*-module* M *est la borne supérieure de l'ensemble des entiers* $n$ *tels qu'il existe une suite* $M_0 \subsetneq M_1 \cdots \subsetneq M_n$ *strictement croissante de sous-*A*-modules de* M*. On la note* $\ell_A(M)$ *ou* $\ell(M)$.

*Exemple 12.1.5.* — a) Si M est un A-module simple, sa longueur est 1 puisque la seule suite strictement croissante de sous-modules de M est $0 \subset M$.

b) Réciproquement, un A-module de longueur 1 est simple. Tout sous-module de N de M qui est distinct de 0 et de M fournit en effet une suite $0 \subsetneq N \subsetneq M$ de longueur 2.

c) Si A est un corps, suite strictement croissante de sous-modules se traduit en suite de sous-espaces vectoriels emboîtés. À chaque fois, la dimension augmente au moins de 1. Par suite, la longueur d'un module sur un corps est sa dimension en tant qu'espace vectoriel.

d) L'anneau $\mathbf{Z}$ n'est pas un $\mathbf{Z}$-module de longueur finie puisque l'on a de suites strictement croissantes arbitrairement longues d'idéaux de $\mathbf{Z}$ :

$$2^n\mathbf{Z} \subset 2^{n-1}\mathbf{Z} \subset \cdots \subset \mathbf{Z}.$$

e) Si I est un idéal de A, un A-module M annulé par I a même longueur (éventuellement infinie) en tant que A-module qu'en tant que A/I-module.

PROPOSITION 12.1.6. — *Soit* A *un anneau. Soit* M *un* A*-module et* N *un sous-module de* N*. Si deux des modules* M, N *et* M/N *sont de longueur finie, le troisième l'est aussi et on a l'égalité*

$$\ell_A(M) = \ell_A(N) + \ell_A(M/N).$$

*Démonstration.* — Si $N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_a$ et $M_0/N \subsetneq \cdots \subset M_b/N$ sont des chaînes de sous-modules de N et M/N respectivement,

$$N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_a \subsetneq M_1 \subsetneq \cdots \subsetneq M_b$$

est une chaîne de sous-modules de M de longueur $a+b$, d'où, avec la convention habituelle $\infty + n = +\infty$, l'inégalité $\ell(M) \geq \ell(N) + \ell(M/N)$.

En particulier, si M est de longueur finie, N et M/N aussi. Réciproquement, on suppose que N et M/N sont de longueur finie et on veut prouver que M est de longueur finie égale à $\ell(N)+\ell(M/N)$. Soit donc $M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_a$ une chaîne de sous-A-modules de M. On rappelle (ce fait est établi dans la démonstration de la proposition 7.2.5) que si $M' \subset M''$ sont deux sous-A-modules de M tels que $M' \cap N = M'' \cap N$ et $M' + N = M'' + N$, alors $M' = M''$. Par suite, pour tout $i$, au moins une des deux inclusions

$$M_i \cap N \subset M_{i+1} \cap N \quad \text{et} \quad M_i + N \subset M_{i+1} + N$$

est stricte, ce qui implique que $\ell(N) + \ell(M/N) \geq a$. Autrement dit, prenant la borne supérieure sur $a$, $\ell(N) + \ell(M/N) \geq \ell(M)$ et la proposition est démontrée. □

PROPOSITION 12.1.7. — *Soit* A *un anneau,* S *une partie multiplicative de* A *et soit* M *un* A*-module de longueur finie. Alors,* $S^{-1}M$ *est un* $S^{-1}A$*-module de longueur finie inférieure ou égale à* $\ell_A(M)$.

*Démonstration.* — En effet, soit $N = S^{-1}M$ et soit $N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_n$ une suite strictement croissante de sous-modules de N. Posons $M_i = N_i \cap M$ (image réciproque de $N_i$ dans M par l'homomorphisme canonique $M \to S^{-1}M$). On a $M_0 \subset \cdots \subset M_n$ et comme $S^{-1}M_i = N_i$ pour tout $i$ (voir la proposition 6.5.10), les inclusions sont strictes. Ainsi, $\ell_A(M) \geq n$. En passant à la borne supérieure, on a donc $\ell_A(M) \geq \ell_{S^{-1}A}(S^{-1}M)$. □

THÉORÈME 12.1.8 (Jordan–Hölder). — *Soit* A *un anneau et soit* M *un* A*-module de longueur finie.*

*Alors si* $M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n$ *est une suite strictement croissante de sous-*A*-modules de* M *qui est maximale*[(1)]*, alors* $n = \ell_A(M)$.

*De plus, les* A*-modules* $M_i/M_{i-1}$ *(pour* $1 \leq i \leq n$*) sont des* A*-modules simples.*

*À l'ordre près, la famille* $(\mathrm{Ann}(M_i/M_{i-1}))$ *de leurs annulateurs (pour* $1 \leq i \leq n$*) ne dépend pas de la suite strictement croissante maximale choisie.*

*Démonstration.* — Dire que la suite est maximale signifie exactement trois choses :

(1) $M_0 = 0$, sinon on peut rajouter le module 0 à gauche ;

(2) $M_n = M$, sinon on peut rajouter le module M à droite ;

(3) pour tout $i \in \{1; \ldots; n\}$, le sous-module $M_i/M_{i-1}$ est simple. Il aurait sinon un sous-module de la forme $N/M_{i-1}$ avec $N \neq M_i$ et $N \neq M_{i-1}$, ce qui permettrait de rajouter le sous-module N entre $M_{i-1}$ et $M_i$.

Alors, $\ell(M_0) = 0$, $\ell(M_1) = 1$ car $M_1$ est simple et par récurrence, si $\ell(M_i) = i$, $\ell(M_{i+1}) = \ell(M_{i+1}/M_i) + \ell(M_i) = 1 + i$ puisque $M_{i+1}/M_i$ est simple. Ainsi, $\ell(M) = \ell(M_n) = n$.

Pour la dernière partie, il nous faut démontrer auparavant un lemme.

LEMME 12.1.9. — *Soit* A *un anneau,* $N \subset M$ *une inclusion de* A*-modules telle que* M/N *soit simple, isomorphe à* $A/\mathfrak{m}$ *pour un idéal maximal* $\mathfrak{m}$ *de* A.

*Soit* $\mathfrak{p}$ *un idéal maximal de* A.

*Alors,* $M_\mathfrak{p}/N_\mathfrak{p}$ *est simple si* $\mathfrak{p} = \mathfrak{m}$*, et est nul sinon.*

*Démonstration du lemme.* — D'après l'exactitude de la localisation, $M_\mathfrak{p}/N_\mathfrak{p}$ est isomorphe à $(M/N)_\mathfrak{p} = (A/\mathfrak{m})_\mathfrak{p}$, donc à $A_\mathfrak{p}/\mathfrak{m}A_\mathfrak{p}$.

(1) au sens où on ne peut pas l'allonger en rajoutant un module au milieu de la chaîne

Si $\mathfrak{m}$ n'est pas contenu dans $\mathfrak{p}$, $\mathfrak{m}A_{\mathfrak{p}} = A_{\mathfrak{p}}$ donc le quotient est nul. Dans l'autre cas, si $\mathfrak{m}$ est contenu dans $\mathfrak{p}$, comme $\mathfrak{m}$ est maximal, $\mathfrak{m} = \mathfrak{p}$ et $\mathfrak{m}A_{\mathfrak{m}}$ est l'idéal maximal de $A_{\mathfrak{m}}$. Par suite, le quotient est simple. □

Reprenons maintenant la preuve du théorème 12.1.8.

*Fin de la démonstration.* — Pour $1 \leq i \leq n = \ell(M)$, notons $\mathfrak{m}_i = \mathrm{Ann}(M_i/M_{i-1})$. Soit alors $\mathfrak{m}$ un idéal maximal de A et localisons par rapport à la partie multiplicative $A \setminus \mathfrak{m}$. On obtient une suite de sous-modules

$$M_{0,\mathfrak{m}} \subset M_{1,\mathfrak{m}} \subset \cdots \subset M_{n,\mathfrak{m}}.$$

Appliquons maintenant le lemme : dans cette suite, toutes les inclusions deviennent des égalités *sauf* les inclusions $M_{i-1,\mathfrak{m}} \subset M_{i,\mathfrak{m}}$ si $\mathfrak{m} = \mathfrak{m}_i$. Par suite, on a une formule

$$\ell_{A_{\mathfrak{m}}}(M_{\mathfrak{m}}) = \mathrm{card}\left\{i \in \{1; \ldots; n\}\,;\, \mathfrak{m} = \mathfrak{m}_i\right\}.$$

Cela prouve que les idéaux maximaux $\mathfrak{m}_i$ qui interviennent ne dépendent que de M, de même que le nombre de fois qu'ils interviennent. □

## 12.2. Modules et anneaux artiniens

Définition 12.2.1. — *Soit* A *un anneau et soit* M *un module. On dit que* M *est artinien si toute suite décroissante de sous-*A*-modules de* M *est stationnaire.*

*On dit que* A *est artinien si c'est un* A*-module artinien.*

C'est en quelque sorte la définition « duale » de celle d'un module noethérien.

*Remarque 12.2.2.* — Un A-module M est artinien si et seulement si toute famille non vide de sous-modules de M admet un élément minimal.

Les modules artiniens jouissent d'un certain nombre de propriétés analogues à celles des modules noethériens.

Proposition 12.2.3. — *Soit* A *un anneau.*

*a) Soit* M *un* A*-module et* N *un sous-module de* M*. Alors,* M *est un* A*-module artinien si et seulement* N *et* M/N *sont des* A*-modules artiniens.*

*b) Produits, puissances (finies) de modules artiniens sont artiniens.*

*c) Si* S *est une partie multiplicative de* A *et si* M *est un* A*-module artinien,* $S^{-1}M$ *est un* $S^{-1}A$*-module artinien.*

*Démonstration.* — a) Notons cl: $M \to M/N$ l'homomorphisme canonique. Supposons d'abord que N et M/N sont artiniens. Soit $(M_n)$ une suite décroissante de sous-modules de M. Les suites $(M_n \cap N)$ et $(\mathrm{cl}(M_n))$ de sous-modules de N et M/N respectivement sont décroissantes, donc stationnaires. Par suite, pour $n$ assez grand, $M_n \cap N = M_{n+1} \cap N$ et $\mathrm{cl}(M_n) = \mathrm{cl}(M_{n+1})$. Puisque $M_{n+1} \subset M_n$, le

même argument qu'à la proposition 7.2.5 montre que $M_n = M_{n+1}$. La suite $(M_n)$ est ainsi stationnaire.

Réciproquement, supposons M artinien. Une suite décroissante de sous-modules de N est aussi une suite décroissante de sous-modules de M, donc est stationnaire. Ainsi, N est noethérien. Si maintenant $(P_n)$ est une suite décroissante de sous-modules de M/N, on en déduit une suite décroissante $\mathrm{cl}^{-1}(P_n)$ de sous-modules de M. Cette dernière est donc stationnaire et puisque $P_n = \mathrm{cl}(\mathrm{cl}^{-1}(P_n))$, la suite $(P_n)$ est elle-même stationnaire.

b) Si M et N sont deux A-modules artiniens, la suite exacte $0 \to M \to M \times N \to N \to 0$ montre que $M \times N$ est artinien.

Il en résulte par récurrence que si M est un A-module artinien, $M^n$ est, pour tout entier $n \geq 1$, un A-module artinien.

c) Supposons que M est un A-module artinien et notons $i\colon M \to S^{-1}M$ l'homomorphisme canonique de A-modules. Si $(P_n)$ est une suite décroissante de sous-modules de $S^{-1}M$, la suite $i^{-1}(P_n)$ est une suite décroissante de sous-modules de M. Elle est donc stationnaire. Comme $P_n = S^{-1}(i^{-1}(P_n))$, la suite $(P_n)$ est aussi stationnaire. □

THÉORÈME 12.2.4. — *Soit* A *un anneau. Un* A*-module* M *est de longueur finie si et seulement si il est artinien et noethérien.*

*Démonstration.* — Supposons M de longueur finie et considérons une suite monotone $(M_n)$ de sous-modules de M. La suite des longueurs $\ell(M_n)$ est donc monotone, minorée par 0 et majorée par $\ell(M)$. Elle est donc stationnaire. La suite $(M_n)$ est donc stationnaire. (Se rappeler que si $P \subset Q$ sont deux modules de même longueur finie, $\ell(Q/P) = \ell(Q) - \ell(P) = 0$ donc $Q/P = 0$ et $Q = P$.) Ainsi, M est à la fois artinien (en considérant des suites décroissantes) et noethérien (en considérant des suites croissantes).

Supposons maintenant que M est artinien et noethérien et montrons que M est de longueur finie.

Si $M \neq 0$, l'ensemble des sous-modules non nuls de M n'est pas vide. Comme M est artinien, il admet un élément minimal $M_1$ : c'est un sous-module de M dont le seul sous-module strict est nul. Autrement dit, $M_1$ est simple. Si $M_1 \neq M$, on peut recommencer avec $M/M_1$ et obtenir ainsi un sous-module $M_2$ de M contenant $M_1$ tel que $M_2/M_1$ est simple. On continue ainsi par récurrence en construisant une suite strictement croissante (éventuellement finie) $0 \subset M_1 \subset M_2 \subset \ldots$ de sous-modules de M tels que $M_n/M_{n-1}$ est simple pour tout entier $n$.

C'est une suite croissante de sous-modules de M et M est noethérien. Ainsi, cette suite est stationnaire, donc est finie. Cela signifie qu'il existe $n$ tel que $M_n = M$. Alors, $\ell(M) = \ell(M_n) = n$ et M est de longueur finie. □

Passons maintenant à l'étude des anneaux artiniens.

LEMME 12.2.5. — *Soit* A *un anneau artinien.*
*a) Si* A *est intègre,* A *est un corps.*
*b)* A *n'a qu'un nombre fini d'idéaux premiers, tous maximaux.*

*Démonstration.* — a) Supposons A intègre. Si $x \in \mathrm{A} \setminus \{0\}$, la suite d'idéaux $(x) \supset (x^2) \supset \dots$ est stationnaire. Il existe ainsi $n$ tel que $(x^n) = (x^{n+1})$, d'où un élément $a \in \mathrm{A}$ tel que $ax^{n+1} = x^n$. Puisque A est intègre et $x \neq 0$, on peut simplifier par $x^n$ et $ax = 1$ ; $x$ est donc inversible.

b) Supposons par l'absurde que A possède une infinité d'idéaux maximaux distincts $\mathfrak{m}_1$, $\mathfrak{m}_2$,... La suite décroissante d'idéaux

$$\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supset \dots$$

est alors stationnaire, d'où une égalité $\mathfrak{m}_1 \dots \mathfrak{m}_{n-1} = \mathfrak{m}_1 \dots \mathfrak{m}_n$ qui implique évidemment l'inclusion $\mathfrak{m}_1 \dots \mathfrak{m}_{n-1} \subset \mathfrak{m}_n$. D'après le lemme d'évitement (exercice 4.3.3), l'un des $\mathfrak{m}_i$ pour $i < n$ est contenu dans $\mathfrak{m}_n$, ce qui contredit le fait que $\mathfrak{m}_i$ est maximal. Ainsi, A n'a qu'un nombre fini d'idéaux maximaux.

Enfin, si $\mathfrak{p}$ est un idéal premier de A, $\mathrm{A}/\mathfrak{p}$ est un anneau artinien intègre, donc un corps d'après le a). Ainsi, $\mathfrak{p}$ est maximal. □

THÉORÈME 12.2.6 (Akizuki). — *Soit* A *un anneau. Les conditions suivantes sont équivalentes :*
(1) A *est noethérien et tous ses idéaux premiers sont maximaux ;*
(2) A *est un* A*-module de longueur finie ;*
(3) A *est artinien.*

*Démonstration.* — D'après le théorème 12.2.4, la condition (2) implique que A est à la fois artinien et noethérien, d'où l'assertion (3) et la première partie de (1).

D'autre part, supposant (3), le lemme précédent affirme que tout idéal premier de A est maximal. En particulier, (2)⇒(3) et (2)⇒(1).

Supposons (1) et montrons (2), c'est-à-dire que A est de longueur finie. Raisonnons par l'absurde en supposant que A n'est pas de longueur finie et définissons $\mathscr{I}$ comme l'ensemble des idéaux I de A tels que A/I n'est pas de longueur finie. Comme $\mathrm{I} = (0)$ appartient à $\mathscr{I}$, $\mathscr{I} \neq \varnothing$. Comme A est noethérien, $\mathscr{I}$ possède un élément maximal, notons le I. Montrons que I est un idéal premier de A. En effet, soit $a$ et $b$ deux éléments de A tels que $ab \in \mathrm{I}$ mais $a \notin \mathrm{I}$. Introduisons la suite exacte

$$0 \to a(\mathrm{A}/\mathrm{I}) \to \mathrm{A}/\mathrm{I} \to \mathrm{A}/(\mathrm{I} + (a)) \to 0.$$

Comme $a \notin \mathrm{I}$, $\mathrm{I} \subsetneq \mathrm{I}+(a)$ et l'idéal $\mathrm{I}+(a)$ n'appartient pas à $\mathscr{S}$. Ainsi, $\mathrm{A}/(\mathrm{I}+(a))$ est de longueur finie. Comme A/I n'est pas de longueur finie, $a(\mathrm{A}/\mathrm{I})$ non plus. Or, $a(\mathrm{A}/\mathrm{I})$ est l'image de l'homomorphisme $\varphi\colon \mathrm{A} \to \mathrm{A}/\mathrm{I}$ défini par $x \mapsto \mathrm{cl}(ax)$. On a donc $\mathrm{A}/\operatorname{Ker}\varphi \simeq a(\mathrm{A}/\mathrm{I})$ si bien que $\mathrm{A}/\operatorname{Ker}\varphi$ n'est pas de longueur finie, soit $\operatorname{Ker}\varphi \in \mathscr{S}$. Or, le noyau de $\varphi$ est l'idéal $(\mathrm{I} : a)$ des $x \in \mathrm{A}$ tels que $ax \in \mathrm{I}$. En particulier, il contient I. Ainsi, nécessairement, $\mathrm{I} = (\mathrm{I} : a)$. Comme $ab \in \mathrm{I}$, $b \in (\mathrm{I} : a)$, et donc $b \in \mathrm{I}$. Finalement, I est un idéal premier de A.

Par hypothèse, I est donc maximal. Alors, A/I est un A-module simple, donc de longueur finie, ce qui est une contradiction. Il en résulte que A est de longueur finie.

Il reste à montrer qu'un anneau artinien est de longueur finie comme A-module. Soit $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ les idéaux maximaux de A, en nombre fini d'après le lemme précédent. Introduisons l'idéal

$$\mathrm{I} = \mathfrak{m}_1 \ldots \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n.$$

(C'est le radical de Jacobson de A.) La suite $\mathrm{I} \supset \mathrm{I}^2 \supset \ldots$ étant stationnaire, il existe un entier $s$ tel que $\mathrm{I}^s = \mathrm{I}^{s+1}$. On va montrer que $\mathrm{I}^s = 0$.

Soit donc $\mathrm{J} = (0 : \mathrm{I}^s)$ l'ensemble des $a \in \mathrm{A}$ tels que $a\mathrm{I}^s = 0$. Si $\mathrm{J} \neq \mathrm{A}$, comme A est artinien, il existe un plus petit idéal $\mathrm{J}' \subset \mathrm{A}$ contenant strictement J. Soit $a \in \mathrm{J}'$ un élément non nul. On a $a\mathrm{I} + \mathrm{J} \neq a\mathrm{A} + \mathrm{J}$. Sinon, posant $\mathrm{M} = (\mathrm{A}/\mathrm{J})a$, on aurait $\mathrm{IM} = \mathrm{M}$ et, M étant de type fini, il existerait d'après le théorème de Nakayama un élément $x \in 1 + \mathrm{I}$ tel que $x\mathrm{M} = 0$. Un tel $x$ est inversible, d'où $\mathrm{M} = 0$, contrairement au fait que $a \neq 0$. L'inclusion $\mathrm{J} \subset a\mathrm{I} + \mathrm{J} \subset \mathrm{J}'$ montre alors que $\mathrm{J} = a\mathrm{I} + \mathrm{J}$, soit $a\mathrm{I} \subset \mathrm{J}$. Pour tout $b \in \mathrm{I}$, on a $ab \in \mathrm{J}$, c'est-à-dire $ab\mathrm{I}^s = 0$ et donc $a\mathrm{I}^{s+1} = 0$. Comme $\mathrm{I}^s = \mathrm{I}^{s+1}$, $a\mathrm{I}^s = 0$ et $a \in \mathrm{J}$. Ainsi, $\mathrm{J}' = \mathrm{J}$, ce qui est absurde ; nous avons donc prouvé que $\mathrm{J} = \mathrm{A}$, c'est-à-dire $\mathrm{I}^s = 0$.

Dans la suite décroissante d'idéaux

$$\mathrm{A} \supset \mathfrak{m}_1 \supset \cdots \supset \mathfrak{m}_1 \ldots \mathfrak{m}_n = \mathrm{I} \supset \mathrm{I}\mathfrak{m}_1 \supset \mathrm{I}\mathfrak{m}_1\mathfrak{m}_2 \supset \ldots \supset \mathrm{I}^2 \supset \mathrm{I}^2\mathfrak{m}_1 \supset \cdots \supset \mathrm{I}^s = 0$$

chaque quotient successif est un A-module artinien de la forme $\mathrm{M}/\mathfrak{m}\mathrm{M}$. C'est ainsi un espace vectoriel sur le corps $\mathrm{A}/\mathfrak{m}$, nécessairement de dimension finie. Par suite, la longueur de chaque quotient successif est finie et A est de longueur finie comme A-module. □

*Remarque 12.2.7.* — Voici une autre démonstration de l'implication (1)⇒(2). On étblira au paragraphe suivant (théorème 12.3.11) que si A est un anneau noethérien, il existe une suite d'idéaux

$$0 \subset \mathrm{I}_n \subset \mathrm{I}_{n-1} \subset \cdots \subset \mathrm{I}_1 \subset \mathrm{I}_0 = \mathrm{A}$$

où pour tout $k$, $\mathrm{I}_k/\mathrm{I}_{k+1} \simeq \mathrm{A}/\mathfrak{p}_k$ pour un certain idéal premier $\mathfrak{p}_k$. Si la condition (1) du théorème est vérifiée, $\mathfrak{p}_k$ est un idéal maximal. Par suite, les quotients $\mathrm{I}_k/\mathrm{I}_{k+1}$ sont simples et A est de longueur finie (égale à $n$) comme A-module.

## 12.3. Support et idéaux associés

DÉFINITION 12.3.1. — *Soit* A *un anneau et soit* M *un* A*-module. Le* support *de* M *est l'ensemble des idéaux premiers* $\mathfrak{p}$ *de* A *tels que* $\mathrm{M}_\mathfrak{p} \neq 0$. *On le note* $\mathrm{supp}(\mathrm{M})$.

THÉORÈME 12.3.2. — *Soit* A *un anneau et soit* M *un* A*-module.*

*a) Si* $\mathrm{M} \neq 0$, *alors* $\mathrm{supp}(\mathrm{M}) \neq \varnothing$.

*b) Si* $\mathfrak{p} \in \mathrm{supp}(\mathrm{M})$, *alors* $\mathfrak{p}$ *contient* $\mathrm{Ann}(\mathrm{M})$.

*c) Réciproquement, si* M *est de type fini,* $\mathrm{supp}(\mathrm{M})$ *est l'ensemble des idéaux premiers de* A *qui contiennent* $\mathrm{Ann}(\mathrm{M})$.

*Démonstration.* — a) Supposons que $\mathrm{supp}(\mathrm{M}) = \varnothing$. Ainsi, pour tout $m \in \mathrm{M}$ et tout idéal premier $\mathfrak{p} \subset \mathrm{A}$, l'image $m/1$ de $m$ dans $\mathrm{M}_\mathfrak{p}$ est nulle. Cela signifie qu'il existe $a \in \mathrm{A} \setminus \mathfrak{p}$ tel que $am = 0$. Autrement dit, l'idéal $\mathrm{Ann}(m)$ annulateur de $m$ n'est pas contenu dans $\mathfrak{p}$. Il n'est *a fortiori* contenu dans aucun maximal de A donc est égal à A. On a donc $m = 1m = 0$. Ainsi, $\mathrm{M} = 0$.

b) On raisonne par contraposition. Soit $\mathfrak{p}$ un idéal premier de A ne contenant pas $\mathrm{Ann}(\mathrm{M})$ et soit $a \in \mathrm{A} \setminus \mathfrak{p}$ tel que $a\mathrm{M} = 0$. On a donc $\mathrm{M}_\mathfrak{p} = 0$, si bien que $\mathfrak{p}$ n'appartient pas au support de M.

c) Soit $(m_1; \ldots; m_n)$ une famille fini d'élément de M qui engendre M. Remarquons que l'on a

$$\mathrm{Ann}(\mathrm{M}) = \mathrm{Ann}(m_1) \cap \cdots \cap \mathrm{Ann}(m_n).$$

L'inclusion $\subset$ est évidente et réciproquement, si $a \in \mathrm{Ann}(m_i)$ pour tout $i$, $a$ annule toute combinaison linéaire des $m_i$, donc tout M. Soit $\mathfrak{p}$ un idéal premier de A tel que $\mathrm{M}_\mathfrak{p} = 0$. Par exactitude de la localisation (proposition 6.5.8), $\mathrm{M}_\mathfrak{p}$ est engendré par les images $m_i/1$ des $m_i$ dans $\mathrm{M}_\mathfrak{p}$. Ainsi, pour tout $i$, on a $m_i/1 = 0$ dans $\mathrm{M}_\mathfrak{p}$. Cela signifie qu'il existe pour tout $i$ un élément $a_i \in \mathrm{A} \setminus \mathfrak{p}$ tel que $a_i m_i = 0$. Alors, posons $a = \prod a_i$. On a $am_i = 0$ pour tout $i$ donc $a \in \mathrm{Ann}(\mathrm{M})$ et comme $\mathfrak{p}$ est premier, $a \notin \mathfrak{p}$. Ainsi, $\mathrm{Ann}(\mathrm{M})$ n'est pas contenu dans $\mathfrak{p}$. □

*Exercice 12.3.3.* — Soit A un anneau et soit M un A-module. Montrer que $\mathrm{M} = 0$ si et seulement si pour tout idéal maximal $\mathfrak{m}$ de A, on a $\mathrm{M}_\mathfrak{m} = 0$.

PROPOSITION 12.3.4. — *Soit* A *un anneau et considérons une suite exacte de* A*-modules*

$$0 \to \mathrm{M}' \to \mathrm{M} \to \mathrm{M}'' \to 0.$$

*Alors, on a* $\mathrm{supp}(\mathrm{M}) = \mathrm{supp}(\mathrm{M}') \cup \mathrm{sup}(\mathrm{M}'')$.

*Démonstration.* — Par exactitude de la localisation, on a pour tout idéal premier $\mathfrak{p}$ de A une suite exacte

$$0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0.$$

Ainsi, $M_{\mathfrak{p}} = 0$ si et seulement si $M'_{\mathfrak{p}} = M''_{\mathfrak{p}} = 0$, autrement dit

$$\mathfrak{p} \notin \operatorname{supp}(M) \qquad \Leftrightarrow \qquad \mathfrak{p} \notin \operatorname{supp}(M') \cup \operatorname{supp}(M''),$$

c'est-à-dire $\operatorname{supp}(M) = \operatorname{supp}(M') \cup \operatorname{sup}(M'')$. □

Définition 12.3.5. — *Soit* A *un anneau et* M *un* A*-module. On dit qu'un idéal premier* $\mathfrak{p}$ *de* A *est* associé *à* M *s'il existe un élément* $m \in M$ *tel que* $\mathfrak{p} = \operatorname{Ann}(m)$.

*L'ensemble des idéaux associés à* M *est noté* $\operatorname{Ass}_A(M)$.

*Remarque 12.3.6.* — Dire que $\mathfrak{p} = \operatorname{Ann}(m)$ signifie aussi que l'homomorphisme $A \to M$ tel que $a \mapsto am$ induit une injection $A/\mathfrak{p} \hookrightarrow M$, autrement dit que $A/\mathfrak{p}$ est (isomorphe à) un sous-module de M.

*Exemple 12.3.7.* — Si A est un anneau et $\mathfrak{p}$ un idéal premier de A, $\operatorname{Ass}_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$.

En effet, notons $\mathrm{cl}\colon A \to A/\mathfrak{p}$ la surjection canonique. Si $x \in A$, calculons l'annulateur de $\mathrm{cl}(x)$ dans A. Si $x \in \mathfrak{p}$, $\mathrm{cl}(x) = 0$ donc $\operatorname{Ann}(\mathrm{cl}(x)) = A$. Supposons maintenant que $\mathrm{cl}(x) \neq 0$, c'est-à-dire $x \notin \mathfrak{p}$. Si $a\,\mathrm{cl}(x) = 0$, cela signifie $\mathrm{cl}(ax) = 0$ donc $ax \in \mathfrak{p}$. Comme $x \notin \mathfrak{p}$, $a \in \mathfrak{p}$ et $\operatorname{Ann}(\mathrm{cl}(x)) = \mathfrak{p}$. Ainsi, le seul idéal premier de A qui est l'annulateur d'un élément non nul de $A/\mathfrak{p}$ est justement $\mathfrak{p}$.

Proposition 12.3.8. — *Soit* A *un anneau et* M *un* A*-module non nul. Alors, tout élément maximal parmi les idéaux de la forme* $\operatorname{Ann}(x)$*, avec* $x \in M \setminus \{0\}$ *est premier et est donc un idéal associé à* M.

*Démonstration.* — Soit I un idéal maximal parmi les idéaux de la forme $\operatorname{Ann}(x)$ avec $x \in M$, $x \neq 0$. Soit $x \in M$ tel que $I = \operatorname{Ann}(x)$. Soit $a \notin I$, de sorte que $ax \neq 0$. L'annulateur de $ax$ est un idéal de A qui contient I. Puisque I est supposé maximal parmi les idéaux qui sont les annulateurs d'un élément non nul, $\operatorname{Ann}(ax) = I$. Ainsi, si $ab \in I$, c'est-à-dire $abx = 0$ ou encore $b \in \operatorname{Ann}(ax)$, on a $b \in I$, ce qui montre bien que I est premier. □

Corollaire 12.3.9. — *Soit* A *un anneau noethérien et* M *un* A*-module non nul. Un élément* $a \in A$ *est diviseur de zéro dans* M *si et seulement s'il appartient à un des idéaux associés à* M.

*En particulier,* $\operatorname{Ass}_A(M) \neq \varnothing$ *:* M *possède au moins un idéal premier associé.*

*Démonstration.* — Si $a \in A$ annule un élément non nul $x$ de M. Considérons l'ensemble $\mathscr{S}$ des idéaux de A de la forme $\operatorname{Ann}(y)$ pour $y \in M \setminus \{0\}$ et soit $\mathscr{S}_a \subset \mathscr{S}$ ceux qui contiennent $a$. Comme toute famille (non vide) d'idéaux d'un

anneau noethérien admet un élément maximal, $\mathscr{S}_a$ admet un élément maximal I, lequel est aussi un élément maximal de $\mathscr{S}$.

D'après la proposition précédente, I est un idéal premier associé à M ; il contient $a$.

Réciproquement, si $\mathfrak{p}$ est un idéal premier associé à M, soit $x \in \mathrm{M}$ tel que $\mathfrak{p} = \mathrm{Ann}(x)$. En particulier, $x \neq 0$. Si $a \in \mathfrak{p}$, on a $ax = 0$, ce qui prouve que $a$ est diviseur de zéro dans M. □

PROPOSITION 12.3.10. — *Soit* A *un anneau noethérien et* M *un* A*-module de type fini. Si* S *est une partie multiplicative de* A *(ne contenant pas* 0*) et* $\mathfrak{p}$ *un idéal premier de* A *ne rencontrant pas* S*, alors*

$$\mathfrak{p} \in \mathrm{Ass}_{\mathrm{A}}(\mathrm{M}) \quad \textit{si et seulement si} \quad \mathfrak{p}(\mathrm{S}^{-1}\mathrm{A}) \in \mathrm{Ass}_{\mathrm{S}^{-1}\mathrm{A}}(\mathrm{S}^{-1}\mathrm{M}).$$

*Démonstration.* — Supposons que $\mathfrak{p}$ est associé à M. Il existe donc un homomorphisme injectif $\varphi\colon \mathrm{A}/\mathfrak{p} \hookrightarrow \mathrm{M}$. Localisons cet homomorphisme par rapport à la partie multiplicative S. D'après l'exactitude de la localisation, on en déduit un homomorphisme injectif $\mathrm{S}^{-1}(\mathrm{A}/\mathfrak{p}) \hookrightarrow \mathrm{S}^{-1}\mathrm{M}$. Comme $\mathrm{S}^{-1}(\mathrm{A}/\mathfrak{p})$ est isomorphe à $\mathrm{S}^{-1}\mathrm{A}/\mathrm{S}^{-1}\mathfrak{p}$, $\mathrm{S}^{-1}\mathfrak{p}$ est un idéal premier de $\mathrm{S}^{-1}\mathrm{A}$ associé à $\mathrm{S}^{-1}\mathrm{M}$.

Réciproquement, supposons que $\mathrm{S}^{-1}\mathfrak{p}$ est associé à $\mathrm{S}^{-1}\mathrm{M}$. Soit $m \in \mathrm{M}$ et $s \in \mathrm{S}$ tel que $\mathrm{Ann}(m/s) = \mathrm{S}^{-1}\mathfrak{p}$. Comme $s$ est inversible dans S, on a en fait $\mathrm{Ann}(m/1) = \mathrm{S}^{-1}\mathfrak{p}$ et même, pour tout $t \in \mathrm{S}$, $\mathrm{Ann}(tm/1) = \mathrm{S}^{-1}\mathfrak{p}$.

Soit $\mathrm{I} = \mathrm{Ann}(m)$ l'annulateur de $m$ dans A. Si $a \in \mathrm{I}$, $(a/1)(m/1) = 0$ donc $a/1 \in \mathrm{S}^{-1}\mathfrak{p}$ si bien qu'il existe $s \in \mathrm{S}$ tel que $sa \in \mathfrak{p}$. Comme $s \in \mathrm{S}$, $s \notin \mathfrak{p}$ et $a \in \mathfrak{p}$. Ainsi, $\mathrm{I} \subset \mathfrak{p}$. De même, pour tout $s \in \mathrm{S}$, $\mathrm{Ann}(sm) \subset \mathfrak{p}$.

Si maintenant $a \in \mathfrak{p}$, $(a/1)(m/1) = 0$, donc il existe $s \in \mathrm{S}$ tel que $sam = 0$. Comme A est noethérien, $\mathfrak{p}$ est de type fini ; soit $a_1, \ldots, a_r$ des éléments de $\mathfrak{p}$ tels que $\mathfrak{p} = (a_1, \ldots, a_r)$. Soit pour $i \in \{1; \ldots; r\}$, $s_i \in \mathrm{S}$ tel que $s_i a_i m = 0$. Alors, posons $s = s_1 \ldots s_r$. On a donc $sa_i m = 0$, si bien que $a_i \in \mathrm{Ann}(sm)$ pour tout $i$, d'où l'inclusion $\mathfrak{p} \subset \mathrm{Ann}(sm)$.

En définitive, $\mathfrak{p} = \mathrm{Ann}(sm)$ et est associé à M. □

THÉORÈME 12.3.11. — *Soit* A *un anneau noethérien et soit* M *un* A*-module de type fini. Il existe alors une suite finie*

$$0 = \mathrm{M}_0 \subset \mathrm{M}_1 \subset \cdots \subset \mathrm{M}_n = \mathrm{M}$$

*de sous-modules de* M *et pour tout* $i \in \{1; \ldots; n\}$ *un idéal premier* $\mathfrak{p}_i \subset \mathrm{A}$ *tel que* $\mathrm{M}_i/\mathrm{M}_{i-1} \simeq \mathrm{A}/\mathfrak{p}_i$.

*Démonstration.* — Si $\mathrm{M} \neq 0$, il possède un idéal premier associé $\mathfrak{p}_1$. C'est l'annulateur d'un élément $x \in \mathrm{M}$, $x \neq 0$ et le sous-module $\mathrm{M}_1 = \mathrm{A}x \subset \mathrm{M}$ est isomorphe à $\mathrm{A}/\mathfrak{p}_1$. On continue avec $\mathrm{M}/\mathrm{M}_1$ qui contient un sous-module de la forme $\mathrm{A}/\mathfrak{p}_2$, d'où un sous-module $\mathrm{M}_2$ de M qui contient $\mathrm{M}_1$ et tel que $\mathrm{M}_2/\mathrm{M}_1 \simeq \mathrm{A}/\mathfrak{p}_2$.

Par récurrence, on construit ainsi une suite croissante de sous-module de M, strictement croissante tant qu'elle n'atteint pas M. Comme A est noethérien et M de type fini, cette suite est stationnaire et il existe $n$ tel que $M_n = M$. □

PROPOSITION 12.3.12. — *Soit* A *un anneau et soit* $0 \to M' \to M \to M'' \to 0$ *une suite exacte de* A*-modules. Alors, on a les inclusions*

$$\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'').$$

*Démonstration.* — L'inclusion $\mathrm{Ass}(M') \subset \mathrm{Ass}(M)$ est évidente : un idéal $\mathfrak{p} \in \mathrm{Ass}(M')$ est de la forme $\mathrm{Ann}(x)$ avec $x \in M'$. L'annulateur de $x$ vu comme élément de M est encore égal à $\mathfrak{p}$, d'où $\mathfrak{p} \in \mathrm{Ass}(M)$.

Soit maintenant $\mathfrak{p} = \mathrm{Ann}(x) \in \mathrm{Ass}(M)$. Supposons pour commencer que $Ax \cap M' = (0)$. Alors, l'annulateur de l'image $y$ de $x$ dans $M''$ est égal à $\mathfrak{p}$ : si $ay = 0$, $ax \in M'$ d'où $ax = 0$ et $x \in \mathfrak{p}$. Cela prouve que $\mathfrak{p} \in \mathrm{Ass}(M'')$. Dans l'autre cas, si $a \in A$ est tel que $ax \in M' \setminus \{0\}$, donc en particulier $a \notin \mathfrak{p}$, l'annulateur de $ax$ est formé des $b$ tels que $abx = 0$, soit $ab \in \mathfrak{p}$, d'où $b \in \mathfrak{p}$ puisque $\mathfrak{p}$ est premier. Ainsi, $\mathfrak{p} \in \mathrm{Ass}(M')$. □

THÉORÈME 12.3.13. — *Soit* A *un anneau noethérien et soit* M *un* A*-module de type fini.*

*a)* $\mathrm{Ass}_A(M)$ *est un ensemble fini.*

*b) Tout idéal premier* $\mathfrak{p} \in \mathrm{Ass}_A(M)$ *contient* $\mathrm{Ann}(M)$.

*c) Réciproquement, si* $\mathfrak{p}$ *est un idéal premier minimal parmi ceux contenant* $\mathrm{Ann}(M)$, *alors* $\mathfrak{p} \in \mathrm{Ass}_A(M)$.

Remarquons que sous les hypothèses du théorème, l'ensemble des idéaux premiers qui contiennent $\mathrm{Ann}(M)$ est égal au support de M. On peut ainsi reformuler les points b) et c) du théorème comme suit : $\mathrm{Ass}_A(M)$ *est contenu dans* $\mathrm{supp}(M)$ *et ces deux ensembles ont mêmes éléments minimaux.*

*Démonstration.* — a) Considérons une suite de composition

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

comme en fournit le théorème 12.3.11. Notons aussi $\mathfrak{p}_i = M_i/M_{i-1}$ si $1 \leq i \leq n$.

D'après la proposition 12.3.12, $\mathrm{Ass}(M) \subset \mathrm{Ass}(M_{n-1}) \cup \mathrm{Ass}(A/\mathfrak{p}_n)$. Nous avons démontré dans l'exemple 12.3.7 que $\mathrm{Ass}(A/\mathfrak{p}_n)) = \{\mathfrak{p}_n\}$. Ainsi, on a $\mathrm{Ass}(M) \subset \mathrm{Ass}(M_{n-1}) \cup \{\mathfrak{p}_n\}$ et par récurrence sur $n$,

$$\mathrm{Ass}_A(M) \subset \{\mathfrak{p}_1; \ldots; \mathfrak{p}_n\}.$$

C'est en particulier un ensemble fini.

b) Un idéal premier associé est l'annulateur d'un élément $x \neq 0$. Il contient donc l'annulateur de M.

c) Supposons que $\mathfrak{p}$ est un idéal premier minimal parmi ceux qui contiennent $\mathrm{Ann}(M)$. On considère le module localisé $M_\mathfrak{p}$ sur l'anneau noethérien $A_\mathfrak{p}$. Remarquons que $M_\mathfrak{p} \neq 0$. Supposons par l'absurde que $M_\mathfrak{p} = 0$ et considérons une famille $(m_1, \ldots, m_r)$ de générateurs de M. Pour tout $i \in \{1; \ldots; r\}$, $m_i/1 = 0$ dans $M_\mathfrak{p}$, donc il existe $s_i \in A \setminus \mathfrak{p}$ tel que $s_i m_i = 0$. Posons $s = s_1 \ldots s_r$ ; on a $sm_i = 0$ pour tout $i$, si bien que $sM = 0$. Par suite $s \in \mathrm{Ann}(M)$. Mais comme $\mathfrak{p}$ est premier, $s \notin \mathfrak{p}$ et ceci contredit l'inclusion $\mathrm{Ann}(M) \subset \mathfrak{p}$.

Comme $M_\mathfrak{p} \neq 0$, il admet donc un idéal premier associé $\mathfrak{q}A_\mathfrak{p}$ et $\mathfrak{q}A_\mathfrak{p}$ contient l'annulateur $\mathrm{Ann}(M)A_\mathfrak{p}$ de $M_\mathfrak{p}$. L'hypothèse que $\mathfrak{p}$ est minimal parmi ceux qui contiennent $\mathrm{Ann}(M)$ implique que $\mathfrak{q} = \mathfrak{p}$. D'après la proposition 12.3.10, $\mathfrak{p}$ est associé à M. □

COROLLAIRE 12.3.14. — *Soit* A *un anneau noethérien et soit* M *un* A*-module de type fini. Alors,* M *est de longueur finie si et seulement si tous ses idéaux premiers associés sont maximaux.*

*Démonstration.* — Supposons que M est de longueur finie et considérons une suite de composition

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

de sorte que pour tout $i$, il existe un idéal maximal $\mathfrak{m}_i$ de A tel que $M_i/M_{i-1} \simeq A/\mathfrak{m}_i$. D'après la démonstration du théorème précédent, les idéaux premiers associés à M sont contenus dans l'ensemble $\{\mathfrak{m}_1; \ldots; \mathfrak{m}_n\}$. Par suite, tous les idéaux premiers associés à M sont maximaux.

Réciproquement, considérons une suite de composition

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

telle que fournie par le théorème 12.3.11, c'est-à-dire que pour tout $i$, il existe un idéal premier $\mathfrak{p}_i$ de A tel que $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$. D'après la proposition 12.3.4,

$$\mathrm{supp}(M) = \{\mathfrak{p}_1; \ldots; \mathfrak{p}_n\}.$$

D'après le théorème 12.3.13, les idéaux premiers minimaux parmi $\mathrm{supp}(M)$ sont associés à M, donc sont des idéaux maximaux de A. Nécessairement, tous les idéaux de $\mathrm{supp}(M)$ sont maximaux. Il en résulte que pour tout $i$, $M_i/M_{i-1}$ est un A-module simple et M est de longueur finie. □

## 12.4. Décomposition primaire

DÉFINITION 12.4.1. — *Soit* A *un anneau et soit* I *un idéal de* A *distinct de* A. *On dit que* I *est un idéal* primaire *s'il vérifie la condition suivante : soit $a$ et $b$ dans* A *tels que $ab \in I$ et $a \notin I$, alors il existe $n \geq 1$ tel que $b^n \in I$.*

Une autre formulation de cette condition est parfois pratique : un idéal $I \neq A$ est primaire si et seulement si pour tous $a$ et $b$ dans A tels que $ab \in I$ et $b \notin \sqrt{I}$, alors $a \in I$.

*Exercice 12.4.2.* — Un idéal $I \neq A$ d'un anneau A est primaire si et seulement si tout élément non nilpotent de A/I est simplifiable.

PROPOSITION 12.4.3. — *Le radical d'un idéal primaire est un idéal premier.*

Si I est un idéal primaire de radical $\mathfrak{p}$, on dira aussi que I est $\mathfrak{p}$*-primaire.*

*Démonstration.* — Soit A un anneau, I un idéal primaire de A et $\sqrt{I}$ son radical. Comme $I \neq A$, $\sqrt{I} \neq A$. Soit $a$ et $b$ deux éléments de A tels que $ab \in \sqrt{I}$ mais $a \notin \sqrt{I}$. Soit $n \geq 1$ tel que $(ab)^n = a^n b^n \in I$. Comme $a \notin \sqrt{I}$, $a^n \notin I$ et il existe $p \geq 1$ tel que $(b^n)^p \in I$. Ainsi, $b^{np} \in I$ et $b \in \sqrt{I}$. □

*12.4.4. Exemples.* — a) *Un idéal premier est primaire.* En effet, si $I \subset A$ est premier, on a $I = \sqrt{I}$. Par suite, si $ab \in I$ avec $b \notin \sqrt{I}$, le fait que I soit premier implique $a \in I$.

b) *Si* A *est un anneau principal, les idéaux primaires de* A *sont les puissances des idéaux premiers.* Si I est un idéal primaire et si $p \in A$ est un générateur de l'idéal premier $\sqrt{I}$, alors il existe $n \geq 1$ tel que $I = (p^n)$. Il suffit donc de montrer que l'idéal $(p^n)$ est primaire si $n \geq 1$. Or, si $ab$ est multiple de $p^n$ mais $b$ n'est pas multiple de $p$, le lemme de Gauß implique que $a$ est multiple de $p^n$, donc $a \in (p^n)$.

*Exercice 12.4.5.* — Si $f : A \to B$ est un homomorphisme d'anneaux et si I est un idéal primaire de B, $f^{-1}(I)$ est un idéal primaire de A.

*Solution.* — Soit $a$ et $b$ deux éléments de A tels que $ab \in f^{-1}(I)$ mais $b \notin \sqrt{f^{-1}(I)}$. Cela signifie $f(ab) \in I$ et $f(b) \notin \sqrt{I}$. Comme I est primaire, $f(a) \in I$, d'où $a \in f^{-1}(I)$. □

PROPOSITION 12.4.6. — *Soit* A *un anneau et soit* I *un idéal de* A *dont le radical est maximal. Alors,* I *est primaire.*

*Démonstration.* — Notons $\mathfrak{m} = \sqrt{I}$. Par hypothèse, $\mathfrak{m}$ est un idéal maximal de A. En particulier, $I \neq A$.

Soit $a$ et $b$ deux éléments de A tels que $ab \in I$ mais $b \notin \mathfrak{m}$. Comme $\mathfrak{m}$ est maximal, $b$ est inversible dans $A/\mathfrak{m}$ et il existe $c \in A$ et $x \in \mathfrak{m}$ tels que $1 = bc + x$. Alors, $x \in \sqrt{I}$, donc il existe $n \geq 1$ tel que $x^n \in I$. Comme $x = 1 - bc$, il existe $y \in A$ tel que $x^n = 1 + ybc$. Alors, $a = a(x^n - ybc) = ax^n - yc(ab) \in I$. □

*Exercice 12.4.7.* — Soit A un anneau.

a) Soit $\mathfrak{m}$ un idéal maximal de A. Si $n$ est un entier $\geq 1$, $\mathfrak{m}^n$ est un idéal primaire de A.

b) Soit $\mathfrak{p}$ un idéal premier de A et soit $n$ un entier $\geq 1$. Soit $\mathfrak{q}_n$ l'image réciproque dans A de l'idéal $\mathfrak{p}^n A_{\mathfrak{p}}$ du localisé $A_{\mathfrak{p}}$. Montrer que $\mathfrak{q}_n$ est l'ensemble des $x \in A$ tels qu'il existe $y \notin \mathfrak{p}$ vériviant $xy \in \mathfrak{p}^n$. Montrer que $\mathfrak{q}_n$ est un idéal $\mathfrak{p}$-primaire.

PROPOSITION 12.4.8. — *Soit* A *un anneau et* $\mathfrak{p}$ *un idéal premier de* A. *Soit* I *et* J *deux idéaux* $\mathfrak{p}$*-primaires de* A. *Alors,* $I \cap J$ *est un idéal* $\mathfrak{p}$*-primaire.*

*Démonstration.* — Tout d'abord, on a $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \mathfrak{p}$. D'autre part, soit $a$ et $b$ deux éléments de A tels que $ab \in I \cap J$ et $b \notin \mathfrak{p}$. Comme $I \cap J \subset I$ et comme I est $\mathfrak{p}$-primaire, $a \in I$. De même, $a \in J$. Ainsi, $a \in I \cap J$. □

PROPOSITION 12.4.9. — *Soit* A *un anneau noethérien et soit* $\mathfrak{p}$ *un idéal premier de* A. *Un idéal* I *de* A *est* $\mathfrak{p}$*-primaire si et seulement si* $\mathrm{Ass}_A(A/I) = \{\mathfrak{p}\}$.

*Démonstration.* — Supposons que I est $\mathfrak{p}$-primaire et soit $\mathfrak{q}$ un idéal premier associé à A/I. Nécessairement, $\mathfrak{q}$ contient $\mathrm{Ann}(A/I) = I$, donc $\mathfrak{q}$ contient $\sqrt{I} = \mathfrak{p}$. Soit $x \in A$ tel que $\mathfrak{q} = \mathrm{Ann}(\mathrm{cl}(x))$. Supposons par l'absurde que $\mathfrak{q} \neq \mathfrak{p}$. Il existe alors $a \in \mathfrak{q} \setminus \mathfrak{p}$ et $ax \in I$. Puisque I est supposé $\mathfrak{p}$-primaire, $x \in I$, donc $\mathrm{cl}(x) = 0$, ce qui est absurde. Par suite, $\mathrm{Ass}_A(A/I) = \{\mathfrak{p}\}$.

Réciproquement, supposons que $\mathrm{Ass}_A(A/I) = \{\mathfrak{p}\}$. Tout d'abord, $\mathfrak{p}$ est d'après le théorème 12.3.13 l'unique idéal premier minimal contenant $\mathrm{Ann}(A/I) = I$, si bien que $\mathfrak{p} = \sqrt{I}$. Soit $a$ et $b$ dans A avec $ab \in I$ mais $a \notin I$. Ainsi, $b$ est diviseur de 0 dans A/I. D'après le théorème 12.3.9, $b$ appartient à l'un des idéaux associés à A/I, autrement dit $b \in \mathfrak{p}$. Cela prouve que I est $\mathfrak{p}$-primaire. □

*12.4.10. Décomposition primaire dans les anneaux principaux.* — Soit A un anneau principal. Soit I un idéal de A et soit $n$ un générateur de I. On écrit la décomposition en facteurs premiers de $n$ en fixant des représentants des éléments irréductibles de A : $n = \prod p^{\alpha_p}$ avec $\alpha_p \geq 0$ et $\alpha_p = 0$ pour presque tout $p$. Alors, $I = (n) = \bigcap (p^{\alpha_p})$ est intersection d'idéaux primaires de A.

THÉORÈME 12.4.11. — *Dans un anneau noethérien, tout idéal est intersection d'une famille d'idéaux primaires.*

*Démonstration.* — Soit A un anneau noethérien et I un idéal de A. Remarquons que le résultat à démontrer est vrai si I est primaire. Il est aussi vrai si $I = A$ (car alors $\mathrm{Ass}_A(A/I) = \varnothing$ et l'intersection d'une famille vide d'idéaux de A est égale à A).

S'il est néanmoins faux, comme A est noethérien, l'ensemble des idéaux I pour lesquels le théorème n'est pas vérifié admet un élément maximal I. Un tel idéal I ne peut pas être primaire.

Il existe ainsi $a \notin \mathrm{I}$ et $b \notin \sqrt{\mathrm{I}}$ tels que $ab \in \mathrm{I}$. Introduisons les idéaux $\mathrm{J}_m = (\mathrm{I} : b^m)$ formés des $x \in \mathrm{A}$ tels que $b^m x \in \mathrm{I}$. Ils forment une suite croissante d'idéaux de A. Comme A est noethérien, cette suite est stationnaire et il existe $m$ tel que $\mathrm{J}_m = \mathrm{J}_{m+1}$. Montrons alors que $\mathrm{I} = \mathrm{I} + (a) \cap \mathrm{I} + (b^m)$. L'inclusion $\subset$ est claire et réciproquement, si $x \in \mathrm{I} + (a) \cap \mathrm{I} + (b^m)$, alors $x = y + az = y' + b^m z'$ avec $y$, $y' \in \mathrm{I}$ et $z$, $z' \in \mathrm{A}$. Alors, $bx = by + abz \in \mathrm{I}$. Comme $bx = by' + b^{m+1}z'$, $b^{m+1}z' \in \mathrm{I}$ et $z' \in (\mathrm{I} : b^{m+1}) = (\mathrm{I} : b^m)$ donc $b^m z' \in \mathrm{I}$. Ainsi, $x = y' + b^m z' \in \mathrm{I}$. Comme $a \notin \mathrm{I}$, $\mathrm{I} \subsetneq \mathrm{I} + (a)$ et $\mathrm{I} + (a)$ est intersection d'une famille finie d'idéaux primaires de A. De même, $b^m \notin \mathrm{I}$ donc $\mathrm{I} + (b^m)$ contient strictement I et est intersection d'une famille finie d'idéaux primaires. Il en résulte que I est intersection d'une famille finie d'idéaux primaires de A. □

Définition 12.4.12. — *Soit* A *un anneau noethérien et* I *un idéal de* A. *Une* décomposition primaire *de* I *est une expression* $\mathrm{I} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ *où les* $\mathfrak{q}_i$ *sont des idéaux primaires de* A.

*Une décomposition primaire est dite* minimale *si elle vérifie les deux propriétés :*

(1) *pour tous* $i \neq j$, $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ ;

(2) *pour tout* $j$, $\mathrm{I} \neq \bigcap_{i \neq j} \mathfrak{q}_i$.

Corollaire 12.4.13. — *Tout idéal d'un anneau noethérien admet une décomposition primaire minimale.*

*Démonstration.* — Soit I un idéal d'un anneau noethérien A et partons d'une décomposition $\mathrm{I} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ dont l'existence est affirmée par le théorème 12.4.11. D'après le lemme 12.4.8, l'intersection des $\mathfrak{q}_i$ de même radical $\mathfrak{p}$ est encore un idéal primaire, si bien qu'il existe une décomposition primaire où tous les $\sqrt{\mathfrak{q}_i}$ soient distincts.

Si on peut ôter un idéal primaire de la décomposition sans changer l'intersection, on le fait, et ainsi de suite, jusqu'à obtenir une décomposition primaire de I qui vérifie la condition (2) de la définition d'une décomposition primaire minimale. Il en existe donc. □

Théorème 12.4.14. — *Soit* A *un anneau noethérien. Soit* I *un idéal de* A *et soit* $\mathrm{I} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ *une décomposition primaire minimale de* I. *Pour tout* $i$, *notons* $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$.

*a) Alors,* $\mathrm{Ass}_{\mathrm{A}}(\mathrm{A}/\mathrm{I}) = \{\mathfrak{p}_1; \ldots; \mathfrak{p}_n\}$.

*b) Si* $\mathfrak{p}_i$ *est un idéal premier associé minimal,* $\mathfrak{q}_i = (\mathrm{I}\mathrm{A}_{\mathfrak{p}_i}) \cap \mathrm{A}$.

*Démonstration.* — a) Montrons que les idéaux $\mathfrak{p}_i$ sont associés à A/I. Il suffit bien sûr de démontrer que $\mathfrak{p}_1$ est associé à A/I. Alors, il faut établir l'existence d'un élément $a \in \mathrm{A}$ tel que $\mathfrak{p}_1 = (\mathrm{I} : a)$. Comme la décomposition est minimale, $\mathrm{I} \neq \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$ et il existe $x \in q_2 \cap \ldots$ tel que $x \notin \mathrm{I}$. Alors, $x\mathfrak{q}_1$ est contenu dans l'intersection $\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots$ donc $x\mathfrak{q}_1 \subset \mathrm{I}$. Comme A est noethérien, il

existe un entier $m$ tel que $\mathfrak{q}_1$ contienne $\mathfrak{p}_1^m$ et $x\mathfrak{p}_1^m$ est a fortiori contenu dans I. Considérons alors un entier $m$ minimal tel que $x\mathfrak{p}_1^m \subset \mathrm{I}$. Comme $x \notin \mathrm{I}$, $m \geq 1$. De plus, $x\mathfrak{p}_1^{m-1} \not\subset \mathrm{I}$ si bien qu'il existe $a \in x\mathfrak{p}_1^{m-1}$ tel que $a \notin \mathrm{I}$. Montrons que $(\mathrm{I} : a) = \mathfrak{p}_1$. Si $t \in \mathfrak{p}_1$, $ta \in x\mathfrak{p}_1^m$ donc $ta \in \mathrm{I}$ et $t \in (\mathrm{I} : a)$. Réciproquement, si $at \in \mathrm{I}$, $at \in \mathfrak{q}_1$. Puisque $a \in (x)$, $a \in \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$ et comme $a \notin \mathrm{I}$, $a \notin \mathfrak{q}_1$. Comme $\mathfrak{q}_1$ est primaire, $t \in \sqrt{\mathfrak{q}_1} = \mathfrak{p}_1$.

Nous avons ainsi démontré que $\mathfrak{p}_1$ est associé à A/I, ce qui conclut la démonstration de l'inclusion $\{\mathfrak{p}_i\} \subset \mathrm{Ass}_{\mathrm{A}}(\mathrm{A}/\mathrm{I})$.

Dans l'autre sens, soit $\mathfrak{p}$ un idéal premier associé à A/I et soit $a \in \mathrm{A}$ tel que $\mathfrak{p} = \mathrm{Ann}_{\mathrm{A}}(\mathrm{cl}(a)) = (\mathrm{I} : a)$. Si $x \in (\mathrm{I} : a)$, alors $ax \in \mathrm{I} = \bigcap \mathfrak{q}_i$, donc $ax \in \mathfrak{q}_i$ pour tout $i$. Ainsi, $x \in (\mathfrak{q}_i : a)$ pour tout $i$. Réciproquement, si $x \in \bigcap(\mathfrak{q}_i : a)$, $ax \in \mathfrak{q}_i$ pour tout $i$ donc $ax \in \mathrm{I}$. Par suite, on a

$$\mathfrak{p} = (\mathrm{I} : a) = (\mathfrak{q}_1 : a) \cap \cdots \cap (\mathfrak{q}_n : a).$$

Puisque $\mathfrak{p}$ est premier, il existe $i$ tel que $\mathfrak{p} = (\mathfrak{q}_i : a)$ (voir le lemme 12.4.15 ci-dessous). Par suite, $\mathfrak{p} \in \mathrm{Ass}_{\mathrm{A}}(\mathrm{A}/\mathfrak{q}_i) = \{\mathfrak{p}_i\}$ d'après la proposition 12.4.9.

b) On a évidemment

$$\mathrm{IA}_{\mathfrak{p}_i} = (\mathfrak{q}_1\mathrm{A}_{\mathfrak{p}_i}) \cap \cdots \cap (\mathfrak{q}_n\mathrm{A}_{\mathfrak{p}_i}).$$

Soit $j \neq i$. Par hypothèse, $\mathfrak{p}_i$ ne contient pas $\mathfrak{p}_j$, si bien qu'il existe $a \in \mathfrak{p}_j$ tel que $a \notin \mathfrak{p}_i$. Si $m \geq 1$ est tel que $a^m \in \mathfrak{q}_j$, on voit donc que $\mathfrak{q}_j\mathrm{A}_{\mathfrak{p}_i}$ contient $a^m\mathrm{A}_{\mathfrak{p}_i} = \mathrm{A}_{\mathfrak{p}_i}$. Par suite, $\mathrm{IA}_{\mathfrak{p}_i} = \mathfrak{q}_i\mathrm{A}_{\mathfrak{p}_i}$.

Posons $\mathrm{J} = (\mathfrak{q}_i\mathrm{A}_{\mathfrak{p}_i}) \cap \mathrm{A}$. D'après l'exercice 12.4.5, J est un idéal $\mathfrak{p}_i$-primaire de A. Il reste à montrer que $\mathrm{I} = \mathrm{J}$. Soit $x \in \mathrm{I}$. Son image $x/1$ dans $\mathrm{A}_{\mathfrak{p}_i}$ appartient à $\mathrm{JA}_{\mathfrak{p}_i}$. Il existe donc $s \notin \mathfrak{p}_i$ tel que $sx \in \mathrm{J}$. Comme J est $\mathfrak{p}_i$-primaire, $x \in \mathrm{J}$. La réciproque se démontre de même, d'où $\mathrm{I} = \mathrm{J}$, ce qu'il fallait démontrer. □

LEMME 12.4.15. — *Soit* A *un anneau, soit* $\mathfrak{p}$ *un idéal premier de* A *et soit* I, J *deux idéaux de* A *tels que* $\mathfrak{p} = \mathrm{I} \cap \mathrm{J}$. *Alors,* $\mathfrak{p} = \mathrm{I}$ *ou* $\mathfrak{p} = \mathrm{J}$.

*Démonstration.* — On a $\mathfrak{p} = \mathrm{I} \cap \mathrm{J} \subset \mathrm{I}$ et de même, $\mathfrak{p} \subset \mathrm{J}$. Si $\mathfrak{p} \neq \mathrm{I}$ et $\mathfrak{p} \neq \mathrm{J}$, soit $x \in \mathrm{I}$ tel que $x \notin \mathfrak{p}$ et soit $y \in \mathrm{J}$ tel que $y \notin \mathfrak{p}$. Alors, $xy \in \mathrm{I} \cap \mathrm{J}$, donc $xy \in \mathfrak{p}$, ce qui contredit le fait que $\mathfrak{p}$ est premier. □

## 12.5. Exercices

*Exercice 12.5.1.* — Soit A l'anneau $\mathbf{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et M un A-module de longueur finie. Montrer que $\ell_{\mathrm{A}}(\mathrm{M}) = \dim_{\mathbf{C}} \mathrm{M}$.

*Exercice 12.5.2.* — Soit A un anneau local noethérien d'idéal maximal $\mathfrak{m}$. Soit I un idéal de A contenu dans $\mathfrak{m}$. Montrer que A/I est un module de longueur finie si et seulement si il existe $n > 0$ tel que $\mathfrak{m}^n \subset \mathrm{I}$.

*Exercice 12.5.3.* — Soit M un A-module artinien et $u$ un endomorphisme de M Si $u$ est injectif, montrer qu'il est bijectif.

*Exercice 12.5.4.* — Soit M un A-module artinien et $\varphi$ un endomorphisme de M. Montrer qu'il existe un entier $n \geq 1$ tel que $\operatorname{Ker}\varphi^n + \operatorname{Im}\varphi^n = \mathrm{M}$.

En utilisant l'exercice 7.6.11 et sous l'hypothèse suppleméntaire que M est de longueur finie, montrer que la somme est directe.

*Exercice 12.5.5.* — Soit A un anneau.

**a)** Soit M un A-module de longueur finie.

Montrer que l'homomorphisme canonique $\mathrm{M} \to \prod_{\mathfrak{m}} \mathrm{M}_{\mathfrak{m}}$ (où le produit est sur l'ensemble des idéaux maximaux de A) est un isomorphisme de A-modules.

**b)** Si A est artinien, montrer que l'homomorphisme canonique $\mathrm{A} \to \prod_{\mathfrak{m}} \mathrm{A}_{\mathfrak{m}}$ est un isomorphisme d'anneaux : *un anneau artinien est un produit d'anneaux locaux.*

*Exercice 12.5.6.* — On dit qu'un anneau R est gradué s'il existe une décomposition $\mathrm{R} = \bigoplus_{n=0}^{\infty} \mathrm{R}_n$ où les $\mathrm{R}_n$ sont des sous-groupes de $(\mathrm{R}, +)$ vérifiant $\mathrm{R}_n \cdot \mathrm{R}_m \subset \mathrm{R}_{n+m}$.

**a)** Montrer que $\mathrm{R}_0$ est alors un sous-anneau de R. Montrer aussi que $\mathrm{I} = \bigoplus_{n\geq 1} \mathrm{R}_n$ est un idéal de R.

**b)** On suppose que $\mathrm{R}_0$ est noethérien et que R est de type fini comme $\mathrm{R}_0$-algèbre. Montrer que R est noethérien.

**c)** Réciproquement, on suppose que R est noethérien. Montrer que $\mathrm{R}_0$ est noethérien. Montrer qu'il existe des éléments $x_1, \ldots, x_r \in \mathrm{R}$, avec $x_i \in \mathrm{R}_{n(i)}$ pour un entier $n(i) \geq 1$ tels que $\mathrm{I} = (x_1, \ldots, x_r)$. Montrer alors par récurrence que pour tout $n$, $\mathrm{R}_n \subset \mathrm{R}_0[x_1, \ldots, x_r]$. En déduire que R est une $\mathrm{R}_0$-algèbre de type fini.

**d)** On se donne un anneau noethérien A et I un idéal de A. Soit R(I) l'ensemble des polynômes $\mathrm{P} \in \mathrm{A}[\mathrm{T}]$ tels que $\mathrm{P} = \sum a_n \mathrm{T}^n$ avec $a_n \in \mathrm{I}^n$. Montrer que R(I) est noethérien.

*Exercice 12.5.7.* — Soit $\mathrm{R} = \oplus \mathrm{R}_n$ un anneau gradué noethérien. Soit $\mathrm{M} = \oplus \mathrm{M}_n$ un R-module gradué (ce qui signifie $\mathrm{R}_n \mathrm{M}_m \subset \mathrm{M}_{n+m}$ pour tous $m$ et $n$.

**a)** Justifier que pour tout $n$, $\mathrm{M}_n$ est un $\mathrm{R}_0$-module. Si M est un R-module de type fini, montrer que $\mathrm{M}_n$ est un $\mathrm{R}_0$-module de type fini.

**b)** On suppose que $\mathrm{R}_0$ est un anneau artinien. Soit alors

$$\mathrm{P}_{\mathrm{M}}(t) = \sum_{n=0}^{\infty} \ell_{\mathrm{R}_0}(\mathrm{M}_n) t^n \in \mathbf{Z}[[t]].$$

On se donne des éléments $x_i \in \mathrm{R}_{d(i)}$ tels que $\mathrm{R} = \mathrm{R}_0[x_1, \ldots, x_r]$. Montrer par récurrence sur $r$ qu'il existe $f_{\mathrm{M}} \in \mathbf{Z}[t]$ telle que

$$f(t) = \mathrm{P}_{\mathrm{M}}(t) \prod_{i=1}^{r} (1 - t^{d(i)}).$$

**c)** On suppose de plus que $d(i) = 1$ pour tout $i$. Établir qu'il existe un polynôme $\varphi_{\mathrm{M}} \in \mathbf{Q}[t]$ tel que pour tout entier $n$ assez grand,

$$\ell_{\mathrm{R}_0}(\mathrm{M}_n) = \varphi_{\mathrm{M}}(n).$$

*Exercice 12.5.8.* — **a)** Si $\mathrm{M} \subset \mathrm{N}$ sont deux A-modules, montrer que les idéaux associés de M sont inclus dans ceux de N.

**b)** Donner des exemples montrant qu'il n'existe en général aucune inclusion entre les idéaux associés d'un module M et ceux d'un quotient de M.

**c)** Soit M un A-module et $\mathrm{M}_1$, $\mathrm{M}_2$ deux sous-modules tels que $\mathrm{M} = \mathrm{M}_1 + \mathrm{M}_2$. Que peut-on dire des idéaux associés de M par rapport à ceux des $\mathrm{M}_i$ ?

*Exercice 12.5.9.* — Soient A un anneau noethérien et $x \in \mathrm{A}$ un élément qui n'est ni inversible ni diviseur de zéro. Montrer que pour $n \geq 1$, $\mathrm{A}/x\mathrm{A}$ et $\mathrm{A}/x^n\mathrm{A}$ ont les mêmes idéaux associés.

*Exercice 12.5.10.* — Soit A l'anneau des fonctions continues sur $[-1; 1]$.

**a)** L'anneau A est-il intègre ? réduit ?

**b)** Montrer que l'idéal I des fonctions nulles en 0 n'est pas de type fini. Montrer que $\mathrm{I} = \mathrm{I}^2$.

**c)** Montrer que l'idéal $(x)$ n'est pas primaire.

*Exercice 12.5.11.* — Soit $\mathrm{A} = k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]/(\mathrm{XY} - \mathrm{Z}^2)$. On note $x = \mathrm{cl}(\mathrm{X})$, etc. Soit $\mathfrak{p}$ l'idéal $(x, z) \subset \mathrm{A}$.

**a)** Montrer que $\mathfrak{p}$ est premier mais que $\mathfrak{p}^2$ n'est pas primaire.

**b)** Montrer que $(x) \cap (x^2, y, z)$ est une décomposition primaire minimale de $\mathfrak{p}^2$.

*Exercice 12.5.12.* — Soit A un anneau noethérien et I un idéal de A. Soit J l'idéal $\bigcap_{n \geq 1} \mathrm{I}^n$.

**a)** En considérant une décomposition primaire de IJ, montrer que $\mathrm{J} = \mathrm{IJ}$.

**b)** En déduire que $\mathrm{J} = 0$ si et seulement si aucun élément de $1 + \mathrm{I}$ n'est diviseur de zéro dans A.

**c)** On suppose que $\mathrm{I} \neq \mathrm{A}$ et que A est ou bien local, ou bien intègre. Montrer que $\mathrm{J} = 0$.

*Exercice 12.5.13.* — Soit A un anneau noethérien. Montrer que les conditions suivantes sont équivalentes :

a) Le radical de A est nul.

b) Pour tout idéal premier $\mathfrak{p}$ dans $\mathrm{Ass}(A)$, l'anneau local $A_{\mathfrak{p}}$ est un corps.

c) Pour tout idéal premier $\mathfrak{p}$ dans $\mathrm{Ass}(A)$, l'anneau local $A_{\mathfrak{p}}$ est un anneau intègre.

(*On pourra considérer une décomposition primaire minimale de l'idéal* $(0)$.)

## 12.6. Solutions

*Solution de l'exercice 12.5.1.* — Soit

$$0 = M_0 \subset M_1 \subset \cdots \subset M_\ell = M$$

une suite de Jordan-Hölder, où $M_i/M_{i-1}$ est un A-module simple pour tout $i$. On a donc $\ell = \ell_A(M)$. D'après le théorème des zéros de Hilbert, $M_i/M_{i-1}$ est de la forme

$$A/\mathfrak{m} = A/(X_1 - \alpha_1, \ldots, X_n - \alpha_n)$$

qui est isomorphe à $\mathbf{C}$ comme $\mathbf{C}$-espace vectoriel. Ainsi,

$$\dim_{\mathbf{C}} M = \sum_{i=1}^{\ell} \dim_{\mathbf{C}}(M_i/M_{i-1}) = \ell.$$

*Solution de l'exercice 12.5.2.* — Supposons que $A/I$ est de longueur finie. Comme un sous-module de $A/I$ de de la forme $J/I$ où $J$ est un idéal de A, il existe une suite d'idéaux

$$I = J_0 \subset J_1 \subset \cdots \subset J_n = A$$

tels que pour tout $i$, $J_i/J_{i-1} \subset A/\mathfrak{m}$. (Comme A est local, il n'a qu'*un seul* idéal maximal !)

Par suite, $\mathfrak{m}$ annule $J_i/J_{i-1}$ et $\mathfrak{m}J_i \subset J_{i-1}$. Par récurrence sur $i$, il en résulte que $\mathfrak{m}^i J_i \subset I$. d'où $\mathfrak{m}^n \subset I$.

Réciproquement, supposons que $\mathfrak{m}^n \subset I$. Considérons la suite croissante d'idéaux

$$\mathfrak{m}^n + I = I \subset \mathfrak{m}^{n-1} + I \subset \cdots \subset \mathfrak{m} + I \subset A.$$

Il suffit de montrer que chacun des quotients successifs est de longueur finie. Or, $V_i = (\mathfrak{m}^{i-1}+I)/(\mathfrak{m}^i+I)$ est un A-module annulé par $\mathfrak{m}$, donc un $A/\mathfrak{m}$-espace vectoriel. Comme A est noethérien, l'idéal $\mathfrak{m}^{i-1} + I$ est de type fini, si bien que $V_i$ est un A-module de type fini, donc un $A/\mathfrak{m}$-espace vectoriel de dimension finie, donc un A-module de longueur finie, ce qu'il fallait démontrer.

*Solution de l'exercice 12.5.3.* — Les $u^n(M)$ forment une suite décroissantes de sous-modules de M. Comme M est artinien, cette suite est stationnaire. Soit $n$ le plus petit entier tel que $u^n(M) = u^{n+1}(M)$. Soit $m \in M$. Comme $u^n(M) = u^{n+1}(M)$, il existe $m' \in M$ tel que $u^n(m) = u^{n+1}(m')$. Alors, $u(m') - m$ appartient au noyau de $u^n$, donc $u(m') = m$ et $u$ est surjectif. Par suite, $u$ est bijectif.

*Solution de l'exercice 12.5.4.* — La suite des sous-modules images $\operatorname{Im}\varphi^n$ est décroissante. Il existe ainsi un entier $n$ tel que $\operatorname{Im}\varphi^n = \operatorname{Im}\varphi^{n+1} = \dots$. Montrons que $n$ convient. Soit en effet $m \in M$. Comme $\operatorname{Im}\varphi^n = \operatorname{Im}\varphi^{2n}$, on peut écrire $\varphi^n(m) = \varphi^{2n}(m')$, ce qui implique que $m - \varphi^n(m') \in \operatorname{Ker}\varphi^n$. Alors, $m \in \operatorname{Ker}\varphi^n + \operatorname{Im}\varphi^n$. Par suite, $\operatorname{Ker}\varphi^n + \operatorname{Im}\varphi^n = M$.

Si de plus M est de longueur finie, l'isomorphisme $M/\operatorname{Ker}\varphi^n \simeq \operatorname{Im}\varphi^n$ implique que $\ell(M) = \ell(\operatorname{Ker}\varphi^n) + \ell(\operatorname{Im}\varphi^n)$. La suite exacte

$$0 \to \operatorname{Ker}\varphi^n \cap \operatorname{Im}\varphi^n \to \operatorname{Ker}\varphi^n \oplus \operatorname{Im}\varphi^n \to M \to 0$$

et l'additivité des longueurs dans les suites exactes implique alors que $\operatorname{Ker}\varphi^n \cap \operatorname{Im}\varphi^n$ est de longueur 0, donc nul. La somme est donc directe.

*Solution de l'exercice 12.5.5.* — **a)** On a vu au cours de la démonstration du théorème de Jordan–Hölder pour les modules de longueur finie que les deux A-modules M et $\prod M_{\mathfrak{m}}$ ont même longueur. Il suffit donc de montrer que cet homomorphisme est, disons, injectif. Considérons donc $m \in M$ d'image nulle dans tout localisé $M_{\mathfrak{m}}$. Si $\mathfrak{m}$ est un idéal maximal, dire que $m/1 = 0$ dans $M_{\mathfrak{m}}$ signifie qu'il existe $a \notin \mathfrak{m}$ tel que $am = 0$. Par suite, l'idéal I annulateur de $m$ dans A n'est pas contenu dans $\mathfrak{m}$. Il n'est ainsi contenu dans aucun idéal maximal de A, ce qui implique $I = A$ et $m = 0$.

**b)** Cet homomorphisme est effectivement un homomorphisme d'anneaux. En tant qu'homomorphisme de A-modules, c'est le même qu'à la question précédente. Puisque A est artinien, A est de longueur finie et cet homomorphisme est donc bijectif. C'est un isomorphisme.

*Solution de l'exercice 12.5.6.* — **a)** Il est clair que $R_0$ est stable par l'addition, l'opposé et la multiplication. C'est donc un sous-anneau. De même, I est un sous-groupe abélien de R et si $x = \sum x_n \in R$ et $y = \sum y_n \in I$ (donc $y_0 = 0$), alors

$$xy = \sum_{n=0}^{\infty} \sum_{k+m=n} x_k y_m$$

et la composante de degré 0 est nulle, donc $xy \in I$. Autrement dit, I est un idéal de R.

**b)** Toute algèbre de type fini sur un anneau noethérien est un anneau noethérien.

**c)** Comme l'application $R/I \to R_0$, $[\sum x_n] \mapsto x_0$ est un isomorphisme, $R_0$ est un quotient d'un anneau noethérien, donc noethérien.

Soient $x_i$ des générateurs (en nombre fini) de I. Si $x_i = \sum_n x_{i,n}$ avec $x_{i,n} \in R_n$, on a $x_{i,n} \in I$ et les $x_{i,n}$ engendrent a fortiori I. Quitte à remplacer les $x_i$ par les $x_{i,n}$, on peut donc supposer que pour tout $i$, $x_i \in R_{n(i)}$.

Montrons par récurrence que $R_n \subset R_0[x_1, \dots, x_r]$. C'est vrai pour $n = 0$. Supposons ceci vrai pour $n - 1 \geq 0$ et soit $y \in R_n$. Comme $y \in I$, il existe des $y_i \in R$ tels que $y = \sum_{i=1}^{r} y_i x_i$. En comparant les composantes des deux membres dans $R_n$, on trouve

$$y = \sum_{i=1}^{r} y_{i,n-n(i)} x_i, \qquad y_{i,n-n(i)} \in R_{n-n(i)}.$$

Pour tout $i$, soit $n - n(i) < 0$ et $y_{i,n-n(i)} = 0$, soit $0 \leq n - n(i) < n$ et $y_{i,n-n(i)} \in R_0[x_1, \dots, x_r]$. On voit donc que $y \in R_0[x_1, \dots, x_r]$ et $R_n \subset R_0[x_1, \dots, x_r]$.

Il en résulte que $R = \bigoplus_n R_n \subset R_0[x_1, \dots, x_r]$. L'autre inclusion étant évidente, R est engendrée par les $x_i$ comme $R_0$-algèbre.

**d)** On a $R(I) = \bigoplus_n R(I)_n$, avec $R(I)_n = I^n T^n \simeq I^n$. Si I est engendré par $P_1, \dots, P_r$, on voit que R(I) est engendré par les $P_i T$ comme $R(I)_0 = k$-algèbre. Par suite, R(I) est un anneau noethérien.

*Solution de l'exercice 12.5.7.* — **a)** $M_n$ est un groupe abélien, et si $x \in R_0$, $m \in M_n$, $xm \in M_{0+n} = M_n$ donc $M_n$ est un sous-$R_0$-module de M.

Si M est un R-module de type fini, on peut en trouver des générateurs $m_1, \dots, m_r$ tels que $m_i \in M_{p(i)}$. Soient aussi des $x_i$ avec $x_i \in R_{n(i)}$ tels que $R = R_0[x_1, \dots, x_s]$. Comme $R_0$-module, $M_n$ est engendré par les

$$x_1^{a_1} \dots x_s^{a_s} m_i, \qquad a_1 n(1) + \dots + a_s n(s) + p(i) = n.$$

Cela fait un nombre fini d'éléments.

**b)** La série formelle $P_M$ a un sens car, $M_n$ étant un module de type fini sur un anneau artinien, $M_n$ est de longueur finie.

Si $r = 0$, $R = R_0$, M est engendré par $m_1, \dots, m_s$, avec $m_i \in M_{p(i)}$. Autrement dit, seuls $M_{p(1)}, \dots, M_{p(s)}$ sont non nuls et $f(t)$ est un polynôme.

Si $r \geq 1$, on considère l'homomorphisme

$$M_n \to M_{n+d(r)}, \qquad m \mapsto x_r m.$$

Son image est $x_r M_n$ ; notons $P_n$ son noyau et $Q_{n+d(r)} = M_{n+d(r)}/x_r M_n$ le conyau. Alors, $P = \bigoplus_n P_n$ est un sous-R-module de M (le noyau de $m \mapsto x_r m$), et c'est un $R[x_1, \dots, x_{r-1}]$-module gradué de type fini. De même, $Q = \bigoplus_n Q_n$ est un $R[x_1, \dots, x_{r-1}]$-module gradué de type fini. En particulier, on a des polynômes $f_P$ et $f_Q \in \mathbf{Z}[t]$ tels que

$$f_P = P_P \prod_{i=1}^{r-1} (1 - t^{d(i)}) \quad \text{et} \quad f_Q = P_Q \prod_{i=1}^{r-1} (1 - t^{d(i)}).$$

Or,

$$\ell(Q_{n+d(r)}) = \ell(M_{n+d(r)}) - \ell(x_r M_n) = \ell(M_{n+d(r)}) - \ell(M_n) + \ell(P_n)$$

si bien que

$$\begin{aligned}&\sum_n \ell(\mathrm{Q}_{n+d(r)})t^{n+d(r)}\\ &= \sum_n \ell(\mathrm{M}_{n+d(r)})t^{n+d(r)} - t^{d(r)}\sum_n \ell(\mathrm{M}_n)t^n + t^{d(r)}\sum_n \ell(\mathrm{P}_n)\\ &= \mathrm{P_M}(t) - \sum_{n<d(r)} \ell(\mathrm{M}_n)t^n - t^{d(r)}\mathrm{P_M}(t) + t^{d(r)}\mathrm{P_P}(t)\end{aligned}$$

et

$$(1-t^{d(r)})\mathrm{P_M}(t) = \mathrm{P_Q}(t) - t^{d(r)}\mathrm{P_P}(t) + \sum_{n<d(r)} (\ell(\mathrm{M}_n) - \ell(\mathrm{Q}_n))t^n.$$

Par conséquent,

$$\begin{aligned}f_\mathrm{M} &= \prod_{i=1}^{r}(1-t^{d(i)})\mathrm{P_M}(t)\\ &= \prod_{i<r}(1-t^{d(i)})\mathrm{P_Q}(t) - t^{d(r)}\prod_{i<r}(1-t^{d(i)})\mathrm{P_P}(t)\\ &\quad + \prod_{i<r}(1-t^{d(i)})\Big(\sum_{n<d(r)} (\ell(\mathrm{M}_n) - \ell(\mathrm{Q}_n))t^n\Big)\\ &= f_\mathrm{Q}(t) - t^{d(r)}f_\mathrm{P}(t) + \prod_{i<r}(1-t^{d(i)})\Big(\sum_{n<d(r)} (\ell(\mathrm{M}_n) - \ell(\mathrm{Q}_n))t^n\Big)\end{aligned}$$

est un élément de $\mathbf{Z}[t]$, ainsi qu'il fallait démontrer.

**c)** On suppose de plus $d(i) = 1$ pour tout $i$. (Remarquer au passage que c'est le cas pour $\mathrm{R} = \mathrm{R(I)}$.) Alors,

$$\mathrm{P_M}(t) = f_\mathrm{M}(t)/(1-t)^r.$$

Si $r = 0$, $\mathrm{P_M}$ est un polynôme, on a $\ell_(\mathrm{M}_n) = 0$ pour $n$ assez grand et on peut prendre $\varphi_\mathrm{M} = 0$.

Sinon, on a

$$\begin{aligned}\frac{1}{(1-t)^r} &= \frac{1}{(r-1)!}\frac{d^{r-1}}{dt^{r-1}}\frac{1}{1-t} = \frac{1}{(r-1)!}\frac{d^{r-1}}{dt^{r-1}}\sum_{n=0}^{\infty} t^n\\ &= \sum_{n=0}^{\infty}\frac{(n+1)\dots(n+r-1)}{(r-1)!}t^n\end{aligned}$$

et si $f_\mathrm{M}(t) = \sum a_p t^p$ et $n > \deg f_\mathrm{M}$,

$$\ell(\mathrm{M}_n) = \sum_{k+p=n} a_p\frac{(k+1)\dots(k+r-1)}{(r-1)!} = \sum_{p=0}^{\deg f_\mathrm{M}} a_p\frac{(n-p+1)\dots(n-p+r-1)}{(r-1)!}.$$

Cette expression est une somme finie de polynômes en $n$ donc il existe un polynôme $\varphi_\mathrm{M} \in \mathbf{Q}[t]$ tel que pour tout $n \gg 0$, $\varphi_\mathrm{M}(n) = \ell_{\mathrm{R}_0}(\mathrm{M}_n)$.

*Solution de l'exercice 12.5.8.* — **a)** Dire qu'un idéal premier $\mathfrak{p}$ est associé à M signifie qu'il existe un élément $m \in \mathrm{M}$ dont $\mathfrak{p}$ soit l'annulateur. Comme $\mathrm{M} \subset \mathrm{N}$, $\mathfrak{p}$ est l'annulateur d'un élément de N...

**b)** L'idéal $(0) \subset \mathbf{Z}$ est le seul idéal associé à $\mathbf{Z}$. L'idéal $(2)$ est en revanche associé au quotient $\mathbf{Z}/2\mathbf{Z}$. Ainsi, les idéaux associés d'un quotient ne sont pas forcément inclus dans les idéaux associés.

Dans l'autre sens, $(2)$ est un idéal associé de $\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}$, mais il n'est pas associé au quotient $\mathbf{Z}$ par le sous-module $(0)\oplus\mathbf{Z}/2\mathbf{Z}$.

**c)** On a déjà l'inclusion

$$\mathrm{Ass}_A(M_1)\cup\mathrm{Ass}_A(M_2)\subset\mathrm{Ass}_A(M).$$

L'autre inclusion n'est pas toujours vraie. Soit $M=\mathbf{Z}\oplus\mathbf{Z}$ et N le sous-module des $(2n,2n)$ pour $n\in\mathbf{Z}$. Le module M/N contient l'image $M_1$ de $\mathbf{Z}\oplus(0)$ et l'image $M_2$ de $(0)\oplus\mathbf{Z}$. En fait, $M_1$ et $M_2$ sont isomorphes à $\mathbf{Z}$. De plus, $M_1+M_2=M/N$. Les idéaux associés de $M_1$ et de $M_2$ sont réduits à l'idéal $(0)$. En revanche, M/N admet $(2)$ comme idéal associé puisque l'annulateur de l'image de $(1,1)$ est exactement l'idéal premier $(2)$.

*Solution de l'exercice 12.5.9.* — Si $A/xA$ contient un sous-module isomorphe à $A/\mathfrak{p}$, soit $m\in A$ un élément dont la classe dans $A/xA$ est d'annulateur $\mathfrak{p}$. Alors, $A/x^nA$ contient le sous-module $x^{n-1}m/x^nA$ qui est d'annulateur $\mathfrak{p}$ puisque $x$ n'est pas diviseur de 0. Autrement dit, $\mathrm{Ass}_A(A/x^nA)\supset\mathrm{Ass}_A(A/xA)$.

Dans l'autre sens, la suite exacte

$$0\to xA/x^2A\to A/x^2A\to A/xA\to 0$$

montre que les idéaux associés à $A/x^2A$ sont inclus dans la réunion de ceux de $A/xA$ et ceux de $xA/x^2A$. Comme $xA/x^2A$ est isomorphe à $A/xA$ comme A-module (multiplier par $x$), les idéaux associés à $A/x^2A$ sont inclus dans ceux de $A/xA$. Par récurrence, on prouve de même que $\mathrm{Ass}(A/x^nA)\subset\mathrm{Ass}(A/xA)$.

*Solution de l'exercice 12.5.10.* — **a)** Il n'est pas intègre : soit $f_1(x)=x+|x|$ et $f_2(x)=x-|x|$. On a $f_1(x)f_2(x)=x^2-|x|^2=0$, et pourtant, ni $f_1$ ni $f_2$ ne sont identiquement nulles sur $[-1;1]$.

En revanche, il est réduit : si $f(x)^n=0$ pour tout $x$, alors $f(x)=0$ pour tout $x$ puisque $\mathbf{R}$ est intègre. Donc $f=0$.

**b)** cf. la question b) de l'exercice 7.6.8. Soit $f:[-1;1]\to\mathbf{R}$ nulle en 0. Posons $g(x)=\sqrt{|f(x)|}$ et $h(x)=\mathrm{signe}(f(x))g(x)$. Les fonctions $f$ et $g$ sont continues, nulles en 0 et $f(x)=g(x)h(x)$ pour tout $x$. DOnc $f\in I^2$, soit $I\subset I^2$. L'autre inclusion est claire.

**c)** Il faut trouver deux fonctions $f$ et $g$ continues telles que
- $f$ ne s'écrit pas $xf_1(x)$ pour une fonction continue $f_1$ ;
- $f(x)g(x)=xh(x)$, où $h$ est continue ;
- pour aucun $n$, $g^n(x)$ n'est le produit de $x$ par une fonction continue.

On pose

$$f(x) = x \log |x/2| \quad \text{et} \quad g(x) = 1/\log |x/2|.$$

La fonction $g$ se prolonge par continuité en 0 et est donc un élément de A. De même pour $f$. On a $f(x)g(x) = x$. La fonction $\log |x/2|$ ne se prolonge pas par continuité en 0, donc $f \notin (x)$. De plus, $g(x)^n/x$ tend vers $+\infty$ quand $x \to 0+$, donc $g \notin \sqrt{(x)}$. Par conséquent, l'idéal $(x)$ n'est pas primaire.

*Solution de l'exercice 12.5.11.* — **a)** Cela revient à prouver que l'idéal $(\mathrm{X}, \mathrm{Z}, \mathrm{XY} - \mathrm{Z}^2)$ est premier dans $k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$. Or, le quotient

$$k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]/(\mathrm{X}, \mathrm{Z}, \mathrm{XY} - \mathrm{Z}^2) \simeq k[\mathrm{Y}, \mathrm{Z}]/(\mathrm{Z}, \mathrm{Z}^2) \simeq k[\mathrm{Y}]$$

est intègre.

Des générateurs de $(\mathrm{X}, \mathrm{Z}, \mathrm{XY} - \mathrm{Z}^2)^2 + (\mathrm{XY} - \mathrm{Z}^2)$ sont $\mathrm{X}^2$, XZ, $\mathrm{Z}^2$, $\mathrm{X}^2\mathrm{Y} - \mathrm{XZ}^2$, $\mathrm{XYZ} - \mathrm{Z}^3$, $\mathrm{X}^2\mathrm{Y}^2 + \mathrm{Z}^4 - 2\mathrm{XYZ}^2$ et $\mathrm{XY} - \mathrm{Z}^2$ dont on extrait les générateurs

$$\mathrm{X}^2, \mathrm{XZ}, \mathrm{Z}^2, \mathrm{XY}.$$

Ainsi,

$$\mathrm{A}/\mathfrak{p}^2 \simeq k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]/(\mathrm{X}^2, \mathrm{XZ}, \mathrm{Z}^2, \mathrm{XY}).$$

Dans cet anneau, Y est diviseur de 0 mais n'est pas nilpotent. Donc $\mathfrak{p}^2$ n'est pas primaire.

**b)** On a $\mathfrak{p}^2 = (x^2, xz, xy)$. Ainsi,

$$\mathfrak{p}^2 \subset (x) \quad \text{et} \quad \mathfrak{p}^2 \subset (x^2, y, z).$$

Soit d'autre par un élément de $(x) \cap (x^2, y, z)$. C'est la classe d'un polynôme $\mathrm{P} \in k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$ qui appartient à l'idéal $(\mathrm{X}^2, \mathrm{Y}, \mathrm{Z})$ et qui est multiple de X modulo $\mathrm{XY} - \mathrm{Z}^2$, soit donc

$$\mathrm{P} = \mathrm{XA} + (\mathrm{XY} - \mathrm{Z}^2)\mathrm{B} = \mathrm{X}^2\mathrm{C} + \mathrm{YD} + \mathrm{ZE}.$$

Notons $\mathrm{D} = \mathrm{XD}_1 + \mathrm{D}_0$ la division euclidienne de D par X, et de même pour B et E. On écrit ainsi

$$\begin{aligned} \mathrm{P} &= \mathrm{X}(\mathrm{XC} + \mathrm{YD}_1 + \mathrm{ZE}_1) + \mathrm{YD}_0 + \mathrm{ZE}_0 \\ &= \mathrm{X}(\mathrm{A} + \mathrm{YXB}_1 + \mathrm{YB}_0) - \mathrm{Z}^2\mathrm{B}_0, \end{aligned}$$

d'où il résulte que $\mathrm{YD}_0 + \mathrm{ZE}_0 = -\mathrm{Z}^2\mathrm{B}_0$. Ainsi,

$$\mathrm{P} = \mathrm{X}^2\mathrm{C} + \mathrm{XYD}_1 + \mathrm{XZE}_1 - \mathrm{Z}^2\mathrm{B}_0$$

appartient à l'idéal $(\mathrm{X}^2, \mathrm{XY}, \mathrm{XZ}, \mathrm{Z}^2)$ et donc

$$\mathrm{P}(x, y, z) \in (x^2, xy, xz, z^2) = (x^2, xy, xz).$$

On a ainsi l'autre inclusion, soit

$$\mathfrak{p}^2 = (x) \cap (x^2, y, z).$$

L'idéal $(x)$ est primaire : $A/(x)$ est isomorphe à $k[X,Y,Z]/(X,XY-Z^2) \simeq k[Y,Z]/(Z^2)$. Les diviseurs de zéro sont les multiples de Z, et ils sont nilpotents.

De même, $A/(x^2,y,z)$ est isomorphe à

$$k[X,Y,Z]/(X^2,Y,Z,XY-Z^2) \simeq k[X]/(X^2)$$

dont les diviseurs de zéro sont les multiples de X et donc nilpotents. Ainsi, $(x^2,y,z)$ est primaire.

Enfin, cette décomposition est minimale puisque $x$ est non nul dans $A/(x^2,y,z)$ et $z$ est non nul dans $A/(x)$.

*Solution de l'exercice 12.5.12.* — **a)** Soit $IJ = \bigcap_j \mathfrak{q}_j$ une décomposition primaire de IJ ; notons $\mathfrak{p}_j$ l'idéal premier radical de $\mathfrak{q}_j$.

On va montrer que pour tout $j$, $J \subset \mathfrak{q}_j$.

– Si $I \not\subset \mathfrak{p}_j$, soit $a \in I$ tel que $a \notin \mathfrak{p}_j$. Alors, pour tout $b \in J$, $ab \in IJ \subset \mathfrak{q}_j$. Comme $\mathfrak{q}_j$ est $\mathfrak{p}_j$-primaire et $a \notin \mathfrak{p}_j$, on a $b \in \mathfrak{q}_j$. Ainsi, $J \subset \mathfrak{q}_j$.

– Si $I \subset \mathfrak{p}_j$, soit $n$ un entier assez grand pour tout $\mathfrak{p}_j^n \subset \mathfrak{q}_j$. On a alors $I^n \subset \mathfrak{q}_j$. Puisque $J \subset I^n$, $J \subset \mathfrak{q}_j$.

Par suite, $J \subset IJ$. Comme l'autre inclusion est évidente, on a bien $J = IJ$.

**b)** Comme A est noethérien, I est de type fini et le lemme de Nakayama implique qu'il existe $a \in I$ tel que $(1+a)J = 0$. Si aucun élément de $1+I$ n'est diviseur de zéro dans A, $1+a$ n'est pas diviseur de 0 et $J = 0$.

Réciproquement, si $a \in I$ est tel que $1+a$ est diviseur de zéro dans A, soit $b \in A$, $b \neq 0$ tel que $(1+a)b = 0$. On a alors $b = -ab = a^2b = \cdots = (-a)^n b$ pour tout $n \geq 1$. Par suite, $b \in (a^n) \subset I^n$ pour tout $n$, d'où $b \in J$ qui est donc non nul.

**c)** Si A est intègre, seul 0 est diviseur de zéro. Comme $I \neq A$, $0 \notin 1+I$ et $J = 0$.

Si A est local, I est contenu dans l'idéal maximal et les éléments de $1+I$ sont inversibles dans A. Par suite, $J = 0$.

*Solution de l'exercice 12.5.13.* — Montrons a) $\Rightarrow$ b). Si le radical de A est nul, la décomposition primaire minimale de l'idéal (0) est constituée des idéaux premiers minimaux $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ de A qui sont donc les idéaux associés à A.

On a $(0) = \bigcap_j \mathfrak{p}_j$ et, si $j \in \{1,\ldots,n\}$, $\bigcap_{i\neq j} \mathfrak{p}_i \neq (0)$.

Soit $j \in \{1,\ldots,n\}$. Comme l'idéal maximal de $A_{\mathfrak{p}_j}$ est $\mathfrak{p}_j A_{\mathfrak{p}_j}$, il faut démontrer que $\mathfrak{p}_j A_{\mathfrak{p}_j} = 0$. Soit donc $x \in \mathfrak{p}_j$. Comme $\bigcap_{i\neq j} \mathfrak{p}_i \neq (0)$, choisissons un élément $y$ non nul dans cette intersection. Alors $y \notin \mathfrak{p}_j$, sinon $y$ serait nul. De plus, $xy \in \mathfrak{p}_j \cap \bigcap_{i\neq j} \mathfrak{p}_i = (0)$. Donc l'image de $x$ dans $A_{\mathfrak{p}_j}$ est nulle et $\mathfrak{p}_j A_{\mathfrak{p}_j} = 0$.

L'implication b) $\Rightarrow$ c) est triviale, un corps étant en particulier un anneau intègre.

Enfin, supposons c) et montrons que le radical de A est nul. Considérons une décomposition primaire minimale de (0),

$$(0) = \bigcap_{1 \leq j \leq n} \mathfrak{q}_j, \quad \mathfrak{p}_j = \sqrt{\mathfrak{q}_j}$$

et soit $x \in \sqrt{(0)} = \bigcap \mathfrak{p}_j$. L'élément $x$ est nilpotent. Supposons $x \neq 0$ et soit I son annulateur. On sait qu'il existe un idéal associé à A, soit $\mathfrak{p}_j$ tel que $\mathrm{I} \subset \mathfrak{p}_j$. L'image de $x$ dans $\mathrm{A}_{\mathfrak{p}_j}$ est donc nilpotente et puisque $\mathrm{A}_{\mathfrak{p}_j}$ est intègre, $x/1 = 0$. Il existe ainsi $s \notin \mathfrak{p}_j$ tel que $sx = 0$, ce qui contredit l'hypothèse que $\mathrm{I} \subset \mathfrak{p}_j$.

Cette contradiction montre que A est réduit.

# 13 Extensions de corps

*Dans ce chapitre, nous poursuivons l'étude des extensions de corps, déjà entamée au chapitre 9. Après quelques résultats concernant les corps finis, nous donnons les résultats principaux de la théorie de* Galois *des extensions algébriques. Nous définissons enfin le degré de transcendance d'une extension de corps non nécessairement algébrique.*

## 13.1. Corps finis

Un *corps fini* est un corps dont le cardinal est fini.

*Exemples 13.1.1.* — a) Pour tout nombre premier $p$, $\mathbf{Z}/p\mathbf{Z}$ est un corps fini de caractéristique $p$ et de cardinal $p$.

b) Si $P \in (\mathbf{Z}/p\mathbf{Z})[X]$ est un polynôme irréductible de degré $d \geq 1$, le corps de rupture de P, défini par $F = (\mathbf{Z}/p\mathbf{Z})[X]/(P)$, est un $(\mathbf{Z}/p\mathbf{Z})$-espace vectoriel de dimension $d$. Ainsi, F est un corps fini de caractéristique $p$ et de cardinal $p^d$.

Proposition 13.1.2. — *La caractéristique d'un corps fini est un nombre premier $p$ ; son cardinal est une puissance de $p$.*

*Démonstration.* — Soit F un corps fini. Comme $\mathbf{Z}$ est infini, l'homomorphisme canonique $\mathbf{Z} \to F$ tel que $1 \mapsto 1_F$ n'est pas injectif et son noyau est un idéal non nul $I = (n)$ de $\mathbf{Z}$. Comme F est un corps, I est un idéal premier, soit $I = (p)$ pour un nombre premier $p$ et par définition, la caractéristique de F est égale à $p$.

Par suite, cet homomorphisme induit un homomorphisme de corps $\mathbf{Z}/p\mathbf{Z} \to F$. Il en résulte que F est un espace vectoriel sur le corps $\mathbf{Z}/p\mathbf{Z}$, nécessairement de dimension finie. Si $d$ est cette dimension, le cardinal de F est égal à $p^d$. □

Théorème 13.1.3. — *Soit* K *un corps et* G *un sous-groupe fini du groupe multiplicatif de* K. *Alors,* G *est un groupe cyclique.*

*En particulier, le groupe multiplicatif d'un corps fini est cyclique.*

*Démonstration.* — G est un groupe abélien fini ; notons $n$ son cardinal. D'après le théorème des facteurs invariants, il existe des entiers $d_1|\dots|d_r$, avec $d_1 > 1$, tels que $G \simeq (\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_r\mathbf{Z})$ et $n = d_1 \dots d_r$. En particulier, tout élément de G est annulé par $d_r$. Autrement dit, tout élément $x$ de G vérifie $x^{d_r} = 1$.

Cependant, un polynôme à coefficients dans un corps (commutatif) a moins de racines que son degré (sauf s'il s'agit du polynôme nul). Ainsi, $d_r \geq n = d_1 \dots d_r$. On a donc $r = 1$, $d_1 = n$ et $G \simeq \mathbf{Z}/n\mathbf{Z}$ est cyclique d'ordre $n$. □

Si $q$ est une puissance d'un nombre premier ($q > 1$), nous allons montrer qu'il existe, à isomorphisme près, un unique corps de cardinal $q$.

THÉORÈME 13.1.4. — *Soit $p$ un nombre premier et $f$ un entier $\geq 1$ ; posons $q = p^f$. Si $\Omega$ est un corps algébriquement clos de caractéristique $p$, il existe alors un sous-corps $\mathbf{F}_q$ de $\Omega$ et un seul qui soit de cardinal $q$ : c'est l'ensemble des racines du polynôme $X^q - X$.*

*De plus, tout corps fini de cardinal $q$ est isomorphe à $\mathbf{F}_q$.*

LEMME 13.1.5. — *Soit F un corps de caractéristique $p$. L'application $\sigma\colon F \to F$ telle que $\sigma(x) = x^p$ pour tout $x \in F$ est un homomorphisme de corps.*

*Démonstration.* — On a $\sigma(0) = 0$ et $\sigma(1) = 1$. De plus, pour tous $x$ et $y$ dans F, $\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)$. Il reste à montrer que $\sigma$ est additif. Or, si $x$ et $y$ sont dans F,

$$\sigma(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.$$

Or, $\binom{p}{k} = p!/k!(p-k)!$ et, $p$ étant premier, si $1 \leq k \leq p-1$, $p$ ne divise ni $k!$ ni $(p-k)!$. Par suite, $p$ ne divise pas $k!(p-k)!$. Comme il divise le numérateur $p!$, $p$ divise $\binom{p}{k}$ dès que $1 \leq k \leq p-1$. Comme F est de caractéristique $p$,

$$\sigma(x+y) = x^p + y^p = \sigma(x) + \sigma(y),$$

ainsi qu'il fallait démontrer. □

DÉFINITION 13.1.6. — *Si F est un corps de caractéristique $p$, l'homomorphisme de corps défini par $x \mapsto x^p$ est appelé* homomorphisme de Frobenius.

*Démonstration du théorème.* — Notons $\sigma_q$ l'endomorphisme de $\Omega$, puissance $f^{\text{e}}$ de l'endomorphisme $\sigma$. Ainsi, si $x \in F$, $\sigma_q(x) = x^q$. L'ensemble des $x \in \Omega$ tels que $\sigma_q(x) = x$ est alors un sous-corps de $\Omega$. Notons le $\mathbf{F}_q$. La dérivée du polynôme $X^q - X \in \Omega[X]$ est $qX^{q-1} - 1 = -1$ puisque $\Omega$ est de caractéristique $p$ et que $q$ est une puissance de $p$. Ainsi, le polynôme $X^q - X$ n'a pas de racine double et $\mathbf{F}_q$ est de cardinal $q$.

Réciproquement, si K est un sous-corps de cardinal $q$ de $\Omega$, tout élément de $x \in K^\times$ vérifie $x^{q-1} = 1$ (c'est le théorème de Lagrange, l'ordre d'un élément

divise l'ordre du groupe), donc $x^q = x$ et $x \in \mathrm{F}$, si bien que $\mathrm{K} \subset \mathrm{F}$. Comme ces deux corps ont même cardinal, $\mathrm{K} = \mathrm{F}$, ce qui montre l'unicité.

Soit enfin K un corps fini de cardinal $q$. Comme $\Omega$ est une extension algébriquement close du corps $\mathbf{Z}/p\mathbf{Z}$, il existe un homomorphisme de corps $i\colon \mathrm{K} \hookrightarrow \Omega$ (voir le théorème 13.2.8). Alors, $i(\mathrm{K})$ est un corps de cardinal $q$ contenu dans $\Omega$ donc $i(\mathrm{K}) = \mathbf{F}_q$ et $\mathrm{K} \simeq \mathbf{F}_q$. □

Corollaire 13.1.7. — *Soit* F *un corps fini de cardinal* $q$ *et* $d$ *un entier* $\geq 2$. *Alors, il existe un polynôme irréductible unitaire* $\mathrm{P} \in \mathrm{F}[\mathrm{X}]$ *de degré* $d$ *et son corps de rupture* $\mathrm{F}[\mathrm{X}]/(\mathrm{P})$ *est un corps fini contenu* F *de cardinal* $q^d$.

*Démonstration.* — On peut supposer que $\mathrm{F} = \mathbf{F}_q \subset \Omega$. Soit $\mathrm{F}' = \mathbf{F}_{q^e}$ et soit $x \in \mathrm{F}'^{\times}$ un générateur du groupe multiplicatif de F′. Le corps $\mathrm{F}[x]$ est alors contenu dans F′ mais contient $\mathrm{F}'^{\times}$ si bien que $\mathrm{F}' = \mathrm{F}[x]$. Soit P le polynôme minimal de $x$ sur F : c'est un polynôme unitaire à coefficients dans F, noyau de l'homomorphisme $\mathrm{F}[\mathrm{X}] \to \mathrm{F}'$ tel que $\mathrm{X} \mapsto x$. Par suite, F′ est isomorphe au corps de rupture de P et P est irréductible de degré $d$. □

Un défaut de la démonstration précédente est qu'elle ne fournit pas de moyen *effectif* de déterminer un corps fini. D'après le corollaire, on sait toutefois qu'il nous faut dénicher un polynôme irréductible de degré convenable.

*Exemple 13.1.8.* — Construisons un corps de cardinal 8. Il nous faut pour cela trouver un polynôme irréductible de degré 3 à coefficients dans $\mathbf{Z}/2\mathbf{Z}$. Comme un polynôme sans racine de degré 3 est nécessairment irréductible, il suffit donc de trouver un polynôme sans racine. Il y a $8 = 2^3$ polynômes unitaires de degré 3, donc 4 s'annulent en 0. Les 4 autres sont $\mathrm{X}^3 + a\mathrm{X}^2 + b\mathrm{X} + 1$ avec $(a, b) \in \{0; 1\}^2$ et leur valeur en 1 est $a + b$. On a ainsi 2 polynômes irréductibles unitaires de degré 3 : $\mathrm{X}^3 + \mathrm{X} + 1$ et $\mathrm{X}^3 + \mathrm{X}^2 + 1$. Ainsi, $\mathbf{F}_8 \simeq \mathbf{F}_2[\mathrm{X}]/(\mathrm{X}^3 + \mathrm{X} + 1)$.

## 13.2. Séparabilité

Définition 13.2.1. — *Une extension de corps* $\mathrm{K} \subset \mathrm{L}$ *est dite* monogène *s'il existe* $x \in \mathrm{L}$ *tel que* $\mathrm{L} = \mathrm{K}[x]$.

Proposition 13.2.2. — *Soit* $i\colon \mathrm{K} \to \mathrm{L}$ *un homomorphisme de corps et soit* $\mathrm{K} \subset \mathrm{E}$ *une extension monogène. Soit* $x \in \mathrm{E}$ *un élément tel que* $\mathrm{E} = \mathrm{K}[x]$ *et soit* $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ *son polynôme minimal.*

*L'ensemble des homomorphismes de corps* $j\colon \mathrm{E} \to \mathrm{L}$ *tels que* $j|_{\mathrm{K}} = i$ *et l'ensemble des racines de* P *dans* L *sont en bijection par l'application* $j \mapsto j(x)$.

*Démonstration.* — On peut identifier K à un sous-corps de L, ce qui permet de sous-entendre l'homomorphisme $i$.

Remarquons pour commencer que $j(x)$ vérifie $\mathrm{P}(j(x)) = j(\mathrm{P}(x)) = j(0) = 0$, donc $j(x)$ est effectivement une racine de P dans L.

Par hypothèse, tout élément de $\mathrm{E} = \mathrm{K}[x]$ est de la forme $f(x)$ pour un polynôme $f \in \mathrm{K}[\mathrm{X}]$. Par suite, $j(f(x)) = f(j(x))$ si bien que la donnée de $j(x)$ détermine $j$ et l'application définie dans la proposition est injective.

Réciproquement, soit $a$ une racine de P dans L. On définit un homomorphisme $\tilde{j}_a \colon \mathrm{K}[\mathrm{X}] \to \mathrm{L}$ par $\mathrm{X} \mapsto a$. Le noyau de cet homomorphisme $\tilde{j}_a$ est le polynôme minimal de $a$ dans L. Comme $\mathrm{P}(a) = 0$ et comme P est irréductible, $\operatorname{Ker} \tilde{j}_a = (\mathrm{P})$ et il en résulte un homomorphisme de corps $j_a \colon \mathrm{K}[\mathrm{X}]/(\mathrm{P}) \to \mathrm{L}$ tel que $\mathrm{cl}(\mathrm{X}) \mapsto a$. Comme d'autre part $\mathrm{E} = \mathrm{K}[x]$, on a un isomorphisme $\varphi \colon \mathrm{K}[\mathrm{X}]/(\mathrm{P}) \to \mathrm{E}$ tel que $\mathrm{cl}(\mathrm{X}) \mapsto x$ et l'application $j_a \circ \varphi^{-1}$ est un homomorphisme de corps $\mathrm{E} \to \mathrm{L}$ tel que $x \mapsto a$ et dont la restriction à K est l'identité. L'application définie dans la proposition est donc surjective. □

Définition 13.2.3. — *Soit* K *un corps. Un polynôme irréductible* $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ *est dit* séparable *s'il n'a pas de racines multiples dans une clôture algébrique de* K.

*Soit* $\mathrm{K} \subset \mathrm{L}$ *une extension algébrique. Un élément* $x \in \mathrm{L}$ *est dit* séparable *sur* K *si son polynôme minimal dans* $\mathrm{K}[\mathrm{X}]$ *est séparable.*

*Une extension algébrique de corps* $\mathrm{K} \subset \mathrm{L}$ *est dite* séparable *si tout élément* $x \in \mathrm{L}$ *est séparable sur* K.

Proposition 13.2.4. — *a) Si* K *est un corps de caractéristique* 0*, tout polynôme irréductible de* $\mathrm{K}[\mathrm{X}]$ *est séparable. Par suite, toute extension algébrique de* K *est séparable sur* K.

*b) Si* K *est un corps de caractéristique* $p$*, un polynôme irréductible de* $\mathrm{K}[\mathrm{X}]$ *n'est pas séparable si et seulement si c'est un polynôme en* $\mathrm{X}^p$.

*c) Si* K *est un corps de caractéristique dont l'homomorphisme de Frobenius* $\sigma \colon \mathrm{K} \to \mathrm{K}$ *est surjectif, tout polynôme de* $\mathrm{K}[\mathrm{X}]$ *est séparable. Toute extension algébrique de* K *est alors séparable sur* K.

*Démonstration.* — a) Soit P un polynôme irréductible de $\mathrm{K}[\mathrm{X}]$. On note $\mathrm{P} = a_n\mathrm{X}^n + \cdots + a_0$, $n$ étant le degré de P, soit $a_n \neq 0$. Par suite, $\mathrm{P}' = na_n\mathrm{X}^{n-1} + \cdots + a_1$ est de degré $n-1$. Si P a une racine double, P et P′ ont un facteur commun (si $a$ est racine double de P, $(\mathrm{X}-a)^2$ divise P et $(\mathrm{X}-a)$ divise P′ si bien que $(\mathrm{X}-a)$ divise $\operatorname{pgcd}(\mathrm{P}, \mathrm{P}')$) et puisque P est irréductible, P′ est multiple de P, ce qui est absurde étant donné que $\mathrm{P}' \neq 0$ et $\deg \mathrm{P}' < \deg \mathrm{P}$. Il en résulte que P est séparable.

b) Si K est de caractéristique $p$ et si $\mathrm{P}' \neq 0$, le même argument montre que P est séparable. Si réciproquement $\mathrm{P}' = 0$, toutes les racines de P sont multiples et P n'est pas séparable. Enfin, $\mathrm{P}' = 0$ si et seulement si $ia_i = 0$ pour tout $i \in \{0; \ldots; n\}$, c'est-à-dire $a_i = 0$ dès que $p$ ne divise pas $i$, autrement dit, $\mathrm{P} = \sum_i a_{pi}\mathrm{X}^{pi} \in \mathrm{K}[\mathrm{X}^p]$.

c) Supposons que l'homomorphisme de Frobenius de K est surjectif. Si $P = \sum_i a_{pi} X^{pi}$ n'est pas séparable, choisissons pour tout $i$ un élément $b_i \in K$ tel que $\sigma(b_i) = b_i^p = a_{pi}$. Alors, $P = \sum_i b_i^p X^{pi} = \sum_i (b_i X^i)^p = (\sum_i b_i X^i)^p$ n'est pas irréductible dans $K[X]$. Cette contradiction montre que dans ce cas, tout polynôme irréductible est séparable. □

Définition 13.2.5. — *Un corps de caractéristique $p > 0$ dont l'homomorphisme de Frobenius est surjectif est dit* parfait.

*Exemple 13.2.6.* — a) Un corps fini est parfait. En effet, l'homomorphisme $\sigma : F \to F$ est injectif. Comme F est fini, $\sigma(F)$ a pour cardinal $\operatorname{card} F$, si bien que $\sigma$ est surjectif.

b) Soit F un corps de caractéristique $p$. Le corps $K = F(T)$ n'est pas parfait. En effet, il n'existe pas de fraction rationnelle Q telle que $Q^p = T$. Remarquons que le polynôme $X^p - T \in K[X]$ est irréductible. En effet, il est irréductible dans $F[T, X] = F[X][T]$ puisque de degré 1 en T ; d'après le théorème de Gauß, étant irréductible dans $F[T][X] = F[T, X]$, il est irréductible dans $F(T)[X]$. De plus, sur l'extension $F(T^{1/p})$ de $F(T)$, le polynôme $X^p - T$ n'est plus irréductible mais égal à $(X - T^{1/p})^p$ et a pour seule racine $T^{1/p}$.

Lemme 13.2.7. — *Soit $K \subset L$ et $L \subset E$ deux extensions algébriques de corps.*

*Si $x \in E$ est séparable sur K, il est séparable sur L. Par suite, si E est séparable sur K, E est séparable sur L.*

*Démonstration.* — Il suffit de démontrer la première assertion. Soit $x \in E$ un élément séparable sur K. Soit $P \in K[X]$ son polynôme minimal sur K et $Q \in L[X]$ son polynôme minimal sur L. Comme $x$ est séparable sur K, P est scindé à racines simples dans une clôture algébrique de E. D'autre part, par définition de Q, P est un multiple de Q. Il s'ensuit que les racines de Q dans une clôture algébrique de K sont simples et donc que $x$ est séparable sur L. □

Théorème 13.2.8. — *Soit $K \subset L$ une extension algébrique finie de corps et $\Omega$ une clôture algébrique de K. Le nombre d'homomorphismes de corps $j : L \to \Omega$ qui coïncident avec l'inclusion sur K est a) non nul ; b) inférieur ou égal au degré $[L : K]$ ; c) égal à $[L : K]$ si et seulement si L est engendré comme K-algèbre par des éléments séparables sur K.*

*Démonstration.* — Soit $\{x_1; \ldots; x_r\}$ une famille finie d'éléments de L telle que $L = K[x_1, \ldots, x_r]$. On va démontrer le théorème par récurrence sur $r$.

Pour $r = 0$, $L = K$ et le résultat est vrai. Supposons le vrai pour $r - 1$. Posons $E = K[x_1]$. Soit P le polynôme minimal de $x_r$ sur K, de sorte que $[E : K] = \deg P$. D'après la proposition 13.2.2, le nombre $n_E$ d'homomorphismes $j : E \to \Omega$ qui étendent l'inclusion $K \to \Omega$ est égal au nombre $\nu_P$ de racines

distinctes de P dans $\Omega$. Par récurrence, pour chacun de ces homomorphismes, le nombre $n_E$ d'homomorphismes $L \to \Omega$ qui l'étendent est non nul et majoré par $[L : E]$. Il en résulte que le nombre d'homomorphismes $L \to \Omega$ qui étendent l'inclusion $K \to \Omega$ est d'une part non nul, et d'autre part majoré par $[L : E]\, \nu_P \leq [L : E]\, [E : K] = [L : K]$.

Si $x_1$ n'est pas séparable sur K, $\nu_P < [E : K]$ et on a une inégalité stricte. Réciproquement, si tous les $x_i$ sont séparables sur K, on a $\deg P = [E : K]$ homomorphismes $E \to \Omega$ qui étendent l'inclusion de K dans $\Omega$. Ensuite, remarquons que d'après le lemme 13.2.7, les $x_i$ pour $i \geq 2$ sont séparables sur E. Par récurrence, chacun des $[E : K]$ homomorphismes $E \to \Omega$ admet donc $[L : E]$ prolongements $L \to \Omega$. Finalement, il existe $[L : E]\, [E : K] = [L : K]$ homomorphismes de L dans $\Omega$ qui étendent l'inclusion de K dans $\Omega$. □

COROLLAIRE 13.2.9. — *Soit* $K \subset L$ *une extension algébrique finie de corps. Alors,* L *est séparable sur* K *si et seulement si* L *est engendrée comme* K*-algèbre par une famille d'éléments de* L *séparables sur* K.

*Démonstration.* — Si L est séparable sur K, elle est *a fortiori* engendrée par une famille d'éléments séparables. Dans l'autre sens, la démonstration du théorème précédent montre que dès que L contient un élément non séparable sur K, le nombre de K-homomorphismes de L dans une clôture algébrique de K est strictement inférieur à $[L : K]$. Par suite, L ne peut pas être engendrée par une famille d'éléments séparables sur K. □

COROLLAIRE 13.2.10. — *Soit* $K \subset L$ *et* $L \subset E$ *deux extensions algébriques finies de corps. Si* E *est séparable sur* L *et si* L *est séparable sur* K*, alors* E *est séparable sur* K.

*Démonstration.* — Soit $\Omega$ une clôture algébrique de E. Comme L est séparable sur K, il existe $[L : K]$ K-homomorphismes $L \to \Omega$. Comme E est séparable sur L, chacun de ces homomorphismes se prolonge en $[E : L]$ K-homomorphismes $L \to \Omega$. Par suite, le nombre de K-homomorphismes $E \to \Omega$ est égal à $[L : K]\, [E : L] = [L : K]$. D'après le théorème, E est séparable sur K. □

## 13.3. Théorie de Galois

DÉFINITION 13.3.1. — *Soit* $K \subset L$ *une extension finie de corps. On appelle groupe de Galois de* L *sur* K*, noté* $\mathrm{Gal}(L/K)$ *le groupe des* K*-automorphismes de* L.

*Exemple 13.3.2.* — Si $c : \mathbf{C} \to \mathbf{C}$ désigne la conjugaison complexe, $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \{\mathrm{Id}, c\} \simeq \mathbf{Z}/2\mathbf{Z}$.

*Démonstration.* — En effet, soit $\sigma : \mathbf{C} \to \mathbf{C}$ tel que pour tout $x \in \mathbf{R}$, $\sigma(x) = x$. On a $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$ donc $\sigma(i) \in \{\pm i\}$. Alors, si $z = x + iy \in \mathbf{C}$,

$\sigma(z) = \sigma(x) + \sigma(i)\sigma(y) = x + \sigma(i)y$ et $\sigma = \mathrm{Id}$ si $\sigma(i) = i$ tandis que si $\sigma(i) = -i$, $\sigma = c$. □

*Exercice 13.3.3.* — a) Soit K un corps, $a \in \mathrm{K}$ un élément qui n'est pas un carré et $\mathrm{L} = \mathrm{K}(\sqrt{a}) = \mathrm{K}[\mathrm{X}]/(\mathrm{X}^2 - a)$. Déterminer $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ et montrer en particulier qu'il est d'ordre 2.

b) Plus généralement, soit $n$ un entier $\geq 2$ et K un corps qui contient $n$ racines $n^{\mathrm{e}}$ de l'unité distinctes. Soit $a$ un élément de K qui n'est pas la puissance $n^{\mathrm{e}}$ d'un élément de K. Soit $\mathrm{L} = \mathrm{K}(\sqrt[n]{a})$ une extension de K, corps de rupture d'un facteur irréductible de $\mathrm{X}^n - a$. Montrer que $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ est cyclique d'ordre $n$.

c) Le groupe de Galois de l'extension $\mathbf{Q}(\sqrt[3]{2})$ de $\mathbf{Q}$ est réduit à l'identité.

LEMME 13.3.4. — *Soit* $\mathrm{K} \subset \mathrm{L}$ *une extension finie. Alors,* $\operatorname{card}\mathrm{Gal}(\mathrm{L}/\mathrm{K}) \leq [\mathrm{L} : \mathrm{K}]$.

*Démonstration.* — Soit $\Omega$ une clôture algébrique de L. On a démontré au théorème 13.2.8 que le nombre de K-homomorphismes $\mathrm{L} \to \Omega$ est inférieur ou égal à $[\mathrm{L} : \mathrm{K}]$. A fortiori, le nombre de K-homomorhpismes $\mathrm{L} \to \mathrm{L}$ est inférieur ou égal à $[\mathrm{L} : \mathrm{K}]$. □

DÉFINITION 13.3.5. — *On dit qu'une extension finie de corps* $\mathrm{K} \subset \mathrm{L}$ *est* galoisienne *si* $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ *a pour cardinal* $[\mathrm{L} : \mathrm{K}]$.

*Exemples 13.3.6.* — a) L'extension $\mathbf{R} \subset \mathbf{C}$ est galoisienne.

b) Soit $q$ une puissance d'un nombre premier et $e$ un entier $\geq 2$. Alors, $\mathrm{Gal}(\mathbf{F}_{q^e}/\mathbf{F}_q)$ est cyclique d'ordre $e$, engendré par l'automorphisme $x \mapsto x^q$. L'extension $\mathbf{F}_q \subset \mathbf{F}_{q^e}$ est donc galoisienne.

*Démonstration.* — a) On a vu que $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) \simeq \mathbf{Z}/2\mathbf{Z}$ donc est de cardinal $2 = [\mathbf{C} : \mathbf{R}]$.

b) Notons $\sigma_q : \mathbf{F}_{q^e} \to \mathbf{F}_{q^e}$ l'automorphisme donné par $x \mapsto x^q$. Ses puissances sont les automorphismes donnés par $x \mapsto x^{q^i}$ pour $0 \leq i \leq e-1$ et sont distinctes (car si $x^{q^i} = x^{q^j}$ pour $i \neq j$ dans $\{0; \ldots; e-1\}$ et tout $x \in \mathbf{F}_{q^e}$, le polynôme $\mathrm{X}^{q^i} - \mathrm{X}^{q^j}$ a $q^e$-racines et $q^e > \max(q^i, q^j) = \deg(\mathrm{X}^{q^i} - \mathrm{X}^{q^j})$). Ainsi, $\mathrm{Gal}(\mathbf{F}_{q^e}/\mathbf{F}_q)$ est d'ordre au moins $e$. Comme $[\mathbf{F}_{q^e} : \mathbf{F}_q] = e$, l'extension $\mathbf{F}_q \subset \mathbf{F}_{q^e}$ est galoisienne de groupe $\mathrm{Gal}(\mathbf{F}_{q^e}/\mathbf{F}_q) = \{\mathrm{Id}; \sigma_q; \sigma_q^2; \ldots; \sigma_q^{e-1}\} \simeq \mathbf{Z}/e\mathbf{Z}$. □

Le lemme suivant fournit un autre exemple d'extension galoisienne.

LEMME 13.3.7. — *Soit* L *un corps et* G *un groupe fini d'automorphismes de* L. *Soit* $\mathrm{K} = \mathrm{L}^{\mathrm{G}}$ *l'ensemble des* $x \in \mathrm{L}$ *tels que pour tout* $\sigma \in \mathrm{G}$, $\sigma(x) = x$. *Alors,* K *est un sous-corps de* L *et* $\mathrm{K} \subset \mathrm{L}$ *est une extension finie de degré* $[\mathrm{L} : \mathrm{K}] = \operatorname{card}\mathrm{G}$.

*Démonstration.* — Le fait que K est un sous-corps de L est laissé en *exercice*. Comme $\mathrm{G} \subset \mathrm{Gal}(\mathrm{L}/\mathrm{K})$, le lemme 13.3.4 affirme que $\operatorname{card}\mathrm{G} \leq [\mathrm{L} : \mathrm{K}]$. Supposons par

l'absurde que l'inégalité stricte est vérifiée et soit $a_1, \dots, a_n$ des éléments de L linéairement indépendants sur K, avec donc $n > [L : K]$. La famille d'équations linéaires $\sum_{i=1}^{n} x_i \sigma(a_i) = 0$, où $\sigma$ parcourt G a plus d'inconnues que d'équations donc possède une solution non nulle $(x_1, \dots, x_n)$ dans $E^n$. Considérons une telle solution pour laquelle le nombre de coefficients $x_i$ nuls est maximal. Quitte à renuméroter les indices, on peut supposer que $x_1, \dots, x_m$ sont non nuls, mais que $x_{m+1} = \cdots = x_n = 0$. Par linéarité, on peut supposer que $x_m = 1$, d'où les relations

$$\sum_{i=1}^{m-1} x_i \sigma(a_i) + \sigma(a_m) = 0, \qquad \sigma \in G.$$

Soit alors $\tau \in G$ et appliquons $\tau$ à l'égalité précédente. On obtient

$$\sum_{i=1}^{m-1} \tau(x_i)(\tau \circ \sigma)(a_i) + (\tau \circ \sigma)(a_m) = 0.$$

En lui soustrayant la relation correspondant à l'élément $\tau \circ \sigma \in G$, on obtient

$$\sum_{i=1}^{m-1} (\tau(x_i) - x_i)(\tau \circ \sigma)(a_i) = 0.$$

Cette relation vaut pour tout $\sigma \in G$ et les $\tau \circ \sigma$ parcourant G, on en déduit que pour tout $\sigma \in G$,

$$\sum_{i=1}^{m-1} (\tau(x_i) - x_i)\sigma(a_i) = 0,$$

ce qui contredit la minimalité de l'entier $m$. Par suite, $\operatorname{card} G = [L : K]$. □

Donnons maintenant deux caractérisations des extensions galoisiennes. La première contient l'essentiel des informations nécessaires à la démonstration du théorème fondamental de la théorie de Galois (théorème 13.3.11), la seconde est la caractérisation usuelle (extension « normale et séparable »).

PROPOSITION 13.3.8. — *Une extension finie* $K \subset L$ *est galoisienne si et seulement si elle vérifie les deux propriétés suivantes :*

(1) *elle est séparable ;*

(2) *si* $K \subset L \subset \Omega$ *est une clôture algébrique de* L, *tout* K*-homomorphisme* $L \to \Omega$ *a pour image* L.

*Démonstration.* — Fixons une clôture algébrique $\Omega$ de L. Supposons que $K \subset L$ est une extension finie galoisienne. On a alors exactement $[L : K]$ K-homomorphismes $L \to \Omega$ : ce sont les éléments de $\mathrm{Gal}(L/K)$. Par suite, l'extension $K \subset L$ est séparable et l'image de tout K-homomorphisme $L \to \Omega$ est égale à L.

Réciproquement, comme l'extension $K \subset L$ est séparable, il existe exactement $[L : K]$ K-homomorphismes $L \to \Omega$, fournis par le théorème 13.2.8. Notons les $j_1, \dots, j_{[L:K]}$. Par hypothèse, $j_i(L) = L$ pour tout $i$. Par suite, les $j_i$ définissent des

éléments de $\mathrm{Gal}(L/K)$ et $\operatorname{card}\mathrm{Gal}(L/K) \geq [L : K]$. Comme l'autre inégalité est toujours vraie, l'extension $K \subset L$ est galoisienne. □

PROPOSITION 13.3.9. — *Soit* $K \subset L$ *une extension finie de corps. Les conditions suivantes sont équivalentes :*

(1) *l'extension* $K \subset L$ *est galoisienne ;*

(2) *elle est séparable et tout polynôme irréductible dans* $K[X]$ *qui a une racine dans* L *est scindé dans* L *;*

(3) *il existe un polynôme* $P \in K[X]$ *scindé à racines simples* $x_1, \ldots, x_d$ *dans* L *tel que* $L = K(x_1, \ldots, x_d)$.

*Démonstration.* — Fixons une clôture algébrique $\Omega$ de L.

Supposons (1), c'est-à-dire que l'extension $K \subset L$ est galoisienne. Alors, elle est séparable. Soit P un polynôme irréductible de $K[X]$ ayant une racine $x$ dans L. Soit $y$ une autre racine de P dans $\Omega$. Il existe unique K-homomorphisme de corps $\varphi_1 : K[x] \to \Omega$ tel que $\varphi_1(x) = y$. D'après le théorème 13.2.8, $\varphi$ s'étend en un K-homomorphisme $\varphi : L \to \Omega$. L'extension $K \subset L$ étant galoisienne, il résulte de la proposition 13.3.8 que $\varphi(L) = L$. Par suite, $\varphi(x) \in L$. Nous avons donc prouvé que P est scindé dans L.

Supposons maintenant (2) et soit $x_1, \ldots, x_d$ des éléments de L tels que $L = K(x_1, \ldots, x_d)$. Comme l'extension $K \subset L$ est séparable, les $x_i$ sont racines d'un polynôme iréductible séparable $P_i \in K[X]$. Par hypothèse, les $P_i$ sont scindés dans L. Soit P le ppcm des $P_i$. C'est donc un polynôme séparable de $K[X]$ et scindé dans L. Comme les $x_i$ engendrent L, les racines de P (qui contiennent l'ensemble $\{x_1; \ldots; x_d\}$) engendrent L.

Supposons maintenant (3). Comme L est engendrée par des éléments séparables sur K, L est séparable sur K. D'après la proposition 13.3.8, il suffit ainsi de montrer que pour tout K-homomorphisme $\varphi : L \to \Omega$, $\varphi(L) = L$. Or, si $1 \leq i \leq d$, $P(\varphi(x_i)) = \varphi(P(x_i)) = 0$, si bien que $\varphi(x_i)$ est une des racines de P. Ainsi, $\varphi(x_i)$ est l'une des racines $x_j$ et en particulier, $\varphi(x_i) \in L$. Comme les $x_i$ engendrent L sur K et comme $\varphi$ est un K-homomorphisme, $\varphi(L) \subset L$. Comme L et $\varphi(L)$ ont même degré sur K ($\varphi$ définit un isomorphisme de K-espaces vectoriels $L \to \varphi(L)$), $L = \varphi(L)$. □

COROLLAIRE 13.3.10. — *Si* $K \subset L$ *est une extension algébrique finie séparable, il existe une plus petite extension finie galoisienne* $K \subset L^g$ *contenant* L.

*Démonstration.* — Soit $x_1, \ldots, x_d$ des éléments de L tels que $L = K[x_1, \ldots, x_d]$. Pour tout $i \in \{1; \ldots; d\}$, soit $P_i$ le polynôme minimal de $x_i$ sur K et soit P le ppcm des $P_i$. Soit $\Omega$ une clôture algébrique de L. Alors, si $K \subset L^g \subset \Omega$ est une extension galoisienne contenant L, $P_i$ ayant une racine dans L est scindé dans $L^g$. Par suite, $L^g$ contient le corps engendré par les racines de P dans $\Omega$.

Réciproquement, ce corps est engendré par les racines du polynôme à racines simples P, donc est une extension galoisienne de K. □

THÉORÈME 13.3.11 (Théorème fondamental de la théorie de Galois)
*Soit* $K \subset L$ *une extension finie galoisienne de groupe de Galois* $G = \mathrm{Gal}(L/K)$.
*a) Pour tout sous-groupe* $H \subset G$, *l'ensemble*

$$L^H = \{x \in L\,;\, \forall \sigma \in H, \quad \sigma(x) = x\}$$

*est un sous-corps de* L *contenant* K. *En outre,* $[L^H : K]$ *est égal à l'indice* $(H : G)$ *de* H *dans* G.
*b) Pour toute sous-extension* $K \subset E \subset L$, *l'ensemble*

$$\mathrm{Gal}(L/E) = \{\sigma \in \mathrm{Gal}(L/K)\,;\, \forall x \in E, \quad \sigma(x) = x\}$$

*est un sous-groupe de* G *d'indice* $[E : K]$.
*c) Les applications* $H \mapsto L^H$ *et* $E \mapsto \mathrm{Gal}(L/E)$ *sont des bijections décroissantes, réciproques l'une de l'autre.*

*Démonstration.* — a) D'après le lemme 13.3.7, l'extension $L^H \subset L$ est galoisienne de groupe $\mathrm{Gal}(L/L^H) = H$.

b) Les éléments de $\mathrm{Gal}(L/E)$ sont des E-homomorphismes $L \to L$. Ce sont en particulier des K-homomorphismes, d'où l'inclusion $\mathrm{Gal}(L/E) \subset \mathrm{Gal}(L/K)$, ce qui démontre la formule annoncée pour $\mathrm{Gal}(L/E)$. On a bien sûr $\mathrm{card}\,\mathrm{Gal}(L/E) \leq [L : E]$. Mais il résulte de la proposition 13.3.8 que l'extension $E \subset L$ est galoisienne : elle est séparable et, si $L \subset \Omega$ est une extension algébriquement close, tout E-homomorphisme $L \to \Omega$, étant aussi un K-homomorphisme, a pour image L. Ainsi, $\mathrm{card}\,\mathrm{Gal}(L/E) = [L : E]$. Autrement dit, $\mathrm{Gal}(L/E)$ est d'indice $\mathrm{card}\,\mathrm{Gal}(L/K)/\mathrm{card}\,\mathrm{Gal}(L/E) = [L : K]/[L : E] = [E : K]$.

c) On a démontré dans le lemme 13.3.7 que $\mathrm{Gal}(L/L^H) = H$. En particulier, l'application $H \mapsto L^H$ est injective. Montrons alors que $E = L^{\mathrm{Gal}(L/E)}$. L'inclusion $E \subset L^{\mathrm{Gal}(L/E)}$ est évidente. Réciproquement, ces deux extensions de K ont toutes deux pour degré $[E : K]$, donc sont égales. □

PROPOSITION 13.3.12. — *Soit* $K \subset L$ *une extension finie galoisienne de groupe* $G = \mathrm{Gal}(L/K)$. *Soit* H *un sous-groupe de* G.
*a) Si* $\sigma \in \mathrm{Gal}(L/K)$, *on a* $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.
*Soit alors* $N_G(H) = \{\sigma \in \mathrm{Gal}(L/K)\,;\, \sigma H \sigma^{-1} = H\}$ *le normalisateur de* H *dans* $\mathrm{Gal}(L/K)$.
*b)* $\mathrm{Gal}(L^H/K)$ *s'identifie naturellement à* $N_G(H)/H$. *En particulier, l'extension* $K \subset L^H$ *est galoisienne si et seulement si* H *est un sous-groupe distingué de* G. *On a alors* $\mathrm{Gal}(L^H/K) = G/H$

*Démonstration.* — a) Un élément $x \in L$ appartient à $L^H$ si et seulement si $h(x) = x$ pour tout $h \in H$. Par suite, $y = \sigma(x)$ appartient à $\sigma(L^H)$ si et seulement si $h\sigma^{-1}(y) = \sigma^{-1}(y)$ pour tout $h \in H$, c'est-à-dire $\sigma h\sigma^{-1}(y) = y$ pour tout $h \in H$, soit encore $y \in L^{\sigma H\sigma^{-1}}$.

b) Comme l'extension $K \subset L$ est galoisienne, tout K-homomorphisme $L^H \to L^H$ est la restriction à $L^H$ d'un K-homomorphisme $L \to L$, c'est-à-dire d'un élément $\sigma \in \mathrm{Gal}(L/K)$. Un tel $\sigma$ vérifie $\sigma(L^H) = L^H$ si et seulement si $\sigma H\sigma^{-1} = H$, d'où un homomorphisme surjectif $N_G(H) \to \mathrm{Gal}(L^H/K)$. Le noyau de cet homomorphisme s'identifie aux $\sigma \in N_G(H)$ tels que $\sigma(x) = x$ pour tout $x \in L^H$, c'est-à-dire à H. On a donc construit un isomorphisme $N_G(H)/H \simeq \mathrm{Gal}(L^H/K)$.

En particulier, l'extension $K \subset L^H$ est galoisienne si et seulement si $[L^H : K] = (H : N_G(H))$, c'est-à-dire, puisque $[L^H : K] = (H : G)$ si et seulement si $G = N_G(H)$, c'est-à-dire H distingué dans G. □

## 13.4. Compléments

THÉORÈME 13.4.1 (Théorème de l'élément primitif). — *Soit* E *un corps et* $E \subset F$ *une extension algébrique finie séparable. Alors, il existe* $x \in F$ *tel que* $F = E[x]$.

*De plus, si* E *est infini et si* $F = E[x_1, \ldots, x_d]$, *on peut choisir* $x$ *de la forme* $x_1 + c_2x_2 + \cdots + c_dx_d$ *avec* $c_2, \ldots, c_d$ *dans* E.

*Démonstration.* — Si E est fini, F est un corps fini. D'après le théorème 13.1.3, $F^\times$ est un groupe cyclique. Si $x$ en est un générateur, $E[x]$ contient $F^\times$ et 0, donc $E[x] = F$.

On suppose maintenant que E est infini. Par récurrence, il suffit de démontrer le résultat suivant, que nous isolons en un lemme. □

LEMME 13.4.2. — *Soit* $E \subset F = E[x, y]$ *une extension finie algébrique de corps. On suppose que* E *est infini et que* $y$ *est séparable sur* E. *Alors, pour tout* $c \in E$ *sauf un nombre fini d'entre eux,* $F = E[x + cy]$.

*Démonstration.* — Soit P et $Q \in E[X]$ les polynômes minimaux de $x$ et $y$ respectivement. Notons $p$ et $q$ leurs degrés. Soit aussi $\Omega$ une extension finie de E dans laquelle P et Q sont scindés. On note alors $x_1, \ldots, x_p$ les racines de P et $y_1, \ldots, y_q$ les racines de Q dans $\Omega$, avec $x = x_1$ et $y = y_1$. Par hypothèse, les $y_j$ sont deux à deux distincts. Ainsi, si $i \in \{1; \ldots; p\}$ et $j \in \{2; \ldots; q\}$, l'équation (d'inconnue $c$) $x_i + cy_j = x_1 + cy_1$ n'a qu'une solution. Ainsi, à part pour un nombre fini d'éléments $c \in E$, aucune de ces relations n'est vérifiée. Puisque E est infini, il existe en particulier un tel $c$. Posons alors $z = x + cy$ et montrons que $F = E[z]$.

Le polynôme $R(X) = P(z - cX)$ a ses coefficients dans $E[z]$ et s'annule en $X = y$ puisque $R(y) = P(z - cy) = P(x) = 0$. Si $j \geq 2$, $z - cy_j = x_1 + cy_1 - cy_j \notin \{x_1; \ldots; x_p\}$

donc $P(z - cy_j) \neq 0$ et $R(y_j) \neq 0$. Ainsi, $y = y_1$ est la seule racine commune à R et à Q. Il en résulte que $\operatorname{pgcd}(R, Q) = X - y$. Comme R et Q sont deux polynômes à coefficients dans $E[z]$, le théorème de Bézout implique que $\operatorname{pgcd}(R, Q) \in (E[z])[X]$, d'où $y \in E[z]$. On a alors $x = z - cy \in E[z]$ si bien que $E[x, y] \subset E[z] \subset E[x, y]$, d'où l'égalité $F = E[z]$. □

Définition 13.4.3. — *Soit* $K \subset L$ *une extension algébrique finie de corps. On appelle* trace *(resp.* norme*) d'un élément* $x \in L$ *la trace (resp. le déterminant) du* K*-endomorphisme de* L *défini par la multiplication par* $x$*. On les note* $\mathrm{Tr}_{L/K}(x)$ *et* $N_{L/K}(x)$.

Proposition 13.4.4. — *Soit* $K \subset L$ *une extension finie.*

*a) Si* $x \in K$, $\mathrm{Tr}_{L/K}(x) = [L : K]x$ *et* $N_{L/K}(x) = x^{[L:K]}$.

*b) pour tous* $x$ *et* $y$ *dans* L, $\mathrm{Tr}_{L/K}(x + y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$ *et* $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.

*Démonstration.* — a) Si $x \in K$, la multiplication par $x$ dans L est représentée, dans n'importe quelle base de L, par la matrice scalaire $xI_{[L:K]}$ associée à $x$. Sa trace est $[L : K]x$ et son déterminant $x^{[L:K]}$.

b) Si $x \in L$, notons $\mu_x$ le K-endomorphisme de multiplication par $x$ dans L, de sorte que pour tout $z \in L$, $\mu_x(z) = xz$. On a alors $\mu_{x+y}(z) = (x + y)z = xz + yz = \mu_x(z) + \mu_y(z)$ et donc $\mu_{x+y} = \mu_x + \mu_y$. Par suite, $\operatorname{Tr} \mu_{x+y} = \operatorname{Tr} \mu_x + \operatorname{Tr} \mu_y$, d'où $\mathrm{Tr}_{L/K}(x + y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$.

L'argument pour les normes est analogue : avec les mêmes notations, on a $\mu_{xy} = \mu_x \circ \mu_y$, donc

$$N_{L/K}(xy) = \det \mu_{xy} = \det \mu_x \det \mu_y = N_{L/K}(x)N_{L/K}(y).$$

□

Proposition 13.4.5. — *Soit* $K \subset L$ *une extension galoisienne de groupe* G*. Alors, pour tout* $x \in L$*, on a*

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x) \quad \textit{et} \quad N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x).$$

*Démonstration.* — Soit $\Omega$ une clôture algébrique de L. Soit $P \in K[X]$ le polynôme minimal de $x$ et notons $x = x_1, \ldots, x_d$ ses racines dans $\Omega$. On a ainsi

$$P(X) = (X - x_1) \ldots (X - x_d) = X^d - a_1 X^{d-1} + \cdots + (-1)^d a_d,$$

avec $a_1 = x_1 + \cdots + x_d$ et $a_d = x_1 \dots x_d$. Dans la base $\{1; x; \dots; x^{d-1}\}$, l'homomorphisme de multiplication par $x$ admet pour matrice

$$\begin{pmatrix} 0 & & & (-1)^{d-1}a_d \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_2 \\ & & 1 & a_1 \end{pmatrix}$$

c'est-à-dire la matrice compagnon associée au polynôme P. Par suite, $\det \mu_x = a_d$ et $\operatorname{Tr} \mu_x = a_1$. Autrement dit,

$$\operatorname{Tr}_{K[x]/K}(x) = \sum_{i=1}^{d} x_i \quad \text{et} \quad \operatorname{N}_{K[x]/K}(x) = \prod_{i=1}^{d} x_i.$$

Soit $\{e_1; \dots; e_s\}$ une base de L sur $K[x]$. Alors, la famille

$$\{e_1; xe_1; \dots; x^{d-1}e_1; e_2; \dots; x^{d-1}e_s\}$$

est une base de L sur K. Dans cette base, la matrice de l'endomorphisme de multiplication par $x$ est diagonale par blocs, formée de $s$ blocs égaux à la matrice compagnon précédente. On a donc

$$\operatorname{Tr}_{L/K}(x) = [L : K[x]] \operatorname{Tr}_{K[x]/K}(x) \quad \text{et} \quad \operatorname{N}_{L/K}(x) = \operatorname{N}_{K[x]/K}(x)^{[L:K[x]]}.$$

Si $i \in \{1; \dots; d\}$, soit $\tau_i$ l'unique K-homomorphisme de corps $K[x] \to L$ tel que $\tau_i(x) = x_i$. D'après le théorème 13.2.8, il existe exactement $[L : K[x]]$ homomorphismes $L \to \Omega$ qui étendent $\tau_i$. Comme l'extension $K \subset L$ est galoisienne, ces homomorphismes sont à valeurs dans L et on obtient ainsi les $[L : K] = [L : K[x]]\ [K[x] : K]$ éléments de G. Par suite,

$$\prod_{\sigma \in G} \sigma(x) = \Big(\prod_{i=1}^{d} \tau_i(x)\Big)^{[L:K[x]]} = \Big(\prod_{i=1}^{d} x_i\Big)^{[L:K[x]]} = \operatorname{N}_{K[x]/K}(x)^{[L:K[x]]} = \operatorname{N}_{L/K}(x).$$

L'argument pour les traces est analogue :

$$\sum_{\sigma \in G} \sigma(x) = [L : K[x]] \sum_{i=1}^{d} \tau_i(x) = [L : K[x]] \operatorname{Tr}_{K[x]/K}(x) = \operatorname{Tr}_{L/K}(x).$$

□

THÉORÈME 13.4.6. — *Soit* $K \subset L$ *une extension finie. L'application* $L \times L \to K$ *définie par* $(x, y) \mapsto \operatorname{Tr}_{L/K}(xy)$ *est une forme* K*-bilinéaire symétrique. Elle est non dégénérée si l'extension* $K \subset L$ *est séparable et nulle sinon.*

*Démonstration.* — Posons $t(x,y) = \mathrm{Tr}_{L/K}(xy)$. Comme L est commutatif, il est évident que $t$ est symétrique. Le fait que $t$ soit K-bilinéaire découle des formules

$$\begin{aligned} t(ax+a'x',y) &= \mathrm{Tr}_{L/K}((ax+a'x')y) = \mathrm{Tr}_{L/K}(axy+a'x'y) \\ &= a\,\mathrm{Tr}_{L/K}(xy) + a'\,\mathrm{Tr}_{L/K}(x'y) = at(x,y) + a't(x',y). \end{aligned}$$

Supposons que l'extension $K \subset L$ est séparable et montrons que $t$ est non-dégénérée. Soit $d = [L:K]$ et $\sigma_1, \ldots, \sigma_d$ les $d$ K-homomorphismes de L dans une clôture algébrique $\Omega$ de L. Alors, pour tout $x \in L$,

$$\mathrm{Tr}_{L/K}(x) = \sum_{j=1}^{d} \sigma_j(x).$$

Supposons que $x \in L$ appartienne au noyau de $t$. Alors, pour tout $y \in L$, $\mathrm{Tr}_{L/K}(xy) = 0$, d'où

$$0 = \sum_{j=1}^{d} \sigma_j(xy) = \sum_{j=1}^{d} \sigma_j(x)\sigma_j(y).$$

Comme les $\sigma_j$ sont linéairement indépendants sur L (cf. l'exercice 13.6.3), on a $\sigma_j(x) = 0$ pour tout $j$, d'où $x = 0$.

Réciproquement, supposons que $K \subset L$ n'est pas séparable et montrons que pour tout $x \in L$, $\mathrm{Tr}_{L/K}(x) = 0$. Notons $p > 0$ la caractéristique de K. Soit $L_s \subset L$ l'extension de K engendrée par tous les éléments de L qui sont séparables sur K. D'après le corollaire 13.2.9, l'extension $K \subset L_s$ est séparable. De plus, si $x \in L \setminus L_s$, $x$ n'est pas séparable sur $L_s$, sinon, d'après le corollaire 13.2.10, $x$ serait séparable sur K et on aurait $x \in L_s$. En particulier, le polynôme minimal de $x$ a pour degré un multiple de $p$, si bien que $p$ divise $[L:L_s]$.

Soit $x \in L_s$. On a vu que

$$\mathrm{Tr}_{L/K}(x) = [L:K[x]]\,\mathrm{Tr}_{K[x]/K}(x).$$

Comme $p$ divise $[L:L_s]$ et comme $K[x] \subset L_s$, $p$ divise $[L:K[x]]$, si bien que $\mathrm{Tr}_{L/K}(x) = 0$.

Soit maintenant $x \in L \setminus L_s$. Puisque $x$ n'est pas séparable sur K, son polynôme minimal sur K est de la forme $X^{np} + a_n X^{(n-1)p} + \cdots + a_{np}$ et le coefficient de $X^{np-1}$ est donc nul. Par suite, $\mathrm{Tr}_{K[x]/K}(x) = 0$ et

$$\mathrm{Tr}_{L/K}(x) = [L:K[x]]\,\mathrm{Tr}_{K[x]/K}(x) = 0.$$

□

*Remarque 13.4.7.* — Soit $K \subset L$ une extension finie de corps de caractéristique $p > 0$. Soit $L_s \subset L$ l'extension de K engendrée par les éléments de L qui sont séparables sur K. Alors, le degré de l'extension $L_s \subset L$ est une puissance de $p$.

*Démonstration.* — Prouvons tout d'abord que le degré du polynôme minimal sur $L_s$ de tout élément de $L \setminus L_s$ est une puissance de $p$. Soit en effet $x \in L \setminus L_s$ et soit $P = X^n + \cdots + a_0$ son polynôme minimal sur $L_s$. Comme $x$ n'est pas séparable sur $L_s$, P est un polynôme en $X^p$. Soit $r$ un entier $\geq 1$ maximal tel qu'il existe $Q \in L_s[X]$ tel que $P = Q(X^{p^r})$ Alors, Q est le polynôme minimal de $x^{p^r}$. Comme Q n'est pas un polynôme en $X^p$ (sinon, si $Q = Q_1(X^p)$, $P = Q_1(X^{p^{r+1}})$), $x^{p^r}$ est séparable sur $L_s$, d'où $x^{p^r} \in L_s$ et $Q(X) = X - x^{p^r}$, d'où $P = X^{p^r} - x^{p^r}$. En particulier, le degré de l'extension $L_s \subset L_s[x]$ est une puissance de $p$.

Soit maintenant $x_1, \ldots, x_n$ des éléments de $L \setminus L_s$ tels que $L = L_s[x_1, \ldots, x_n]$ et raisonnons par récurrence sur $n$. Si $n \leq 1$, cela résulte du paragraphe précédent. Soit $E = L_s[x_1, \ldots, x_{n-1}]$, de sorte que par récurrence, $[E : L_s]$ est une puissance de $p$. Pour alléger les notations, notons $x = x_n$ et $r = r_n$, si bien que $L = E[x]$, le polynôme minimal de $x$ sur $L_s$ étant $P = X^{p^r} - x^{p^r}$. Soit $Q \in E[X]$ le polynôme minimal de $x$ sur E. Il divise donc $P = X^{p^r} - x^{p^r}$, mais, considéré comme polynôme de L[X], puisque $P = (X - x)^{p^r}$, il existe un entier $m$ tel que $Q = (X - x)^m$. Notons $m = p^s u$ où $p$ ne divise pas $u$, de sorte que $Q = (X - x)^{p^s u} = (X^{p^s} - x^{p^s})^u$. Puisque $Q \in E[X]$ et

$$Q = X^{p^s u} - u x^{p^s} X^{p^s (u-1)} + \cdots + (-1)^u x^{p^s u},$$

on a $u x^{p^s} \in E$. Comme $p$ ne divise pas $u$, $x^{p^s} \in E$. Cela implique que $X^{p^s} - x^{p^s}$ divise Q, d'où $Q = X^{p^s} - x^{p^s}$ (et $u = 1$). Ainsi, $[L : E] = p^s$ et $[L : L_s] = [L : E]\,[E : L_s]$ est une puissance de $p$. □

## 13.5. Degré de transcendance

Pour simplifier, on n'expose la théorie que dans le cas de degré de transcendance fini. On a les mêmes énoncés dans le cas général. Il faut cependant utiliser le lemme de Zorn pour établir certains énoncés.

PROPOSITION 13.5.1. — *Soit* $K \subset L$ *une extension de corps et soit* $(x_1, \ldots, x_n)$ *une famille d'éléments de* K. *Les propositions suivantes sont équivalentes :*

(1) *pour tout polynôme non nul* $P \in K[X_1, \ldots, X_n]$, $P(x_1, \ldots, x_n) \neq 0$ *;*

(2) *l'homomorphisme canonique de* K*-algèbres,* $K[X_1, \ldots, X_n] \to L$ *tel que* $X_i \mapsto x_i$ *est injectif ;*

(3) *il existe un* K*-homomorphisme de corps* $K(X_1, \ldots, X_n) \to L$ *tel que* $X_i \mapsto x_i$.

DÉFINITION 13.5.2. — *Si ces conditions sont vérifiées, on dit que la famille* $(x_1, \ldots, x_n)$ *est* algébriquement indépendante *sur* K.

*Preuve de la proposition.* — Notons $\varphi\colon K[X_1, \ldots, X_n] \to L$ l'unique homomorphisme de K-algèbres tel que $\varphi(X_i) = x_i$. La condition (1) signifie que si $P \neq 0$, $\varphi(P) \neq 0$. Elle équivaut donc à l'égalité $\operatorname{Ker} \varphi = (0)$, si bien que (1) et (2) sont

équivalents. Supposons (2). Comme $K[X_1, \ldots, X_n]$ est un anneau intègre de corps des fractions $K(X_1, \ldots, X_n)$, et puisque L est un corps, l'homomorphisme injectif $\varphi$ s'étend en un homomorphisme de $K(X_1, \ldots, X_n) \to L$, d'où (3). Supposons maintenant (3) et soit $\bar{\varphi}\colon K(X_1, \ldots, X_n) \to L$ un K-homomorphisme de corps tel que $X_i \mapsto x_i$ pour tout $i$. Nécéssairement, la restriction de $\bar{\varphi}$ à $K[X_1, \ldots, X_n]$ est égale à $\varphi$. Comme tout homomorphisme de corps, $\bar{\varphi}$ est injectif et par suite, $\operatorname{Ker}\varphi = \operatorname{Ker}\bar{\varphi} \cap K[X_1, \ldots, X_n] = (0)$, d'où (2). □

Définition 13.5.3. — *Soit* $K \subset L$ *une extension de corps. On dit qu'une partie* $(x_1, \ldots, x_n)$ *est une* base de transcendance *de* L *sur* K *si elle est algébriquement indépendante sur* K *et si* L *est algébrique sur le sous-corps* $K(x_1, \ldots, x_n)$ *engendré par les* $x_i$ *dans* L.

Théorème 13.5.4 (Théorème de la base incomplète). — *Soit* $K \subset L$ *une extension de corps et soit* $A \subset C$ *deux parties finies de* L *telles que* A *soit algébriquement indépendante sur* K *et telle que* L *soit algébrique sur la sous-extension de* L *engendré par les éléments de* C. *Alors, il existe une base de transcendance* B *de* L *sur* K *telle que* $A \subset B \subset C$.

*Démonstration.* — On raisonne par récurrence sur le cardinal de $C \setminus A$. Si $C = A$, il n'y a rien à démontrer. Supposons le résultat vrai si $\operatorname{card}(C \setminus A) = n$ et montrons le pour $n+1$. Soit $\theta$ un élément de $C \setminus A$ et examinons les deux seules possibilités :

– Supposons que $\theta$ est algébrique sur l'extension K(A) engendrée par A dans L. Posons alors $A' = A$ et $C' = C \setminus \{\theta\}$. Par hypothèse, tout $x \in L$ est algébrique sur $K(C')[\theta]$. Puisque $\theta$ est algébrique sur $K(A) \subset K(C')$, tout élément de L est donc algébrique sur $K(C')$. On peut alors appliquer l'hypothèse de récurrence à $A \subset C'$, d'où l'existence d'une base de transcendance B avec $A \subset B \subset C'$ ; en particulier, $B \subset C$.

– Supposons que $\theta$ n'est pas algébrique sur K(A). Alors, la partie $A' = A \cup \{\theta\}$ est algébriquement indépendante sur K. Notons en effet $A = \{x_1, \ldots, x_r\}$ et soit $P \in K[X_1, \ldots, X_r, T]$ un polynôme tel que $P(x_1, \ldots, x_r, \theta) = 0$. Si P ne fait pas intervenir T, c'est-à-dire sir $P \in K[X_1, \ldots, X_r]$, on a une relation de dépendance algébrique entre $x_1, \ldots, x_r$, d'où $P = 0$. Sinon, P fait intervenir T et $\theta$ est algébrique sur $K[x_1, \ldots, x_r]$, c'est-à-dire sur K(A), ce qui est une contradiction. L'extension L est algébrique sur K(C) et $A' \subset C$ est une partie algébriquement indépendante sur K. Par récurrence, il existe une base de transcendance B avec $A' \subset B \subset C$ ; en particulier, $A \subset B$.

Ceci achève la démonstration par récurrence du théorème. □

Corollaire 13.5.5. — *Soit* $K \subset L$ *une extension de corps de type fini. Alors, il existe une base de transcendance de* L *sur* K.

*Démonstration.* — Soit C une partie de L telle que $L = K(C)$, de sorte que L est algébrique sur K(C) ! Posons $A = \varnothing$ ; c'est une partie algébriquement indépendante. D'après le théorème, il existe une base de transcendance $B \subset C$. □

*Exercice 13.5.6.* — Soit $K \subset L$ une extension de corps et soit $(x_1, \ldots, x_n)$ une partie de L.

Établir l'équivalence des conditions suivantes :

(1) la partie $(x_1, \ldots, x_n)$ est algébriquement indépendante et est maximale pour cette propriété ;

(2) L est algébrique sur $K(x_1, \ldots, x_n)$ et $(x_1, \ldots, x_n)$ est minimale pour cette propriété ;

(3) $(x_1, \ldots, x_n)$ est une base de transcendance de L sur K.

Lemme 13.5.7 (Lemme d'échange). — *Soit* $K \subset L$ *une extension de corps. Soit* $(x_1, \ldots, x_n)$ *et* $(y_1, \ldots, y_m)$ *deux bases de transcendance de* L *sur* K. *Alors, pour tout* $i \in \{1; \ldots; n\}$, *il existe* $j \in \{1; \ldots; m\}$ *tel que* $(x_1, \ldots, x_{i-1}, y_j, x_{i+1}, \ldots, x_n)$ *soit une base de transcendance de* L *sur* K.

*Démonstration.* — Pour simplifier les notations, on suppose que $i = 1$.

Par définition, tout élément de L est algébrique sur le corps $K(x_1, \ldots, x_n)$ engendré par les $x_i$ dans L. Pour tout $j \in \{1; \ldots; m\}$, soit donc $P_j \in K(x_1, \ldots, x_n)[Y]$ un polynôme irréductible tel que $P_j(y_j) = 0$. Quitte à multiplier $P_j$ par un « dénominateur commun », on peut supposer que pour tout $j$, $P_j \in K[x_1, \ldots, x_n][Y]$.

Supposons qu'aucun des $P_j$ ne fait intervenir $x_1$. Alors, pour tout $j$, $y_j$ est algébrique sur $K(x_2, \ldots, x_n)$. Comme L est algébrique sur $K(y_1, \ldots, y_m)$, L est algébrique sur $K(x_2, \ldots, x_n)$. En particulier, $x_1$ est algébrique sur $K(x_2, \ldots, x_n)$ mais ceci contredit l'hypothèse que $(x_1, \ldots, x_n)$ est algébriquement libre. Il existe donc $j \in \{1; \ldots; m\}$ tel que $P_j$ fait intervenir $x_1$. Montrons qu'un tel $j$ convient, c'est-à-dire que $(y_j, x_2, \ldots, x_n)$ est une base de transcendance de L sur K.

En effet, puisque $P_j$ fait intervenir $x_1$, la relation $P_j(y_j) = 0$ montre que $x_1$ est algébrique sur $K[y_j, x_2, \ldots, x_n]$. Comme tout élément de L est algébrique sur $K[x_1, \ldots, x_n]$, L est ainsi algébrique sur $K[y_j, x_2, \ldots, x_n]$. De plus, $(y_j, x_2, \ldots, x_n)$ est algébriquement indépendante : soit par l'absurde $P \in K[Y, X_2, \ldots, X_n]$ un polynôme non nul vérifiant $P(y_j, x_2, \ldots, x_n) = 0$. Comme la famille $(x_2, \ldots, x_n)$ est algébriquement indépendante, P fait intervenir Y. et $y_j$ est algébrique sur $K[x_2, \ldots, x_n]$. Par suite, L est algébrique sur $K[x_2, \ldots, x_n]$ et en particulier, $x_1$ est algébrique sur $K[x_2, \ldots, x_n]$ ce qui contredit l'hypothèse que $(x_1, \ldots, x_n)$ est algébriquement indépendante. □

Théorème 13.5.8. — *Soit* $K \subset L$ *une extension de corps (de type fini). Alors, toutes les bases de transcendance de* L *sur* K *ont même cardinal.*

DÉFINITION 13.5.9. — *Le cardinal d'une base de transcendance quelconque est appelé* degré de transcendance *de* L *sur* K *et est noté* $\deg \mathrm{tr}_{\mathrm{K}}(\mathrm{L})$.

*Démonstration du théorème.* — Soit $(y_1, \ldots, y_m)$ une base de transcendance de L sur K de cardinal minimal. Soit $(x_1, \ldots, x_n)$ une autre base de transcendance. On va montrer que $m = n$ par récurrence descendante sur le cardinal $r$ de l'intersection

$$\{x_1; \ldots; x_n\} \cap \{y_1; \ldots; y_m\}.$$

Si $r = m$, la famille $(y_1; \ldots; y_m)$ est contenue dans $(x_1, \ldots, x_n)$. Comme ce sont toutes deux des bases, ces deux familles sont égales et $m = n$.

Supposons maintenant $r < m$ et modifions les notations de sorte que $x_1 = y_1$, …, $x_r = y_r$, si bien que

$$\{x_1; \ldots; x_n\} \cap \{y_1; \ldots; y_m\} = \{x_1; \ldots; x_r\}.$$

Soit $i = r + 1$ et soit $j \in \{1; \ldots; m\}$ un entier fourni par le lemme d'échange 13.5.7, si bien que $(x_1, \ldots, x_r, y_j, x_{r+2}, \ldots, x_n)$ est une base de transcendance de L sur K. Comme $(x_1, \ldots, x_n)$ est une base de transcendance de L sur K, $(x_1, \ldots, x_r, x_{r+2}, \ldots, x_n)$ n'en est pas une et $j > r$. L'intersection de cette base et de la base $(y_1, \ldots, y_n)$ vérifie

$$\{x_1, \ldots, x_r, y_j, x_{r+1}, \ldots, x_n\} \cap \{y_1, \ldots, y_m\} = \{y_1; \ldots; y_r; y_j\}$$

et est donc de cardinal $r+1$. Par récurrence, ces deux bases ont même cardinal et $m = n$. □

*Exemple 13.5.10.* — Si K est un corps, $\mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ est de degré de transcendance $n$.

En effet, la famille $(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ est algébriquement indépendante sur K et $\mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ est algébrique sur l'extension de K engendrée par les $\mathrm{X}_i$ (puisque égale !).

*Exemple 13.5.11.* — Soit $\mathrm{P} \in \mathrm{K}[\mathrm{X}, \mathrm{Y}]$ un polynôme irréductible et soit L le corps des fractions de l'anneau intègre $\mathrm{K}[\mathrm{X}, \mathrm{Y}]/(\mathrm{P})$. Alors, $\deg \mathrm{tr}_{\mathrm{K}} \mathrm{L} = 1$.

*Démonstration.* — Notons $x$ et $y$ les classes de X et Y dans L. Comme $\mathrm{K}(x, y) = \mathrm{L}$, L est de degré de transcendance $\leq 2$. De plus, puisque $\mathrm{P}(x, y) = 0$ et $\mathrm{P} \neq 0$, $(x, y)$ n'est pas algébriquement indépendante et $\deg \mathrm{tr}_{\mathrm{K}} \mathrm{L} \leq 1$. Comme P est irréductible, il n'est pas constant et fait intervenir l'une des variables X ou Y. Supposons, pour fixer les idées que ce soit Y. Alors, l'homomorphisme $\varphi\colon \mathrm{K}[\mathrm{X}] \to \mathrm{L}$ tel que $\mathrm{X} \mapsto x$ est injectif : si $\mathrm{Q} \in \operatorname{Ker} \varphi$, on a $\mathrm{Q}(x) = 0$. Par suite, Q(X) est multiple de P(X,Y). Considérons les degrés par rapport à Y ; on trouve si $\mathrm{Q} \neq 0$ que

$$0 = \deg_{\mathrm{Y}} \mathrm{Q}(\mathrm{X}) \geq \deg_{\mathrm{Y}} \mathrm{P} > 0,$$

ce qui est absurde. Donc $Q = 0$ et $\varphi$ est injectif. Par suite, $(x)$ est une partie algébriquement libre sur K et $\deg \mathrm{tr}_K L \geq 1$. □

## 13.6. Exercices

*Exercice 13.6.1.* — Soit K un corps et soit $n$ un entier tel que $n \geq 2$. Soit $E = K[\zeta]$ une extension de K engendrée par une racine primitive $n^e$ de l'unité.

**a)** Montrer que l'ensemble des racines $n^e$ de l'unité dans E est un groupe cyclique d'ordre $n$, engendré par $\zeta$.

**b)** Soit $\sigma$ un élément de $\mathrm{Gal}(E/K)$. Montrer qu'il existe un entier $d$ premier à $n$ tel que $\sigma(\zeta) = \zeta^d$.

**c)** Construire un homomorphisme de groupes injectif $\varphi$: $\mathrm{Gal}(E/K) \to (\mathbf{Z}/n\mathbf{Z})^*$. En déduire que $\mathrm{Gal}(E/K)$ est un groupe abélien.

*Exercice 13.6.2.* — Soit K un corps et soit $E = K(X)$ le corps des fractions rationnelles à coefficients dans K.

**a)** Montrer qu'il existe deux K-automorphismes de E, uniques, $\alpha$ et $\beta$ tels que $\alpha(X) = 1/X$ et $\alpha(X) = 1 - X$. Montrer que le sous-groupe G de $\mathrm{Gal}(E/K)$ engendré par $\alpha$ et $\beta$ est fini, isomorphe au groupe symétrique $\mathfrak{S}_3$.

**b)** Soit F le corps $E^G$ formé des fractions rationnelles $P \in K(X)$ telles que $\alpha(P) = \beta(P) = P$. Montrer que F contient la fraction

$$f(X) = \frac{(X^2 - X + 1)^3}{X^2(X-1)^2}.$$

**c)** Montrer que l'extension $K(f) \subset E$ est finie de degré 6. En déduire que $F = K(f)$.

*Exercice 13.6.3.* — **a)** Soit G un groupe et F un corps. Soit $\sigma_1, \ldots, \sigma_n$ $n$ homomorphismes distincts de G dans le groupe multiplicatif $F^\times$. Montrer que $\sigma_1, \ldots, \sigma_n$ sont linéairement indépendants : si $a_1, \ldots, a_n$ sont des éléments de F tels que $a_1\sigma_1 + \cdots + a_n\sigma_n = 0$, alors $a_1 = \cdots = a_n = 0$.

**b)** Soit E et F deux corps et $\sigma_1, \ldots, \sigma_n$ $n$ homomorphismes de corps distincts $E \to F$. Montrer qu'ils sont linéairement indépendants sur F.

*Exercice 13.6.4.* — Soit K un corps infini et $K \subset L$ une extension finie galoisienne de degré $d$. On note $\sigma_1, \ldots, \sigma_d$ les éléments de $\mathrm{Gal}(L/K)$.

**a)** Soit $(e_1, \ldots, e_d)$ une famille d'éléments de L. Montrer que le déterminant de la matrice $(\sigma_i(e_j))_{1 \leq i,j \leq d}$ est non nul si et seulement si $(e_1, \ldots, e_d)$ est une base de L comme K-espace vectoriel.

Dans la suite, on fixe une telle base $(e_1, \ldots, e_d)$. Soit $P \in L[X_1, \ldots, X_d]$ tel que pour tout $x \in K$,

$$P(\sigma_1(x), \ldots, \sigma_d(x)) = 0.$$

**b)** Soit $Q \in L[X_1, \ldots, X_d]$ le polynôme

$$Q = P(\sum_{i=1}^{d} \sigma_1(e_i)X_i, \ldots, \sum_{i=1}^{d} \sigma_d(e_i)).$$

Montrer que pour tous $(x_1, \ldots, x_d) \in K^d$, $Q(x_1, \ldots, x_d) = 0$. En déduire que $Q = 0$.

**c)** Montrer que $P = 0$ (*indépendance algébrique des* $\sigma_i$).

**d)** Montrer qu'il existe $\theta \in L$ tel que $(\sigma_1(\theta), \ldots, \sigma_d(\theta))$ soit une K-base de L. (Une telle base est appelée *base normale* de L sur K.)

*Exercice 13.6.5.* — Soit $F \subset E$ une extension galoisienne de corps, de groupe de Galois $G = \mathrm{Gal}(E/F)$.

**a)** Soit $\alpha \in E^\times$ et $c\colon G \to E^\times$ l'application telle que $c(\sigma) = \alpha/\sigma(\alpha)$ pour tout $\sigma \in G$. Montrer que pour tous $\sigma$ et $\tau$ dans G, on a

$$c(\sigma\tau) = c(\sigma)\sigma(c(\tau)).$$

**b)** Réciproquement, soit $c\colon G \to E^\times$ une application vérifiant cette relation. En utilisant l'exercice 13.6.3, montrer qu'il existe $x \in E$ tel que

$$\alpha = \sum_{\sigma \in G} c(\sigma)\sigma(x) \neq 0.$$

En déduire que pour tout $\sigma \in G$, $c(\sigma) = \alpha/\sigma(\alpha)$.

**c)** Soit $\chi\colon G \to F^\times$ un homomorphisme de groupes. Montrer qu'il existe $\alpha \in E$ tel que $\chi(\sigma) = \alpha/\sigma(\alpha)$ pour tout $\sigma \in G$.

**d)** On suppose que G est cyclique. Soit $\sigma$ un générateur de G. Soit $x \in F$. Montrer que $N_{L/K}(x) = 1$ si et seulement s'il existe $\alpha \in F$ tel que $x = \alpha/\sigma(\alpha)$.

*Exercice 13.6.6.* — Si $n \geq 1$, soit $\Phi_n \in \mathbf{C}[X]$ l'unique polynôme unitaire dont les racines sont simples, égales aux racines primitives $n^{\mathrm{e}}$ de l'unité dans $\mathbf{C}$.

**a)** Montrer que $\prod_{d|n} \Phi_d = X^n - 1$. En déduire par récurrence que pour tout $n$, $\Phi_n \in \mathbf{Z}[X]$.

**b)** Si $p$ est un nombre premier, calculer $\Phi_p(X)$. Montrer qu'il existe des entiers $a_1, \ldots, a_{p-1}$ tels que $\Phi_p(1+X) = X^{p-1} + pa_1X^{p-2} + \cdots + pa_{p-1}$, avec $a_{p-1} = 1$. À l'aide du critère d'Eisenstein de l'exercice 5.6.5, en déduire que $\Phi_p$ est irréductible dans $\mathbf{Q}[X]$.

**c)** Soit $n$ un entier, $n \geq 2$ et soit $\zeta$ une racine primitive $n^{\mathrm{e}}$ de l'unité. On va montrer que $\Phi_n$ est irréductible dans $\mathbf{Q}[X]$. Soit P le polynôme minimal de $\zeta$. Montrer que $P \in \mathbf{Z}[X]$ et qu'il divise $\Phi_n$ dans $\mathbf{Z}[X]$.

Soit $p$ un nombre premier ne divisant pas $n$. Montrer qu'il existe $b \in \mathbf{Z}[\zeta]$ tel que $P(\zeta^p) = pb$.

**d)** Montrer que $\zeta^p$ est une racine primitive $n^{\text{e}}$ de l'unité. Si $\mathrm{P}(\zeta^p) \neq 0$, montrer en dérivant le polynôme $\mathrm{X}^n - 1$ que $n\zeta^{p(n-1)} \in p\mathbf{Z}[\zeta]$. En déduire une contradiction et donc que pour tout nombre premier $p$ premier à $n$, $\mathrm{P}(\zeta^p) = 0$.

**e)** Montrer que $\Phi_n$ est irréductible dans $\mathbf{Q}[\mathrm{X}]$.

*Exercice 13.6.7.* — Soit K un corps fini, soit $p$ sa caractéristique et $q$ son cardinal.

**a)** Si $m \in \mathbf{N}$, calculer $\mathrm{S}_m = \sum_{x \in \mathrm{K}} x^m$.

**b)** Si $\mathrm{P} \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, on note $\mathrm{S}(\mathrm{P}) = \sum_{x \in \mathrm{K}} x^m$. Si $\deg \mathrm{P} < n(q-1)$, montrer que $\mathrm{S}(\mathrm{P}) = 0$.

**c)** Soit $\mathrm{P}_1, \ldots, \mathrm{P}_r$ des polynômes de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ tels que $\sum_{i=1}^{r} \deg \mathrm{P}_i < n$. Soit $\mathrm{P} = (1 - \mathrm{P}_1^{q-1}) \ldots (1 - \mathrm{P}_r^{q-1})$. Montrer que $\mathrm{S}(\mathrm{P}) = 0$.

Si V désigne l'ensemble des $x \in \mathrm{K}^n$ tels que $\mathrm{P}_1(x) = \cdots = \mathrm{P}_n(x) = 0\}$, en déduire que $\operatorname{card} \mathrm{V}$ est multiple de $p$ (*théorème de Chevalley–Warning*).

**d)** Soit $\mathrm{P} \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ un polynôme homogène de degré $d > 0$. Si $d < n$, montrer qu'il existe $(x_1, \ldots, x_n) \in \mathrm{K}^n$ tel que $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ et $\mathrm{P}(x_1, \ldots, x_n) = 0$.

*Exercice 13.6.8.* — Soit $\mathrm{K} \subset \mathrm{L}$ et $\mathrm{L} \subset \mathrm{M}$ deux extensions de corps de type fini. Montrer l'égalité

$$\deg \mathrm{tr}_{\mathrm{K}} \mathrm{M} = \deg \mathrm{tr}_{\mathrm{K}} \mathrm{L} + \deg \mathrm{tr}_{\mathrm{L}} \mathrm{M}.$$

*Exercice 13.6.9.* — Soit $\mathrm{K} \subset \mathbf{C}(\mathrm{T})$ un sous-corps contenant $\mathbf{C}$ mais distinct de $\mathbf{C}$.

**a)** Montrer que l'extension $\mathrm{K} \subset \mathbf{C}(\mathrm{T})$ est algébrique, finie.

**b)** On note $n = [\mathbf{C}(\mathrm{T}) : \mathrm{K}]$ son degré. Montrer que le polynôme minimal de T sur K est de la forme

$$f(\mathrm{X}) = \mathrm{X}^n + k_1 \mathrm{X}^{n-1} + \cdots + k_n$$

et qu'il existe $j \in \{1; \ldots; n\}$ tel que $k_j \notin \mathbf{C}$.

**c)** On fixe un tel entier $j$ et on note $u = k_j = g/h$ où $g, h \in \mathbf{C}[\mathrm{T}]$ sont deux polynômes premiers entre eux. Soit $m = \max(\deg g, \deg h)$. Montrer que $m \geq n$. Montrer aussi qu'il existe $q \in \mathrm{K}[\mathrm{X}]$ tel que $g(\mathrm{X}) - uh(\mathrm{X}) = q(\mathrm{X}) f(\mathrm{X})$.

**d)** Montrer qu'il existe des polynômes $c_0, \ldots, c_n \in \mathbf{C}[\mathrm{T}]$ premiers entre eux tels que pour tout $i$, $c_i/c_0 = k_i$.

On pose $f(\mathrm{X}, \mathrm{T}) = c_0(\mathrm{T})\mathrm{X}^n + \cdots + c_n(\mathrm{T})$. Montrer que $f(\mathrm{X}, \mathrm{T})$ est irréductible dans $\mathbf{C}[\mathrm{X}, \mathrm{T}]$.

**e)** Montrer qu'il existe $q \in \mathbf{C}[\mathrm{X}, \mathrm{T}]$ tel que

$$g(\mathrm{X})h(\mathrm{T}) - g(\mathrm{T})h(\mathrm{X}) = q(\mathrm{X}, \mathrm{T}) f(\mathrm{X}, \mathrm{T}).$$

En déduire que $m = n$ et donc que $\mathrm{K} = \mathbf{C}(u)$ (*théorème de Lüroth*).

## 13.7. Solutions

*Solution de l'exercice 13.6.1.* — **a)** L'ensemble $\mu_n = \{1; \zeta; \zeta^2; \ldots; \zeta^{n-1}\}$ est un sous-groupe cyclique de $E^*$, d'ordre $n$, et tout élément $x$ de $\mu_n$ vérifie $x^n = 1$. D'autre part, l'ensemble des racines du polynôme $X^n - 1$ dans E a pour cardinal au plus $n$. Il en résulte que $\mu_n$ est l'ensemble des racines $n^e$ de l'unité dans E. Par suite, c'est ensemble est un sous-groupe cyclique de $E^*$ d'ordre $n$, engendré par $\zeta$.

**b)** Comme $\zeta^n = 1$, $\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$ et $\sigma(\zeta)$ est une racine $n^e$ de l'unité. Par suite, il existe un entier $d \in \{0; \ldots; n-1\}$ tel que $\sigma(\zeta) = \zeta^d$. Soit $k$ l'ordre de $\sigma(\zeta)$, c'est-à-dire le plus petit entier $\geq 1$ tel que $\sigma(\zeta)^k = 1$. On a donc $\sigma(\zeta^k) = 1$, d'où $\zeta^k = 1$. Comme $\zeta$ est une racine primitive, $k \geq n$ et $\sigma(\zeta)$ est une racine primitive $n^e$ de l'unité. Cela implique que $d$ est premier à $n$.

**c)** Soit $\varphi$ l'application de $\mathrm{Gal}(E/K)$ dans $(\mathbf{Z}/n\mathbf{Z})^*$ telle que $\varphi(\sigma) = [d]$, si $\sigma(\zeta) = \zeta^d$. Elle est bien définie d'après la question précédente. Montrons que c'est un homomorphisme de groupes. Soit donc $\sigma$ et $\tau$ deux éléments de $\mathrm{Gal}(E/K)$, avec $\sigma(\zeta) = \zeta^d$ et $\tau(\zeta) = \zeta^e$. Soit $f$ un entier tel que $ef \equiv 1 \pmod{n}$. Alors, $\tau(\zeta^f) = \tau(\zeta)^f = \zeta^{ef} = \zeta$, c'est-à-dire $\tau^{-1}(\zeta) = \zeta^f$ et $(\sigma\tau^{-1})(\zeta) = \sigma(\zeta^f) = \zeta^{df}$. On a ainsi $\varphi(\sigma\tau^{-1}) = [df] = [d][f] = [d]/[e] = \varphi(\sigma)/\varphi(\tau)$, comme il fallait démontrer.

De plus, si $\varphi(\sigma) = [1]$, c'est-à-dire si $\sigma(\zeta) = \zeta$, alors pour tout polynôme $P \in K[X]$, $\sigma(P(\zeta)) = P(\sigma(\zeta)) = P(\zeta)$. Puisque $E = K[\zeta]$, on a $\sigma(x) = x$ pour tout $x \in E$ et $\sigma = \mathrm{Id}_E$. Ainsi, $\varphi$ est injectif.

Cela montre que $\mathrm{Gal}(E/K)$ est isomorphe à un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$, donc est un groupe commutatif.

*Solution de l'exercice 13.6.2.* — **a)** $\alpha$ et $\beta$ vérifient $\alpha(P) = P(1/X)$ et $\beta(P) = P(1-X)$ pour toute fraction rationnelle $P \in K(X)$. De plus, $\alpha^2(P) = \alpha(P(1/X)) = P$ donc $\alpha^2 = \mathrm{Id}$ et $\beta^2(P) = \beta(P(1-X)) = P$ donc $\beta^2 = \mathrm{Id}$. Ce sont donc des K-automorphismes de E.

On constate que les trois « points » 0, 1 et $\infty$ (de la droite projective sur K) sont préservés par $\alpha$ et $\beta$. Ils seront donc préservés par le sous-groupe qu'ils engendrent. Considérons ainsi l'ensemble $X = \{0; 1; \infty\}$. Associons à $\alpha$ la transposition $a = (0\,\infty)$ dans $\mathfrak{S}_3$ et à $\beta$ la transposition $b = (0\,1)$. Les deux permutations $a$ et $b$ engendrent le groupe (isomorphe à $\mathfrak{S}_3$) des permutations de X. De plus, $ab$ est la permutation circulaire $(1\,\infty\,0)$, d'ordre 3. Les éléments de $\mathfrak{S}_3$ sont ainsi Id, $a$, $b$, la troisième transposition $(1, \infty) = bab$ et les deux permutations circulaires $ab$ et $(ab)^2$.

Remarquons ensuite que $\alpha^2 = \mathrm{Id}$ et $\beta^2 = \mathrm{Id}$. De plus, soit $\gamma = \alpha\beta$, de sorte que $\gamma(X) = \alpha(1-X) = 1/(1-X)$. On a alors

$$\gamma^2(X) = \Big(1 - \frac{1}{1-X}\Big)^{-1} = \Big(\frac{-X}{1-X}\Big)^{-1} = 1 - \frac{1}{X}$$

et

$$\gamma^3(\mathrm{X}) = \alpha\beta(1 - \frac{1}{\mathrm{X}}) = \alpha(1/\mathrm{X}) = \mathrm{X},$$

donc $\gamma^3 = \mathrm{Id}$.

Or, remarquons le groupe engendré par deux éléments $x$ et $y$ avec les relations $x^2 = y^2 = (xy)^3 = 1$ est fini d'ordre 6. Un élément de ce groupe est un « mot » en les lettres $x$ et $y$ (car $x = x^{-1}$ et $y = y^{-1}$) dans lequel il n'y a ni deux $x$ ni deux $y$ consécutifs. Ils sont ainsi de la forme $xyx\ldots x$, $xyx\ldots y$, $yx\ldots x$ ou $yx\ldots y$. Toutefois, comme $(xy)^3 = 1$, on peut supposer que le mot $xyxyxy$ n'apparaît pas, et le mot $yxyxyx = (xyxyxy)^{-1} = 1$ non plus. Ainsi, on ne doit considérer que des mots de longueur inférieure ou égale à 5 parmi lesquels 1, $x$, $y$, $xy$, $xyx$, $xyxy$. Les autres se réduisent à ceux-là : $xyxyx = (xy)^3x^{-1} = x$, puis pour ceux commençant par $y$, $yx = (xy)^{-1} = (xy)^2 = xyxy$, $yxy = xyxyy = xyx$, $yxyx = xyxx = xy$ et $yxyxy = xyy = x$.

Les deux éléments $a$ et $b$ de $\mathfrak{S}_3$ vérifient les relations $a^2 = b^2 = (ab)^3$, si bien que le groupe $\mathfrak{S}_3$ est un quotient de ce groupe. On a ainsi un isomorphisme. L'homomorphisme $\mathfrak{S}_3 \to \langle\alpha, \beta\rangle$ qu'on en déduit est injectif : son noyau ne contient pas $a$, donc ne contient aucune transposition (qui sont conjuguées à $a$) et ne contient pas $ab$, donc ne contient aucun 3-cycle (l'autre est conjugué à $ab$).

**b)** Il faut vérifier que $f(1/\mathrm{X}) = f(1 - \mathrm{X}) = f(\mathrm{X})$. Or,

$$f(1/\mathrm{X}) = \frac{((1/\mathrm{X})^2 - (1/\mathrm{X}) + 1)^3}{(1/\mathrm{X})^2(1/\mathrm{X} - 1)^2} = \frac{\mathrm{X}^{-6}(1 - \mathrm{X} + \mathrm{X}^3)^3}{\mathrm{X}^{-4}(1 - \mathrm{X})^2} = \frac{(\mathrm{X}^2 - \mathrm{X} + 1)^3}{\mathrm{X}^2(\mathrm{X} - 1)^2} = f(\mathrm{X})$$

et, avant de caculer $f(1 - \mathrm{X})$, remarquons que

$$(1 - \mathrm{X})^2 - (1 - \mathrm{X}) + 1 = 1 - 2\mathrm{X} + \mathrm{X}^2 + \mathrm{X} = 1 - \mathrm{X} + \mathrm{X}^2$$

si bien que

$$f(1 - \mathrm{X}) = \frac{(1 - \mathrm{X} + \mathrm{X}^2)^3}{(1 - \mathrm{X})^2(\mathrm{X})^2} = f(\mathrm{X}).$$

Enfin, l'ensemble des fractions rationnelles P telles que $\alpha(\mathrm{P}) = \beta(\mathrm{P}) = \mathrm{P}$ est le sous-corps F de E fixe par le groupe de K-automorphismes de E engendré par $\alpha$ et $\beta$.

**c)** Montrons que $[\mathrm{E} : \mathrm{K}(f)]]$ est égal à 6. Pour cela, il suffit de montrer que X est annulé par un polynôme irréductible de degré 6, en l'occurrence

$$(\mathrm{X}^2 - \mathrm{X} + 1)^3 - f\mathrm{X}^2(\mathrm{X} - 1)^2.$$

Le polynôme $(\mathrm{X}^2 - \mathrm{X} + 1)^3 - \mathrm{Y}\mathrm{X}^2(\mathrm{X} - 1)^2$ de K[X,Y] est irréductible car de degré 1 en Y et ses coefficients (en tant que polynôme de K[X][Y]) sont premiers entre eux. Par suite, il est irréductible dans $\mathrm{K}(\mathrm{Y})[\mathrm{X}] \simeq \mathrm{K}(f)[\mathrm{X}]$.

Comme le groupe engendré par $\alpha$ et $\beta$ est d'ordre 6 (isomorphe à $\mathfrak{S}_3$), $[\mathrm{E}:\mathrm{F}]=6$. On a alors $[\mathrm{E}:\mathrm{F}][\mathrm{F}:\mathrm{K}(f)]=[\mathrm{E}:\mathrm{K}(f)]=6$, donc $\mathrm{F}=\mathrm{K}(f)$.

*Solution de l'exercice 13.6.3.* — **a)** On démontre ce résultat par récurrence sur $n$. Si $n=1$ et $a_1\sigma_1=0$, on a $a_1\sigma_1(1_\mathrm{G})=a_1=0$, d'où l'assertion pour $n=1$. Supposons la vraie pour $n-1$ sous la forme : « $n-1$ homomorphismes distincts de G dans $\mathrm{F}^\times$ sont linéairement indépendants » et montrons la pour $n$. Soit $a_1,\dots,a_n$ des éléments de F tels que $a_1\sigma_1+\cdots+a_n\sigma_n=0$.

Soit $g_0\in\mathrm{G}$. Écrivons alors la relation de dépendance linéaire en $g\in\mathrm{G}$ et en $gg_0$. Cela fournit deux relations

$$\begin{aligned} a_1\sigma_1(g)+\cdots+a_n\sigma_n(g)&=0\\ a_1\sigma_1(g_0)\sigma_1(g)+\cdots+a_n\sigma_n(g_0)\sigma_n(g)&=0. \end{aligned}$$

Multiplions la première équation par $\sigma_n(g_0)$ puis soustrayons la seconde. Il vient

$$\begin{aligned} a_1(\sigma_n(g_0)-\sigma_1(g_0))\sigma_1(g)+a_2(\sigma_n(g_0)-\sigma_2(g_0))\sigma_2(g)&\\ +\cdots+a_{n-1}(\sigma_n(g_0)-\sigma_{n-1}(g_0))\sigma_{n-1}(g)&=0. \end{aligned}$$

Cette relation étant vérifiée par tout $g\in\mathrm{G}$, on a par récurrence, $a_i(\sigma_n(g_0)-\sigma_i(g_0))=0$ pour tout $i\leq n-1$ et tout $g_0\in\mathrm{G}$.

S'il existe $i$ avec $a_i\neq 0$, cette relation implique $\sigma_i=\sigma_n$, ce qui est absurde. Donc $a_i=0$ pour tout $i\leq n-1$. Il vient alors $a_n\sigma_n=0$, d'où $a_n=0$ d'après le cas $n=1$.

**b)** C'est une conséquence immédiate de la première question : la restriction des $\sigma_i$ à $\mathrm{E}^\times=\mathrm{E}\setminus\{0\}$ définit $n$ homomorphismes distincts du groupe $\mathrm{E}^\times$ dans $\mathrm{F}^\times$. Ceux-ci sont linéairement indépendants sur F d'après la première question. Par suite, aucune combinaison linéaire non triviale $a_1\sigma_1+\cdots+a_n\sigma_n$ peut n'être nulle.

*Solution de l'exercice 13.6.4.* — **a)** Notons A la matrice $(\sigma_i(e_j))_{1\leq i,j\leq d}$ et T la matrice $(\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(e_ie_j))_{1\leq i,j\leq d}$. On a donc

$$\mathrm{T}_{ij}=\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(e_ie_j)=\sum_{k=1}^{d}\sigma_k(e_ie_j)=\sum_{k=1}^{d}\sigma_k(e_i)\sigma_k(e_j)=\sum_{k=1}^{d}\mathrm{A}_{ki}\mathrm{A}_{kj}$$

si bien que $\mathrm{T}={}^t\mathrm{A}\mathrm{A}$. Par suite, $\det\mathrm{T}=(\det\mathrm{A})^2$ et les deux matrices A et T sont simultanément inversibles ou non inversibles.

Comme l'extension $\mathrm{K}\subset\mathrm{L}$ est galoisienne, elle est en particulier séparable. Par suite, la forme bilinéaire $(x,y)\mapsto\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(xy)$ est non dégénérée. Sa matrice dans la base $(e_1,\dots,e_d)$, qui n'est autre que T, est donc inversible.

**b)** Pour tout $(x_1,\dots,x_d)\in \mathrm{K}^d$, si l'on pose $x=x_1e_1+\cdots+x_de_d\in \mathrm{L}$, alors $\sigma_i(x)=\sum_{j=1}^{d}\sigma_i(e_j)x_j$, si bien que

$$\begin{aligned}\mathrm{Q}(x_1,\dots,x_d)&=\mathrm{P}\Big(\sum_{j=1}^{d}\sigma_1(e_j)x_j,\dots,\sum_{j=1}^{d}\sigma_d(e_j)x_j\Big)\\&=\mathrm{P}(\sigma_1(x),\dots,\sigma_d(x))=0.\end{aligned}$$

Comme le corps K est infini, le polynôme Q est nécessairement nul.

**c)** On remarque que l'on passe du polynôme P au polynôme Q par un *changement de variables* linéaires sur les inconnues. Ce changement de variables est fourni par la matrice $\mathrm{A}=(\sigma_i(e_j))$ qui est inversible. Soit $\mathrm{B}=(b_{ij})$ sa matrice inverse. Puisque

$$\mathrm{Q}(\mathrm{X}_1,\dots,\mathrm{X}_d)=\mathrm{P}((\mathrm{X}_1,\dots,\mathrm{X}_d)\cdot {}^{\mathrm{t}}\mathrm{A}),$$

on a

$$\mathrm{P}(\mathrm{X}_1,\dots,\mathrm{X}_d)=\mathrm{Q}((\mathrm{X}_1,\dots,\mathrm{X}_d)\cdot {}^{\mathrm{t}}\mathrm{B})$$

et donc $\mathrm{P}=0$.

**d)** D'après la première question, la famille $(\sigma_1(\theta),\dots,\sigma_d(\theta))$ est une K-base de L si et seulement si le déterminant $\mathrm{D}(\theta)=\det((\sigma_i(\sigma_j(\theta))))$ n'est pas nul. Si $i$ et $j$ sont dans $\{1;\dots;d\}$, notons $m(i,j)$ l'unique entier de $\{1;\dots;d\}$ tel que $\sigma_i\circ\sigma_j=\sigma_{m(i,j)}$. On a donc $\mathrm{D}(\theta)=\det(\sigma_{m(i,j)}(\theta))$. Si P désigne le polynôme $\det(\mathrm{X}_{m(i,j)})$, on a donc $\mathrm{D}(\theta)=\mathrm{P}(\sigma_1(\theta),\dots,\sigma_d(\theta))$.

Le polynôme P n'est pas le polynôme nul. En effet, si l'on applique la définition du déterminant

$$\mathrm{P}(\mathrm{X}_1,\dots,\mathrm{X}_d)=\sum_{s\in\mathfrak{S}_d}\varepsilon_s\prod_{i=1}^{d}\mathrm{X}_{m(i,s(i))},$$

on constate que le coefficient de $\mathrm{X}_1^d$ est égal à $\pm1$ : c'est la signature de l'unique permutation $s$ telle que pour tout $i$, $m(i,s(i))=1$, autrement dit, $\sigma_i\circ\sigma_{s(i)}=\sigma_1$, soit encore $\sigma_{s(i)}=\sigma_i^{-1}\circ\sigma_1$. D'après la question précédente, il existe donc $\theta\in\mathrm{L}$ tel que $\mathrm{D}(\theta)\neq0$.

*Solution de l'exercice 13.6.5.* — **a)** En effet, on a

$$\begin{aligned}c(\sigma\tau)&=\frac{\alpha}{\sigma(\tau(\alpha))}=\frac{\alpha}{\sigma(\alpha)}\frac{\sigma(\alpha)}{\sigma(\tau(\alpha)}\\&=c(\sigma)\sigma(\alpha/\tau(\alpha))=c(\sigma)\sigma(c(\tau)).\end{aligned}$$

**b)** Comme les $c(\sigma)$ sont non nuls, $\sum c(\sigma)\sigma$ est une combinaison linéaire non triviale d'homomorphismes de corps $\mathrm{E}\to\mathrm{E}$. D'après l'exercice 13.6.3, elle est non nulle et il existe $x\in\mathrm{E}$ tel que $\alpha=\sum c(\sigma)\sigma(x)\neq0$.

Alors, si $\sigma \in \mathrm{G}$,

$$\sigma(\alpha) = \sigma\Big(\sum_{\tau\in\mathrm{G}} c(\tau)\tau(x)\Big) = \sum_{\tau\in\mathrm{G}} \sigma(c(\tau))\sigma(\tau(x)).$$

Faisons le changement d'indices $g = \sigma\tau$ dans la sommation : on a alors $\sigma(c(\tau)) = c(\sigma\tau)/c(\sigma) = c(g)/c(\sigma)$. On obtient donc

$$\sigma(\alpha) = c(\sigma)^{-1} \sum_{g\in\mathrm{G}} c(g)g(x) = c(\sigma)^{-1}\alpha,$$

d'où la relation $c(\sigma) = \alpha/\sigma(\alpha)$, ainsi qu'il fallait démontrer.

**c)** Si $\chi\colon \mathrm{G} \to \mathrm{F}^\times$ est un homomorphisme de groupes, on a

$$\chi(\sigma\tau) = \chi(\sigma)\chi(\tau) = \chi(\sigma)\sigma(\chi(\tau))$$

puisque $\chi(\tau) \in \mathrm{F}$ et que $\sigma$ est un F-automorphisme de E. Ainsi, $\chi$ est justiciable de la question précédente et il existe $\alpha \in \mathrm{E}$ tel que $\chi(\sigma) = \alpha/\sigma(\alpha)$.

**d)** Si $\sigma$ est d'ordre $d$, on a $\mathrm{N}_{\mathrm{L/K}}(x) = x\sigma(x)\dots\sigma^{d-1}(x)$.

Supposons que $x = \alpha/\sigma(\alpha)$ pour $\alpha \in \mathrm{F}^\times$. Alors,

$$\mathrm{N}_{\mathrm{L/K}}(x) = \frac{\alpha}{\sigma(\alpha)}\frac{\sigma(\alpha)}{\sigma^2(\alpha)}\dots\frac{\sigma^{d-1}(\alpha)}{\sigma^d(\alpha)} = \frac{\alpha}{\alpha} = 1.$$

Réciproquement, supposons $\mathrm{N}_{\mathrm{L/X}}(x) = 1$ et définissons $c\colon \mathrm{G} \to \mathrm{E}^\times$ comme suit :

$$c(1) = 1, \quad c(\sigma) = x, \quad c(\sigma^r) = x\sigma(x)\dots\sigma^{r-1}(x), \quad c(\sigma^{d-1}(x) = x\sigma(x)\dots\sigma^{d-2}(x).$$

Comme $x\sigma(x)\dots\sigma^{d-1}(x) = 1$, remarquons que pour tout entier $n \geq 1$,

$$c(\sigma^n) = x\sigma(x)\dots\sigma^{n-1}(x).$$

Soit alors $n$ et $m$ deux entiers. On a

$$\begin{aligned} c(\sigma^n\sigma^m) &= x\sigma(x)\dots\sigma^{n-1}(x)\sigma^n(x)\sigma^{n+m-1}(x) \\ &= \big(x\sigma(x)\dots\sigma^{n-1}(x)\big)\sigma^n\big(x\sigma(x)\dots\sigma^{m-1}(x)\big) \\ &= c(\sigma^n)\sigma^n(c(\sigma^m)), \end{aligned}$$

c'est-à-dire qu'on peut appliquer la première question à l'application $c$. Il existe donc $\alpha \in \mathrm{E}^\times$ tel que $c(\sigma) = \alpha/\sigma(\alpha)$, autrement dit, $x = \alpha/\sigma(\alpha)$, ainsi qu'il fallait démontrer.

*Solution de l'exercice 13.6.6.* — Il est question dans cet exercice d'irréductibilité de polynômes de $\mathbf{Z}[\mathrm{X}]$. Comme $\mathbf{Z}$ est un anneau factoriel, rappelons qu'un tel polynôme est irréductible dans $\mathbf{Z}[\mathrm{X}]$ si et seulement si il est irréductible dans $\mathbf{Q}[\mathrm{X}]$ et si ses coefficients sont premiers entre eux dans leur ensemble. En particulier, un polynôme unitaire de $\mathbf{Z}[\mathrm{X}]$ est irréductible dans $\mathbf{Q}[\mathrm{X}]$ si et seulement s'il l'est dans $\mathbf{Q}[\mathrm{X}]$.

**a)** Pour toute racine $n^{\text{e}}$ de l'unité $\zeta$, il existe un unique entier $d$ divisant $n$ tel que $\zeta$ soit une racine primitive d'ordre $d$. Par suite, les racines de $\prod_{d|n} \Phi_d$ sont — avec multiplicités 1 — les racines $n^{\text{e}}$ de l'unité. Comme ce polynôme est unitaire, il est égal à $X^n - 1$.

Montrons par récurrence sur $n$ que pour tout entier $n \geq 1$, $\Phi_n \in \mathbf{Z}[X]$. Si $n = 1$, on a $\Phi_1 = X - 1 \in \mathbf{Z}[X]$. Supposons ce fait vrai pour tout entier $< n$. Alors, le polynôme $P = \prod_{\substack{d|n \\ d \neq n}} \Phi_d$ est unitaire et à coefficients entiers et divise $X^n - 1$. L'algorithme de division euclidienne fournit donc un polynôme Q, unitaire à coefficients entiers, tel que $X^n - 1 = PQ$. On a donc $\Phi_n = Q \in \mathbf{Z}[X]$.

**b)** Si $p$ est premier, $\Phi_p = (X^p - 1)/(X - 1) = X^{p-1} + \cdots + X + 1$. On a

$$\Phi_p(1 + X) = \frac{(1 + X)^p - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1},$$

d'où le résultat annoncé avec $a_k = \binom{p}{p-k}/p = (p-1)!/k!(p-k)!$. (On a bien $a_{p-1} = \binom{p}{1}/p = 1$.)

D'après le critère d'Eisenstein (exercice 5.6.5), le polynôme $\Phi_p(1 + X)$ est irréductible dans $\mathbf{Q}[X]$. Par suite, $\Phi_p$ lui-même est irréductible. (Si $\Phi_p = PQ$, on a $\Phi_p(1+X) = P(1+X)Q(1+X)$, ce qui impose $P(1+X)$ ou $Q(1+X)$ constant, d'où P ou Q constant.)

**c)** Comme $\zeta$ est entier sur $\mathbf{Z}$, son polynôme minimal P est à coefficients entiers et est unitaire. Comme $\Phi_n(\zeta) = 0$, P divise $\Phi_n$. Notons donc $P(X) = a_0 + a_1 X + \cdots + a_d X^d$, avec $a_i \in \mathbf{Z}$ pour tout $i$ et $a_d = 1$. L'application $x \mapsto x^p$ dans l'anneau $\mathbf{Z}[\zeta]/(p)$ est additive. Par suite, il existe $b_1 \in \mathbf{Z}[\zeta]$ tel que

$$P(\zeta)^p = pb_1 + \sum_{k=0}^{d} a_k^p \zeta^{pk}.$$

De plus, pour tout entier $j$, $j^p \equiv j \pmod{p}$, si bien qu'il existe $b_2 \in \mathbf{Z}[\zeta]$ tel que

$$P(\zeta)^p = pb_1 + pb_2 + \sum_{k=0}^{d} a_k \zeta^{pk} = p(b_1 + b_2) + P(\zeta^p).$$

Puisque $P(\zeta) = 0$, il en résulte que $P(\zeta^p) = -p(b_1 + b_2) \in p\mathbf{Z}[\zeta]$.

**d)** Comme $p$ ne divise pas $n$, $\zeta^p$ est encore une racine primitive $n^{\text{e}}$ de l'unité. Supposons $P(\zeta^p) \neq 0$. Alors, $\Phi_n$ admet un autre facteur irréductible Q tel que $Q(\zeta^p) = 0$. On écrit alors

$$X^n - 1 = \Phi_n \prod_{d|n, d \neq n} \Phi_d = P(X)Q(X)R(X)$$

avec $R \in \mathbf{Z}[X]$. Dérivons : on obtient

$$nX^{n-1} = Q'(X)\,(P(X)R(X)) + Q(X)\,(PR)'.$$

Évaluons cette égalité en $X = \zeta^p$. On obtient alors, puisque $Q(\zeta^p) = 0$,

$$n\zeta^{p(n-1)} = Q'(\zeta^p)^p P(\zeta^p) R(\zeta^p),$$

d'où $n\zeta^{p(n-1)} \in p\mathbf{Z}[\zeta]$, et en multipliant par $\zeta^p$, $n \in p\mathbf{Z}[\zeta]$. Or, ceci est absurde : $\mathbf{Z}[\zeta]$ est un $\mathbf{Z}$-module libre de rang $d$, de base $(1, \zeta, \dots, \zeta^{d-1})$. Dans cette base, $n = n \cdot 1 + 0 \cdot \zeta + \dots$ et $p$ ne divise pas $n$. Ainsi, $P(\zeta^p) = 0$.

**e)** Si P est le polynôme minimal de $\zeta$, nous avons donc prouvé que pour tout nombre premier $p$ ne divisant pas $n$, $P(\zeta^p) = 0$. Par récurrence sur le nombre de facteurs dans une décomposition en facteurs premiers, pour tout entier $d$ qui est premier à $n$, $P(\zeta^d) = 0$. Comme toute racine primitive $n^e$ de l'unité est de la forme $\zeta^d$ pour un entier $d$ premier à $n$, P s'annule en toutes les racines primitives $n^e$ de l'unité, donc par définition, P est multiple de $\Phi_n$. Comme P divise $\Phi_n$ et que ces deux polynômes sont unitaires, $P = \Phi_n$.

Nous avons donc prouvé que $\Phi_n$ est irréductible.

*Solution de l'exercice 13.6.7.* — **a)** Si $n = 0$, $x^m = 1$ pour tout $x$ (pour $x = 0$, c'est une convention). Par suite, $S_0 = q = 0$.

Supposons maintenant $m > 0$. Alors, $S_m = \sum_{x \in K^*} x^m$. Soit $r = \operatorname{pgcd}(m, q-1)$ et $d = (q-1)/r$, de sorte que lorsque $x$ parcourt $K^*$, c'est-à-dire les racines $(q-1)^e$ de l'unité, $x^m$ parcourt les racines $d^e$ de l'unité, chacune $r$ fois. Par suite,

$$S_m = r \sum_{\zeta^d = 1} \zeta.$$

Si $d = 1$, c'est-à-dire $r = q - 1$, ou encore $m$ multiple de $q - 1$, $S_m = q - 1 = -1$. Si $d > 1$, les racines $d^e$ de l'unité sont les racines du polynôme $X^d - 1$. Leur somme est l'opposé du terme de degré $d - 1$, donc nulle puisque $d \geq 2$. On a alors $S_m = 0$.

En conclusion :

$$S_m = \begin{cases} 0 & \text{si } m = 0\,; \\ 0 & \text{si } m \text{ n'est pas multiple de } q-1\,; \\ -1 & \text{si } m \geq 1 \text{ est multiple de } q-1. \end{cases}$$

**b)** On écrit

$$P = \sum_{\mathbf{m} \in \mathbf{N}^n} c_{\mathbf{m}} X_1^{m_1} \dots X_n^{m_n}.$$

Par définition, on a

$$S(P) = \sum_{\mathbf{m} \in \mathbf{N}^n} c_{\mathbf{m}} \sum_{(x_1, \dots, x_n) \in K^n} x_1^{m_1} \dots x_n^{m_n} = \sum_{\mathbf{m} \in \mathbf{N}^n} c_{\mathbf{m}} S_{m_1} \dots S_{m_n}.$$

Soit $\mathbf{m} \in \mathbf{N}^n$ avec $c_{\mathbf{m}} \neq 0$. Puisque $\deg \mathrm{P} < n(q-1)$, $\sum_{i=1}^{n} m_i < n(q-1)$ et par suite, l'un au moins des $m_i$ est $< q-1$. D'après la première question, $\mathrm{S}_{m_i} = 0$. Il en résulte bien que $\mathrm{S}(\mathrm{P}) = 0$.

**c)** Le degré de P est égal à $(q-1)\sum_{i=1}^{r} \deg \mathrm{P}_i$. On a donc $\deg \mathrm{P} < n(q-1)$ et d'après la question précédente, $\mathrm{S}(\mathrm{P}) = 0$.

D'autre part, si $(x_1, \ldots, x_n) \in \mathrm{V}$, on a $\mathrm{P}_i(x_1, \ldots, x_n) = 0$ pour tout $i$, d'où $\mathrm{P}(x_1, \ldots, x_n) = 1$. Dans l'autre cas, si $(x_1, \ldots, x_n) \notin \mathrm{V}$, soit $i$ tel que $\mathrm{P}_i(x_1, \ldots, x_n) \neq 0$. Comme $\mathrm{P}_i(x_1, \ldots, x_n) \in \mathrm{K}^*$ et comme $\operatorname{card} \mathrm{K} = q$, $\mathrm{P}_i(x_1, \ldots, x_n)^{q-1} = 1$, d'où $\mathrm{P}(x_1, \ldots, x_n) = 0$. On a donc

$$\mathrm{S}(\mathrm{P}) = \sum_{x \in \mathrm{V}} 1 = \operatorname{card} \mathrm{V} \pmod{p}.$$

Puisque $\mathrm{S}(\mathrm{P}) = 0$, on a donc $\operatorname{card} \mathrm{V} \equiv 0 \pmod{p}$.

**d)** Puisque P est homogène de degré $d > 0$, $\mathrm{P}(0, \ldots, 0) = 0$ et $\mathrm{V} \neq \varnothing$. On a donc $\operatorname{card} \mathrm{V} \geq 1$. Si $d < n$, la question précédente implique que $\operatorname{card} \mathrm{V}$ est multiple de $p$, d'où $\operatorname{card} \mathrm{V} \geq p \geq 2$. En particulier, il existe $(x_1, \ldots, x_n) \in \mathrm{V}$, avec $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$, ce qu'il fallait démontrer.

*Solution de l'exercice 13.6.8.* — Soit $(x_1, \ldots, x_n)$ une base de transcendance de L sur K et $(y_1, \ldots, y_m)$ une base de transcendance de M sur L. Montrons que la famille $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ est une base de transcendance de M sur K.

a) *Elle est algébriquement indépendante.* Soit $\mathrm{P} \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n, \mathrm{Y}_1, \ldots, \mathrm{Y}_m]$ non nul tel que $\mathrm{P}(x_1, \ldots, x_n, y_1, \ldots, y_m)$. On écrit P comme un polynôme de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n][\mathrm{Y}_1, \ldots, \mathrm{Y}_m]$ :

$$\mathrm{P} = \sum_{\mathbf{k} \in \mathbf{N}^m} \mathrm{P}_{\mathbf{k}}(\mathrm{X}_1, \ldots, \mathrm{X}_n)\mathrm{Y}_1^{k_1} \ldots \mathrm{Y}_m^{k_m}.$$

Les polynômes $\mathrm{P}_{\mathbf{k}}$ appartiennent à $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et puisque $\mathrm{P} \neq 0$, l'un des $\mathrm{P}_{\mathbf{k}}$ n'est pas nul. Comme la famille $(x_1, \ldots, x_n)$ est algébriquement indépendante, pour un tel multi-indice $\mathbf{k}$, $\mathrm{P}_{\mathbf{k}}(x_1, \ldots, x_n) \neq 0$. Par suite, le polynôme

$$\mathrm{P}(x_1, \ldots, x_n, \mathrm{Y}_1, \ldots, \mathrm{Y}_m) \in \mathrm{K}(x_1, \ldots, x_n)[\mathrm{Y}_1, \ldots, \mathrm{Y}_m] \subset \mathrm{L}[\mathrm{Y}_1, \ldots, \mathrm{Y}_m]$$

n'est pas nul. La relation $\mathrm{P}(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$ contredit cependant le fait que la famille $(y_1, \ldots, y_m)$ soit algébriquement indépendante sur L.

b) *Tout élément de* M *est algébrique sur* $\mathrm{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$. En effet, L est algébrique sur $\mathrm{K}[x_1, \ldots, x_n]$, donc $\mathrm{L}[y_1, \ldots, y_m]$ est algébrique sur $\mathrm{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Comme M est algébrique sur $\mathrm{L}[y_1, \ldots, y_m]$, elle est algébrique sur $\mathrm{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$.

*Solution de l'exercice 13.6.9.* — **a)** L'extension $\mathbf{C} \subset \mathbf{C}(\mathrm{T})$ est de degré de transcendance égal à 1. Par suite, $\mathbf{C}(\mathrm{T})$ est algébrique sur toute extension de $\mathbf{C}$ dont le degré de transcendance est (nécessairement) égal à 1. Comme $\mathrm{K} \neq \mathbf{C}$, il existe

$u \in \mathrm{K}$ et $u$ est transcendant sur $\mathbf{C}$. Par suite, $\deg \mathrm{tr}(\mathrm{K}/\mathbf{C}) \geq \deg \mathrm{tr}\, \mathbf{C}(u)/\mathbf{C} = 1$ et $\mathbf{C}(\mathrm{T})$ est algébrique sur K.

Comme c'est une extension de type fini, elle est nécessairement de degré fini.

**b)** Soit $d$ le degré du polynôme minimal de T sur K. L'extension $\mathrm{K} \subset \mathrm{K}[\mathrm{T}]$ est donc algébrique de degré $d$. Mais $\mathrm{K}[\mathrm{T}]$ est un corps qui contient $\mathbf{C}$ et T, donc $\mathrm{K}[\mathrm{T}]$ contient $\mathbf{C}(\mathrm{T})$ et l'on a $\mathbf{C}(\mathrm{T}) = \mathrm{K}[\mathrm{T}]$, d'où $d = n$. Il en résulte que le polynôme minimal de T sur K est de degré $n$.

Comme T est transcendant sur $\mathbf{C}$, $f \notin \mathbf{C}[\mathrm{X}]$. Il existe donc $j$ tel que $k_j \notin \mathbf{C}$.

**c)** On a les inclusions $\mathbf{C}(u) \subset \mathrm{K} \subset \mathbf{C}(\mathrm{T})$. Par suite,

$$[\mathbf{C}(\mathrm{T}) : \mathbf{C}(u)] = [\mathbf{C}(\mathrm{T}) : \mathrm{K}]\, [\mathrm{K} : \mathbf{C}(u)] \geq [\mathbf{C}(\mathrm{T}) : \mathrm{K}] = n.$$

Il suffit donc de prouver que $[\mathbf{C}(\mathrm{T}) : \mathbf{C}(u)] = m$. Or, T est racine du polynôme $g(\mathrm{X}) - uh(\mathrm{X}) \in \mathbf{C}[u, \mathrm{X}]$. Comme ce polynôme est de degré 1 en $u$, il est irréductible en tant que polynôme de $\mathbf{C}(\mathrm{X})[u]$, et comme ses coefficients $g(\mathrm{X})$ et $h(\mathrm{X})$ sont premiers entre eux deux à deux, il est, d'après le lemme de Gauß, irréductible en tant que polynôme de $\mathbf{C}[u, \mathrm{X}]$, voire en tant que polynôme de $\mathbf{C}(u)[\mathrm{X}]$. Par suite, le degré de T sur $\mathbf{C}(u)$ est égal au degré en X de $g(\mathrm{X}) - uh(\mathrm{X})$, c'est-à-dire $m$. On a ainsi $[\mathbf{C}(\mathrm{T}) : \mathbf{C}(u)] = m \geq n$.

Puisque $g(\mathrm{X}) - uh(\mathrm{X})$ est à coefficients dans $\mathbf{C}(u) \subset \mathrm{K}$ et s'annule en $\mathrm{X} = \mathrm{T}$, il est multiple du polynôme minimal de T sur K. Il existe donc $q(\mathrm{X}) \in \mathrm{K}[\mathrm{X}]$ tel que

$$g(\mathrm{X}) - uh(\mathrm{X}) = q(\mathrm{X}) f(\mathrm{X}).$$

**d)** Mettons les $k_j \in \mathbf{C}(\mathrm{T})$ sous forme de fraction irréductible $k_j = g_j/h_j$, avec $g_j$ et $h_j \in \mathbf{C}[\mathrm{T}]$. Soit $c_0$ le ppcm des $h_j$ et, si $1 \leq j \leq n$, posons $c_j = k_j c_0 = (k_j/h_j) g_j$. Il en résulte que $\mathrm{pgcd}(c_0, c_1, \ldots, c_n) = 1$. Par suite, le polynôme

$$f(\mathrm{X}, \mathrm{T}) = c_0(\mathrm{T})\mathrm{X}^n + \cdots + c_n(\mathrm{T}) \in \mathbf{C}[\mathrm{X}, \mathrm{T}]$$

est irréductible en tant que polynôme de $\mathbf{C}(\mathrm{T})[\mathrm{X}]$ et est à coefficients premiers entre eux dans leur ensemble. D'après le lemme de Gauß, il est irréductible.

**e)** On a

$$\begin{aligned} g(\mathrm{X})h(\mathrm{T}) - g(\mathrm{T})h(\mathrm{X}) &= h(\mathrm{T})\big(g(\mathrm{X}) - \frac{f(\mathrm{T})}{h(\mathrm{T})} h(\mathrm{X})\big) \quad = h(\mathrm{T})\big(g(\mathrm{X}) - uh(\mathrm{X})\big) \\ &= h(\mathrm{T}) q(\mathrm{X}) f(\mathrm{X}) \\ &= \big(\frac{h(\mathrm{T})}{c_0(\mathrm{T})} g(\mathrm{X})\big) f(\mathrm{X}, \mathrm{T}). \end{aligned}$$

Ainsi, $f(\mathrm{X}, \mathrm{T})$ divise le polynôme $g(\mathrm{X})h(\mathrm{T}) - g(\mathrm{T})h(\mathrm{X})$ dans $\mathbf{C}(\mathrm{T})[\mathrm{X}]$. Étant irréductible, le lemme de Gauß implique qu'il le divise aussi dans $\mathbf{C}[\mathrm{T}, \mathrm{X}]$, d'où l'existence de $q(\mathrm{X}, \mathrm{T}) \in \mathbf{C}[\mathrm{X}, \mathrm{T}]$ tel que

$$g(\mathrm{X})h(\mathrm{T}) - g(\mathrm{T})h(\mathrm{X}) = q(\mathrm{X}, \mathrm{T}) f(\mathrm{X}, \mathrm{T}).$$

Comparons les degrés en T des deux membres : Comme $\deg g \leq m$ et $\deg h \leq m$, le membre de gauche est de degré $\leq m$ ; le degré du membre de droite est au moins

$$\deg_{\mathrm{T}} f(\mathrm{X},\mathrm{T}) = \max(\deg c_0(\mathrm{T}),\ldots,\deg c_n(\mathrm{T})) \geq \max(\deg c_0, \deg c_j).$$

Comme $u = g/h = c_j/c_0$ et comme $\operatorname{pgcd}(g,h) = 1$, il existe $\mathrm{D} = \operatorname{pgcd}(c_0, c_j)$ tel que $c_j = \mathrm{D}g$ et $c_0 = \mathrm{D}h$. Par suite, $\max(\deg c_0, \deg c_j) = \max(\deg g, \deg h) + \deg \mathrm{D} \geq m$. Ces deux inégalités impliquent que le degré en T des deux membres est égal à $m$, que $\deg_{\mathrm{T}} f(\mathrm{X},\mathrm{T}) = m$ et que $\deg_{\mathrm{T}} q(\mathrm{X},\mathrm{T}) = 0$, d'où $q(\mathrm{X},\mathrm{T}) \in \mathbf{C}[\mathrm{X}]$.

Considéré comme polynôme de $\mathbf{C}(\mathrm{X})[\mathrm{T}]$, le pgcd des coefficients du membre de gauche est égal au pgcd de $g(\mathrm{X})$ et $h(\mathrm{X})$, donc 1. Il en est de même du membre de gauche, d'où le fait que $q(\mathrm{X},\mathrm{T})$ est constant.

Le degré en X du membre de gauche est égal à $m$. Celui du membre de droite aussi par conséquent, d'où $m = \deg_{\mathrm{X}} q(\mathrm{X},\mathrm{T}) + \deg_{\mathrm{X}} f(\mathrm{X},\mathrm{T}) = n$.

Pour conclure, il suffit de remarquer que l'extension $\mathbf{C}(u) \subset \mathrm{K}$ a pour degré $m/n = 1$, d'où $\mathrm{K} = \mathbf{C}(u)$.

*Remarque.* — Ce résultat est vrai si $\mathbf{C}$ est remplacé par un corps arbitraire. Si $k$ est un corps algébriquement clos, il reste vrai (et bien plus difficile à démontrer) que tout corps $\mathrm{K} \subset k(\mathrm{X},\mathrm{Y})$ de degré de transcendance égal à 2 est de la forme $\mathrm{K}(f,g)$ pour deux fractions rationnelles $f$ et $g$, mais ce n'est pas vrai si $k$ est algébriquement clos. Avec plus de 3 variables, le résultat analogue est faux.

# 14 Algèbres de type fini sur un corps

*On étudie dans ce chapitre quelques propriétés fondamentales des algèbres de type fini sur un corps. Ces propriétés ont des traductions géométriques pour les ensembles algébriques que, malheureusement, nous ne pouvons exposer ici.*

## 14.1. Le théorème de normalisation de Noether

Ce théorème, joint aux propriétés des extensions entières, est un outil extrêmement puissant dans l'étude des algèbres de type fini sur un corps. Tout ce chapitre en est plus ou moins l'illustration.

THÉORÈME 14.1.1 (Théorème de normalisation). — *Soit $k$ un corps et soit* A *une $k$-algèbre de type fini, intègre. Il existe alors des éléments $x_1, \dots, x_n \in \mathrm{A}$ algébriquement indépendantents sur $k$ tels que* A *soit entier sur $k[x_1, \dots, x_n]$.*

*Démonstration.* — Soit $y_1, \dots, y_m$ des éléments de A qui engendrent A comme $k$-algèbre. Nous allons raisonner par récurrence sur $m$, le résultat étant trivial si $m = 0$.

Si $y_1, \dots, y_m$ sont algébriquement indépendants sur $k$, le lemme de normalisation est démontré.

Supposons donc qu'ils sont algébriquement dépendants et soit $\mathrm{P} \in k[\mathrm{Y}_1, \dots, \mathrm{Y}_m]$ un polynôme non nul tels que $\mathrm{P}(y_1, \dots, y_m) = 0$. On va montrer que l'on peut choisir des entiers $r_i \geq 1$ pour $i \geq 2$ de sorte que A est entière sur la sous-$k$-algèbre de A engendrée par les $z_i = y_i - y_1^{r_i}$. En effet, si $\mathrm{P} = \sum_{\mathbf{n}=(n_i)} a_{\mathbf{n}} \prod_i \mathrm{Y}_i^{n_i}$, on a

$$0 = \mathrm{P}(y_1, \dots, y_m) = \mathrm{P}(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = \sum_{\mathbf{n}} a_{\mathbf{n}} y_1^{n_1} \prod_{i=2}^{m} (z_i + y_1^{r_i})^{n_i}$$

$$= \sum_{\mathbf{n}} \sum_{j_2=0}^{n_2} \cdots \sum_{j_m=0}^{n_m} a_{\mathbf{n}} \prod_{i \geq 2} \binom{n_i}{j_i} y_1^{n_1 + \sum j_i r_i} \prod_{i \geq 2} z_i^{n_i - j_i}.$$

Soit $k$ un entier strictement plus grand que le degré de P en chaque variable et posons $r_i = k^i$. Ainsi, les sommes $n_1 + \sum j_i r_i$ sont toutes distinctes et l'équation précédente fournit une relation de dépendance algébrique pour $y_1$ donc les coefficients sont dans $k[z_2, \dots, z_m]$ et dont le coefficient de plus haut degré est nécessairement obtenu pour $j_i = n_i$, donc est un coefficient non nul de P, donc inversible. Cela prouve que $y_1$ est entier sur $k[z_2, \dots, z_m]$. Puis, si $i \geq 2$, $y_i = z_i + y_1^{r_i}$ est aussi entier sur $k[z_2, \dots, z_m]$. Par conséquent, A est entière sur $k[z_2, \dots, z_m]$.

Par récurrence, il existe des éléments $x_1, \dots, x_n \in k[z_2, \dots, z_m]$ algébriquement indépendants sur $k$ et tels que $k[z_2, \dots, z_m]$ est entière sur $k[x_1, \dots, x_n]$. Il en résulte que A est entière sur $k[x_1, \dots, x_n]$. □

Comme première application, nous donnons une démonstration générale du théorème des zéros de Hilbert que nous avions établi au chapitre 4 lorsque le corps était le corps des nombres complexes.

La forme la plus fondamentale de ce théorème est la suivante.

THÉORÈME 14.1.2. — *Soit $k$ un corps et soit* A *une $k$-algèbre de type fini. On suppose que* A *est un corps. Alors,* A *est une extension algébrique de $k$.*

Avant de la démontrer, rappelons une propriété importante des extensions entières.

PROPOSITION 14.1.3. — *Soit* $A \subset B$ *deux anneaux intègres tels que* B *est entier sur* A. *Alors,* A *est un corps si et seulement si* B *est un corps.*

*Démonstration.* — Si A est un corps, on a vu au lemme 9.1.9 que tout $x \in B \setminus \{0\}$ est inversible dans A. Réciproquement, supposons que B est un corps et soit $x \in A \setminus \{0\}$. Comme B est un corps, il existe $y \in B$ tel que $xy = 1$ et $y$ est entier sur A. Soit $y^n + c_1 y^{n-1} + \cdots + c_n = 0$ une relation de dépendance intégrale pour $y$, où les $c_i \in A$. Multiplions cette relation par $x^{n-1}$, on trouve

$$y = x^{n-1} y^n = -c_1 - x c_2 - \cdots - x^{n-1} c_n,$$

d'où $y \in A$ et $x$ est inversible dans A. Par suite, A est un corps. □

*Démonstration du théorème.* — Soit $x_1, \dots, x_n$ des éléments de A algébriquement indépendants sur $k$ tels que A soit entière sur $k[x_1, \dots, x_n]$. Comme A est un corps et l'extension $k[x_1, \dots, x_n] \subset A$ entière, $k[x_1, \dots, x_n]$ est aussi un corps. Mais, l'homomorphisme canonique $k[X_1, \dots, X_n] \to k[x_1, \dots, x_n]$ est un isomorphisme, si bien que $k[X_1, \dots, X_n]$ est un corps, ce qui est absurde si $n \geq 1$ (l'anneau des polynômes *n'est pas* un corps...). Par suite, $n = 0$ et A est entière (algébrique) sur $k$. Comme A est une $k$-algèbre de type fini, A est même finie sur $k$. □

Comme corollaire, on peut en déduire le cas général du théorème 4.2.2.

COROLLAIRE 14.1.4. — *Soit $k$ un corps algébriquement clos et soit $\mathfrak{m}$ un idéal maximal de l'anneau de polynômes $k[X_1, \ldots, X_n]$. Alors, il existe un unique $(a_1, \ldots, a_n) \in k^n$ tel que $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$.*

*Démonstration.* — Notons K le corps résidual $k[X_1, \ldots, X_n]/\mathfrak{m}$ et soit $\theta$ l'homomorphisme surjectif canonique $k[X_1, \ldots, X_n] \to K$. Par construction, K est une $k$-algèbre de type fini et c'est un corps. D'après le théorème précédent, c'est une extension algébrique finie de $k$. Puisque $k$ est supposé algébriquement clos, $k = K$ et il existe pour tout $i$ un unique élément $a_i \in k$ tel que $\theta(X_i) = a_i$, c'est-à-dire $X_i - a_i \in \mathfrak{m}$. Alors, $\mathfrak{m}$ contient l'idéal $(X_1 - a_1, \ldots, X_n - a_n)$ et puisque cet idéal est maximal, $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$. □

On laisse en exercice le soin de relire les définitions et théorèmes du paragraphe 4.2 concernant les ensembles algébriques. Ils s'étendent *tous* du cas où le corps est $\mathbf{C}$ au cas d'un corps *algébriquement clos* arbitraire.

Donnons une autre application importante.

THÉORÈME 14.1.5. — *Soit $k$ un corps algébriquement clos et soit A, B deux $k$-algèbres de type fini intègres. Alors, $A \otimes_k B$ est une $k$-algèbre (de type fini) intègre.*

*Démonstration.* — Soit $f$ et $g$ deux éléments de $A \otimes_k B$ tels que $fg = 0$. On peut écrire $f = \sum_{i=1}^{r} a_i \otimes b_i$ où les $b_i$ sont linéairement indépendants sur $k$, et de même $g = \sum_{j=1}^{s} a'_j \otimes b'_j$.

Si $\mathfrak{m}$ est un idéal maximal de A, $A/\mathfrak{m}$ est un corps qui est une $k$-algèbre de type fini. C'est donc une extension finie de $k$, d'où $A/\mathfrak{m} \simeq k$. Notons $\mathrm{cl}_{\mathfrak{m}} : A \to A/\mathfrak{m}$ la surjection canonique et soit $\theta_{\mathfrak{m}}$ l'homomorphisme surjectif de $k$-algèbres

$$\theta_{\mathfrak{m}} : A \otimes_k B \to (A/\mathfrak{m}) \otimes_k B \simeq B$$

qui s'en déduit. On a

$$\theta_{\mathfrak{m}}(f) = \sum_{i=1}^{r} \mathrm{cl}_{\mathfrak{m}}(a_i) b_i \quad \text{et} \quad \theta_{\mathfrak{m}}(g) = \sum_{j=1}^{s} \mathrm{cl}_{\mathfrak{m}}(a'_j) b'_j.$$

Puisque

$$\theta_{\mathfrak{m}}(f)\theta_{\mathfrak{m}}(g) = \theta_{\mathfrak{m}}(fg) = 0$$

et puisque B est intègre, $\theta_{\mathfrak{m}}(f) = 0$ ou $\theta_{\mathfrak{m}}(g) = 0$. Comme les $b_i$ (resp. les $b'_j$) sont linéairement indépendants, on a $\mathrm{cl}_{\mathfrak{m}}(a_i) = 0$ pour tout $i$ dans le premier cas et $\mathrm{cl}_{\mathfrak{m}}(a'_j) = 0$ pour tout $j$ dans le second. Autrement dit, ou bien tous les $a_i$ appartiennent à $\mathfrak{m}$, ou bien tous les $a'_j$ appartiennent à $\mathfrak{m}$. Ce qu'on reformule encore : si $I = (a_1, \ldots, a_r)$ et $J = (a'_1, \ldots, a'_s)$, alors, pour tout idéal maximal $\mathfrak{m}$ de A, ou bien $I \subset \mathfrak{m}$, ou bien $J \subset \mathfrak{m}$. Ainsi, pour tout idéal maximal $\mathfrak{m}$ de A, $I \cap J \subset \mathfrak{m}$.

Pour conclure la démonstration, nous utilisons le fait que A est un anneau de Jacobson : l'intersection de tous les idéaux maximaux de A est réduite au nilradical de A, c'est-à-dire, A étant intègre, à (0). On a donc $I \cap J = (0)$.

Si $f \neq 0$ et $g \neq 0$, on a $I \neq (0)$ et $J \neq (0)$. Choisissons $x \in I \setminus \{0\}$ et $y \in I \setminus \{0\}$. Alors, $xy = 0$, ce qui contredit le fait que A est intègre. Par suite, $f = 0$ ou $g = 0$. □

Donnons maintenant la preuve du fait admis dans la démonstration précédente. Je renvoie aussi à l'exercice 4.3.9 page 55 concernant la définition des anneaux de Jacobson.

PROPOSITION 14.1.6. — *Soit k un corps et soit* A *une k-algèbre de type fini. Alors,* A *est un anneau de Jacobson : pour tout idéal* I *de* A, $\sqrt{I}$ *est l'intersection des idéaux maximaux de* A *qui contiennent* I.

*Démonstration.* — Soit B la *k*-algèbre de type fini A/I. Il faut alors montrer que l'intersection des idéaux maximaux de B est réduite à l'ensemble des éléments nilpotents de B. (Lorsque B est intègre, c'est d'ailleurs le résultat dont on a eu besoin dans la démonstration du théorème ci-dessus.)

Si $x \in B$ n'est pas nilpotent, il faut donc montrer qu'il existe un idéal maximal de B ne contenant pas $x$. Or, $B_x = B[1/x]$ est encore une *k*-algèbre de type fini. Comme $x$ n'est pas nilpotent, $B_x \neq 0$. Par suite, $B_x$ admet un idéal maximal $\mathfrak{m}_x$ dont l'intersection avec B est un idéal premier $\mathfrak{p}_x$ ne contenant pas $x$.

Montrons qu'en fait $\mathfrak{p}_x$ est maximal. On a en effet un homomorphisme injectif de *k*-algèbres $B/\mathfrak{p}_x \hookrightarrow B_x/\mathfrak{m}_x$. Comme $B_x/\mathfrak{m}_x$ est une *k*-algèbre de type fini et est un corps, c'est, d'après le théorème des zéros 14.1.2, une extension algébrique finie de $k$. Alors, $B/\mathfrak{p}_x$ est une *k*-algèbre intègre qui est de dimension finie comme *k*-espace vectoriel (inférieure à celle de $B_x/\mathfrak{m}_x$). C'est donc un corps et $\mathfrak{p}_x$ est ainsi un idéal maximal de B qui ne contient pas $x$, ce qui établit la proposition. □

## 14.2. Finitude de la clôture intégrale

THÉORÈME 14.2.1. — *Soit k un corps et soit* A *une k-algèbre de type finie intègre. Soit* E *le corps des fractions de* A *et soit* $E \subset F$ *une extension algébrique finie. Soit enfin* B *la clôture intégrale de* A *dans* F.

*Alors,* B *est un* A*-module de type fini.*

La démonstration repose sur un énoncé de théorie de Galois et sur le théorème de normalisation.

PROPOSITION 14.2.2. — *Soit* A *un anneau noethérien intègre,* E *son corps des fractions. Soit* F *une extension algébrique finie* séparable *de* E *et soit* B *la clôture intégrale de* A *dans* F. *On suppose que* A *est intégralement clos. Alors,* B *est un* A*-module de type fini.*

*Démonstration.* — Soit $\Omega$ une clôture algébrique de E. Notons $n = [F : E]$ et soit $\sigma_1, \dots, \sigma_n : F \to \Omega$ les $n$ E-homomrphismes de corps distincts de F dans $\Omega$. Si $i \in \{1; \dots; n\}$ et $x \in B$, $\sigma_i(x)$ est entier sur A (annulé par le même polynôme unitaire que $x$), si bien que $\mathrm{Tr}_{F/E}(x) = \sum_{i=1}^{n} \sigma_i(x)$ est entier sur A. Comme c'est un élément de E et comme A est supposé intégralement clos (dans E), $\mathrm{Tr}_{F/E}(x) \in A$.

Soit $(e_1, \dots, e_n)$ une base de F sur E. Quitte à les multiplier par un élément non nul de F, on peut supposer qu'ils appartiennent à B. Comme l'extension $E \subset F$ est séparable, la forme bilinéaire définie par la trace est non dégénérée. Il existe donc une base $(f_1, \dots, f_n)$ telle que pour tous $i$ et $j \in \{1; \dots; n\}$, $\mathrm{Tr}_{E/F}(e_i f_j) = 0$ si $i \neq j$ et 1 si $i = j$. Soit D un élément de A tel que $Df_i \in B$ pour tout $i$.

Alors, soit $x = \sum_{i=1}^{n} x_i e_i$ un élément de B. Pour tout $i \in \{1; \dots; n\}$, $x(Df_i) \in B$, donc $\mathrm{Tr}_{F/E}(Dx f_i) \in A$, d'où $Dx_i \in A$. Il en résulte que $B \subset D^{-1} \sum_{i=1}^{n} A e_i$. Autrement dit, B est un sous-A-module d'un A-module libre de rang $n$ sur A. Comme A est noethérien, B est un A-module de type fini. □

Nous pouvons maintenant démontrer le théorème. Pour simplifier la démonstration, *nous supposons que k est de caractéristique zéro.* Le cas général se démontre de la même façon mais nécessite une étude particulière des extensions inséparables dans le style de la remarque 13.4.7

*Démonstration.* — Appliquons à A le lemme de normalisation de Noether 14.1.1. Soit $x_1, \dots, x_n$ des élements de A algébriquement indépendants sur $k$ tels que A est entière sur $A_0 = k[x_1, \dots, x_n]$.

Remarquons qu'un élément de F est entier sur A si et seulement s'il est entier sur $A_0$. Par suite, B est la clôture intégrale de $A_0$ dans F. Comme l'extension $E_0 = k(x_1, \dots, x_n) \subset E$ est algébrique finie, l'extension $E_0 \subset F$ est finie.

Remarquons aussi que $A_0$ est un anneau factoriel (théorème 7.4.4) donc intégralement clos (théorème 9.2.10). Comme $k$ est supposé de caractéristique zéro, l'extension $E_0 \subset F$ est séparable. D'après la proposition 14.2.2, B est un $A_0$-module de type fini. C'est donc a fortiori un A-module de type fini. □

## 14.3. Dimension et degré de transcendance

DÉFINITION 14.3.1. — *Soit* A *un anneau. On appelle* dimension *de* A *la borne supérieure des longueurs des chaînes strictement croissantes*

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

*d'idéaux premiers de* A.

*Exemple 14.3.2.* — a) La dimension d'un corps, plus généralement d'un anneau artinien, est 0.

b) Dans $\mathbf{Z}$, les chaînes d'idéaux premiers sont $(0) \subset (p)$ pour $p$ un nombre premier. Par suite, $\dim \mathbf{Z} = 1$. Plus généralement, un anneau principal qui n'est pas un corps est de dimension 1. En particulier, si $k$ est un corps, $\dim k[\mathrm{X}] = 1$.

c) L'un des buts du paragraphe est de montrer que $\dim k[\mathrm{X}_1, \ldots, \mathrm{X}_n] = n$.

*Remarque 14.3.3* (Interprétation géométrique). — Soit $k$ un corps algébriquement clos, soit $\mathrm{I} \subset k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et $\mathrm{A} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathrm{I}$. Un idéal premier de A définit un ensemble algébrique irréductible contenu dans $\mathscr{V}(\mathrm{I})$. Ainsi, la dimension de A est la borne supérieure des longueurs de suites strictement croissantes de fermés irréductibles contenus dans $\mathscr{V}(\mathrm{I})$.

*Exemple 14.3.4.* — Si $k$ est un corps, on a $\dim k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \geq n$. En effet, on a la suite d'idéaux premiers

$$(0) \subset (\mathrm{X}_1) \subset (\mathrm{X}_1, \mathrm{X}_2) \subset \cdots \subset (\mathrm{X}_1, \ldots, \mathrm{X}_n).$$

Le théorème principal de ce paragraphe est le suivant. Il est le fondement de la théorie de la dimension en géométrie algébrique.

THÉORÈME 14.3.5. — *Soit $k$ un corps,* A *une $k$-algèbre de type fini intègre et soit* K *son corps des fractions. Alors,* $\dim \mathrm{A} = \deg \mathrm{tr}_k \mathrm{K}$.

Avant de le démontrer, il nous faut étudier le comportement de la dimension dans une extension entière.

THÉORÈME 14.3.6 (Premier théorème de Cohen-Seidenberg)

*Soit* $\mathrm{A} \subset \mathrm{B}$ *une extension entière d'anneaux.*

*a) Soit* $\mathfrak{q}$ *un idéal premier de* B *et soit* $\mathfrak{p} = \mathfrak{q} \cap \mathrm{A}$. *Alors,* $\mathfrak{p}$ *est maximal si et seulement si* $\mathfrak{q}$ *est maximal.*

*b) Soit* $\mathfrak{q} \subset \mathfrak{q}'$ *deux idéaux premiers de* B *tels que* $\mathfrak{q} \cap \mathrm{A} = \mathfrak{q}' \cap \mathrm{A}$. *Alors,* $\mathfrak{q} = \mathfrak{q}'$.

*c) Pour tout idéal premier* $\mathfrak{p}$ *de* A, *il existe un idéal premier* $\mathfrak{q}$ *de* B *tel que* $\mathfrak{q} \cap \mathrm{A} = \mathfrak{p}$.

*Démonstration.* — a) Par construction, on a une extension entière d'anneaux intègres $\mathrm{A}/\mathfrak{p} \subset \mathrm{B}/\mathfrak{q}$. Par suite, $\mathrm{A}/\mathfrak{p}$ est un corps si et seulement si $\mathrm{B}/\mathfrak{q}$ est

un corps (proposition 14.1.3), c'est-à-dire : $\mathfrak{p}$ est un idéal maximal de A si et seulement si $\mathfrak{q}$ est un idéal maximal de B.

b) Considérons l'extension entière $A_\mathfrak{p} \subset B_\mathfrak{p}$ obtenue par localisation par la partie multiplicative $A \setminus \mathfrak{p}$. Alors, $\mathfrak{q}B_\mathfrak{p} \subset \mathfrak{q}'B_\mathfrak{p}$ sont deux idéaux premiers de $B_\mathfrak{p}$ dont l'intersection avec $A_\mathfrak{p}$ est l'unique idéal maximal $\mathfrak{p}A_\mathfrak{p}$ de $A_\mathfrak{p}$. En effet, l'inclusion $\mathfrak{p}A_\mathfrak{p} \subset \mathfrak{q}B_\mathfrak{p}$ est évidente. D'autre part, $\mathfrak{q}'B_\mathfrak{p}$ ne contient pas 1, donc $\mathfrak{q}'B_\mathfrak{p} \neq A_\mathfrak{p}$ et par suite est contenu dans $\mathfrak{p}A_\mathfrak{p}$.

Puisque $\mathfrak{p}A_\mathfrak{p}$ est maximal, $\mathfrak{q}B_\mathfrak{p}$ et $\mathfrak{q}'B_\mathfrak{p}$ sont tous deux maximaux. Comme ils sont inclus l'un dans l'autre, ils sont égaux. Puisque la localisation $\mathfrak{q} \mapsto \mathfrak{q}B_\mathfrak{p}$ est une *bijection* de l'ensemble des idéaux premiers de B disjoints de $A \setminus \mathfrak{p}$ sur l'ensemble des idéaux premiers de $B_\mathfrak{p}$, $\mathfrak{q} = \mathfrak{q}'$.

c) Soit $\mathfrak{m}$ un idéal maximal de l'anneau $B_\mathfrak{p}$. On a vu au a) que $\mathfrak{m} \cap A_\mathfrak{p}$ est un idéal maximal de $A_\mathfrak{p}$, d'où $\mathfrak{m} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. D'autre part, il existe un idéal premier $\mathfrak{q}$ de B tel que $\mathfrak{m} = \mathfrak{q}B_\mathfrak{p}$. Alors, si $b \in_m athfrakq \cap A$, $b/1 \in \mathfrak{q}B_\mathfrak{p} \cap A_\mathfrak{p}$ ; il existe donc $a \in A \setminus \mathfrak{p}$ tel que $ab \in \mathfrak{p}$, d'où, $\mathfrak{p}$ étant premier, $b \in \mathfrak{p}$. Réciproquement, si $a \in \mathfrak{p}$, $a/1 \in \mathfrak{p}A_\mathfrak{p} \subset qB_\mathfrak{p}$. Par suite, il existe $a' \in A \setminus \mathfrak{p}$ tel que $aa' \in \mathfrak{q}$. Puisque $a' \notin \mathfrak{p}$, $a' \notin \mathfrak{q}$ (sinon, $a' \in \mathfrak{q} \cap A = \mathfrak{p}$) et, $\mathfrak{q}$ étant premier, $a \in \mathfrak{q}$. Ainsi, $\mathfrak{q} \cap A = \mathfrak{p}$. □

Corollaire 14.3.7. — *Soit* $A \subset B$ *une extension entière d'anneaux. Alors,* $\dim A = \dim B$.

*Démonstration.* — Soit $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ une suite strictement croissante d'idéaux premiers de B. Prenons les intersections avec A. On obtient une suite croissante d'idéaux premiers de A, $(\mathfrak{q}_0 \cap A) \subset \cdots \subset (\mathfrak{q}_n \cap A)$. D'après le théorème 14.3.6, b), cette suite est strictement croissante. Par suite, $\dim A \geq \dim B$.

Réciproquement, soit $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ une suite strictement croissante d'idéaux premiers de A. D'après le théorème 14.3.6, c), il existe un idéal premier $\mathfrak{q}_0$ de B tel que $\mathfrak{q}_0 \cap A = \mathfrak{q}_0$. Supposant avoir construit par récurrence des idéaux premiers $\mathfrak{q}_0, \ldots, \mathfrak{q}_r$ tels que $\mathfrak{q}_j \cap A = \mathfrak{p}_j$ pour $0 \leq j \leq r$, considérons l'extension entière $A/\mathfrak{p}_r \subset B/\mathfrak{q}_r$ d'anneaux intègres. Il existe alors un idéal premier $\mathfrak{q}$ de $B/\mathfrak{q}_r$ dont l'intersection avec $A/\mathfrak{p}_r$ est l'idéal premier $\mathfrak{p}_{r+1}/\mathfrak{p}_r$. Or, $\mathfrak{q}$ est de la forme $\mathfrak{q}_{r+1}/\mathfrak{q}_r$, $\mathfrak{q}_{r+1}$ étant un idéal premier de B qui vérifie donc $\mathfrak{q}_{r+1} \cap A = \mathfrak{p}_{r+1}$. Ainsi, $\dim B \geq \dim A$. □

*Démonstration du théorème 14.3.5.* — Nous démontrons ce théorème par récurrence sur le degré de transcendance de K. Si $n = \deg \mathrm{tr}_k K$, rappelons qu' existe, d'après le lemme de normalisation de Noether, des éléments $x_1, \ldots, x_n \in A$, algébriquement indépendants sur $k$, tels que A soit entière sur $k[x_1, \ldots, x_n]$.

Si $n = 0$, A est entier sur $k$, donc est un corps. On a donc $\dim A = 0$.

Supposons le théorème démontré en dimension $< n$. Alors, A étant entière sur $k[x_1, \ldots, x_n]$,

$$\dim \mathrm{A} = \dim k[x_1, \ldots, x_n].$$

De plus, $\deg \mathrm{tr}\, k(x_1, \ldots, x_n) = n$ si bien qu'il suffit de démontrer un corollaire du théorème. □

Corollaire 14.3.8. — *Soit $k$ un corps. Alors,* $\dim k[\mathrm{X}_1, \ldots, \mathrm{X}_n] = n$.

*Preuve du corollaire.* — (On suppose démontré le théorème en dimension $< n$.) On a déjà vu que $\dim k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \geq n$. Récproquement, soit

$$(0) \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

une suite strictement croissante d'idéaux premiers de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et considérons la $k$-algère de type fini intègre $\mathrm{A}' = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathfrak{p}_1$. On a $\dim \mathrm{A}' \geq r - 1$. D'autre part, si $\mathrm{P} \in \mathfrak{p}_1$ est un polynôme non nul, il fournit une relation de dépendance algébrique non triviale entre les classes $x_i$ des $\mathrm{X}_i$ dans A′. Si P fait intervenir $\mathrm{X}_n$, $x_n$ est alors algébrique sur le corps des fractions de la sous-algèbre $k[x_1, \ldots, x_{n-1}] \subset \mathrm{A}'$ qui est de degré de transcendance $\leq n-1$. Par suite, $\deg \mathrm{tr}\, \mathrm{A}' \leq n - 1$. Par récurrence, $\deg \mathrm{tr}\, \mathrm{A}' = \dim \mathrm{A}'$, d'où l'inégalité

$$r - 1 \leq \dim \mathrm{A}' = \deg \mathrm{tr}\, \mathrm{A}' \leq n - 1$$

et $r \leq n$. □

## 14.4. Exercices

*Exercice 14.4.1.* — Soit $\mathrm{K} \subset \mathrm{L}$ une extension algébrique finie et $\Omega$ un corps algébriquement clos contenant K.

Montrer que $\mathrm{L} \otimes_{\mathrm{K}} \Omega$ est réduit si et seulement si l'extension $\mathrm{K} \subset \mathrm{L}$ est séparable.

*Exercice 14.4.2.* — Soit $k$ un corps algébriquement clos et soit A, B deux $k$-algèbres de type fini réduites. Montrer que $\mathrm{A} \otimes_k \mathrm{B}$ est réduite.

*Exercice 14.4.3.* — Soit $k$ un corps et soit $f : \mathrm{A} \to \mathrm{B}$ un morphisme de $k$-algèbres de type fini. Si $\mathfrak{m}$ est un idéal maximal de B, montrer que $f^{-1}(\mathfrak{m})$ est un idéal maximal de A.

*Démonstration.* — Soit $\mathfrak{m}$ un idéal maximal de B et notons $\mathrm{K} = \mathrm{B}/\mathfrak{m}$ le corps résiduel. Alors, K est une $k$-algèbre de type fini et un corps, donc d'après le théorème des zéros de Hilbert (sous la forme du théorème 14.1.2) implique que K est une extension algébrique finie de $k$ : K est un $k$-espace vectoriel de dimension finie.

L'homomorphisme $f$ induit un homomorphisme injectif de $k$-algèbres de type fini :

$$\mathrm{A}/f^{-1}(\mathfrak{m}) \to \mathrm{B}/\mathfrak{m} = \mathrm{K}.$$

Par suite, $\mathrm{A}/f^{-1}(\mathfrak{m})$ est une $k$-algèbre de type fini intègre et est de dimension finie comme $k$-espace vectoriel.

Il en résulte que $\mathrm{A}/f^{-1}(\mathfrak{m})$ est un corps. (Remarquer par exemple le fait que K étant finie sur $k$ est a fortiori finie sur $\mathrm{A}/f^{-1}(\mathfrak{m})$ et utiliser la proposition 14.1.3.) Ainsi, $f^{-1}(\mathfrak{m})$ est un idéal maximal de A. □

## 14.5. Solutions

*Solution de l'exercice 14.4.1.* — Supposons que l'extension n'est pas séparable. Notons $p$ la caractéristique de K et soit $x \in \mathrm{L}$ dont le polynôme minimal $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ appartient à $\mathrm{K}[\mathrm{X}^p]$. On écrit $\mathrm{P}(\mathrm{X}) = \mathrm{Q}(\mathrm{X}^p)$. Soit $d$ le degré de Q et notons $\mathrm{Q} = a_0 + a_1\mathrm{X} + \cdots + a_{d-1}\mathrm{X}^{d-1} + \mathrm{X}^d$. Comme $\Omega$ est algébriquement clos, il existe pour tout $i$ un élément $b_i \in \Omega$ tel que $b_i^p = a_i$. Posons $\mathrm{R}(\mathrm{X}) = b_0 + b_1\mathrm{X} + \cdots + b_{d-1}\mathrm{X}^{d-1} + \mathrm{X}^d$, si bien que

$$\mathrm{R}(\mathrm{X})^p = (b_0 + b_1\mathrm{X} + \cdots + b_{d-1}\mathrm{X}^{d-1} + \mathrm{X}^d)^p = b_0^p + b_1^p\mathrm{X}^p + \cdots + b_{d-1}^p\mathrm{X}^{dp-p} + \mathrm{X}^{dp} = \mathrm{P}(\mathrm{X}).$$

Alors, l'élément $\mathrm{R}(x \otimes 1)$ de $\mathrm{L} \otimes_{\mathrm{K}} \Omega$,

$$\mathrm{R}(x \otimes 1) = 1 \otimes b_0 + x \otimes b_1 + \cdots + x^{d-1} \otimes b_{d-1} + x^d \otimes 1,$$

vérifie

$$\mathrm{R}(x \otimes 1)^p = \mathrm{P}(x \otimes 1) = \mathrm{P}(x) \otimes 1$$

puisque $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$. Par suite, $\mathrm{R}(x \otimes 1)^p = 0$. Or, comme $d \leq dp - 1$, les éléments $1, \ldots, x^d$ de L sont linéairement indépendants sur K. Par suite, les éléments $1 \otimes 1$, $x \otimes 1$, …, $x^d \otimes 1$ de $\mathrm{L} \otimes_{\mathrm{K}} \Omega$ sont encore linéairement indépendants sur $\Omega$ et $\mathrm{R}(x \otimes 1) \neq 0$. Il en résulte que $\mathrm{L} \otimes_{\mathrm{K}} \Omega$ n'est pas un anneau réduit.

Réciproquement, supposons que l'extension $\mathrm{K} \subset \mathrm{L}$ est séparable. Notons $d = [\mathrm{L} : \mathrm{K}]$ soit $\sigma_1, \ldots, \sigma_d$ les $d$ K-homomorphismes de L dans $\Omega$. On en déduit une application K-linéaire

$$\sigma : \mathrm{L} \to \Omega^d, \quad x \mapsto (\sigma_1(x), \ldots, \sigma_d(x)),$$

d'où par changement de base un homomorphisme $\Omega$-linéaire

$$\tau : \mathrm{L} \otimes_{\mathrm{K}} \Omega \to \Omega^d, \quad x \otimes t \mapsto (t\sigma_1(x), \ldots, t\sigma_d(x)).$$

Comme $\sigma$ est injectif, $\tau$ l'est encore. Comme les deux membres sont des $\Omega$-espaces vectoriels de même dimension $d$, $\tau$ est un isomorphisme.

Comme l'anneau $\Omega^d$ est réduit, $\mathrm{L} \otimes_{\mathrm{K}}$ est réduit.

*Solution de l'exercice 14.4.2.* — On reprend les arguments de la démonstration du théorème 14.1.5. Soit $f$ un élément de $\mathrm{A}\otimes_k \mathrm{B}$ et $d$ un entier tel que $f^d = 0$. On écrit $f = \sum_{i=1}^{r} a_i \otimes b_i$ où les $b_i$ sont linéairement indépendants sur $k$.

Si $\mathfrak{m}$ est un idéal maximal de A, on a vu dans la démonstration du théorème que $\mathrm{A}/\mathfrak{m}$ est isomorphe à $k$ et que l'on a un homomorphisme canonique

$$\theta_{\mathfrak{m}} : \mathrm{A}\otimes_k \mathrm{B} \to \mathrm{B}, \quad a\otimes b \mapsto \mathrm{cl}_{\mathfrak{m}}(a)b.$$

Puisque $f^d = 0$, $\theta_{\mathfrak{m}}(f)^d = 0$ dans B. Comme B est réduite, $\theta_{\mathfrak{m}}(f) = 0$. Comme les $b_i$ sont supposés linéairement indépendants sur $k$, $\mathrm{cl}_{\mathfrak{m}}(a_i) = 0$ pour tout $i$, si bien que les $a_i$ appartiennent à $\mathfrak{m}$.

Ainsi, les $a_i$ appartiennent à tout idéal maximal de A, donc au radical de Jacobson de A. Comme A est une $k$-algèbre de type fini, son radical de Jacobson est égal à son nilradical, donc à (0) puisque A est réduite. Il en résulte que tous les $a_i$ sont nuls, d'où $f = 0$.

*Démonstration.* — Soit $\mathfrak{m}$ un idéal maximal de B et notons $\mathrm{K} = \mathrm{B}/\mathfrak{m}$ le corps résiduel. Alors, K est une $k$-algèbre de type fini et un corps, donc d'après le théorème des zéros de Hilbert (sous la forme du théorème 14.1.2) implique que K est une extension algébrique finie de $k$ : K est un $k$-espace vectoriel de dimension finie.

L'homomorphisme $f$ induit un homomorphisme injectif de $k$-algèbres de type fini :

$$\mathrm{A}/f^{-1}(\mathfrak{m}) \to \mathrm{B}/\mathfrak{m} = \mathrm{K}.$$

Par suite, $\mathrm{A}/f^{-1}(\mathfrak{m})$ est une $k$-algèbre de type fini intègre et est de dimension finie comme $k$-espace vectoriel.

Il en résulte que $\mathrm{A}/f^{-1}(\mathfrak{m})$ est un corps. (Remarquer par exemple le fait que K étant finie sur $k$ est a fortiori finie sur $\mathrm{A}/f^{-1}(\mathfrak{m})$ et utiliser la proposition 14.1.3.) Ainsi, $f^{-1}(\mathfrak{m})$ est un idéal maximal de A. □

# Bibliographie


[1] E. Artin – *Galois theory*, second éd., Dover Publications Inc., 1998, Edited and with a supplemental chapter by Arthur N. Milgram.

[2] M. F. Atiyah & I. G. Macdonald – *Introduction to commutative algebra*, Addison–Wesley, 1969.

[3] N. Bourbaki – *Algèbre commutative*, Masson, 1983, Chapitres 8 et 9.

[4] D. Eisenbud – *Commutative algebra with a view towards algebraic geometry*, Graduate Texts in Math., no. 150, Springer Verlag, 1995.

[5] H. Matsumura – *Commutative ring theory*, Cambridge studies in advanced mathematics, Cambridge Univ. Press, 1986. 179

[6] J. S. Milne – « Algebraic geometry », 1998, notes du cours Math 631, disponible à l'adresse *http://www.jmilne.org/math/*.

[7] _____, « Field theory », 1998, notes du cours Math 594, disponible à l'adresse *http://www.jmilne.org/math/*.

[8] D. Mumford – *The red book of varieties and schemes*, Lect. Notes Math., no. 1358, Springer Verlag, 1994.

[9] D. Perrin – *Géométrie algébrique*, InterÉditions, 1994.

[10] M. Reid – *Undergraduate commutative algebra*, London Math. Society Student Texts, vol. 29, Cambridge University Press, 1995.

[11] J.-P. Serre – *Algèbre locale, multiplicités*, Lect. Notes Math., no. 11, Springer Verlag, 1965.

[12] J.-P. Serre – *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1977, Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

# Index