# Anneaux et Modules

MAT 3543

Automne 2020

Alistair Savage

Département de mathématiques et de statistique

Université d'Ottawa

# Table des matières

# Préface

Ces notes sont destinées aux étudiants du cours *Anneaux et Modules* (MAT 3543) à l'Université d'Ottawa. Il s'agit d'un premier cours de la théorie des anneaux et des modules. Dans ce cours, nous étudions la définition générale d'un anneau et les fonctions entre eux, avant de porter notre attention sur l'exemple important des anneaux des polynômes. Ensuite nous discutons des classes d'anneaux qui ont quelques propriétés intéressantes supplémentaires (par exemple, les anneaux euclidiens, anneaux principaux, et anneaux factoriels). On discutons ensuite des modules, qui sont des généralisations d'espaces vectoriels, où on considère les scalaires dans un anneau.

*Notation* : Dans ce cours $\mathbb{N} = \mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, \dots\}$ indique l'ensemble des entiers non négatifs.

*Acknowledgement* : Certaines parties de ces notes sont basées sur des notes d'Erhard Neher, Hadi Salmasian et Damien Roy. Quelques autres parties suivent le manuel Abstract algebra: theory and applications par Tom Judson, qui est le manuel recommandé du cours. Les sections 4.8 et 4.9 suivent Abstract: abstract and concrete par Frederick Goodman. De nombreux exercices de ces notes sont empruntés à ces manuels, et aussi du manuel *Introduction to abstract algebra* par W. Keith Nicholson.

Alistair Savage

*Site web du cours :* https://alistairsavage.ca/mat3543

# Chapitre 1

# Anneaux

Dans ce chapitre, nous introduisons l'objet principal de ce cours. Nous commençons par la définition d'un anneau, donnons plusieurs exemples importants et en déduisons quelques propriétés importantes. Nous tournons ensuite notre attention vers les anneaux intègres et les corps, deux types d'anneaux importants. Puis, nous discutons les idéals et les anneaux quotients. Enfin, nous concluons par une discussion sur les morphismes d'anneaux et énonçons le premier théorème d'isomorphisme. Une référence pour le matériel de ce chapitre est [Jud19, Ch. 16].

## 1.1 Exemples et propriétés de base

**Définition 1.1.1** (Anneau)**.** Un *anneau* est un ensemble non vide $R$ avec deux operations binaires, généralement écrits comme (et appelés) *addition* et *multiplication*, qui remplissent les axiomes suivants.

**(A1)** $a+b=b+a$ pour tous $a,b\in R$.
**(A2)** $(a+b)+c=a+(b+c)$ pour tous $a,b,c\in R$.
**(A3)** Il existe un élément $0\in R$ tel que $a+0=a$ pour tout $a\in R$.
**(A4)** Pour tout $a\in R$, il existe un élément $-a\in R$ tel que $a+(-a)=0$.
**(A5)** $(ab)c=a(bc)$ pour tous $a,b,c\in R$.
**(A6)** Il existe un élément $1\in R$ tel que $1a=a1=a$ pour tout $a\in R$.
**(A7)** $a(b+c)=ab+ac$ et $(a+b)c=ac+bc$ pour tous $a,b,c\in R$.

Un anneau $R$ et *commutatif* si, en plus,

**(A8)** $ab=ba$ pour tous $a,b\in R$.

Lorsqu'on veut spécifier l'anneau, on écrit parfois $0_R$ et $1_R$ pour les éléments 0 et 1.

Parfois, la condition (A6) est omise de la définition d'un anneau et on se réfère à un *anneau unitaire* pour spécifier que la condition (A6) est satisfaite. Cependant, dans ce cours, nous supposerons toujours que nos anneaux aient une unité et utiliserons le terme *anneau général* pour les objets qui remplissent tous les axiomes d'un anneau autre que (A6). Les axiomes (A1)–(A4) sont équivalents au fait que $(R,+)$ est groupe abélien. Les axiomes (A5)–(A6) impliquent que $(R,\cdot)$ est un monoïde. Ainsi, l'élément 1, appelé l'*unité*, ou *élément neutre*, de $R$, est unique. L'élément zéro 0 est également unique. Voir l'exercice 1.1.1.

*Remarque* 1.1.2. Les *anneaux non associatifs* sont également un domaine d'étude important. Ce sont des objets pour lesquels nous ne demandons pas que (A5) soit satisfaite. (Un meilleur nom pourrait être «anneaux pas nécessairement associatifs».) Les *algèbres de Lie* sont une classe bien étudiée d'anneaux non associatifs.

*Exemple* 1.1.3. Chacun de $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, et $\mathbb{C}$ est un anneau commutatif.

*Exemple* 1.1.4. Soit $n$ un entier positif et soit $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ avec l'addition et la multiplication modulo $n$. Puis $\mathbb{Z}_n$ est un anneau commutatif.

*Exemple* 1.1.5 (Matrices). L'ensemble $\mathrm{Mat}_n(\mathbb{Q})$ de tous les matrices de taille $n \times n$ avec des coefficients rationnels et un anneau sous l'addition et la multiplication des matrices. Si $n \geq 2$, cet anneau n'est pas commutatif. Plus généralement, si $R$ et un anneau, alors $\mathrm{Mat}_n(R)$ est aussi un anneau (avec les mêmes règles d'addition et de multiplication des matrices).

*Exemple* 1.1.6 (Anneaux des polynômes). Pour tout anneau $R$, on a l'anneau

$$R[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m : a_0, \dots, a_m \in R\},$$

appelé *l'anneau des polynômes avec coefficients dans* $R$. Ici $x$ est une indéterminée. Nous allons discutons les anneaux polynomiaux dans plus de détaille dans le chapitre suivant.

*Exemple* 1.1.7 (Anneaux des fonctions). Si $X$ est un ensemble non vide, alors l'ensemble $\mathcal{F}(X, \mathbb{R})$ des fonctions à valeurs réelles $f\colon X \to \mathbb{R}$ est un anneau commutatif sous addition et multiplication ponctuelle.

*Exemple* 1.1.8 (Produit direct d'anneaux). Si $R_1, \dots, R_n$ sont des anneaux, alors leur *produit direct* est le produit cartésien $R_1 \times \cdots \times R_n$ munit des opérations

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n),$$
$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n).$$

*Exemple* 1.1.9 (Anneau nul). Le plus petit anneau est l'*anneau nul* $R = \{0\}$. Un anneau $R$ est l'anneau nul (c.-à-d. a seulement un élément, son élément zéro) si et seulement si $1_R = 0_R$. Voir l'exercice 1.1.2. Puisque l'anneau nul n'est pas très intéressant, nous souvent supposons que les anneaux ne soient pas nuls.

*Exemple* 1.1.10. L'ensemble $2\mathbb{Z}$ d'entiers pairs, avec l'addition et la multiplication naturelles, est un anneau général qui n'est pas un anneau. Un autre exemple est l'ensemble de toutes les matrices réelles de taille $3 \times 3$ dont la ligne du bas est zéro, avec l'addition et la multiplication de matrices naturelles.

**Définition 1.1.11** (Unité, inverse multiplicatif)**.** Soit $R$ un anneau. Un élément $a \in R$ est appelé une *unité* s'il existe un élément $b \in R$ tel que $ab = ba = 1$. L'élément $b$ est appelé l'*inverse multiplicatif* de $a$. L'ensemble des unités de $R$ est noté $R^\times$. (Dans certaines textes, l'ensemble d'unités est noté $R^*$. Nous utilisons la notation $R^\times$ pour éviter toute confusion avec le dual d'un espace vectoriel.)

**Proposition 1.1.12** (L'unicité des inverses multiplicatifs)**.** *Si $a \in R$ a un inverse multiplicatif, alors cet inverse est unique.*

*Démonstration.* Si $b$ et $c$ sont des inverses multiplicatifs de $a$, alors

$$b = b1 = b(ac) = (ba)c = 1c = c. \qquad \square$$

**Proposition 1.1.13.** *Pour tout anneau $R$, l'ensemble $R^\times$ est un groupe sous multiplication.*

*Démonstration.* La démonstration de cette proposition et l'exercice 1.1.5. $\square$

Désormais, nous appellerons $R^\times$ le *groupe d'unités* de $R$.
Supposons que $R$ soit un anneau. Si $m \in \mathbb{Z}$ et $a \in R$, alors nous définissons

$$ma := \begin{cases} \underbrace{a + a + \cdots + a}_{m \text{ termes}} & \text{si } m > 0, \\ 0 & \text{si } m = 0, \\ \underbrace{-a + (-a) + \cdots + (-a)}_{|m| \text{ termes}} & \text{si } m < 0. \end{cases} \tag{1.1}$$

Si $m \in \mathbb{N}$, alors nous définissons

$$a^m := \underbrace{a \cdot a \cdots a}_{m \text{ facteurs}}.$$

Ici on interprète $a^0 = 1$. Si $a$ est une unité, alors $a^m$ est défini pour tout $m \in \mathbb{Z}$. Pour $m$ négatif, on définit

$$a^m := \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{|m| \text{ facteurs}}.$$

Il est facile à montrer (voir l'exercise 1.1.6) que

$$(m+n)a = ma + na, \quad m(na) = (mn)a \quad \text{pour tous } m, n \in \mathbb{Z},\ a \in R, \tag{1.2}$$

$$a^{m+n} = a^m a^n, \quad (a^m)^n = a^{mn} \quad \text{pour tous } m, n \in \mathbb{N},\ a \in R. \tag{1.3}$$

Si $a$ est une unité, alors (1.3) est satisfaite pour tous $m, n \in \mathbb{Z}$.

**Théorème 1.1.14.** *Soit $R$ un anneau et soient $r, s \in R$. Alors*

*(a)* $r0 = 0 = 0r$,
*(b)* $(-r)s = r(-s) = -(rs)$,
*(c)* $(-r)(-s) = rs$, *et*
*(d)* $(mr)(ns) = (mn)(rs)$ *pour tous* $m, n \in \mathbb{Z}$.

*(Ici $0 = 0_R$, par opposition à l'entier zéro.)*

*Démonstration.* Pour $r \in R$, nous avons $r0 = r(0+0) = r0 + r0$. Additionner $-r0$ aux deux côtés donne $r0 = 0$. La preuve de la relation $0r = 0$ est similaire. Les autres relations sont laissés en exercice (ou voir [Jud19, Prop. 16.8]). $\square$

**Définition 1.1.15** (Soustraction)**.** Si $r$ et $s$ sont des éléments d'un anneau $R$, leur *différence* est

$$r - s := r + (-s).$$

De cette façon, nous pouvons définir la *soustraction* dans un anneau.

**Définition 1.1.16** (Caractéristique)**.** Si $R$ est un anneau, la *caractéristique* de $R$, notée $\mathrm{car}(R)$, est l'ordre de $1_R$ dans $(R, +)$ si cet ordre est fini et nulle si cet ordre est infini.

*Exemple* 1.1.17. Nous avons

$$\mathrm{car}(\mathbb{Z}) = 0, \quad \mathrm{car}(\mathbb{R}) = 0, \quad \mathrm{car}(\mathbb{C}) = 0, \quad \mathrm{car}(\mathbb{Z}_n) = n, \quad \mathrm{car}(\text{anneau nul}) = 1.$$

*Remarque* 1.1.18. Noter que si l'anneau $R$ est fini (c.-à-d. $|R| < \infty$), alors $\mathrm{car}(R) > 0$.

**Lemme 1.1.19.** *La caractéristique d'un anneau $R$ est l'exposant du groupe additif de l'anneau. Autrement dit, c'est le plus petit entier positif $n$ tel que $na = 0$ pour tout $a \in R$.*

*Démonstration.* Il suffit de montrer que $n1 = 0$ si et seulement si, pour tout $a \in R$, on a $na = 0$. Il est clair que cette dernière condition implique la première (il suffit de prendre $a = 1$). Or, si $n1 = 0$, alors, pour tout $a \in R$, on a $na = n(1a) = (n1)a = 0a = 0$. □

**Définition 1.1.20** (Idempotent, nilpotent)**.** Un élément $a \in R$ est appelé *idempotent* si $a^2 = a$. Il est appelé *nilpotent* s'il existe un entier positif $n$ tel que $a^n = 0$.

*Exemples* 1.1.21. Dans tout anneau $R$, les éléments 0 and 1 sont idempotents et 0 est nilpotent. Dans $\mathrm{Mat}_2(\mathbb{R})$ nous avons des autres éléments idempotents :

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}, \ldots .$$

Dans $\mathrm{Mat}_2(\mathbb{R})$ nous avons aussi beaucoup d'éléments nilpotents :

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ -2 & 0 \end{bmatrix}, \ldots .$$

**Définition 1.1.22** (Sous-anneau)**.** Un sous-ensemble $S \subseteq R$ d'un anneau $R$ est appelé un *sous-anneau* de $R$ s'il est lui-même un anneau avec les mêmes opérations (et la même élément neutre) que $R$.

**Proposition 1.1.23** (Test de sous-anneau)**.** *Un sous-ensemble $S \subseteq R$ d'un anneau $R$ est un sous-anneau de $R$ si*

**(SA1)** *$0 \in S$ et $1 \in S$,*

**(SA2)** *Si $s, t \in S$, alors $s + t$, $st$ et $-s$ sont tous dans $S$.*

*Ou bien, $S$ est un sous-anneau de $R$ si*

**(SA1′)** *$1 \in S$,*

**(SA2′)** *$rs \in S$ pour tous $r, s \in S$, et*

**(SA3′)** *$r - s \in S$ pour tous $r, s \in S$.*

*Démonstration.* La preuve de cette proposition est l'exercice 1.1.7. □

*Exemples* 1.1.24. (a) $\mathbb{Z}$ est un sous-anneau $\mathbb{R}$.

(b) $\mathrm{Mat}_2(\mathbb{Z})$ est un sous-anneau $\mathrm{Mat}_2(\mathbb{Q})$.

(c) $\begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{R} \end{bmatrix} := \left\{ \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} : x, y, z \in \mathbb{R} \right\}$ est un sous-anneau $\mathrm{Mat}_2(\mathbb{R})$.

(d) $2\mathbb{Z}$ n'est *pas* un sous-anneau de $\mathbb{Z}$.

(e) Les *entiers de Gauss* $\mathbb{Z}(i) := \{a + bi : a, b \in \mathbb{Z}\}$ sont un sous-anneau de $\mathbb{C}$.

(f) Si $a, b \in \mathbb{R}$ où $a < b$, alors les fonctions réelles continues sur l'intervalle $[a, b]$ forment un sous-anneau de $\mathcal{F}([a, b], \mathbb{R})$.

*Exemple* 1.1.25. Trouvons $\mathbb{Z}(i)^\times$. Nous avons

$$(a+bi)(c+di) = 1 \implies (a-bi)(c-di) = \overline{(a+bi)(c+di)} = \bar{1} = 1 \implies (a^2+b^2)(c^2+d^2) = 1.$$

Puisque $a^2 + b^2, c^2 + d^2 \in \mathbb{N}$, cela implique que $a^2 + b^2 = 1$. Ainsi, soit $a = 0$, $b = \pm 1$ ou $a = \pm 1$, $b = 0$. Donc $\mathbb{Z}(i)^\times = \{\pm 1, \pm i\}$.

**Définition 1.1.26** (Centre)**.** Le *centre* d'un anneau $R$ est

$$Z(R) := \{r \in R : rs = sr \text{ pour tout } s \in R\}.$$

*Exemple* 1.1.27. Un anneau $R$ est commutatif si est seulement si $Z(R) = R$.

**Lemme 1.1.28.** *Le centre $Z(R)$ d'un anneau $R$ est un sous-anneau de $R$.*

*Démonstration.* La preuve de ce lemme est l'exercice 1.1.10. □

Plus tard, dans la section 1.4, nous discuterons de la notion de morphisme d'anneaux. Cependant, il est utile de donner ici la définition du cas particulier d'un isomorphisme d'anneaux (voir aussi la définition 1.4.10).

**Définition 1.1.29** (Anneaux isomorphes)**.** On dit que deux anneaux $R, S$ sont *isomorphes*, et on écrit $R \cong S$, s'il existe une application $\sigma\colon R \to S$ telle que

(a) $\sigma$ est un bijection,

(b) $\sigma(a + b) = \sigma(a) + \sigma(b)$ pour tous $a, b \in R$, et

(c) $\sigma(ab) = \sigma(a)\sigma(b)$ pour tous $a, b \in R$.

L'application $\sigma$ est appelée un *isomorphisme*.

*Remarque* 1.1.30. Notez que si $\sigma\colon R \to S$ est un isomorphisme d'anneaux, alors nous avons les suivants :

(a) $\sigma$ est un isomorphisme des groupes additifs correspondants. En particulier, $\sigma(0_R) = 0_S$.

(b) $\sigma(1_R) = 1_S$. Cela peut être vu comme suit. Pour tout $s \in S$, il existe $r \in R$ tel que $\sigma(r) = s$. Ainsi $s\sigma(1_R) = \sigma(r)\sigma(1_R) = \sigma(r1_R) = \sigma(r) = s$. De même $\sigma(1_R)s = s$. Puisque $s \in S$ était en élément quelconque, cela implique que $\sigma(1_R)$ est l'élément neutre de $S$.

*Exemple* 1.1.31. Soient

$$R_1 = \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{R} \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\} \quad \text{et} \quad R_2 = \begin{bmatrix} \mathbb{R} & 0 \\ \mathbb{R} & \mathbb{R} \end{bmatrix} = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\}.$$

Considérons l'application $\sigma\colon R_1 \to R_2$ donnée par

$$\sigma\left( \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \right) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} c & 0 \\ b & a \end{bmatrix}$$

Il est facile à voir que $\sigma^2 = \mathrm{id}$. Ainsi $\sigma$ est inversible et donc bijective. Si $M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, nous avons aussi

$$\sigma(A+B) = M(A+B)M^{-1} = MAM^{-1} + MBM^{-1} = \sigma(A) + \sigma(B),$$
$$\sigma(A)\sigma(B) = (MAM^{-1})(MBM^{-1}) = MABM^{-1} = \sigma(AB).$$

Ainsi $\sigma$ est un isomorphisme et donc $R_1 \cong R_2$.

Notez que l'application $A \mapsto A^T$ n'est *pas* un isomorphisme d'anneaux puisque $(AB)^T \neq A^T B^T$ en général.

---

# Exercices.

1.1.1. Prouver que l'élément neutre dans n'importe quel monoïde (donc dans n'importe quel groupe) est unique.

1.1.2. Montrer qu'un anneau $R$ est l'anneau nul (c.-à-d. $R = \{0\}$) si est seulement si $0_R = 1_R$.

1.1.3. Expliquer pourquoi chacun des suivants n'est pas un anneau.

(a) $\mathbb{N} = \{0, 1, 2, 3, \ldots, \}$ sous l'addition et la multiplication naturelles.

(b) $2\mathbb{Z}$.

(c) L'ensemble de tous les applications $f\colon \mathbb{R} \to \mathbb{R}$ sous addition ponctuelle, mais avec multiplication donnée par composition.

1.1.4. Soit $R$ un anneau. L'*anneau opposé* $R^{\mathrm{op}}$ de $R$ est le même ensemble que $R$, avec la même addition, mais avec une multiplication donnée par $r \cdot s = sr$. (Ici $\cdot$ désigne la multiplication dans $R^{\mathrm{op}}$ et la juxtaposition désigne la multiplication dans $R$.) Prouvez que $R^{\mathrm{op}}$ est un anneau.

1.1.5. Démontrer la proposition 1.1.13.

1.1.6. Démontrer (1.2) et (1.3).

1.1.7. Démontrer la proposition 1.1.23.

1.1.8 ([Nic12, Ex. 3.1.3]). Pour chacun des suivants, montrer que $S$ est un sous-anneau de $R$.

(a) $S = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R},\ a + c = b + d \right\}$, $R = \mathrm{Mat}_2(\mathbb{R})$.

(b) $S = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$, $R = \mathrm{Mat}_2(\mathbb{R})$.

(c) $S = \left\{ \begin{bmatrix} a & 0 & b \\ 0 & c & d \\ 0 & 0 & a \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$, $R = \mathrm{Mat}_3(\mathbb{R})$.

(d) $S = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$, $R = \mathrm{Mat}_2(\mathbb{R})$.

1.1.9 ([Nic12, Ex. 3.1.4]). Si $S$ et $T$ sont des sous-anneaux de $R$, montrer que $S \cap T$ est un sous-anneau de $R$. Est-il nécessairement vrai que $S + T = \{s + t : s \in S,\ t \in T\}$ est un sous-anneau de $R$ ?

1.1.10. Démontrer le lemme 1.1.28.

1.1.11. Trouver le centre de $\mathrm{Mat}_2(\mathbb{R})$.

1.1.12. Montrer que si $R$ et $S$ sont des anneaux, alors $(R \times S)^\times = R^\times \times S^\times$.

1.1.13 ([Nic12, Ex. 3.1.5]). Supposons que $X$ soit un sous-ensemble non vide d'un anneau $R$. Le *centralisateur* de $X$ dans $R$ est, par définition,

$$C(X) = \{c \in R : cx = xc \text{ for all } x \in X\}.$$

Démontrer que $C(X)$ est un sous-anneau de $R$.

1.1.14 ([Nic12, Ex. 3.1.10]). Supposons que $a$ et $b$ soient des éléments d'un anneau.

(a) Si $ab + ba = 1$ et $a^3 = a$, démontrer que $a^2 = 1$.

(b) Si $ab = a$ et $ba = b$, démontrer que $a^2 = a$ et $b^2 = b$.

1.1.15 ([Nic12, Ex. 3.1.11]). Montrer que 0 est le seul élément nilpotent dans un anneau $R$ si et seulement si $a^2 = 0$ implique $a = 0$.

1.1.16 ([Nic12, Ex. 3.1.14]). Si $r$ et $s$ sont des éléments d'un anneau $R$, montrer que $1 + rs$ est une unité si et seulement si $1 + sr$ est une unité. *Indice* : $s(1 + rs) = (1 + sr)s$.

1.1.17. Trouver tous les anneaux de caractéristique un.

1.1.18 ([Nic12, Ex. 3.1.18]). Trouver les caractéristiques des anneaux suivants.

(a) $\mathbb{Z}_n \times \mathbb{Z}_m$.

(b) $\mathrm{Mat}_2(\mathbb{Z}_n)$.

(c) $\mathbb{Z} \times \mathbb{Z}_n$.

1.1.19 ([Nic12, Ex. 3.1.20]). Si $ua = au$, où $u$ est une unité et $a$ est nilpotent, montrer que $u + a$ est une unité.

1.1.20 ([Nic12, Ex. 3.1.28]). Pour chacun des anneaux suivants, trouver tous les unités, éléments nilpotents, et idempotents :

(a) $\mathbb{Z}$
(b) $\mathbb{Z}_{24}$
(c) $\mathrm{Mat}_2(\mathbb{Z}_2)$
(d) $\begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{R} \end{bmatrix}$

1.1.21 ([Nic12, Ex. 3.1.36]). Pour toute paire d'anneaux suivante, montrer que les anneaux ne sont pas isomorphes.

(a) $\mathbb{R}$ et $\mathbb{C}$.
(b) $\mathbb{Q}$ et $\mathbb{R}$.
(c) $\mathbb{Z}$ et $\mathbb{Q}$.
(d) $\mathbb{Z}_8$ et $\mathbb{Z}_4 \times \mathbb{Z}_2$.

## 1.2 Les anneaux intègres et les corps

Nous considérons maintenant certains types d'anneaux que nous examinerons en détail plus tard dans le cours.

**Définition 1.2.1** (Diviseur de zéro, anneau intègre, corps gauche, corps)**.** Supposons que $R$ soit un anneau. Un élément non nul $r \in R$ est un *diviseur de zéro* s'il existe un $s \in R$ non nul tel que $rs = 0$ ou $sr = 0$. Un anneau non nul est un *anneau san diviseur de zéro* s'il n'a aucun diviseur de zéro. Un anneau commutatif san diviseur de zéro est appelé un *anneau intègre*. Si chaque élément non nul dans un anneau non nul (pas nécessairement commutatif) est une unité, alors $R$ est appelé un *corps gauche*. Un corps gauche commutatif est appelé un *corps*.

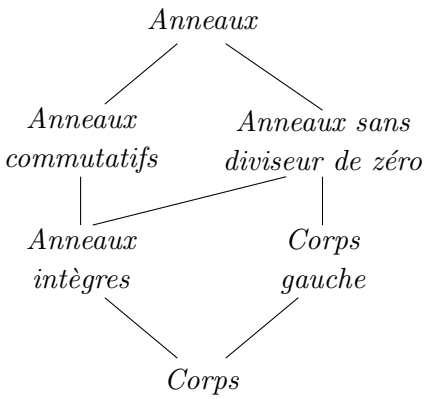


FIGURE 1.1 – Types d'anneaux

*Exemple* 1.2.2. Les anneaux $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ sont des corps. L'anneau $\mathbb{Z}$ est un anneau intègre, mais il n'est pas un corps.

*Exemple* 1.2.3. L'anneau $\mathbb{Z}(i)$ des entiers de Gauss est un anneau intègre (exercice 1.2.1) mais il n'est pas un corps, puisque $\mathbb{Z}(i)^\times = \{\pm 1, \pm i\}$ (voir l'exemple 1.1.25).

*Exemple* 1.2.4. L'anneau $\mathrm{Mat}_2(\mathbb{R})$ n'est pas un anneau sans diviseur de zéro puisque, par exemple,

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

**Proposition 1.2.5.** *L'anneau $\mathbb{Z}_m$ est un corps si et seulement si $m$ est un nombre premier.*

*Démonstration.* Soit $m$ un nombre premier. Pour tous $\bar{a} \in \mathbb{Z}_m$, $\bar{a} \neq 0$, on a $\mathrm{pgcd}(a, m) = 1$ et donc il existe $x, y \in \mathbb{Z}$ tels que $ax + my = 1$. Ainsi $\bar{a}\bar{x} = \bar{1}$ dans $\mathbb{Z}_m$. Donc tout élément non nul de $\mathbb{Z}_m$ est une unité.

Maintenant supposons que $m$ soit un nombre composé. Alors il existe $1 < m_1, m_2 < m$ tels que $m = m_1 m_2$. En particulier, $\bar{m}_1, \bar{m}_2 \neq 0$, mais $\bar{m}_1 \bar{m}_2 = \bar{m} = \bar{0}$. Donc $m_1$ et $m_2$ ne sont pas des unités dans $\mathbb{Z}_m$. □

**Proposition 1.2.6.** *Soit $R$ un anneau tel que $|R| = p$, où $p$ est un nombre premier. Alors $R$ est isomorphe à $\mathbb{Z}_p$. En particulier, $R$ est un corps.*

*Démonstration.* D'après le théorème de Lagrange, le groupe additif $\langle 1 \rangle$ engendré par l'élément neutre est égal à tout $R$ et doit être isomorphe au groupe $\mathbb{Z}_p$ (puisque c'est le seul groupe d'ordre $p$ lorsque $p$ est un nombre premier). Définir $\sigma \colon \mathbb{Z}_p \to R$ par $\sigma(\bar{m}) = m1_R$. Puis on a le suivant :

— $\sigma$ est injective puisque, pour tous $a, b \in \mathbb{Z}$,

$$\sigma(\bar{a}) = \sigma(\bar{b}) \implies a1 = b1 \implies (a-b)1 = 0 \implies p|(a-b) \implies \bar{a} = \bar{b} \text{ dans } \mathbb{Z}_p,$$

où la troisième implication découle du fait que $(a-b)1 = 0$ dans le groupe additif $(R, +) \cong \mathbb{Z}_p$ (isomorphisme des groupes) si et seulement si $p|(a-b)$. (Notez qu'on ne peut pas simplement conclure de $a1 = b1$ que $a = b$, puisque les expressions $a1$ et $b1$ ne représentent pas des produits dans l'anneau $R$. Ils sont plutôt de la forme (1.1).)

— $\sigma$ est bijective puisque $\sigma$ est injective et $|R| = |\mathbb{Z}_p|$.

— On a

$$\sigma(\bar{a} + \bar{b}) = \sigma\left(\overline{a+b}\right) = (a+b)1 = a1 + b1 = \sigma(\bar{a}) + \sigma(\bar{b}).$$

— $\sigma(\overline{ab}) = \sigma(\bar{a})\sigma(\bar{b})$. La preuve de ce fait est similaire à ce qui précède et elle est laissé en exercice. □

**Proposition 1.2.7.** *Soit $R$ un anneau. Les déclarations suivantes sont équivalentes :*

*(a) $R$ est un anneau sans diviseur de zéro.*

*(b) Si $ab = ac$ dans $R$ et $a \neq 0$, alors $b = c$.*

*(c) Si $ba = ca$ dans $R$ et $a \neq 0$, alors $b = c$.*

*Démonstration.* (a) $\implies$ (b). Supposons que $R$ soit un anneau sans diviseur de zéro et que $ab = ac$ dans $R$. Alors $a(b-c) = ab-ac = 0$. Puisque $a \neq 0$ et $R$ est un anneau sans diviseur de zéro, il faut que $b - c = 0$, d'où $b = c$.

(b) $\implies$ (a). Supposons que $R$ remplisse (b) et que $ab = 0$ dans $R$. Alors on a $ab = a0$. Ainsi, si $a \neq 0$, il faut que $b = 0$ par (b). Donc $R$ est un anneau sans diviseur de zéro.

Nous avons démontré l'équivalence de (a) et (b). La démonstration que (a) et (c) sont équivalents est similaire. □

*Exemples* 1.2.8. (a) Tout corps gauche est un anneau sans diviseur de zéro.

(b) Tout corps est un anneau intègre.

(c) Si $R$ est anneau intègre et $S$ est un sous-anneau de $R$, alors $S$ est un anneau intègre.

(d) $\mathbb{Z}(i)$ est un anneau intègre (puisqu'il est un sous-anneau de $\mathbb{C}$).

*Exemple* 1.2.9. Le sous-anneau $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ du corps des nombres complexes est un corps. Étant un sous-anneau de $\mathbb{C}$, il est un anneau intègre. Il reste donc à montrer que chaque élément non nul a un inverse multiplicatif. Supposons que $x \in \mathbb{Q}(\sqrt{2}) \setminus \{0\}$. Alors $x = a + b\sqrt{2}$ où $a \neq 0$ ou $b \neq 0$. Alors

$$x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Notez que $a^2-2b^2 \neq 0$ puisque si $a^2-2b^2 = 0$, alors $\frac{a^2}{b^2} = 2$, ce qui implique que $\sqrt{2} = \pm\frac{a}{b} \in \mathbb{Q}$. Cela contredit le fait que $\sqrt{2}$ est un nombre irrationnel.

**Définition 1.2.10** (Quaternions)**.** Les *quaternions* sont l'anneau

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

avec multiplication déterminé par les règles

$$ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik, \quad i^2 = j^2 = k^2 = -1.$$

Pour $w = a+bi+cj+dk \in \mathbb{H}$, nous définissons $w^* := a-bi-cj-dk$ et $N(w) := a^2+b^2+c^2+d^2$.

Par exemple, nous avons

$$(3 - 4j)(2i + k) = 6i + 3k - 8ji - 4jk = 6i + 3k + 8k - 4i = 2i + 11k.$$

**Lemme 1.2.11.** *Si $w \in \mathbb{H} \setminus \{0\}$, alors $w^{-1} = \frac{1}{N(w)}w^*$.*

*Démonstration.* Voir [Jud19, Example 16.7]. □

D'après le lemme 1.2.11, l'anneau des quaternions est un corps gauche. Cependant, il n'est pas un corps puisqu'il n'est pas commutatif. Donc, les quaternions est un exemple d'un corps gauche non commutatif.

**Proposition 1.2.12.** *La caractéristique d'un anneau intègre est soit zéro, soit un nombre premier.*

*Démonstration.* Soit $R$ un anneau intègre et supposons que la caractéristique de $R$ soit $n \neq 0$. Si $n$ n'est pas premier, alors $n = ab$, où $1 < a < n$ et $1 < b < n$. Alors $0 = n1 = (ab)1 = (a1)(b1)$. Puisque $R$ n'a pas de diviseur de zéro, soit $a1 = 0$, soit $b1 = 0$. Ainsi, la caractéristique de $R$ doit être inférieure à $n$, ce qui est une contradiction. Par conséquent, $n$ doit être premier. □

**Proposition 1.2.13.** *Tout anneau intègre fini est un corps.*

*Démonstration.* Soit $R$ un anneau intègre avec $|R| = n < \infty$. Supposons que $r \in R$ où $r \neq 0$. Alors, d'après la proposition 1.2.7, la fonction $f\colon R \to R$, $f(x) = rx$, est injective. Puisque $R$ est fini, cela implique que $f$ est bijective. Ainsi il existe $s \in R$ tel que $f(s) = rs = 1$. Donc $r$ est une unité. Puisque $r$ était un élément non nul quelconque de $R$, cela implique que $R$ est un corps. □

Une preuve du théorème suivant peut être trouvée dans [Jud19, Th. 16.16]. (Nous n'utiliserons pas ce théorème.)

**Théorème 1.2.14** (Théorème de Wedderburn)**.** *Tout corps gauche fini est un corps.*

Nous concluons cette section en montrant que chaque domaine intégral est «contenu» dans un champ. Nous faisons cela en imitant la construction des nombres rationnels à partir des entiers. Nous supposons pour le reste de cette section que $R$ soit un anneau intègre.

Soit

$$X = \{(r, u) : r, u \in R,\ u \neq 0\}$$

et définissons une relation sur $X$ par

$$(r, u) \equiv (s, v) \iff rv = su.$$

C'est une relation d'équivalence sur $X$. Il est facile à voir que cette relation est réflexive et symétrique. Il faut donc montrer qu'elle est transitive. Supposer que

$$(r, u) \equiv (s, v) \quad \text{et} \quad (s, v) \equiv (t, w).$$

Alors, par définition, on a $rv = su$ et $sw = tv$. Donc,

$$(rw)v = (rv)w = (su)w = u(sw) = utv \qquad \text{(puisque } R \text{ est commutatif).}$$

Puisque $(s, v) \in X$, on a $v \neq 0$ et on peut donc annuler $v$ dans ce qui précède par la proposition 1.2.7. Cela donne $rw = tu$ et donc $(r, u) \equiv (t, w)$. Ainsi $\equiv$ est une relation d'équivalence sur $X$. Nous écrivons $\frac{r}{s}$ pour la classe d'equivalence de $(r, s)$. Ainsi $\frac{r}{s} = \frac{s}{v}$ si et seulement si $(r, s) \equiv (s, v)$.

Maintenant nous définissons

$$Q := \left\{ \frac{r}{u} : r, u \in R,\ u \neq 0 \right\}. \tag{1.4}$$

Nous définissons l'addition et la multiplication sur $Q$ par

$$\frac{r}{u} + \frac{s}{v} = \frac{rv + su}{uv} \quad \text{et} \quad \frac{r}{u} \cdot \frac{s}{v} = \frac{rs}{uv}.$$

Notez que $uv \neq 0$ puisque $u, v \neq 0$ et $R$ est un anneau intègre. Puisque les quotients ci-dessus sont les classes d'equivalence, il faut montrer que ces opérations sont bien définies. On montre cela pour la multiplication et renvoyez le lecteur à [Jud19, Lem. 18.2] pour l'addition. Si $\frac{r}{u} = \frac{r'}{u'}$ et $\frac{s}{v} = \frac{s'}{v'}$, il faut montrer que $\frac{rs}{uv} = \frac{r's'}{u'v'}$. Cela suit du fait que

$$(rs)(u'v') = (ru')(sv') = (r'u)(s'v) = (r's')(uv).$$

Nous la laissons en exercice 1.2.14 de montrer que $Q$ est un corps avec zéro $\frac{0}{1}$ et élément neutre $\frac{1}{1}$. Le négatif d'un élément $\frac{r}{u}$ et $\frac{-r}{u}$. De plus, si $\frac{r}{u}$ est non nul dans $Q$, alors $r \neq 0$. Ainsi $\frac{u}{r} \in Q$ et nous avons $\left(\frac{r}{u}\right)^{-1} = \frac{u}{r}$.

Définissons

$$R' := \left\{ \frac{r}{1} : r \in R \right\}. \tag{1.5}$$

Il est facile (exercice 1.2.15) à vérifier que $R'$ est un sous-anneau de $R$. De plus, ce n'est pas difficile à vérifier que l'application

$$\sigma \colon R \to R', \quad \sigma(r) = \frac{r}{1}, \quad r \in R,$$

est un isomorphisme d'anneaux (voir [Jud19, Th. 18.4]) et donc $R \cong R'$. On identifie généralement $R$ à $R'$ via cet isomorphisme. C'est-à-dire, nous définissons $r = \frac{r}{1}$ pour tout $r \in R$. De cette façon, nous considérons $R$ comme sous-anneau de $\mathbb{Q}$. Nous appelons $Q$ le *corps des fractions* de l'anneau intègre $R$.

*Exemple* 1.2.15. Le corps des fractions de $\mathbb{Z}$ est $\mathbb{Q}$. Le corps des fractions de $\mathbb{R}[x]$ est appelé le corps des *fonctions rationnelles*.

---

## Exercices.

1.2.1. Montrer que l'anneau des entiers de Gauss est un anneau intègre.

1.2.2. Montrer que $\mathbb{Z}_m^\times = \{\bar{k} \in \mathbb{Z}_m : \operatorname{pgcd}(k, m) = 1\}$.

1.2.3 ([Nic12, Ex. 3.2.1]). Trouver tous les racines de $x^2 + 3x - 4$ dans les anneaux $\mathbb{Z}$, $\mathbb{Z}_6$, et $\mathbb{Z}_4$.

1.2.4 ([Nic12, Ex. 3.2.2]). Supposons que $p$ soit un nombre premier est définir

$$\mathbb{Z}_{(p)} = \left\{ \frac{n}{m} \in \mathbb{Q} : p \text{ ne divise pas } m \right\}.$$

Montrer que $\mathbb{Z}_{(p)}$ est un anneau intègre et trouver tous ses unités.

1.2.5 ([Nic12, Ex. 3.2.3]). Déterminer tous les idempotents et tous les éléments nilpotents dans un anneau sans diviseur de zéro.

1.2.6 ([Nic12, Ex. 3.2.4]). Supposons que $R$ et $S$ soient des anneaux non nuls. Est-il possible que $R \times S$ soit un anneau sans diviseur de zéro ?

1.2.7 ([Nic12, Ex. 3.2.5]). Montrer que $\mathrm{Mat}_n(R)$, où $R$ est un anneau, n'est jamais un anneau sans diviseur de zéro si $n \geq 2$.

1.2.8 ([Nic12, Ex. 3.2.6]). Si $a^2 = b^2$ et $a^3 = b^3$ dans un anneau sans diviseur de zéro, montrer que $a = b$. Maintenant faire la même chose pour $a^m = b^m$ et $a^n = b^n$ où $m, n > 1$ et $\mathrm{pgcd}(m, n) = 1$. *Indice* : Il existe $x, y \in \mathbb{Z}$ tels que $1 = xm + yn$.

1.2.9 ([Nic12, Ex. 3.2.7]). Supposons qu'un anneau $R$ n'ait aucun élément nilpotent non nul. Si $ab = 0$ dans $R$, montrer que $ba = 0$.

1.2.10 ([Nic12, Ex. 3.2.8]). Montrer qu'un anneau $R$ est un corps gauche si est seulement si, pour tout $a \in R$ non nul, il exist un élément unique $b \in R$ tel que $aba = a$.

1.2.11 ([Nic12, Ex. 3.2.11]). Si $F$ est un corps à $q$ éléments, montrer que $a^q = a$ pour tout $a \in F$. *Indice* : Utiliser le théorème de Lagrange.

1.2.12 ([Nic12, Ex. 3.2.14]). Montrer qu'il n'y a aucun corps à 6 éléments. *Indice* : Utiliser le théorème de Lagrange.

1.2.13 ([Nic12, Ex. 3.2.15]). Montrer que le centre d'un corps gauche est un corps.

1.2.14. Montrer que $Q$, comme définit dans (1.4), est un corps.

1.2.15. Montrer que $R'$, comme définit dans (1.5), est un sous-anneau de $Q$.

1.2.16 ([Nic12, Ex. 3.2.28]). Soit $R$ un anneau commutatif. On dit que $u \in R$ est un *non diviseur de zéro* si $ur = 0$, $r \in R$, implique que $r = 0$. Soit $U \subseteq R$ un ensemble de non diviseurs de zéro dans $R$ tel que $1 \in U$ et $ab \in U$ pour tous $a, b \in U$. Généraliser la construction du corps des fractions par montrant qu'un anneau des quotients

$$Q = \left\{ \frac{r}{u} : r \in R,\ u \in U \right\}$$

existe. Montrer en outre que $R$ peut être considéré comme sous-anneau de $Q$ et, dans ce cas, que chaque élément de $U$ est une unité dans $Q$ et $Q = \{ru^{-1} : r \in R,\ u \in U\}$.

## 1.3 Idéaux et anneaux quotients

Rappelons que si $G$ est un groupe et $H \subseteq G$, alors pour que l'ensemble quotient $G/H$ soit naturellement un groupe, il faut que $H$ soit un sous-groupe normal de $G$. Quelle est la notion analogue pour les anneaux ? Autrement dit, si $R$ est un anneau et $S \subseteq R$, quand $R/S$ est-il naturellement un anneau ?

*Exemple* 1.3.1. Soit $R = \mathbb{Z} \times \mathbb{Z}$, et $S = \{(x, x) : x \in \mathbb{Z}\}$. Il est simple à vérifier que $S$ est sous-anneau de $R$. Notez que $(0, 1) + S = (-1, 0) + S$. Si nous essayons de définir une

multiplication sur l'ensemble des classes suivant $S$, $R/S$, en multipliant les représentatives, nous avons

$$((0,1)+S)((0,1)+S) = (0,1)+S \neq (0,0)+S = ((0,1)+S)((-1,0)+S),$$

ce qui est une contradiction.

**Définition 1.3.2** (Idéal)**.** Soit $R$ un anneau. Un sous-groupe additive $I \subseteq R$ est appelé un *idéal* de $R$ si pour tout $r \in R$, il est vraie que $rI \subseteq I$ et $Ir \subseteq I$. L'idéal $I$ est *propre* si $I \neq R$.

On veut maintenant définir la structure d'un anneau sur l'ensemble des quotients $R/I := \{a+I : a \in R\}$. (Rappelons que $a+I = a'+I \iff a-a' \in I$.) Nous voulons que l'addition et la multiplication soient données par

$$(a+I)+(b+I) = (a+b)+I \quad \text{et} \quad (a+I)(b+I) = ab+I. \tag{1.6}$$

**Théorème 1.3.3.** *Soit $I \subseteq R$ un idéal de $R$. Alors $R/I$, avec l'addition et la multiplication définies par (1.6), est un anneau. L'élément neutre de $R/I$ est $1+I$ et le zéro est $0+I = I$. Si $R$ est commutatif, alors $R/I$ est également commutatif.*

*Démonstration.* Il faut premièrement montrer que l'addition et la multiplication sont bien définis. Si $a+I = a'+I$ et $b+I = b'+I$, alors $a-a', b-b' \in I$. Ainsi

$$ab - a'b' = (a-a')b + a'(b-b') \in Ib + a'I \subseteq I$$

et donc $ab+I = a'b'+I$. Par conséquent, la multiplication et bien définie. La démonstration que l'addition et aussi bien définie, et que $R/I$ remplit les axiomes de la définition 1.1.1, est l'exercice 1.3.1. Il est claire que $R/I$ est commutatif si $R$ est commutatif. □

**Proposition 1.3.4.** *Soit $I$ un idéal d'un anneau $R$. Alors les affirmations suivantes sont équivalentes :*

*(a)* $1 \in I$.
*(b)* $I$ *contient une unité.*
*(c)* $I = R$.

*Démonstration.* Cette démonstration est l'exercice 1.3.2. □

**Définition 1.3.5** (Idéal principal)**.** Si $a \in Z(R)$, alors $Ra = aR$ et c'est un idéal de $R$, noté $\langle a \rangle$. C'est l'*idéal principal* engendré par $a$.

**Proposition 1.3.6** (Idéaux de $\mathbb{Z}$)**.** *Tout idéal de $\mathbb{Z}$ est principal.*

*Démonstration.* L'idéal nul $\{0\}$ est un idéal principal puisque $0\mathbb{Z} = \{0\}$. Si $I$ est un idéal non nul de $\mathbb{Z}$, alors il faut que $I$ contienne un entier positif. Alors il existe un entier positif $n$ le plus petit dans $I$ par le principe du bien-ordre. Maintenant soit $a$ un élément quelconque de $I$. En utilisant l'algorithme de division, nous savons qu'il existe des entiers $q$ et $r$ tels que

$$a = nq + r$$

où $0 \leq r < n$. Cette équation implique que $r = a - nq \in I$, mais il faut que $r = 0$ puisque $n$ est l'élément positif le plus petit dans $I$. Donc, $a = nq$ et $I = n\mathbb{Z}$. □

*Exemple* 1.3.7. Si $R$ est un anneau, alors $\{0\}$ et $R$ sont des idéaux de $R$. Les anneaux quotients correspondants sont $R/\{0\} \cong R$ et $R/R \cong \{0\}$. L'idéal $\{0\}$ est appelé l'*idéal nul* de $R$.

**Définition 1.3.8** (Anneau simple)**.** Un anneau non nul $R$ est *simple* si ses seuls idéaux sont $\{0\}$ et $R$.

*Exemple* 1.3.9. La proposition 1.3.4 implique que les seules idéaux d'un corps gauche sont $\{0\}$ et $R$. Ainsi les corps gauches sont simples.

*Exemple* 1.3.10. Soit $R = \mathbb{Z}(i)$ l'anneau des entiers de Gauss. Soit $I = \langle 2+i \rangle$. Nous voulons décrire l'anneau $R/I$. Puisque $i-(-2) = 2+i \in I$, nous avons $i+I = (-2)+I$. Donc, pour tous $m, n \in \mathbb{Z}$,

$$(m+ni)+I = (m+I)+(-2n+I) = (m-2n)+I.$$

De plus, $5 = (2+i)(2-i) \in (2+i)R = I$, ce qui implique que $5+I = I$. Ainsi les seuls éléments de $R/I$ sont $I, 1+I, 2+I, 3+I, 4+I$. Tous ces éléments sont-ils distincts ? Supposons que $n, m \in \mathbb{Z}$ et $n+I = m+I$. Ainsi $(m-n)+I = I$. Alors, il existe $a, b \in \mathbb{Z}$ tels que

$$m-n = (2+i)(a+bi) = (2a-b)+(a+2b)i \implies a = -2b \implies m-n = -5b \in 5\mathbb{Z}.$$

Donc, $R/I \cong \mathbb{Z}_5$ (un corps).

**Définition 1.3.11** (Idéal premier)**.** Un idéal $P$ d'un anneau commutatif $R$ est un *idéal premier* si $P \neq R$ et

$$r, s \in R,\ rs \in P \implies r \in P \text{ ou } s \in P.$$

(Voir les exercices 1.3.5 et 1.3.20(d) pour la raison pour laquelle ces idéaux sont appelés *premiers*.)

*Exemples* 1.3.12. (a) $2\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, mais pas $4\mathbb{Z}$.

(b) $\mathbb{Z} \times \{0\}$ est un idéal premier de $\mathbb{Z} \times \mathbb{Z}$, mais les idéaux $2\mathbb{Z} \times \{0\}$ et $\{0\} \times \{0\}$ ne sont pas premiers.

**Théorème 1.3.13.** *Si $R$ est un anneau commutatif, un idéal $P \neq R$ est premier si et seulement si $R/P$ est un anneau intègre.*

*Démonstration.* Supposons que $P$ soit premier et que $(a+P)(b+P) = ab+P = 0+P$ dans $R/P$. Alors $ab \in P$ et donc $a \in P$ ou $b \in P$. Ainsi $a+P = 0+P$ ou $b+P = 0+P$. Donc $R/P$ est un anneau intègre.

Maintenant supposons que $R/P$ soit un anneau intègre et $ab \in P$. Alors $(a+P)(b+P) = ab+P = 0+P$ et donc soit $a+P = 0+P$ soit $b+P = 0+P$. Ainsi $a \in P$ ou $b \in P$. □

*Exemples* 1.3.14. (a) $(\mathbb{Z}\times\mathbb{Z})/(\mathbb{Z}\times\{0\}) \cong \mathbb{Z}$. L'idéal $\mathbb{Z}\times\{0\}$ est premier et $\mathbb{Z}$ est un anneau intègre.

(b) $\mathbb{Z}_n$ est un anneau intègre si et seulement si $n$ est premier (voir l'exercice 1.3.5).

(c) Puisque, pour tout anneau $R$, nous avons $R/\{0\} \cong R$, l'anneau $R$ est un anneau intègre si et seulement si son idéal nul est premier.

**Théorème 1.3.15.** *Soit $I$ un idéal d'un anneau $R$. Alors il existe une bijection, qui préserve les inclusions, entre l'ensemble des idéaux de $R/I$ et l'ensemble des idéaux de $R$ qui contiennent $I$.*

*Démonstration.* Nous divisons la preuve en trois étapes.

(a) Premièrement, nous montrons que si $\tilde{A}$ est un idéal de $R/I$, alors

$$A := \{b \in R : b + I \in \tilde{A}\}$$

est un idéal de $R$ qui contienne $I$, et $\tilde{A} = A/I$. Puisque $0 + I \in \tilde{A}$, nous avons $0 \in A$. Si $a, b \in A$, alors $a + I \in \tilde{A}$ et $b + I \in \tilde{A}$. Puisque $\tilde{A}$ est un sous-groupe additive de $R/A$, nous avons $(a-b)+I = (a+I)-(b+I) \in \tilde{A}$. D'où $a - b \in A$. Ainsi $A$ est un sous-groupe additive de $R$.

Maintenant, si $a \in A$ et $r \in R$, alors

$$\begin{aligned} a + I \in \tilde{A} \text{ e } r + I \in R/I &\implies ra + I = (r + I)(a + I) \in \tilde{A} \quad \text{(puisque } \tilde{A} \text{ est un idéal de } R/I) \\ &\implies ra \in A \quad \text{(par la définition de } A). \end{aligned}$$

De même, on peut montrer que $ar \in A$. Ainsi $A$ est fermé sous la multiplication par des éléments de $R$ and donc $A$ est un idéal de $R$.

Pour voir que $I \subseteq A$, notez que

$$a \in I \implies a + I = 0 + I \in \tilde{A} \implies a \in A \quad \text{(par la définition de } A).$$

Il reste à montrer que $\tilde{A} = A/I$. Puisque

$$r + I \in \tilde{A} \implies r \in A \implies r + I \in A/I,$$

nous avons $\tilde{A} \subseteq A/I$. Pour démontrer l'inclusion inverse, supposons que $x \in A/I$. Alors il existe un élément $a \in A \subseteq R$ tel que $x = a + I$. Cela implique que $x = a + I \in \tilde{A}$ par la définition de $A$.

(b) Ensuite, nous montrons que si $A$ est un idéal de $R$ contenant $I$ alors $\tilde{A} := \{a + I : a \in A\}$ est un idéal de $R/I$ et $\tilde{A} = A/I := \{a + I : a \in A\}$ (ce qui est clairement vrai). Puisque $0 \in I$, nous avons $0 + I \in \tilde{A}$.

Supposons que $x_1, x_2 \in \tilde{A}$. Alors il existe $a_1, a_2 \in A$ tels que $x_1 = a_1 + I$ et $x_2 = a_2 + I$. Puisque $A$ est un idéal de $R$, on a $a_1 - a_2 \in A$. Puis $x_1 - x_2 = (a_1 + I) - (a_2 + I) = (a_1 - a_2) + I \in \tilde{A}$. Ainsi $\tilde{A}$ est un sous-group additive de $R/I$.

Maintenant supposons que $x \in \tilde{A}$ et $r + I \in R/I$. Alors il existe $a \in A$ tel que $x = a + I$. Puisque $A$ est un idéal de $R$, on a $ra \in I$. Ainsi $(r + I)x = (r + I)(a + I) = ra + I \in \tilde{A}$. La preuve que $(a + I)(r + I) \in \tilde{A}$ est similaire. Donc $\tilde{A}$ est un idéal de $R/I$.

(c) Finalement, nous montrons que si $A_1$ et $A_2$ sont des idéaux de $R$ contenant $I$, alors $A_1 \subseteq A_2$ si et seulement si $A_1/I \subseteq A_2/I$. Le fait que $A_1 \subseteq A_2 \implies A_1/I \subseteq A_2/I$ est claire. On montre l'inclusion inverse. Supposons que $A_1/I \subseteq A_2/I$. Alors

$$\begin{aligned} a_1 \in A_1 &\implies a_1 + I \in A_1/I \\ &\implies \exists\ a_2 \in A_2 \text{ tel que } a_1 + I = a_2 + I \\ &\implies a_1 - a_2 \in I \\ &\implies \exists\ a \in I \text{ tel que } a_1 = a_2 + a \\ &\implies a_1 \in A_2 \text{ (puisque } a_2 + a \in A_2 + I \subseteq A_2 \text{ parce que } I \subseteq A_2) \end{aligned}$$

□

**Théorème 1.3.16.** *Un anneau commutatif est simple si et seulement s'il est un corps.*

*Démonstration.* Puisqu'un corps est un corps gauche commutatif par définition, l'implication inverse découle de l'exemple 1.3.9. Il suffit donc de prouver l'implication directe. Supposons que $R$ soit un anneau commutatif simple et soit $a \in R \setminus \{0\}$. Alors $aR \neq \{0\}$ est un idéal et donc $aR = R$. Ainsi il existe $b \in R$ tel que $ab = 1$. □

**Définition 1.3.17** (Idéal maximal)**.** Un idéal $I$ d'un anneau $R$ est *maximal* si $I \neq R$ et il n'existe aucun idéal $J$ tel que $I \subsetneq J \subsetneq R$.

**Théorème 1.3.18.** *Soit $R$ un anneau et soit $I$ un idéal de $R$. Alors $R/I$ est simple si et seulement si $I$ est un idéal maximal.*

*Démonstration.* Supposons que $R/I$ soit simple et $A$ est un idéal de $R$ avec $I \subseteq A \subseteq R$. D'après le théorème 1.3.15, $A/I$ est un idéal de $R/I$ et $I/I \subseteq A/I \subseteq R/I$. Puisque $R/I$ est simple, on a $A/I = R/I$ ou $A/I = I/I$, ce qui implique que $A = R$ ou $A = I$.

Maintenant supposons que $I$ soit maximal et, vers une contradcition, que $R/I$ n'est pas simple. Puis $R/I$ a un idéal propre non nul de la forme $A/I$. Ainsi $I/I \subsetneq A/I \subsetneq R/I$. Alors, d'après le théorème 1.3.15, $A$ est un idéal de $R$ et $I \subsetneq A \subsetneq R$, ce qui est une contradiction. □

**Corollaire 1.3.19.** *Un idéal $I$ d'un anneau commutatif $R$ est maximal si et seulement si $R/I$ est un corps.*

*Démonstration.* Cela découle des théorèmes 1.3.16 et 1.3.18. □

**Corollaire 1.3.20.** *Tout idéal maximal d'un anneau commutatif est un idéal premier.*

*Démonstration.* Supposons $I$ soit un idéal maximal d'un anneau commutatif $R$. Alors, d'après le corollaire 1.3.19, le quotient $R/I$ est un corps. Ainsi $R/I$ est un anneau intègre et donc $I$ est premier d'après le théorème 1.3.13. □

*Exemple* 1.3.21. L'idéal $\{0\}$ de $\mathbb{Z}$ est premier mais pas maximal. De même, $\{0\} \times \mathbb{Z}$ est un idéal de $\mathbb{Z} \times \mathbb{Z}$ qui est premier mais pas maximal.

*Exemple* 1.3.22. D'après le théorème 1.3.15, pour tout idéal $I$ de $\mathbb{Z}/n\mathbb{Z}$, il existe un idéal $A$ de $\mathbb{Z}$ avec $n\mathbb{Z} \subseteq A$ tel que $I = A/n\mathbb{Z}$. D'après la proposition 1.3.6, il existe $m \in \mathbb{Z}$ tel que $A = m\mathbb{Z}$. Puisque $n\mathbb{Z} \subseteq m\mathbb{Z}$ si et seulement si $m|n$, les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont $m\mathbb{Z}/n\mathbb{Z}$ pour $m|n$.

À titre d'exemple explicite, considérons $n = 6$. La correspondance bijective du théorème 1.3.15 est donnée explicitement par :

| Idéal de $\mathbb{Z}/6\mathbb{Z}$ | Idéal de $\mathbb{Z}$ |
|---|---|
| $\mathbb{Z}/6\mathbb{Z} = \langle\bar{1}\rangle$ | $\mathbb{Z}$ |
| $\{\bar{0}, \bar{2}, \bar{4}\} = \langle\bar{2}\rangle$ | $2\mathbb{Z}$ |
| $\{\bar{0}, \bar{3}\} = \langle\bar{3}\rangle$ | $3\mathbb{Z}$ |
| $\{\bar{0}\} = \langle\bar{0}\rangle = \langle\bar{6}\rangle$ | $6\mathbb{Z}$ |

*Exemple* 1.3.23. Nous aborderons les anneaux des polynômes en détail au chapitre 2. Cependant, nous donnons ici un exemple les impliquant. Considérer

$$R = \mathbb{Z}[x] = \{a_0 + a_1x + \cdots + a_kx^k : k \in \mathbb{N},\ a_0, \ldots, a_k \in \mathbb{Z}\},$$
$$I = \{4a_0 + a_1x + a_2x^2 + \cdots + a_kx^k : k \in \mathbb{N},\ a_0, \ldots, a_k \in \mathbb{Z}\}.$$

Puis

$$R/I = \{0 + I, 1 + I, 2 + I, 3 + I\} \cong \mathbb{Z}_4.$$

Et, par exemple, l'idéal $\langle \bar{2} \rangle \subseteq \mathbb{Z}_4$ correspond à l'idéal

$$J = \{2a_0 + a_1x + \cdots + a_kx^k : k \in \mathbb{N},\ a_0, \ldots, a_k \in \mathbb{Z}\}.$$

*Remarque* 1.3.24. On a vu (le théorème 1.3.16) que si un anneau commutatif est simple, alors c'est un corps. Pour les anneaux non commutatifs, cette situation est plus compliquée. Il existe des anneaux simples qui ne sont pas des corps gauches. Par exemple, si $F$ est un corps, alors $\mathrm{Mat}_n(F)$ est un anneau simple qui n'est pas un corps gauche. Cela découle du résultat suivant.

**Théorème 1.3.25.** *Si $R$ est un anneau et $n \in \mathbb{N}_+$, alors tout idéal de $\mathrm{Mat}_n(R)$ et de la forme $\mathrm{Mat}_n(I)$ où $I$ est un idéal de $R$.*

Nous ne prouverons pas le théorème ci-dessus (et nous ne l'utiliserons pas non plus). La preuve peut être trouvée, par exemple, dans [Nic12, Lem. 3.3.3].

---

## Exercices.

1.3.1. Compléter la preuve du théorème 1.3.3.

1.3.2. Démontrer la proposition 1.3.4.

1.3.3 ([Nic12, Ex. 3.3.1]). Pour chacun des éléments suivants, décider si $A$ est un idéal de l'anneau $R$. Justifier votre réponse.

(a) $R = \mathbb{C}$, $A = \mathbb{Z}$.
(b) $R = \mathbb{Z} \times \mathbb{Z}$, $A = \{(k, k) : k \in \mathbb{Z}\}$.
(c) $R = \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{R} \end{bmatrix}$, $A = \begin{bmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{R} \end{bmatrix}$.
(d) $R = \begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix}$, $A = \begin{bmatrix} \mathbb{Z} & 2\mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix}$.
(e) $R = \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{R} \end{bmatrix}$, $A = \begin{bmatrix} \mathbb{Z} & \mathbb{R} \\ 0 & \mathbb{Z} \end{bmatrix}$.
(f) $R = \mathbb{Z}(i)$, $A = \{n + ni : n \in \mathbb{Z}\}$.

1.3.4 ([Nic12, Ex. 3.3.2]). Supposons que $S$ soit un anneau. Si $R = \begin{bmatrix} S & S \\ 0 & S \end{bmatrix}$ et $A = \begin{bmatrix} 0 & S \\ 0 & 0 \end{bmatrix}$, montrer que $A$ est un idéal de $R$ et décrire les éléments de $R/A$.

1.3.5. Montrer que $n\mathbb{Z}$, $n \in \mathbb{N}$, est un idéal premier de $\mathbb{Z}$ si et seulement si $n$ est soit zéro soit un nombre premier.

1.3.6. Supposons que $R$ soit un anneau et que $m \in \mathbb{Z}$. Montrer que $mR = \{mr : R \in R\}$ et $A_m = \{r \in R : mr = 0\}$ sont des idéaux de $R$.

1.3.7. Démontrer que les idéaux maximaux de $\mathbb{Z}$ sont précisément les idéaux $p\mathbb{Z}$ où $p$ est un nombre premier.

1.3.8 ([Nic12, Ex. 3.3.5]). Supposons que $R$ et $S$ soient des anneaux.

(a) Si $A$ est un idéal de $R$ et $B$ est un idéal de $S$, montrer que $A \times B$ est un idéal de $R \times S$.
(b) Montrer que pour tout idéal $\mathcal{A}$ de $R \times S$, il existe un idéal $A$ de $R$ et un idéal $B$ de $S$ tels que $\mathcal{A} = A \times B$. *Indice* : $A = \{a \in R : (a, 0) \in \mathcal{A}\}$.
(c) Montrer le les idéaux maximaux de $R \times S$ sont soit de la forme $A \times S$, où $A$ est un idéal maximal de $R$, soit de la forme $R \times B$, où $B$ est un idéal maximal de $S$.

1.3.9 ([Nic12, Ex. 3.3.6]). Si $A$ est un idéal de $R$, montrer que $\mathrm{Mat}_2(A)$ est un idéal de $\mathrm{Mat}_2(R)$.

1.3.10 ([Nic12, Ex. 3.3.8]). Si $A$ et $B$ sont des idéaux de l'anneau $R$ tels que $A \cap B = 0$, montrer que $ab = 0 = ba$ pour tous $a \in A$ et $b \in B$.

1.3.11 ([Nic12, Ex. 3.3.9]). Soit $R = \mathbb{Z}(i)$ l'anneau des entiers de Gauss. Pour chacun des suivants, trouver le nombre d'éléments dans l'anneau quotient $R/A$ et décrire ces éléments :

(a) $A = Ri$
(b) $A = R(1 - i)$
(c) $A = R(1 + 2i)$
(d) $A = R(1 + 3i)$

*Indice* : $(1 + 2i)(1 - i) = 3 + i$ et $(1 + 3i)(1 - 3i) = 10$.

1.3.12 ([Nic12, Ex. 3.3.10]). Si $R$ est un anneau simple, montrer que $Z(R)$ est un corps. Montrer que l'implication réciproque n'est pas vraie en considérant $R = \begin{bmatrix} F & F \\ 0 & F \end{bmatrix}$ où $F$ est un corps.

1.3.13 ([Nic12, Ex. 3.3.12]). Si $X \subseteq R$ est un sous-ensemble non vide d'un anneau commutatif $R$, définir l'*annulateur* de $X$ par $\mathrm{ann}(X) = \{a \in R : ax = 0 \text{ pour tout } x \in X\}$.

(a) Montrer que $\mathrm{ann}(X)$ est un idéal de $R$.
(b) Si $X \subseteq Y$, montrer que $\mathrm{ann}(Y) \subseteq \mathrm{ann}(X)$.
(c) Montrer que $\mathrm{ann}(X \cup Y) = \mathrm{ann}(X) \cap \mathrm{ann}(Y)$.
(d) Montrer que $X \subseteq \mathrm{ann}\big(\mathrm{ann}(X)\big)$.
(e) Montrer que $\mathrm{ann}(X) = \mathrm{ann}\Big(\mathrm{ann}\big(\mathrm{ann}(X)\big)\Big)$.

1.3.14 ([Nic12, Ex. 3.3.13]). Donner un exemple d'un anneau $R$ et un idéal $A$ tels que $R/A$ est commutatif, mais $R$ ne l'est pas.

1.3.15 ([Nic12, Ex. 3.3.14]). Si $X$ et $Y$ sont des sous-groupes additives de $R$, définir $X+Y = \{x+y : x \in X,\ y \in Y\}$.

(a) Montrer que $X+Y$ est un sous-groupe additive de $R$ qui contient $X$ et $Y$.
(b) Si $A$ et $B$ sont des idéaux de $R$, montrer que $A+B$ est un idéal de $R$.
(c) Si $A$ est un idéal de $R$ et $S$ est un sous-anneau de $R$, montrer que $A+S$ est un sous-anneau de $R$.

1.3.16 ([Nic12, Ex. 3.3.15]). Si $A$ est un idéal de $R$, montrer que $A \cap S$ est un idéal de $S$ pour tout sous-anneau $S$ de $R$.

1.3.17 ([Nic12, Ex. 3.3.16]). Si $A$ est un idéal de $R$, montrer que $R/A$ est commutatif si et seulement si $rs - sr \in A$ pour tous $r, s \in R$.

1.3.18 ([Nic12, Ex. 3.3.17]). Soit $Z = Z(R)$ le centre de l'anneau $R$.

(a) Quand $Z$ est-il un idéal de $R$ ? Justifier votre réponse.
(b) Si $R$ est simple, montrer que $Z$ est un corps.
(c) Si $R/Z$ est un groupe cyclique, montrer que $R$ est commutatif.

1.3.19 ([Nic12, Ex. 3.3.24]). Un sous-groupe additif $L$ de $R$ est appelé une *idéal à gauche* si $Ra \subseteq L$ pour tout $a \in L$. Montrer que $R$ est un corps gauche si et seulement si 0 et $R$ sont les seuls idéaux à gauche de $R$ (prolongement du théorème 1.3.16). *Indice* : $Ra$ est un idéal à gauche pour chaque $a \in R$.

1.3.20 ([Nic12, Ex. 3.3.25]). Soit $R$ un anneau commutatif. Écrire $a|b$ s'il existe $r \in R$ tel que $b = ra$.

(a) Montrer que $Rab \subseteq Ra \cap Rb$ pour tous $a, b \in R$.
(b) Si $Ra + Rb = R$ (voir l'exercice 1.3.15), montrer que $Rab = Ra \cap Rb$.
(c) Montrer que $u \in R$ est une unité si et seulement si $Ru = R$.
(d) Supposons que $p \in R$ et $Rp \neq R$. Montrer que $Rp$ est un idéal premier si et seulement si $p|ab$ implique $p|a$ ou $p|b$.
(e) Si $R$ est un anneau intègre, montrer que $Ra = Rb$ si est seulement s'il existe une unité $u \in R$ tel que $a = ub$.

1.3.21 ([Nic12, Ex. 3.3.26]). Soient $A$, $B$, et $C$ des idéaux de $R$ et définir

$$AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_i \in A,\ b_i \in B,\ n \geq 1\}.$$

(a) Montrer que $AB$ est un idéal de $R$ et que $AB \subseteq A \cap B$.
(b) Montrer que $A(B+C) = AB + AC$ et $(B+C)A = BA + CA$. (Voir l'exercice 1.3.15.)
(c) Montrer que $AR = A = RA$.
(d) Montrer que $A(BC) = (AB)C$.

1.3.22 ([Nic12, Ex. 3.3.27]). Si $a \in R$, soit

$$RaR = \{r_1as_1 + r_2as_2 + \cdots + r_nas_n : r_i, s_i \in R,\ n \geq 1\}.$$

Montrer que $RaR$ est un idéal de $R$ qui contient $a$ et qu'il est contenu dans tout tel idéal.

1.3.23. Soit $R$ un anneau commutatif. L'anneau $R$ est dit *noethérien* s'il remplit la *condition de chaîne ascendante* sur des idéaux : pour toute chaîne ascendante $I_1 \subseteq I_2 \subseteq \cdots$ d'idéaux dans $R$, il existe un entier positif $N$ tel que $I_n = I_N$ pour tout $n \geq N$. Un idéal $I$ de $R$ est de *type fini* s'il existe des éléments $a_1, \ldots, a_m \in I$ (appelés *générateurs* de $I$) tels que pour tout élément $b \in I$ il existe $r_1, \ldots, r_m \in R$ tels que $b = a_1r_1 + \cdots + a_mr_m$. Démontrer que $R$ est noethérien si et seulement si tout idéal de $R$ est de type fini.

1.3.24 (Exercice de bonus). Démontrer que tout anneau non nul possède un idéal maximal.

## 1.4 Morphismes d'anneaux

Nous discutons maintenant des fonctions naturelles entre les anneaux, aussi que certaines de leurs propriétés.

**Définition 1.4.1** (Morphisme d'anneaux)**.** Soient $R$ et $S$ des anneaux. Une application $f\colon R \to S$ est appelée un *morphisme d'anneaux* (ou *homomorphisme d'anneaux*) si elle remplit les conditions suivantes :

**(RH1)** $f(1_R) = 1_S$.
**(RH2)** $f(a+b) = f(a) + f(b)$ pour tous $a, b \in R$.
**(RH3)** $f(ab) = f(a)f(b)$ pour tous $a, b \in R$.

*Exemples* 1.4.2. (a) $f\colon \mathbb{Z} \to \mathbb{Q}$, $f(x) = x$ est un morphisme d'anneaux.
(b) $f\colon \mathbb{Z} \to \mathbb{Z}_n$, $f(x) = \bar{x}$ est un morphisme d'anneaux.
(c) $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f(x, y) = x$ est un morphisme d'anneaux.
(d) $f\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$, $f(x, y) = x+y$ n'est *pas* un morphisme d'anneaux puisque, par exemple,

$$f((1,1)(1,2)) = f(1,2) = 1 + 2 = 3 \text{ mais } f(1,1)f(1,2) = (1+1)(1+2) = 6.$$

*Remarque* 1.4.3. Si $f\colon R \to S$ est un morphisme d'anneaux, alors $f$ est un morphisme de groupes additives :

$$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R) \implies f(0_R) = 0_S,$$
$$f(a) + f(-a) = f(a + (-a)) = f(0_R) = 0_S \implies f(-a) = -f(a).$$

Ici on a seulement utilisé l'axiome (RH2).

Les axiomes (RH2) et (RH3) ne suffisent pas pour conclure que $f(1_R) = 1_S$ comme le montre l'exemple suivant.

*Exemple* 1.4.4. L'application $f\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $f(x) = (x, 0)$ remplit (RH2) et (RH3), mais il ne remplit pas (RH1). Certaines sources utilisent le terme *morphisme d'anneaux généraux* pour les application qui remplissent (RH2) et (RH3) mais pas nécessairement (RH1).

**Proposition 1.4.5.** *Soit $f\colon R \to S$ un morphisme d'anneaux. Alors les déclarations suivantes sont vraies.*

*(a) Pour tous $m \in \mathbb{Z}$ et $r \in R$, on a $f(mr) = mf(r)$.*
*(b) Pour tous $m \in \mathbb{N}$ et $r \in R$, on a $f(r^m) = f(r)^m$.*
*(c) Si $u \in R^\times$, alors $f(u) \in S^\times$ et, pour tout $m \in \mathbb{Z}$, on a $f(u^m) = f(u)^m$. En particulier, $f(u^{-1}) = f(u)^{-1}$.*

*Démonstration.* La preuve de cette proposition est l'exercice 1.4.1. □

*Exemple* 1.4.6. On va montrer que l'équation $m^3 - 6n^3 = 3$ n'a aucune solution pour $m, n \in \mathbb{Z}$. Considérez l'application $f\colon \mathbb{Z} \to \mathbb{Z}_7$ donnée par $f(x) = \bar{x}$. Si $m^3 - 6n^3 = 3$, alors $f(m)^3 + f(n)^3 = \bar{3}$ dans $\mathbb{Z}_7$. Mais, en considérant explicitement toutes les valeurs possibles, on peut voir que, pour $a \in \mathbb{Z}_7$, on a $a^3 \in \{\bar{0}, \bar{1}, \bar{6}\}$. On calcule

$$\bar{0} + \bar{0} = \bar{0},\ \bar{0} + \bar{1} = \bar{1},\ \bar{0} + \bar{6} = \bar{6},\ \bar{1} + \bar{1} = \bar{2}, \bar{1} + \bar{6} = \bar{0},\ \bar{6} + \bar{6} = \bar{5}.$$

Ainsi, l'équation $\bar{m}^3 - 6\bar{n}^3 = \bar{3}$ n'a aucune solution dans $\mathbb{Z}_7$. Il s'ensuit que $m^3 - 6n^3 = 3$ ne peut pas avoir des solutions dans $\mathbb{Z}$.

*Exemple* 1.4.7 (Endomorphisme de Frobenius). Soit $R$ un anneau commutatif, et $p = \operatorname{car}(R)$ un nombre premier. Alors l'application

$$f\colon R \to R, \quad f(r) = r^p,$$

est un morphisme d'anneaux, appelé l'*endomorphisme de Frobenius*. Voir l'exercice 1.4.3.

**Définition 1.4.8** (Noyau, image)**.** Soit $f\colon R \to S$ un morphisme d'anneaux. Le *noyau* de $f$ est $\ker f := \{x \in R : f(x) = 0\}$ et l'*image* de $f$ est $\operatorname{im} f = f(R) := \{f(r) : r \in R\}$.

*Remarque* 1.4.9. Un morphisme d'anneaux $f$ est injective si est seulement si $\ker f = \{0\}$. Cela découle du fait correspondant concernant les morphismes de groupe puisque $f$ est un morphisms de groupes additifs. Par définition, $f$ est surjective si est seulement si $f(R) = S$.

**Définition 1.4.10** (Monomorphisme, épimorphisme, isomorphism, automorphisme)**.** Un morphisme d'anneaux injectif est appelé un *monomorphisme*. Un morphisme d'anneaux surjectif est appelé un *épimorphisme*. Un morphisme d'anneaux qui est à la fois un monomorphisme et un épimorphisme est appelé un *isomorphisme*. S'il existe un isomorphisme d'un anneau $R$ vers un anneau $S$ alors on dit que $R$ et $S$ sont *isomorphes* et on écrit $R \cong S$. (Notez que cette définition est en accord avec la définition 1.1.29.) Un homomorphisme (resp. isomorphisme) d'un anneau à lui-même est appelé un *endomorphisme* (resp. *automorphisme*).

*Exemple* 1.4.11. L'application $\sigma\colon \mathbb{C} \to \mathbb{C}$ donnée par $\sigma(z) = \bar{z}$ est un automorphisme de $\mathbb{C}$.

*Exemple* 1.4.12 (Automorphisme intérieur). Si $R$ est un anneau et $u \in R^\times$, alors

$$\sigma_u\colon R \to R, \quad \sigma_u(r) = uru^{-1},\ r \in R,$$

est un automorphisme de $R$ appelé un *automorphisme intérieur*. La démonstration de ce fait est l'exercice 1.4.4. Voir aussi l'exemple 1.1.31.

**Théorème 1.4.13.** *Soit $f\colon R \to S$ un morphisme d'anneaux. Alors :*

*(a) $f(R)$ est un sous-anneau de $S$.*

*(b) $\ker f$ est un idéal de $R$.*

*Démonstration.* (a) Puisque $f(1_R) = 1_S$, on a $1_S \in f(R)$. Puisque $f(0_R) = 0_S$, on a $0_S \in f(R)$. Maintenant supposons que $r, s \in f(R)$. Alors il existe $s', t' \in R$ tels que $f(s') = s$ et $f(t') = t$. Donc

$$\begin{aligned} -s = -f(s') = f(-s') \in f(R), \\ s + t = f(s') + f(t') = f(s' + t') \in f(R), \\ st = f(s')f(t') = f(s't') \in f(R). \end{aligned}$$

(b) Nous savons (de MAT 2543) que $\ker f$ est un sous-groupe additive de $R$ (puisque $f$ est un morphisme de groupes additives). Maintenant,

$$r \in R,\ x \in \ker f \implies f(rx) = f(r)f(x) = f(r)0_S = 0_S \implies rx \in \ker f.$$

De même, on peut montrer que $r \in R, x \in \ker f$ impliquent $xr \in \ker f$. Ainsi $\ker f$ est un idéal de $R$.

□

*Exemple* 1.4.14. Si $I$ est un idéal de $R$, alors $f\colon R \to R/I$, $f(x) = x + I$, est un épimorphisme d'anneaux et $\ker f = I$.

**Théorème 1.4.15** (Premier théorème d'isomorphisme)**.** *Soit $f\colon R \to S$ un morphisme d'anneaux. Alors l'application*

$$\bar{f}\colon R/(\ker f) \to \operatorname{im} f, \quad \bar{f}(r + \ker f) = f(r)$$

*est un isomorphisme d'anneaux. En particulier, $R/(\ker f) \cong \operatorname{im} f$.*

*Démonstration.* Soit $I = \ker f$. Alors $\bar{f}$ est bien définie puisque

$$\begin{aligned} r + I = s + I \iff r - s \in I \iff f(r - s) = 0 \iff f(r) - f(s) = 0 \\ \iff f(r) = f(s) \iff \bar{f}(r + I) = \bar{f}(s + I). \end{aligned}$$

Les implications inverses ci-dessus montrent que $\bar{f}$ est injective. Il est clair que $f$ est surjectif et il est simple à vérifier que $f$ est un morphisme d'anneaux. □

*Remarque* 1.4.16. Le théorème 1.4.15 est appelé le *premier* théorème d'isomorphisme puisqu'il existe aussi les deuxième et troisième théorèmes d'isomorphisme (voir les exercices 1.4.25 et 1.4.25).

*Exemples* 1.4.17. (a) Considérer $f\colon \mathbb{Z} \to \mathbb{Z}_n$, $f(x) = \bar{x}$. Alors $\ker f = n\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

(b) Considérer $f\colon \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_2$, $f(x) = (\bar{x}, \bar{x})$. Alors $f(\mathbb{Z}) = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\} \cong \mathbb{Z}_2$ et $\ker f = 2\mathbb{Z}$. Ainsi $\mathbb{Z}/2\mathbb{Z} \cong f(\mathbb{Z}) \cong \mathbb{Z}_2$.

(c) Considérer $f\colon \mathbb{Z}_4 \to \mathbb{Z}_{10}$, $f(x) = 5x$. Alors $\ker f = \{\bar{0}, \bar{2}\} \subseteq \mathbb{Z}_4$ et $\operatorname{im} f = \{\bar{0}, \bar{5}\} \subseteq \mathbb{Z}_{10}$. On a $\operatorname{im} f \cong \mathbb{Z}_2$ et donc $\mathbb{Z}_4/(\ker f) \cong \mathbb{Z}_2$. (Notez ici que $f$ n'est pas en fait un morphisme d'anneaux, car il n'envoie pas l'élément neutre à l'élément neutre, mais c'est un morphisme d'anneaux généraux.)

*Exemple* 1.4.18. Soient $m$ et $n$ est entiers positifs et soit $I = n\mathbb{Z}_{mn} = \{n\bar{a} : \bar{a} \in \mathbb{Z}_{mn}\}$. Alors l'application $f\colon \mathbb{Z}_{mn} \to \mathbb{Z}_n$, $f(\bar{x}) = \bar{x}$, est un morphisme d'anneaux avec $\operatorname{im} f = \mathbb{Z}_n$ et $\ker f = I$. Ainsi $\mathbb{Z}_{mn}/I \cong \mathbb{Z}_n$.

*Remarque* 1.4.19. Si $I$ et $J$ sont des idéaux d'un anneau $R$, alors

$$I \cap J,$$
$$IJ := \{r \in R : r = a_1b_1 + \cdots + a_kb_k,\ a_1, \ldots, a_k \in I,\ b_1, \ldots, b_k \in J\}, \quad \text{et}$$
$$I + J := \{r \in R : r = a + b,\ a \in I,\ b \in J\}$$

sont aussi des idéaux de $R$. Voir les exercices 1.3.15(b) et 1.3.21(a).

**Théorème 1.4.20.** *Si $R$ est un anneau, alors $\mathbb{Z}1_R = \{k1_R : k \in \mathbb{Z}\}$ est un sous-anneau de $R$ qui est contenu dans le centre de $R$. De plus, les affirmations suivantes sont vraies.*

*(a) Si $n = \operatorname{car}(R) > 0$, alors $\mathbb{Z}1_R \cong \mathbb{Z}_n$.*
*(b) Si $\operatorname{car}(R) = 0$, alors $\mathbb{Z}1_R \cong \mathbb{Z}$.*

*Démonstration.* Définissons une application

$$\theta\colon \mathbb{Z} \to R, \quad \theta(k) = k1_R \text{ pour tout } k \in \mathbb{Z}.$$

D'après la proposition 1.4.5, $\theta$ est un morphisme d'anneaux. Donc $\mathbb{Z}1_R = \theta(\mathbb{Z})$ est un sous-anneau de $R$ d'après le théorème 1.4.13. De plus, on peut vérifier (exercice 1.4.11), que $\mathbb{Z}1_R$ est contenu dans le centre de $R$.

On a $\ker\theta = \{k \in \mathbb{Z} : k1_R = 0\}$. Si $n = \operatorname{car}(R) > 0$, alors $\ker\theta = n\mathbb{Z}$ d'après le lemme 1.1.19. Ainsi $\mathbb{Z}1_R = \theta(\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ d'après le premier théorème d'isomorphisme (théorème 1.4.15). Si $\operatorname{car}(R) = 0$, alors $\ker\theta = \{0\}$ et le résultat s'ensuit du premier théorème d'isomorphisme. □

**Lemme 1.4.21.** *Si $R$ et $S$ sont des anneaux et $I \subseteq R$ et $J \subseteq S$ sont des idéaux, alors $I \times J$ est un idéal de $R \times S$ et on a $(R \times S)/(I \times J) \cong (R/I) \times (S/J)$.*

*Démonstration.* L'application $f\colon R \times S \to (R/I) \times (S/J)$ donnée par $f(r, s) = (r + I, s + J)$ est un morphisme d'anneaux où $\ker f = I \times J$ et $\operatorname{im} f = (R/I) \times (S/J)$ (exercice). Donc le résultat s'ensuit de premier théorème d'isomorphisme (le théorème 1.4.15). □

**Lemme 1.4.22.** *Soient $R$ et $S$ des anneaux. Alors tout idéal de $R \times S$ est sous la forme $A \times B$ où $A \subseteq R$ et $B \subseteq S$ sont des idéaux.*

*Démonstration.* Soit $I \subseteq R \times S$ un idéal. Soit

$$A = \{r \in R : (r, 0) \in I\}, \quad B = \{s \in S : (0, s) \in I\}.$$

Il est simple (exercice) à montrer que $A$ est un idéal de $R$ et que $B$ est un idéal de $S$. Si $(r,s) \in I$, alors $(r,0) = (r,s)(1,0) \in I$ et $(0,s) = (r,s)(0,1) \in I$. Ainsi $r \in A$ et $s \in B$. Donc $I \subseteq A \times B$. Maintenant, supposons que $(a,b) \in A \times B$. Alors, d'après les définitions de $A$ et $B$, on a $(a,0) \in I$ et $(0,b) \in I$. Ainsi $(a,b) = (a,0) + (0,b) \in I$ (puisque $I$ est fermé sous addition). Donc $A \times B \subseteq I$, d'où $I = A \times B$. □

**Théorème 1.4.23** (Théorème des restes chinois)**.** *Soit $R$ un anneau et soient $A, B$ deux idéaux tels que $A + B = R$. Alors $R/(A \cap B) \cong (R/A) \times (R/B)$.*

*Démonstration.* Considérons l'application

$$f\colon R \to (R/A) \times (R/B), \quad f(r) = (r + A, r + B).$$

Pour $r, s \in R$, on a

$$f(1) = (1 + A, 1 + B) = 1_{(R/A)\times(R/B)},$$
$$f(r + s) = (r + s + A, r + s + B) = (r + A, r + B) + (s + A, s + B) = f(r) + f(s)$$

et

$$f(rs) = (rs + A, rs + B) = ((r + A)(s + A), (r + B)(s + B))$$
$$= (r + A, r + B)(s + A, s + B) = f(r)f(s).$$

Donc $f$ est un morphisme d'anneaux.

On montre ensuite que $f$ est surjectif. Puisque $R = A + B$, il existe $a \in A$ et $b \in B$ tels que $1 = a + b$. Maintenant choisissons $r_1, r_2 \in R$ et définissons $r = r_1 b + r_2 a$. Alors

$$r_1 - r = r_1 - (r_1 b + r_2 a) = r_1(1 - b) - r_2 a = r_1 a - r_2 a \in A \implies r_1 + A = r + A,$$
$$r_2 - r = r_2 - (r_1 b + r_2 a) = r_2(1 - a) - r_1 b = r_2 b - r_1 b \in B \implies r_2 + B = r + B.$$

Ainsi $f(r) = (r + A, r + B) = (r_1 + A, r_2 + B)$. Puisque $r_1, r_2 \in R$ étaient des éléments quelconques, cela implique que $f$ est surjective.

Finalement,

$$f(r) = (0 + A, 0 + B) \iff (r + A = 0 + A \text{ et } r + B = 0 + B)$$
$$\iff (r \in A \text{ et } r \in B) \iff r \in A \cap B.$$

Donc $\ker f = A \cap B$. Le résultat découle alors du premier théorème d'isomorphisme (le théorème 1.4.15). □

*Exemple* 1.4.24. Puisque $\operatorname{pgcd}(5,6) = 1$, on a $5\mathbb{Z} + 6\mathbb{Z} = \mathbb{Z}$. On a aussi $5\mathbb{Z} \cap 6\mathbb{Z} = 30\mathbb{Z}$. Ainsi, d'après le théorème des restes chinois (le théorème 1.4.23), on a $\mathbb{Z}_{30} \cong \mathbb{Z}_5 \times \mathbb{Z}_6$.

Plus généralement, on a le résultat suivant.

**Lemme 1.4.25.** *Si* $\operatorname{pgcd}(m,n) = 1$*, alors* $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

*Démonstration.* Puisque $\operatorname{pgcd}(m,n) = 1$, il existe $a, b \in \mathbb{Z}$ tels que $ma + nb = 1$. Ainsi $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. De plus, on a $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$ puisque si $m|x$ et $n|x$, alors $mn|x$ (puisque $m$ et $n$ sont premiers entre eux). Donc le résultat découle du théorème des restes chinois (le théorème 1.4.23). □

*Exemple* 1.4.26. Combiens d'unités $\mathbb{Z}_{345}$ a-t-il ? Puisque $345 = 3 \cdot 5 \cdot 23$, on a $\mathbb{Z}_{345} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{23}$ d'après le lemme 1.4.25. Ainsi $\mathbb{Z}_{345}$ a $2 \cdot 4 \cdot 22 = 176$ unités (voir l'exercice 1.1.12).

*Exemple* 1.4.27. Mary veut apporter les œufs de la ferme au marché. Elle essaie de les mettre uniformément dans deux paniers, mais l'un est laissé de côté. Elle essaie trois paniers, mais il en reste un. Quatre paniers, un est laissé de côté. Cinq paniers. Ah ! Ça marche ! Combien d'oeufs a Mary ?

Soit $x \in \mathbb{N}$ le nombre d'œufs. Alors on a

$$\begin{aligned} \bar{x} &= \bar{1} \text{ in } \mathbb{Z}_2, \\ \bar{x} &= \bar{1} \text{ in } \mathbb{Z}_3, \\ \bar{x} &= \bar{1} \text{ in } \mathbb{Z}_4, \\ \bar{x} &= \bar{0} \text{ in } \mathbb{Z}_5. \end{aligned}$$

Notez premièrement que la troisième équation implique le première. Nous ignorons donc la première équation. Maintenant, nous savons que $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$ d'après le lemme 1.4.25. Sous cette isomorphisme, $\bar{x}$ (in $\mathbb{Z}_{12}$) est envoyé à $(\bar{1}, \bar{1}) \in \mathbb{Z}_3 \times \mathbb{Z}_4$. Donc $\bar{x} = \bar{1}$ in $\mathbb{Z}_{12}$.

Maintenant, encore d'après le lemme 1.4.25, on a $\mathbb{Z}_{60} \cong \mathbb{Z}_{12} \times \mathbb{Z}_5 \cong \mathbb{Z}_{60}/(12\mathbb{Z}_{60}) \times \mathbb{Z}_{60}/(5\mathbb{Z}_{60})$. Sous cette isomorphisme, $\bar{x}$ (dans $\mathbb{Z}_{60}$) est envoyé à $(\bar{1}, \bar{0}) \in \mathbb{Z}_{12} \times \mathbb{Z}_5$. En vérifiant tous les élément de $\mathbb{Z}_{60}$ qui sont envoyés à $\bar{1} \in \mathbb{Z}_{12}$, c.-à-d. $\bar{1}, \overline{13}, \overline{25}, \overline{37}, \overline{49}$, on voit que $\overline{25}$ se réduit à $\bar{0} \in \mathbb{Z}_5$. Ainsi $\bar{x} = \overline{25}$ in $\mathbb{Z}_{60}$. Donc Mary à $25 + 60k$, $k \in \mathbb{Z}$, œufs.

---

## Exercices.

Dans toutes ces exercices, $R$ est un anneau.

1.4.1. Démontrer la proposition 1.4.5.

1.4.2 ([Nic12, Ex. 3.4.1]). Pour tous les suivants, déterminer si la fonction est un morphisme d'anneaux. Justifier votre réponse.

(a) $\theta\colon \mathbb{Z}_3 \to \mathbb{Z}_{12}$, où $\theta(r) = 4r$.
(b) $\theta\colon \mathbb{Z}_4 \to \mathbb{Z}_{12}$, où $\theta(r) = 3r$.
(c) $\theta\colon R \times R \to R$, où $\theta(r,s) = r + s$.
(d) $\theta\colon R \times R \to R$, où $\theta(r,s) = rs$.
(e) $\theta\colon \mathcal{F}(\mathbb{R},\mathbb{R}) \to \mathbb{R}$, où $\theta(f) = f(1)$.

1.4.3. Montrer que l'endomorphisme de Frobenius (voir l'exemple 1.4.7) est bien un morphisme d'anneaux. *Indice :* Utiliser la formule de binôme de Newton : $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$.

1.4.4. Démontrer que la fonction définie dans l'exemple 1.4.12 est un automorphisme d'anneaux.

1.4.5 ([Nic12, Ex. 3.4.2]). Soit $\theta\colon R \to S$ un morphisme d'anneaux généraux, où $R$ et $S$ sont des anneaux.

(a) Si $\theta$ est surjective, prouver que $\theta$ est un morphisme d'anneaux.
(b) Si $S$ est un anneau sans diviseur de zéro et $\theta(1) \neq 0$, prouver que $\theta$ est un morphisme d'anneaux.

1.4.6 ([Nic12, Ex. 3.4.3]). Montrer qu'un morphisme d'anneaux généraux $\theta\colon \mathbb{Z} \to \mathbb{Z}$ est soit un morphisme d'anneaux soit $\theta(k) = 0$ pour tout $k \in \mathbb{Z}$.

1.4.7 ([Nic12, Ex. 3.4.4]). Déterminer tous les morphismes d'anneaux et tous les morphismes d'anneaux généraux $\mathbb{Z}_{12} \to \mathbb{Z}_6$.

1.4.8 ([Nic12, Ex. 3.4.5]). Si $\theta\colon R \to S$ est un morphisme d'anneaux surjectif, montrer que $\theta(Z(R)) \subseteq Z(S)$. Donner un exemple d'un (pas nécessairement surjectif) morphisme d'anneaux $\theta\colon R \to S$ où $\theta(Z(R)) \neq Z(S)$.

1.4.9 ([Nic12, Ex. 3.4.6]). Si $\theta\colon R \to S$ est un morphisme d'anneaux et $\operatorname{car}(R) > 0$, montrer que $\operatorname{car}(S)$ divise $\operatorname{car}(R)$.

1.4.10. Montrer que la composition de deux morphismes d'anneaux est un morphisme d'anneaux.

1.4.11. Terminer la démonstration du théorème 1.4.20 en montrant que $\mathbb{Z}1_R$ est contenue dans la centre de $R$.

1.4.12. Si $f$ est l'application définie dans la preuve du lemme 1.4.21, montrer que $\ker f = I \times J$ et $\operatorname{im} f = (R/I) \times (S/J)$.

1.4.13. Montrer que $A$ et $B$, comme définis dans la preuve du lemme 1.4.22, sont des idéaux de $R$ et $S$, respectivement.

1.4.14 ([Nic12, Ex. 3.4.9]). Si $R$ est un corps guache, quels sont les anneaux qui peuvent être l'image d'un morphisme d'anneaux avec domaine $R$ ?

1.4.15 ([Nic12, Ex. 3.4.11–3.4.14]). (a) Montrer que $x^3 - 8x^2 + 5x + 3 = 0$ n'a aucune solution $x \in \mathbb{Z}$.
(b) Montrer que $m^3 + 14n^3 = 12$ n'a aucune solution dans $\mathbb{Z}$.
(c) Montrer que $7m^2 + 11n^2 = 9$ n'a aucune solution dans $\mathbb{Z}$.
(d) Montrer que $n^3 + (n+1)^3 + (n+2)^3 = k^2 + 1$ n'a aucune solution dans $\mathbb{Z}$.

1.4.16. Démontrer que l'inverse d'un isomorphisme d'anneaux est aussi un isomorphisme d'anneaux.

1.4.17. Montrer que l'ensemble $\operatorname{Aut} R$ de tous les isomorphismes d'anneaux de $R$ est un groupe sous l'opération de composition.

1.4.18. Montrer que l'isomorphisme est une relation d'équivalence sur la classe de tous les anneaux.

1.4.19 ([Nic12, Ex. 3.4.19]). Soit $\theta\colon R \to S$ un morphisme d'anneaux surjectif.

(a) Si $A$ est un idéal de $R$, montrer que $\theta(A) = \{\theta(a) : a \in A\}$ est un idéal de $S$.

(b) Si aussi $\ker\theta \subseteq A$, montrer que $R/A \cong S/\theta(A)$. *Indice :* Utiliser le premier théorème d'isomorphisme, où $\alpha\colon R \to S/\theta(A)$ est définie par $\alpha(r) = \theta(r)+\theta(A)$ pour tout $r \in R$.

1.4.20 ([Nic12, Ex. 3.4.20]). Si $n > 0$ dans $\mathbb{Z}$, décrire tous les idéaux de $\mathbb{Z}$ qui contiennent $n\mathbb{Z}$.

1.4.21 ([Nic12, Ex. 3.4.21]). Montrer qu'il n'existe aucun morphisme d'anneaux $\mathbb{C} \to \mathbb{R}$.

1.4.22 ([Nic12, Ex. 3.4.22]). Soit $\theta\colon R \to S$ un morphisme d'anneaux. Si ni $\theta(R)$ ni $\ker\theta$ ne contiennent aucun élément nilpotent non nul, montrer que $R$ a la même propriété.

1.4.23 ([Nic12, Ex. 3.4.27]). Soit $R = \begin{bmatrix} S & S \\ 0 & S \end{bmatrix}$ l'anneau des matrices triangulaires supérieures (taille $2 \times 2$) à coefficients dans un anneau $S$. Montrer que $A = \begin{bmatrix} 0 & S \\ 0 & 0 \end{bmatrix}$ est un idéal de $R$ et que $R/A \cong S \times S$.

1.4.24 ([Nic12, Ex. 3.4.31]). Soit $R = S \times T$, où $S$ et $T$ sont des anneaux, et écrire $\bar{S} = \{(s, 0) : s \in S\}$. Montrer que $\bar{S}$ est un idéal de $R$, et que $R/\bar{S} \cong T$ et $\bar{S} \cong S$ en tant qu'anneaux. Quel est l'élément neutre de $\bar{S}$ ?

1.4.25. Démontrer le *deuxième théorème d'isomorphisme* : Si $A$ est un idéal de $R$ et $S$ est un sous-anneau de $R$, alors

(a) $S + A$ est un sous-anneau de $R$,

(b) $A$ et $S \cap A$ sont des idéaux de $S + A$ et $S$, respectivement, et

(c) $(S + A)/A \cong S/(S \cap A)$ en tant qu'anneaux.

1.4.26. Démontrer le *troisième théorème d'isomorphisme* : Si $A \subseteq B \subseteq R$, où $A$ et $B$ sont des idéaux de $R$, alors $B/A = \{b + A : b \in B\}$ est un idéal de $R/A$ et $(R/A)/(B/A) \cong R/B$ en tant qu'anneaux.

1.4.27 ([Nic12, Ex. 3.4.37]). Montrer que $\mathbb{Z}_m \times \mathbb{Z}_n$ a un sous-anneau qui est isomorphe à $\mathbb{Z}_t$, où $t$ est le plus petit commun multiple de $m$ et $n$.

1.4.28 (Problème de bonus). Soit $f\colon \mathbb{R} \to \mathbb{R}$ un morphisme d'anneaux. Démontrer que $f(x) = x$ pour tout $x \in \mathbb{R}$. En d'autres termes, l'application identité est le seul morphisme d'anneaux de $\mathbb{R}$ vers $\mathbb{R}$.

1.4.29 (Problème de bonus). Démontrer que si $f\colon \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{m \text{ fois}} \to \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ fois}}$ est un isomorphisme d'anneaux, alors $m = n$.

# Chapitre 2

# Polynômes

Dans ce chapitre, nous nous intéressons à une classe d'anneaux particulièrement importante : les anneaux des polynômes. Nous introduisons d'abord les anneaux des polynômes en toute généralité et en déduisons certaines de leurs propriétés fondamentales. Nous nous concentrons ensuite sur les polynômes dont les coefficients se trouvent dans un corps. Nous discutons du factorisation de tels polynômes et de la structure des anneaux quotient de ces anneaux des polynômes. Une référence pour le matériel de ce chapitre est [Jud19, Ch. 17].

## 2.1 Anneaux des polynômes

**Définition 2.1.1** (Indéterminée)**.** Si $R \subseteq S$ sont des anneaux, alors un élément $x \in S$ est appelé une *indéterminée* sur $R$ si

$$a_0 + a_1 x + \cdots + a_n x^n = 0,\ a_i \in R \implies a_i = 0\ \forall\ i.$$

**Lemme 2.1.2.** *Si $R$ est un anneau, il existe un anneau $S$ avec les propriétés suivants :*

*(a) $R \subseteq S$.*

*(b) Il existe $x \in S$ tel que $x$ est une indéterminée sur $R$.*

*(c) On a $xa = ax$ pour tout $a \in R$.*

*Aperçu de la preuve.* La preuve de ce lemme est un peu technique. Nous ne donnerons ici qu'un aperçu. Les détails peuvent être trouvés dans [Nic12, §4.6] ou, sous l'hypothèse que $R$ est commutatif, dans [Roy, Prop. 4.2].

Soit $S$ l'ensemble de toutes les suites dans $R$. Autrement dit, $S$ est l'ensemble de toutes les fonctions $\mathbb{N} \to R$. On note souvent un élément $\alpha \in S$ par $(\alpha(0), \alpha(1), \alpha(2), \dots)$. On définit une structure d'anneau sur $S$ en définissant

$$(\alpha + \beta)(k) = \alpha(k) + \beta(k),$$
$$(\alpha\beta)(k) = \sum_{\ell=0}^{k} \alpha(\ell)\beta(k-\ell).$$

Alors $R$ est un sous-anneau de $S$ si on identifie $a = (a, 0, 0, \dots)$ pour $a \in R$. Cela démontre (a).

Maintenant définissons $x = (0, 1, 0, 0, \dots)$. Puis on peut montrer que

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = (a_0, a_1, \dots, a_n, 0, 0, \dots)$$

pour tout $a_0, \dots, a_n \in R$. Cela démontre (b). Puisque $ax = (0, a, 0, \dots) = xa$ pour tout $a \in R$, on a aussi (c). □

**Définition 2.1.3** (Anneau des polynômes)**.** Soit $R$ un anneau et soit $S$ comme dans le lemme 2.1.2. Alors

$$R[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : n \geq 0,\ a_i \in R\ \forall\ i\}$$

est un sous-anneau de $S$ qui s'appelle l'*anneau des polynômes* à coefficients dans $R$. Un *polynôme* à coefficients dans $R$ est un élément

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad n \in \mathbb{N},\ a_0, \dots, a_n \in R,$$

de $R[x]$. Les $a_i$ s'appellent les *coefficients* du polynôme $f(x)$. Nous adoptons la convention que $a_m = 0$ pour $m > n$. On écrit parfois $f$ au lieu de $f(x)$.

*Remarque* 2.1.4. Il découle de la définition 2.1.1 que deux polynômes $f(x) = a_0 + \cdots + a_k x^k$ et $g(x) = b_0 + \cdots + b_\ell x^\ell$ sont *égaux* si et seulement si $a_i = b_i$ pour tout $i \in \mathbb{N}$. Notez que c'est *pas* la même chose que l'égalité des *fonctions polynomiales*. Par exemple, considérez $f(x) = 0, g(x) = x^2 + x \in \mathbb{Z}_2[x]$. Ces deux polynômes ne sont *pas* égaux, mais les fonctions $\mathbb{Z}_2 \to \mathbb{Z}_2$ données par $a \mapsto f(a)$ et $a \mapsto g(a)$ *sont* égales (il sont tous les deux la fonction zéro). Ainsi, nous considérons les polynômes comme des expressions abstraites et *pas* comme des fonctions.

Il s'ensuit également que $R[x]$ est le sous-anneau de $S$ (du lemme 2.1.2) des suites à support fini. C'est-à-dire, les éléments de $R[x]$ sont des suites $\alpha \in S$ pour lesquelles il existe $N \in \mathbb{N}$ tel que $\alpha(k) = 0$ pour tout $k > N$.

Il découle de ce qui précède que si $R$ est un anneau, l'addition et la multiplication sur $R[x]$ sont calculées comme suit. Si

$$f(x) = a_0 + \cdots + a_k x^k \quad \text{et} \quad g(x) = b_0 + \cdots + b_k x^k$$

(notez qu'on peut écrire $f(x)$ et $g(x)$ sous cette forme, avec la même puissance la plus grande $x^k$ de $x$ en laissant certains des coefficients être nuls si nécessaire), alors

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k, \quad \text{et}$$
$$f(x)g(x) = \sum_{i=0}^{2k} \left( \sum_{j=0}^{i} a_j b_{i-j} x^i \right) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots .$$

*Exemple* 2.1.5. On a

$$1 - 3x + x^2 \in \mathbb{Z}[x], \quad 2x - 3 \in \mathbb{Z}[x], \quad \text{mais} \quad 1 - \frac{1}{x} \notin \mathbb{Z}[x].$$

En outre

$$\begin{aligned}(1 - 3x + x^2)(2x - 3) &= (1 - 3x + x^2)(-3 + 2x) \\ &= -3 + (2 + 9)x + (-6 - 3)x^2 + 2x^3 = -3 + 11x - 9x^2 + 2x^3.\end{aligned}$$

*Exemple* 2.1.6. On a

$$\bar{1} - \bar{2}x,\ \bar{1} + \bar{2}x^2 \in \mathbb{Z}_4[x]$$

et

$$(\bar{1} - \bar{2}x) + (\bar{1} + \bar{2}x^2) = (\bar{1} + \bar{1}) - \bar{2}x - \bar{2}x^2 = \bar{2} - \bar{2}x + \bar{2}x^2 = \bar{2} + \bar{2}x + \bar{2}x^2,$$
$$\bar{2}(\bar{1} + \bar{2}x^2) = \bar{2} + \bar{0}x^2 = \bar{2},$$
$$(\bar{1} - \bar{2}x)(\bar{1} + \bar{2}x^2) = \bar{1} + (-\bar{2})x + \bar{2}x^2 - \bar{0}x^3 = \bar{1} + \bar{2}x + \bar{2}x^2.$$

**Définition 2.1.7** (Degré, coefficient dominant, coefficient constant, polynôme unitaire)**.** Soit $f(x) = a_0 + a_1x + \cdots + a_kx^k \in R[x]$.

- Si $a_k \neq 0$, alors le *degré* de $f(x)$ est $\deg f(x) = k$ et $a_k$ est le *coefficient dominant* de $f(x)$.
- $a_0$ est appelé le *coefficient constant* of $f(x)$.
- Si $a_k = 1$, alors $f(x)$ est appelé un *polynôme unitaire*.

**Théorème 2.1.8.** *Soit $R$ un anneau. Alors*

*(a) le centre de $R[x]$ est $Z(R)[x]$,*
*(b) $x \in Z(R[x])$, et*
*(c) si $R$ est commutatif, alors $R[x]$ est aussi commutatif.*

*Démonstration.* La preuve de ce théorème est l'exercice 2.1.4 □

L'élément zéro de $R[x]$ est le *polynôme nul* $0 = 0 + 0x = 0 + 0x + 0x^2 = \cdots$. Un polynôme est appelé un *polynôme constant* s'il existe $a_0 \in R$ tel que $f(x) = a_0 = a_0 + 0x = a_0 + 0x + 0x^2 = \cdots$. Notez que $R$ est le sous-anneau de $R[x]$ dont les éléments sonts les polynômes constants.

**Théorème 2.1.9.** *Soit $R$ un anneau. Si $f(x), g(x) \in R[x] \setminus \{0\}$, alors les affirmations suivantes sont vraies.*

*(a) $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.*
*(b) $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$.*
*(c) Si $R$ est un anneau sans diviseur de zéro, alors $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.*
*(d) Si $R$ est un anneau sans diviseur de zéro, alors $R[x]$ est aussi un anneau sans diviseur de zéro.*
*(e) Si $R$ est un anneau sans diviseur de zéro, alors les seules unités de $R[x]$ sont les unités de $R$.*
*(f) Si le coefficient dominant de $f(x)$ ou $g(x)$ est une unité dans $R$, alors $f(x)g(x) \neq 0$ dans $R[x]$ et $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.*

*Démonstration.* La preuve de ce théorème et l'exercice 2.1.5. □

*Exemple* 2.1.10. Pour voir que les inégalités du théorème 2.1.9 peuvent être stricte quand $R$ possède des diviseurs de zéro, considérez $\bar{1} + \bar{2}x, \bar{2}x \in \mathbb{Z}_4[x]$. Alors $(\bar{1} + \bar{2}x)(\bar{2}x) = \bar{2}x$ et donc

$$\deg(\bar{1} + \bar{2}x)(\bar{2}x) = 1 < 2 = \deg(\bar{1} + \bar{2}x) + \deg(\bar{2}x).$$

De plus,

$$\deg((\bar{1}+\bar{2}x)+(\bar{2}x)) = \deg(\bar{1}) = 0 < 1 = \max\{\deg(\bar{1}+\bar{2}x), \deg(\bar{2}x)\}.$$

*Exemple* 2.1.11. Soit $I \subseteq \mathbb{Z}[x]$ l'idéal engendré par $x$, c.-à-d., $I = \langle x \rangle = x\mathbb{Z}[x]$. Donc

$$I = \{xf(x) : f(x) \in \mathbb{Z}[x]\} = \{a_1x + \cdots + a_kx^k : k \geq 1,\ a_1, \ldots, a_k \in \mathbb{Z}\}.$$

Considérez le morphisme d'anneaux $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}$ donné par $\varphi(a_0 + \ldots + a_kx^k) = a_0$. C'est un exercice simple (l'exercice 2.1.6) de voir que $\varphi$ est un morphisme d'anneaux surjectif et que $\ker\varphi = I$. Donc, d'après le premier théorème d'isomorphisme (le théorème 1.4.15), on a $\mathbb{Z}[x]/I \cong \mathbb{Z}$.

**Théorème 2.1.12** (Division euclidienne des polynômes)**.** *Soient $R$ un anneau, $f(x), g(x) \in R[x]$, $f(x) \neq 0$, et supposons que le coefficient dominant de $f(x)$ est une unité dans $R$. Alors il existe des polynômes uniques $q(x), r(x) \in R[x]$ tels que*

*(a)* $g(x) = q(x)f(x) + r(x)$ *et*
*(b) soit* $r(x) = 0$ *soit* $\deg r(x) < \deg f(x)$.

*Démonstration.* Premièrement, on démontre l'existence par récurrence sur $\deg g(x)$. Si $g(x) = 0$ ou $\deg g(x) < \deg f(x)$, alors on peut prendre $q(x) = 0$ et $r(x) = g(x)$. Donc supposons que $m \geq n$, où $m = \deg g(x)$ et $n = \deg f(x)$. Écrivons

$$f(x) = ux^n + ax^{n-1} + \cdots, \qquad g(x) = bx^m + cx^{m-1} + \cdots,$$

où $u$ est une unité par l'hypothèse. Soit

$$\begin{aligned} g_1(x) &= g(x) - bu^{-1}x^{m-n}f(x) \\ &= (bx^m + cx^{m-1} + \cdots) - bu^{-1}x^{m-n}(ux^n + ax^{n-1} + \cdots) \\ &= 0x^m + (c - bu^{-1}a)x^{m-1} + \cdots. \end{aligned}$$

Alors soit $g_1(x) = 0$ soit $\deg g_1(x) < m$. Ainsi, par l'hypothèse de récurrence, il existe des polynômes $q_1(x)$ et $r(x)$ tels que $g_1(x) = q_1(x)f(x) + r(x)$ avec $r(x) = 0$ où $\deg r(x) < \deg f(x)$. Alors

$$g(x) = g_1(x) + bu^{-1}x^{m-n}f(x) = (q_1(x) + bu^{-1}x^{m-n})f(x) + r(x),$$

ce qui complète l'étape de récurrence.

Il reste à prouver l'unicité. Supposons qu'on a

$$q_1(x)f(x) + r_1(x) = g(x) = q_2(x)f(x) + r_2(x)$$

avec $r_i(x) = 0$ ou $\deg r_i(x) < \deg f(x)$ pour $i = 1, 2$. Alors $r_1(x) - r_2(x) = (q_2(x) - q_1(x))f(x)$. Si $q_2(x) - q_1(x) \neq 0$, alors, puisque le coefficient dominant de $f(x)$ est une unité (voir le théorème 2.1.9(f)), on a $(q_2(x) - q_1(x))f(x) \neq 0$ et

$$\deg(r_1(x) - r_2(x)) = \deg[(q_2(x) - q_1(x))f(x)] = \deg(q_2(x) - q_1(x)) + \deg f(x).$$

Mais cela implique que $\deg(r_1(x) - r_2(x)) \geq \deg f(x)$, ce qui est un contradiction. Ainsi $q_2(x) - q_1(x) = 0$ et donc $r_1(x) - r_2(x) = (q_2(x) - q_1(x))f(x) = 0$. Cela complète la démonstration de l'unicité. □

*Remarque* 2.1.13. Notez que si $R$ est en fait un corps, alors le coefficient dominant de *tout* polynôme non nul est une unité dans $R$. Alors le théorème 2.1.12 nous dit que $R[x]$ est un *anneau euclidien* avec *stathme euclidien* $f(x) \mapsto \deg f(x)$.

*Exemple* 2.1.14. Divisons $x^3 - x^2 + 2x - 3$ par $x - 2$.

$$\begin{array}{rr|llllll} & x^2 & + & x & + & 4 & & \\ x-2 & x^3 & - & x^2 & + & 2x & - & 3 \\ & x^3 & - & 2x^2 & & & & \\ \hline & & & x^2 & + & 2x & - & 3 \\ & & & x^2 & - & 2x & & \\ \hline & & & & & 4x & - & 3 \\ & & & & & 4x & - & 8 \\ \hline & & & & & & & 5 \end{array}$$

Donc,

$$\underbrace{x^3 - x^2 + 2x - 3}_{g(x)} = \underbrace{(x^2 + x + 4)}_{q(x)}\underbrace{(x - 2)}_{f(x)} + \underbrace{5}_{r(x)}.$$

*Exemple* 2.1.15. Divisons $x^3 + \bar{2}$ par $\bar{2}x + \bar{2}$ dans $\mathbb{Z}_3[x]$.

$$\begin{array}{rr|llllll} & \bar{2}x^2 & + & x & + & \bar{2} & & \\ \bar{2}x+\bar{2} & x^3 & + & \bar{0}x^2 & + & \bar{0}x & + & \bar{2} \\ & x^3 & + & x^2 & & & & \\ \hline & & & -x^2 & & & + & \bar{2} \\ & & & \bar{2}x^2 & + & \bar{2}x & & \\ \hline & & & & & -\bar{2}x & + & \bar{2} \\ & & & & & x & + & \bar{1} \\ \hline & & & & & & & \bar{1} \end{array}$$

Donc

$$\underbrace{x^3 + \bar{2}}_{g(x)} = \underbrace{\bar{2}x^2 + x + \bar{2}}_{q(x)}\underbrace{(\bar{2}x + \bar{2})}_{f(x)} + \underbrace{\bar{1}}_{r(x)}.$$

Peut-on toujours évaluer les polynômes en spécialisant l'indéterminé ? On a l'habitude de faire cela en calcul, mais en fait il faut être prudent !

*Exemple* 2.1.16. Considérez le polynôme $f(x) = x^3 - 2x - 4 \in \mathbb{Z}[x]$. On a $f(2) = 0$, ce qui implique que $x - 2$ est un facteur de $f(x)$. En fait, on a $f(x) = (x^2 + 2x + 2)(x - 2)$.

*Exemple* 2.1.17. Supposons que $R$ est un anneau et que $a, b \in R$ avec $ab \neq ba$. Soit $f(x) = (x - a)(x - b) \in R[x]$. Alors $f(a) = (a - a)(b - a) = 0(b - a) = 0$. Mais on a aussi $f(x) = x^2 - ax - bx + ab$ et donc $f(a) = a^2 - a^2 - ba + ab = -ba + ab \neq 0$. Ainsi, «l'évaluation» de $f(x)$ en $a$ ne semble pas bien définie. Le problème est que $x$ se trouve dans le centre de $R[x]$ et nous essayons de construire un morphisme d'anneaux (surjectif) qui envoie $x$ à quelque chose qui n'est *pas* dans le centre de $R$.

**Théorème 2.1.18** (Théorème d'évaluation)**.** *Soient $R$ un anneau et $a \in Z(R)$. Alors l'application $\varphi_a \colon R[x] \to R$, $\varphi_a(f(x)) = f(a)$ est un morphisme d'anneaux surjectif.*

*Démonstration.* Rappelons qu'on peut considérer les éléments de $R$ comme des polynômes constant dans $R[x]$. Pour tout $r \in R$ on a $\varphi_a(r) = r$. Donc $\varphi_a$ est surjectif.

Soit $f(x) = \sum_{i=0}^{k} a_i x^i$ et $g(x) = \sum_{i=0}^{k} b_i x^i$ des éléments quelconques de $R[x]$. Alors on a

$$\begin{aligned}\varphi_a(f(x)+g(x)) = \varphi_a\left(\sum (a_i+b_i)x^i\right) &= \sum (a_i+b_i)a^i \\ &= \sum a_i a^i + \sum b_i a^i = \varphi_a(f(x)) + \varphi_a(g(x),\end{aligned}$$

$$\begin{aligned}\varphi_a(f(x)g(x)) = \varphi_a\left(\sum_{i=0}^{2k}\left(\sum_{j=0}^{i} a_j b_{i-j} x^i\right)\right) &= \sum_{i=1}^{2k}\left(\sum_{j=0}^{i} a_0 b_{i-j} a^i\right) \\ &= \left(\sum_{i=0}^{k} a_i a^i\right)\left(\sum_{i=0}^{k} b_i a^i\right) = \varphi_a(f(x))\varphi_a(g(x)),\end{aligned}$$

$$\varphi_a(1_{R[x]}) = \varphi(1_R) = 1_R. \qquad \square$$

L'application $\varphi_a$ du théorème 2.1.18 est appelée *evaluation* à $a$. Le problème dans l'exemple 2.1.17 était qu'on a essayé d'évaluer un polynôme à un élément qui n'était *pas* dans le centre de l'anneau de coefficients $R$.

*Exemple* 2.1.19. Soit $R$ un anneau. Alors

$$\varphi\colon R[x] \to R, \quad \varphi(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n) = a_0 + a_1 + a_2 + \cdots + a_n,$$

est un morphisme d'anneaux surjectif puisque $\varphi = \varphi_1$.

**Théorème 2.1.20** (Théorème des restes)**.** *Soient $R$ un anneau commutatif et $f(x) \in R[x]$. Alors, pour tout $a \in R$, le reste de la division de $f(x)$ par $x - a$ est $f(a)$.*

*Démonstration.* D'après le théorème 2.1.12, on peut écrire $f(x) = q(x)(x-a) + r(x)$ où $r(x) = 0$ ou $\deg r(x) < 1$. Donc $r(x)$ est un polynôme constant. C'est-à-dire, il existe $r \in R$ tel que $r(x) = r$. Alors

$$f(a) = \varphi_a(f(x)) = \varphi_a(q(x))\varphi_a(x-a) + \varphi_a(r(x)) = 0 + r(a) = r. \qquad \square$$

**Théorème 2.1.21** (Théorème des facteurs)**.** *Soient $R$ un anneau commutatif et $f(x) \in R[x]$. Alors $a \in R$ satisfait $f(a) = 0$ si et seulement s'il existe $q(x) \in R[x]$ tel que $f(x) = (x-a)q(x)$.*

*Démonstration.* Il est claire que $f(a) = 0$ s'il existe $g(x) \in R[x]$ tel que $f(x) = (x-a)g(x)$. L'inverse découle immédiatement du théorème des restes (le théorème 2.1.20). $\square$

**Corollaire 2.1.22.** *Soient $R$ un anneau commutatif et $\varphi_a\colon R[x] \to R$, $\varphi_a(f(x)) = f(a)$. Alors $\ker \varphi_a = \langle x-a \rangle = (x-a)R[x]$ et $R[x]/\langle x-a\rangle \cong R$.*

*Démonstration.* On a

$$\begin{aligned} f(x) \in \ker \varphi_a &\iff f(a) = 0 \\ &\iff \exists\, q(x) \in R[x] \text{ tel que } f(x) = q(x)(x-a) + 0 \\ &\iff f(x) \in \langle x - a \rangle. \end{aligned}$$

La deuxième affirmations découle alors du premier théorème d'isomorphisme (le théorème 1.4.15). □

**Définition 2.1.23** (Racine d'un polynôme)**.** Soient $R$ un anneau commutatif et $f(x) \in R[x] \setminus \{0\}$. Un élément $a \in R$ est appelé un *zéro* ou *racine* de $f(x)$ si $f(a) = 0$.

*Exemple* 2.1.24. Les racines de $x^2 - \bar{1} \in \mathbb{Z}_8[x]$ sont $\bar{1}, \bar{3}, \bar{5}, \bar{7}$.

**Définition 2.1.25** (Multiplicité d'un zéro)**.** Soient $R$ un anneau commutatif et $f(x) \in R[x] \setminus \{0\}$. Si $a \in R$ est une racine de $f(x)$, on dit que $a$ a *multiplicité* $m \geq 0$ si $f(x) = (x-a)^m g(x)$ avec $g(a) \neq 0$.

*Exemple* 2.1.26. Trouvons la multiplicité de la racine $\bar{3}$ pour $f(x) = x^3 + \bar{3}x + \bar{4} \in \mathbb{Z}_5[x]$. On a $f(\bar{3}) = \bar{0}$. La division de $f(x)$ par $x - \bar{3}$ donne $f(x) = (x - \bar{3})g(x)$ avec $g(x) = x^2 + \bar{3}x + \bar{2}$. Puisque $g(\bar{3}) = \bar{0}$, on divise à nouveau pour obtenir $g(x) = (x - \bar{3})(x + \bar{1})$. Ainsi on a $f(x) = (x - \bar{3})^2(x + \bar{1})$. Puisque $\bar{3}$ n'est pas une racine de $x + \bar{1}$, on voit que la multiplicité de la racine $\bar{3}$ est 2.

**Théorème 2.1.27.** *Soient $R$ un anneau intègre et $f(x) \in R[x] \setminus \{0\}$. Si $n = \deg f(x)$, alors $f(x)$ a au plus $n$ racines.*

*Démonstration.* On démontre le résultat par récurrence sur $n$. Les cas $n = 0, 1$ sont clairs. Supposons que $\deg f(x) = n+1$. Alors, si $f(a) = 0$, on a $f(x) = (x-a)g(x)$ avec $\deg g(x) = n$. Si $f$ a plus que $n + 1$ racines, alors on a $f(a_1) = f(a_2) = \cdots = f(a_{n+1}) = 0$ pour des éléments distincts $a_1, \ldots, a_{n+1}$, dont aucun n'est égal à $a$. Alors, pour $i = 1, \ldots, n + 1$, on a $0 = f(a_i) = (a_i - a)g(a_i)$ et $a_i - a \neq 0$, ce qui implique que $g(a_i) = 0$. Ainsi $g(x)$ a au moins $n + 1$ racines, ce qui contredit l'hypothèse de récurrence puisque $\deg g(x) = n$. □

**Théorème 2.1.28** (Théorème de racines rationnelles)**.** *Soit $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ avec $a_0 \neq 0$, $a_n \neq 0$. Si $r \in \mathbb{Q}$ et $f(r) = 0$, alors $r = \frac{c}{d}$ avec $c | a_0$ et $d | a_n$.*

*Démonstration.* Écrivons $r = \frac{c}{d}$ avec $\operatorname{pgcd}(c, d) = 1$. Alors

$$0 = f(r) = a_0 + a_1 \left(\frac{c}{d}\right) + \cdots + a_n \left(\frac{c}{d}\right)^n \implies a_0 d^n + a_1 d^{n-1} c + \cdots + a_n c^n = 0.$$

Ainsi

$$\begin{aligned} a_0 d^n &= -c(a_1 d^{n-1} + a_2 d^{n-2} c + \cdots a_n c^{n-1}) \quad \text{et} \\ a_n c^n &= -d(a_0 d^{n-1} + a_1 d^{n-2} c + \cdots + a_n c^{n-1}). \end{aligned}$$

Puisque $c$ sont $d$ premiers entre eux, cela implique que $c | a_0$ et $d | a_n$. □

*Exemple* 2.1.29. Bien que nous sachions déjà que $\sqrt{2}$ est irrationnel, on peut donner une autre preuve basée sur le théorème de racines rationnelles (le théorème 2.1.28). Considérons le polynôme $x^2 - 2$. S'il avait une racine rationnelle, elle doit être l'un des $\pm 2, \pm 1$. Mais on vérifie facilement qu'aucun de ceux-ci n'est une racine de $x^2 - 2$. Ainsi, $x^2 - 2$ n'a pas de racines rationnelles. Puisque $\sqrt{2}$ est une racine de $x^2 - 2$, ce n'est pas rationnel.

*Exemple* 2.1.30. Si $f(x) \in \mathbb{Z}[x] \setminus \{0\}$ est unitaire, alors toute racine rationnelle de $f(x)$ est un entier.

---

## Exercices.

2.1.1. Calculer $(f + g)(x)$ et $(fg)(x)$, où

$$f(x) = 2 + 3x + x^2,\ g(x) = 1 + x^2 + x^3 + 4x^3 \in \mathbb{Z}_5[x].$$

2.1.2 ([Nic12, Ex. 4.1.2]). (a) Calculer $(1 + x)^5$ dans $\mathbb{Z}_5[x]$.
(b) Calculer $(1 + x)^7$ dans $\mathbb{Z}_7[x]$.
(c) Montrer que $(1 + x)^p = 1 + x^p$ dans $\mathbb{Z}_p[x]$ si $p$ est un nombre premier.

2.1.3 ([Nic12, Ex. 4.1.3]). (a) Combien de polynômes de degré 3 y-a-t-il dans $\mathbb{Z}_5[x]$ ?
(b) Combien de polynômes unitaires de degré 3 y-a-t-il dans $\mathbb{Z}_5[x]$ ?

2.1.4. Démontrer le théorème 2.1.8.

2.1.5. Démontrer le théorème 2.1.9.

2.1.6. Montrer que l'application $\varphi$ de l'exemple 2.1.11 est un morphisme d'anneaux surjectif avec $\ker \varphi = I$.

2.1.7. Donner un exemple d'un anneau commutatif $R$ et un polynôme $f(x) \in R[x] \setminus \{0\}$ de degré $n$ avec plus que $n$ racines distinctes.

2.1.8. Utiliser le théorème de racine rationnelles (le théorème 2.1.28) pour montrer que $\sqrt[3]{5}$ est irrationnel.

2.1.9 ([Nic12, Ex. 4.1.4]). (a) Trouver toutes les racines de $(x - 4)(x - 5)$ dans $\mathbb{Z}_6$ et dans $\mathbb{Z}_7$.
(b) Trouver toutes les racines de $x^3 - x$ dans $\mathbb{Z}_6$ et dans $\mathbb{Z}_4$.

2.1.10 ([Nic12, Ex. 4.1.5(a)]). Trouver le nombre de racines de $x^2 - x$ dans $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, dans tout anneau intègre, et dans $\mathbb{Z}_6$.

2.1.11 ([Nic12, Ex. 4.1.8]). Soit $R$ un sous-anneau d'un anneau $S$, soient $f(x) \neq 0$ et $g(x)$ des polynômes dans $R[x]$, et supposer que le coefficient dominant de $f(x)$ est une unité dans $R$. Si $f(x)$ divise $g(x)$ dans $S[x]$, montrer que $f(x)$ divise $g(x)$ dans $R[x]$. *Indice :* Utiliser la division euclidienne des polynômes.

2.1.12 ([Nic12, Ex. 4.1.9]). Montrer que $R[x]$ et $R$ ont la même caractéristique pour tout anneau $R$.

2.1.13 ([Nic12, Ex. 4.1.11]). Si $a$ est une racine non nulle de $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$, montrer que $a^{-1}$ (s'il existe) est une racine de $g(x) = a_n + a_{n-1}x + \cdots + a_1x^{n-1} + a_0x^n$. Supposons que l'anneau des coefficients $R$ est commutatif.

2.1.14 ([Nic12, Ex. 4.1.12]). Si $a$, $b$, et $c$ sont réels et $f(x) = x^2 - (a+c)x + (ac - b^2)$, montrer que toute racine complexe de $f$ est réelle.

2.1.15 ([Nic12, Ex. 4.1.13]). Diviser $x^3 - 4x + 5$ par $2x + 1$ dans $\mathbb{Q}[x]$. Pourquoi est-ce impossible dans $\mathbb{Z}[x]$ ?

2.1.16 ([Nic12, Ex. 4.1.14]). Dans chaque cas, écrire $g(x) = q(x)f(x) + r(x)$ dans $R[x]$, où $r(x) = 0$ ou $\deg r(x) < \deg f(x)$.

(a) $g(x) = x^5 + 4x^4 + x^3 + 5x^2 + x + 2$, $f = x^2 + x + 1$, $R = \mathbb{Z}_6$.
(b) $g(x) = x^3 + x^2 + 3x + 2$, $f = 3x + 1$, $R = \mathbb{Z}_8$.
(c) $g(x) = 3x^3 + 2x^2 - 8x + 1$, $f = x^2 + 2$, $R = \mathbb{Q}$.

2.1.17 ([Nic12, Ex. 4.1.15]). Lesquels de $x - 1$, $x + 1$, et $x - 2$ sont des facteurs de $x^4 - 2x^3 - x^2 + 3x - 2$ dans $\mathbb{Z}[x]$ ?

2.1.18 ([Nic12, Ex. 4.1.16(a)]). Pour quels nombres premiers $p$ le polynôme $x - 1$ est-il un facteur $f(x) = 3x^4 + 5x^3 + 2x^2 + x + 4$ dans $\mathbb{Z}_p[x]$ ?

2.1.19 ([Nic12, Ex. 4.1.17]). Dans chaque cas, factoriser $f(x)$ en facteurs linéaires dans $F[x]$.

(a) $f(x) = x^4 + 12$, $F = \mathbb{Z}_{13}$.
(b) $f(x) = x^3 - x^2 + x - 1$, $F = \mathbb{Z}_5$.

2.1.20 ([Nic12, Ex. 4.1.18]). Soit $a \neq 0$ dans un corps $F$. Déterminer les entiers $n \geq 1$ tels que $x + a$ est un facteur de $x^n + a^n$ dans $F[x]$. Dans ces cas, écrire le factorisation.

2.1.21 ([Nic12, Ex. 4.1.19]). Si $F$ est un corps, soient $u$, $v$, et $w$ des racines distinctes de $f(x) = x^3 + ax^2 + bx + c$ dans $F[x]$. Montrer que $a = -(u + v + w)$, $b = uv + uw + vw$, et $c = -uvw$.

2.1.22 ([Nic12, Ex. 4.1.21]). (a) Montrer que $\mathbb{Z}_4[x]$ a un nombre infini d'unités et un nombre infini d'éléments nilpotents.
(b) Trouver un polynôme dans $\mathbb{Z}_4[x]$ qui n'est ni une unité ni un élément nilpotent.

2.1.23 ([Nic12, Ex. 4.1.23]). Dans chaque cas, déterminer la multiplicité de $a$ en tant que racine de $f(x) \in R[x]$.

(a) $f(x) = x^3 - 2x^2 - 4x + 3$, $a = 3$, $R = \mathbb{Z}_6$.
(b) $f(x) = x^5 + 2x^4 + x^3 - x^2 + 2x - 1$, $a = 1$, $R = \mathbb{Z}_4$.

2.1.24 ([Nic12, Ex. 4.1.25]). Dans chaque cas, trouver toutes les racines de $f(x)$ et factoriser $f(x)$ autant que possible dans $\mathbb{Q}[x]$.

(a) $f(x) = 4x^4 + x^3 - 3x^2 + 4x - 3$
(b) $f(x) = x^4 - x^3 - x^2 - x - 2$
(c) $f(x) = x^4 + x^3 + 3x^2 + 2x + 2$

2.1.25 ([Nic12, Ex. 4.1.26]). Montrer que $\sqrt[n]{m}$ n'est rationnel que si $m = k^n$ pour un entier $k$.

2.1.26 ([Nic12, Ex. 4.1.27]). Si $f$ est un polynôme unitaire dans $\mathbb{Z}[x]$, montrer que les seules racines rationnelles (s'il existe des racines rationnelles) sont des entiers.

2.1.27. (a) Supposons que $R$ soit un anneau intègre infini. Montrer que si $f(x), g(x) \in R[x]$ remplissent la condition $f(a) = g(a)$ pour tout $a \in R$, alors $f(x) = g(x)$. En d'autres termes, deux polynômes sont égaux si et seulement s'ils correspondent à la même fonction polynomiale.
(b) Supposons que $R$ et un anneau commutatif fini. Montrer qu'il existe un polynôme $f(x) \in R[x] \setminus \{0\}$ tel que $f(a) = 0$ pour tout $a \in R$.

2.1.28. Soit $G$ le groupe multiplicatif des nombres rationnels positifs. Montrer que $G$ est isomorphe en tant que groupe à $(\mathbb{Z}[x], +)$.

2.1.29 (Bonus). Soit $R$ un anneau commutatif. Démontrer que $f(x) \in R[x]$, $f(x) = a_0 + \cdots + a_n x^n$ est un élément nilpotent de $R[x]$ si est seulement si $a_0, \ldots, a_n$ sont des éléments nilpotents de $R$.

## 2.2 Factorisation de polynômes sur un corps

Nous commençons ce chapitre avec quelques exemples.

*Exemple* 2.2.1. Factorisons $f(x) = 3x^3 - x^2 - x - 4 \in \mathbb{Q}[x]$ autant que possible. Par le théorème des racines rationnelles (le théorème 2.1.28), les seules racines rationnelles possibles sont de la forme $\frac{c}{d}$ où $c|4$ et $d|3$. On voit que $x = \frac{4}{3}$ est une racine. La division polynomiale donne alors que $f(x) = \left(x - \frac{4}{3}\right)(3x^2 + 3x + 3) = (3x - 4)(x^2 + x + 1)$. Encore une fois, en utilisant le théorème des racines rationnelles, nous pouvons voir que $x^2 + x + 1$ n'a aucune racine rationnelle et nous ne pouvons donc pas factoriser davantage.

*Exemple* 2.2.2. Factorisons $f(x) = x^4 + 25x + 24 \in \mathbb{Q}[x]$ autant que possible. Puisque $f(-1) = 0$, nous savons que $x + 1$ est un facteur de $f(x)$. La division polynomiale donne alors $f(x) = (x+1)(x^3 - x^2 + x + 24)$. Par le théorème des racines rationnelles (le théorème 2.1.28), toute racine rationnelle de $x^3 - x^2 + x + 24$ doit être dans l'ensemble $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$. Mais aucun de ceux-ci n'est une racine et donc $f(x)$ ne peut plus être factorisé (car s'il était factorisé, au moins un facteur devrait être de degré un).

*Exemple* 2.2.3. Factorisons $f(x) = 2x^5 + x^4 + 4x^3 + 2x^2 + 2x + 1 \in \mathbb{Q}[x]$ autant que possible. Puisque $f(-1/2) = 0$, on obtient $f(x) = (2x + 1)(x^4 + 2x^2 + 1) = (2x + 1)(x^2 + 1)^2$. Puisque $x^2 + 1$ n'a aucune racine rationnelle (ou même réelle), nous ne pouvons plus factoriser $f(x)$ (dans $\mathbb{Q}[x]$).

**Définition 2.2.4** (Polynôme irréductible)**.** Soit $F$ un corps. Un polynôme $f(x) \in F[x]$ est appelé *irréductible* sur $F$ si

(a) $f(x) \neq 0$ et $\deg f(x) \geq 1$ (c.-à-d. $f(x)$ n'est pas un polynôme constant), et
(b) si $f(x) = p(x)q(x)$ in $F[x]$, alors soit $\deg p(x) = 0$ soit $\deg q(x) = 0$.

Un polynôme non nul de degré positif est appelé *réductible* (ou on dit qu'il *se factorise*) s'il n'est pas irréductible.

*Exemple* 2.2.5. Si $\deg f(x) = 1$ alors $f(x)$ est irréductible.

*Exemple* 2.2.6. Si $f(x)$ est irréductible, alors, pour tout $a \neq 0$, le polynôme $af(x)$ est aussi irréductible.

**Théorème 2.2.7.** *Soit $F$ un corps et considérons $f(x) \in F[x] \setminus \{0\}$ tel que $\deg f(x) \geq 2$.*

*(a) Si $f(x)$ est irréductible, alors il n'a aucune racine dans $F$.*
*(b) Supposons que $\deg f(x) \leq 3$. Alors $f(x)$ est irréductible si et seulement si $f(x)$ n'a aucune racine dans $F$.*

*Démonstration.* (a) Si $f(x)$ a une racine $a \in F$, alors il existe $q(x) \in F[x]$ tel que $f(x) = (x-a)q(x)$ d'après le théorème des facteurs (le théorème 2.1.21). Puisque $\deg f(x) \geq 2$, cela implique que $f(x)$ n'est pas irréductible, ce qui contredit l'hypothèse. Donc $f(x)$ n'a aucune racine dans $F$.

(b) Supposons que $f(x)$ n'ait aucune racine dans $F$. Si $f(x)$ est réductible, alors $f(x) = p(x)q(x)$ et donc $p(x)$ et $q(x)$ n'ont aucune racine dans $F$. Ainsi $\deg p(x) \neq 1$ et $\deg q(x) \neq 1$. Mais cela contredit le fait que $\deg p(x) + \deg q(x) = \deg f(x)$ est égal à 2 ou 3. Donc $f(x)$ est irréductible. L'implication réciproque découle de la partie (a). □

*Exemple* 2.2.8. Le polynôme $x^2 - 2$ est irréductible sur $\mathbb{Q}$ mais il est réductible sur $\mathbb{R}$ puisque il a des racines dans $\mathbb{R}$ mais pas dans $\mathbb{Q}$.

*Exemple* 2.2.9. Le polynôme $x^2 + 1$ est irréductible dans $\mathbb{R}[x]$ mais il est réductible dans $\mathbb{C}[x]$.

*Exemple* 2.2.10. Le polynôme $x^3 + 2x^2 + x + 2$ est irréductible dans $\mathbb{Z}_5[x]$ puisque il n'a aucune racine.

*Exemple* 2.2.11. Le polynôme $x^2 - 2$ est réductible dans $\mathbb{R}[x]$ mais il est irréductible dans $\mathbb{Z}_3[x]$. Le polynôme $x^2 + 2$ est irréductible dans $\mathbb{R}[x]$ mais il est réductible dans $\mathbb{Z}_3[x]$ (en particulier, $x^2 + 2 = (x-1)(x+1)$ dans $\mathbb{Z}_3[x]$).

**Théorème 2.2.12** (Théorème fondamental de l'algèbre)**.** *Si $f(x) \in \mathbb{C}[x]$ est un polynôme non constant, alors $f(x)$ a une racine dans $\mathbb{C}$.*

Nous accepterons le théorème fondamental de l'algèbre sans preuve. Pour ceux qui s'intéressent à la lecture de la preuve, elle peut être trouvée dans [Jud19, Th. 23.33].

**Corollaire 2.2.13.** *Supposons que $f(x) \in \mathbb{C}[x]$ avec $\deg f(x) \geq 1$. Si on écrit $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_n \neq 0$, alors $f(x)$ se factorise en $f(x) = a_n(x - z_1)(x - z_2)\cdots(x - z_n)$, où $z_1, \ldots, z_n$ sont les racines de $f(x)$, comptées selon la multiplicité. En particulier, les seuls polynômes irréductibles dans $\mathbb{C}[x]$ sont linéaires.*

*Démonstration.* La preuve est par récurrence sur le degré de $f(x)$, en utilisant le théorème fondamental de l'algèbre (le théorème 2.2.12). Les détailles sont laissés en l'exercice 2.2.1. □

**Théorème 2.2.14.** *Si $f(x) \in \mathbb{R}[x]$ est un polynôme non constant, alors il se factorise (dans $\mathbb{R}[x]$) en un produit des polynômes de degrés au plus deux. En particulier, les polynômes irréductibles dans $\mathbb{R}[x]$ sont soit linéaires soit quadratiques.*

*Démonstration.* La preuve est par récurrence sur $\deg f(x)$. Le cas $\deg f(x) \leq 2$ est immédiat. Supposons que le résultat soit vrai pour les polynômes de degré $\leq n$ et considérons $f(x)$ avec $\deg f(x) = n+1$. Il y a deux cas.

(a) S'il existe $z \in \mathbb{R}$ tel que $f(z) = 0$, alors $f(x) = (x-z)g(x)$ et $\deg g(x) = n$. Le résultat découle alors par l'hypothèse de récurrence appliquée à $g(x)$.

(b) Sinon, $f(x)$ n'a aucune racine réellle. D'après le théorème fondamental de l'algèbre (le théorème 2.2.12), il a une racine complexe $z$. Alors $f(z) = 0$ et donc $f(\bar{z}) = \overline{f(z)} = \bar{0} = 0$. (Ici $\bar{z}$ désigne le conjugué complexe de $z$.) Par conséquent,

$$f(x) = (x-z)(x-\bar{z})g(x) = \underbrace{(x^2 - (z+\bar{z})x + z\bar{z})}_{\in \mathbb{R}[x]} g(x),$$

et le résultat découle encore une fois en appliquant l'hypothèse de récurrence à $g(x)$. □

Si $\alpha\colon R \to S$ est un morphisme d'anneaux, alors on a un morphisme d'anneaux induit

$$R[x] \to S[x], \quad \sum a_i x^i \mapsto \sum \alpha(a_i) x^i, \quad a_i \in \mathbb{R}.$$

En particulier, si $p$ est un nombre premier et $\alpha$ est le morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}_p$, $\alpha(x) = \bar{x}$, on obtient un morphisme d'anneaux $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ appelé la *réduction modulo $p$*.

**Théorème 2.2.15** (Lemme de Gauss)**.** *Soit $f(x) = g(x)h(x)$ dans $\mathbb{Z}[x]$. Si un nombre premier $p \in \mathbb{Z}$ divise tout coefficient de $f(x)$, alors $p$ divise tout coefficient de $g(x)$ ou $p$ divise tout coefficient de $h(x)$.*

*Démonstration.* Considérons la réduction modulo $p$, $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $\varphi(\sum a_i x^i) = \sum \bar{a}_i x^i$. Soit $\bar{f}(x) = \varphi(f(x))$. Si un nombre premier $p$ divise tout coefficient de $f(x)$, alors $\bar{f}(x) = 0$ dans $\mathbb{Z}_p[x]$. Ainsi $0 = \bar{g}(x)\bar{h}(x)$. Puisque $\mathbb{Z}_p$ est un corps, $\mathbb{Z}_p[x]$ est un anneau intègre d'après le théorème 2.1.9(d). Donc $\bar{g}(x) = 0$ ou $\bar{h}(x) = 0$. Mais cela implique que tout coefficient de $g(x)$ est zéro dans $\mathbb{Z}_p$ ou tout coefficient de $h(x)$ est zéro dans $\mathbb{Z}_p$. □

**Définition 2.2.16** (Décomposition propre)**.** Soit $f(x) \in \mathbb{Z}[x]$ un polynôme non constant. Une *décomposition propre* de $f(x)$ est une décomposition $f(x) = g(x)h(x)$, où $g(x), h(x) \in \mathbb{Z}[x]$ avec $\deg g(x), \deg h(x) > 0$.

**Théorème 2.2.17.** *Supposons que $f(x)$ est un polynôme non constant dans $\mathbb{Z}[x]$.*

*(a) Si $f(x) = g(x)h(x)$ avec $g(x), h(x) \in \mathbb{Q}[x]$, alors il existe $g_0(x), h_0(x) \in \mathbb{Z}[x]$ avec $\deg g_0(x) = \deg g(x)$ et $\deg h_0(x) = \deg h(x)$ tels que $f(x) = g_0(x)h_0(x)$.*

*(b) Le polynôme $f(x)$ est irréductible dans $\mathbb{Q}[x]$ si et seulement si il n'a aucune décomposition propre dans $\mathbb{Z}[x]$.*

*Démonstration.* (a) Soient $a$ et $b$ les plus petits communs multiples des dénominateurs des coefficients de $g(x)$ et $h(x)$, respectivement. Alors $g_1(x) := ag(x) \in \mathbb{Z}[x]$ et $h_1(x) := bh(x) \in \mathbb{Z}[x]$. Donc, on a

$$abf(x) = g_1(x)h_1(x)$$

dans $\mathbb{Z}[x]$. Supposons que $p$ soit un nombre premier qui divise $ab$. Alors, d'après le lemme de Gauss (le théorème 2.2.15), $p$ divise tous le coefficients de $g_1(x)$ ou il divise tous les coefficients de $h_1(x)$. Ainsi nous pouvons éliminer $p$ et nous obtenons

$$\frac{ab}{p}f(x) = g_2(x)h_2(x)$$

dans $\mathbb{Z}[x]$. Si nous continuons comme cela, nous pouvons éliminer tout facteur premier de $ab$ et nous obtenons un factorisation

$$f(x) = g_k(x)h_k(x)$$

dans $\mathbb{Z}[x]$. Alors le résultat s'ensuit puisque $\deg g(x) = \deg g_1(x) = \cdots = \deg g_k(x)$ et, de façon similaire, $\deg h(x) = \deg h_k(x)$.

(b) Si $f(x)$ est irréductible dans $\mathbb{Q}[x]$, alors il n'a aucun factorisation propre dans $\mathbb{Z}[x]$, puisqu'un tel factorisation serait aussi un factorisation dans $\mathbb{Q}[x]$. L'implication réciproque découle de la partie (a). □

**Théorème 2.2.18** (Test d'irréductibilité modulaire)**.** *Soient $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $n \geq 1$, $a_n \neq 0$. Supposons qu'il existe un nombre premier $p$ tel que*

*(a) $p \nmid a_n$ et*

*(b) la réduction de $f(x)$ modulo $p$ est irréductible dans $\mathbb{Z}_p[x]$.*

*Alors $f(x)$ est irréductible dans $\mathbb{Q}[x]$.*

*Démonstration.* La première condition nous donne que $\deg \bar{f}(x) = \deg f(x)$. Supposons que $f(x)$ soit réductible dans $\mathbb{Q}[x]$. Alors il existe une décomposition propre $f(x) = g(x)h(x)$ dans $\mathbb{Z}[x]$ d'après le théorème 2.2.17. Alors

$$\deg \bar{g}(x) \leq \deg g(x) < \deg f(x) = \deg \bar{f}(x).$$

De même façon, $\deg \bar{h}(x) < \deg \bar{f}(x)$. Puisque $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$, cela contredit l'irréductibilité de $\bar{f}(x)$ in $\mathbb{Z}_p[x]$. □

*Exemple* 2.2.19. On montre que $f(x) = 4x^4 - 3x^2 - 2x - 1$ est irréductible dans $\mathbb{Q}[x]$. On applique le théorème 2.2.18 avec $p = 3$. Supposons que $\bar{f}(x) = x^4 + x + \bar{2} = \bar{g}(x)\bar{h}(x)$ dans $\mathbb{Z}_3[x]$. Alors $\deg \bar{g}(x) + \deg \bar{h}(x) = 4$. Supposons, sans perte de généralité, que $\deg \bar{g}(x) \leq \deg \bar{h}(x)$. Alors $\deg \bar{g}(x) \leq 2$.

Il n'est pas possible que $\deg \bar{g}(x) = 1$, puisque $x^4 + x + \bar{2}$ n'a aucune racine dans $\mathbb{Z}_3$. donc il reste à considérer le cas où $x^4 + x + \bar{2}$ se factorise en un produit de deux polynômes quadratiques dans $\mathbb{Z}_3[x]$. Donc supposons que, dans $\mathbb{Z}_3[x]$, on a

$$x^4 + x + \bar{2} = (x^2 + ax + b)(x^2 + cx + d).$$

Cela implique que

$$bd = \bar{2}, \quad ad + bc = \bar{1}, \quad b + d + ac = \bar{0}, \quad a + c = \bar{0}. \tag{2.1}$$

La première équation implique que $b = \bar{2}d^{-1}$ et la quatrième implique que $a = -c$. La substitution dans la troisième équation donne alors

$$\bar{2}d^{-1} + d - c^2 = 0 \implies \bar{2} + d^2 = c^2 d. \tag{2.2}$$

D'autre part, en remplaçant dans la deuxième équation de (2.1) donne

$$ad + \bar{2}cd^{-1} = \bar{1} \implies ad^2 + \bar{2}c = d \implies (\bar{2} - d^2)c = d.$$

Puisque $bd = \bar{2}$, on a $d \neq \bar{0}$, et donc ce qui précède implique que $c \neq \bar{0}$. Ainsi $c$ est égal à $\bar{1}$ ou $\bar{2}$. Dans les deux cas, on a $c^2 = \bar{1}$ et donc (2.2) devient $2 + d^2 = d$. D'où $d^2 - d + \bar{2} = \bar{0}$. Mais cette équation n'a aucune racine dans $\mathbb{Z}_3$. Cette contradiction termine la démonstration.

**Théorème 2.2.20** (Critère d'Eisenstein)**.** *Soit $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, $n \geq 1$, $a_n \neq 0$. Supposons qu'il existe un nombre premier $p$ tel que*

*(a) $p$ divise tous les éléments $a_0, \ldots, a_{n-1}$,*
*(b) $p$ ne divise pas $a_n$, et*
*(c) $p^2$ ne divise pas $a_0$.*

*Alors $f(x)$ est irréductibles dans $\mathbb{Q}[x]$.*

*Démonstration.* Supposons, vers une contradiction, que $f(x)$ n'est pas irréductible dans $\mathbb{Q}[x]$. Alors, d'après le théorème 2.2.17, on a une décomposition propre $f(x) = g(x)h(x)$ dans $\mathbb{Z}[x]$. Soient

$$g(x) = b_0 + b_1 x + \cdots + b_s x^s \quad \text{et} \quad h(x) = c_0 + c_1 x + \cdots + c_t x^t,$$

avec $b_s, c_t \neq 0$.

— Puisque $p | b_0 c_0$, mais $p^2 \nmid a_0 = b_0 c_0$, on a que $p$ divise exactement l'un de $b_0$ ou $c_0$. Sans perte de généralité, supposons que $p | b_0$ mais $p \nmid c_0$.
— Puisque $p \nmid a_n = b_s c_t$, on a $p \nmid b_s$.
— Soit $k$ le plus petit entier tel que $p \nmid b_k$. Donc $0 < k \leq s < n$.
— L'égalisation des coefficients de $x^k$ dans $f(x) = g(x)h(x)$ donne

$$a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k.$$

On sait que $p$ divise $a_k$ par hypothèse. Aussi, par notre choix de $k$, $p$ divise chaque terme de la somme après le premier. Ainsi $p$ divise également $b_k c_0$. Puisque $p$ est premier, il faut qu'il divise $b_k$ ou $c_0$, ce qui est une contradiction. □

*Exemple* 2.2.21. Le polynôme $2x^7 - 5x^4 + 10x^2 - 15$ est irréductible dans $\mathbb{Q}[x]$. On peut voir cela en utilisant le critère d'Eisenstein (le théorème 2.2.20) avec $p = 5$.

*Exemple* 2.2.22. Le polynôme $f(x) = x^4 + x^3 + x^2 + x + 1$ est irréductible dans $\mathbb{Q}[x]$. Pour voir cela, notez premièrement que $f(x)(x-1) = x^5 - 1$. Ainsi,

$$f(x+1) = \frac{(x+1)^5 - 1}{(x+1) - 1} = \frac{(x+1)^5 - 1}{x} = x^4 + 5x^3 + 10x^2 + 10x + 5.$$

Puis on voit que $f(x+1)$ ne se factorise pas par le critère d'Eisenstein (le théorème 2.2.20) avec $p = 5$. Par conséquent, $f(x)$ ne se factorise non plus, puisque si $f(x) = g(x)h(x)$, alors $f(x+1) = g(x+1)h(x+1)$.

*Exemple* 2.2.23. Si $p$ est un nombre premier, alors $x^{p-1} + x^{p-2} + \cdots + x + 1$ est appelé un *polynôme cyclotomique*. En utilisant l'argument de l'exemple 2.2.22, on peut montrer que ce polynôme est irréductible.

**Théorème 2.2.24.** *Soient $F$ un corps et $f(x), g(x) \in F[x] \setminus \{0\}$. Alors il existe un est un seul polynôme $d(x) \in F[x] \setminus \{0\}$ tel que*

*(a) $d(x)$ est unitaire,*
*(b) $d(x)|f(x)$ et $d(x)|g(x)$,*
*(c) si $h(x) \in F[x]$ satisfait $h(x)|f(x)$ et $h(x)|g(x)$, alors $h(x)|d(x)$,*
*(d) il existe $u(x), v(x) \in F[x]$ tels que $d(x) = u(x)f(x) + v(x)g(x)$.*

*Démonstration.* Soit $d(x)$ un polynôme unitaire dans $\{u(x)f(x) + v(x)g(x) : u(x), v(x) \in F[x]\}$ de plus petit degré. Alors (a), (c) et (d) sont claires. Pour voir (b), on divise $f(x)$ par $d(x)$ pour obtenir $f(x) = q(x)d(x) + r(x)$ avec $r(x) = 0$ ou $\deg r(x) < \deg d(x)$. Puis, si on écrit $d(x) = u(x)f(x) + v(x)g(x)$ avec $u(x), v(x) \in F[x]$, on a

$$r(x) = f(x) - q(x)d(x) = f(x)(1 - q(x)u(x)) + g(x)(-q(x)v(x)).$$

Ainsi, par notre choix de $d(x)$, on ne peut pas avoir $\deg r(x) < \deg d(x)$. Par conséquent, $r(x) = 0$ et donc $d(x)|f(x)$. La preuve que $d(x)|g(x)$ est similaire. Ainsi (b) est démontré.

Il reste à montrer l'unicité. Supposons que $d_1(x)$ et $d_2(x)$ satisfassent les conditions données. Puis, $d_1(x)|d_2(x)$ et $d_2(x)|d_1(x)$. Ainsi

$$\text{il existe } k_1(x), k_2(x) \in F[x] \text{ tel que } d_1(x) = d_2(x)k_1(x) \text{ et } d_2(x) = d_1(x)k_2(x).$$

Donc $d_1(x) = d_1(x)k_2(x)k_1(x)$. Ainsi $k_1(x)k_2(x) = 1$, ce qui implique que $k_1(x)$ et $k_2(x)$ sont des polynômes constants. Mais puisque $d_1(x)$ et $d_2(x)$ sont tous les deux unitaires, il faut que $k_1(x) = k_2(x) = 1$. Par conséquent, $d_1(x) = d_2(x)$. □

**Définition 2.2.25** (Plus grand commun diviseur des polynômes)**.** Le polynôme $d(x)$ dont l'existence est affirmée dans le théorème 2.2.24 est appelé le *plus grand commun diviseur* de $f(x)$ et $g(x)$ et il est noté $\operatorname{pgcd}(f(x), g(x))$.

**Algorithme 2.2.26** (Algorithme d'Euclide)**.** Soient $f(x), g(x) \in F[x]$ avec $g(x) \neq 0$. Prenez $a_1(x) = f(x)$ et $a_2(x) = g(x)$. Par division polynomiales répétée, on a

$$\begin{cases} a_1(x) = q_1(x)a_2(x) + a_3(x) & \text{avec } a_3(x) \neq 0 \text{ et } \deg a_3(x) < \deg a_2(x), \\ a_2(x) = q_2(x)a_3(x) + a_4(x) & \text{avec } a_4(x) \neq 0 \text{ et } \deg a_4(x) < \deg a_3(x), \\ \quad \dots & \dots \\ a_{k-2}(x) = q_{k-2}(x)a_{k-1}(x) + a_k(x) & \text{avec } a_k(x) \neq 0 \text{ et } \deg a_k(x) < \deg a_{k-1}(x), \\ a_{k-1}(x) = q_{k-1}(x)a_k(x). & \end{cases}$$

Alors $\operatorname{pgcd}(f(x), g(x)) = \frac{1}{c}a_k(x)$, où $c$ est le coefficient dominant de $a_k(x)$. Une démonstration de ce résultat est présentée dans l'exercice 2.2.3.

*Exemple* 2.2.27. Dans $\mathbb{Q}[x]$, on a $\operatorname{pgcd}(x^2+1, 2x-1) = 1$ et $\operatorname{pgcd}(x^4-2x^2+1, 2x^2-2) = x^2-1$.

**Proposition 2.2.28.** *Soient $F$ un corps, $p(x) \in F[x]$ un polynôme irréductible, et $f_1(x), \dots, f_n(x) \in F[x]$. Si $p(x) | f_1(x) \cdots f_n(x)$, alors il existe $1 \leq i \leq n$ tel que $p(x) | f_i(x)$.*

*Démonstration.* On démontre le résultat par récurrence. Le cas $n = 1$ est claire. Maintenant considérez le cas $n = 2$. Supposons que $p(x)$ divise $f_1(x)f_2(x)$. Soit $d(x) = \operatorname{pgcd}(p(x), f_1(x))$. Alors $d(x) | p(x)$ et donc, puisque $p(x)$ est irréductible, on a $\deg d(x) = 0$ (donc $d(x) = 1$) ou $\deg d(x) = \deg p(x)$. Si $\deg d(x) = \deg p(x)$, alors il existe un élément non nul $a \in F$ tel que $p(x) = ad(x)$, et donc $p(x)$ divise $f_1(x)$ puisque $d(x)$ divise $f_1(x)$. D'autre part, si $d(x) = 1$, alors

$$\text{il existe } u(x), v(x) \in F[x] \text{ tels que } u(x)p(x) + v(x)f_1(x) = 1$$

d'après le théorème 2.2.24. Ainsi $u(x)p(x)f_2(x) + v(x)f_1(x)f_2(x) = f_2(x)$. Par conséquent, $p(x)$ divise $f_2(x)$ puisqu'il divise $f_1(x)f_2(x)$. Ainsi le résultat est vrai pour $n = 2$.

Si $n > 2$, alors $p(x) | f_1(x)f_2(x) \cdots f_n(x)$ implique $p(x) | f_1(x)$ ou $p(x) | f_2(x) \cdots f_n(x)$ (en utilisant le cas $n = 2$). Puis le résultat est vrai par l'hypothèse de récurrence. □

**Corollaire 2.2.29.** *Si $F$ est un corps et $p(x) \in F[x]$ est irréductible, alors $\langle p(x) \rangle$ est un idéal premier de $F[x]$.*

*Démonstration.* Supposons que $p(x)$ soit irréductible et $f(x)g(x) \in \langle p(x) \rangle$. Alors $p(x) | f(x)g(x)$. Ainsi, d'après la proposition 2.2.28, $p(x)$ divise $f(x)$ ou $g(x)$, ce qui implique que $f(x) \in \langle p(x) \rangle$ ou $g(x) \in \langle p(x) \rangle$. □

*Exemple* 2.2.30. On a que $\langle x^2 + x + 1 \rangle$ est un idéal premier de $\mathbb{Z}_2[x]$. Nous verrons plus tard que $\langle p(x) \rangle$ est en fait un idéal maximal de $F[x]$ chaque fois que $p(x)$ est irréductible (voir le théorème 2.3.6).

**Théorème 2.2.31** (Théorème de factorisation unique)**.** *Soient $F$ un corps et $f(x) \in F[x]$ un polynôme non constant. Alors*

*(a) $f(x) = ap_1(x) \cdots p_m(x)$ où $a \in F^\times$ et $p_1(x), \dots, p_m(x) \in F[x]$ sont irréductibles et unitaires, et*

*(b) le factorisation de la partie (a) est unique sauf qu'on peut réordonner les $p_i(x)$'s.*

*Démonstration.* (a) Nous démontrons le résultat par récurrence sur $n = \deg f(x)$. Le cas $n = 1$ est claire puisque les polynômes de degré un sont irréductibles. Supposons que le résultat soit vrai pour $n$ et considérons un polynôme $f(x)$ de degré $n+1$. Si $f(x)$ est irréductible, on a fini. Sinon, nous pouvons factoriser $f(x) = g(x)h(x)$ avec $\deg g(x), \deg h(x) \leq n$. Alors le résultat découle de l'hypothèse de récurrence.

(b) Supposons qu'on a deux décompositions

$$f(x) = ap_1(x)\cdots p_m(x) = bq_1(x)\cdots q_\ell(x), \tag{2.3}$$

avec $a, b \in F^\times$ et $p_1(x), \ldots, p_m(x), q_1(x), \cdots, q_\ell(x)$ irréductibles et unitaires. En considérant les coefficients dominants, nous voyons que $a = b$. Maintenant, $p_1(x) | q_1(x)\cdots q_\ell(x)$, et donc il existe $1 \leq i \leq \ell$ tel que $p_1(x)|q_i(x)$ d'après la proposition 2.2.28. Ainsi $p_1(x) = q_i(x)$ puisque les deux sont unitaires et irréductibles. En éliminant $p_1(x)$ et $q_i(x)$ dans (2.3), on obtient

$$p_2(x)\cdots p_m(x) = q_1(x)\cdots q_{i-1}(x)q_i(x)\cdots q_\ell(x).$$

Le théorème s'ensuit après un répétition de l'argument ci-dessus. □

---

## Exercices.

2.2.1. Démontrer le corollaire 2.2.13.

2.2.2. Montrer que si $p$ est un nombre premier, alors le polynôme cyclotomique $x^{p-1} + x^{p-2} + \cdots + x + 1$ est irréductible. Voir l'exemple 2.2.23.

2.2.3. Soient $f(x), g(x) \in F[x]$, avec $g(x) \neq 0$.

(a) Montrer que l'algorithme 2.2.26 se termine après un nombre fini d'étapes.
(b) Avec la notation de cet algorithme, montrer que $\operatorname{pgcd}(a_i(x), a_{i+1}(x)) = \operatorname{pgcd}(a_{i+1}(x), a_{i+2}(x))$ pour tout $i = 1, \ldots, k-2$.
(c) Avec la même notation, montrer que $\operatorname{pgcd}(a_{k-1}(x), a_k(x)) = \frac{1}{c}a_k(x)$.
(d) Conclure que $\operatorname{pgcd}(f(x), g(x)) = \frac{1}{c}a_k(x)$.

2.2.4 ([Nic12, Ex. 4.2.1]). (a) Si $F$ est un corps et $a \in F$, $a \neq 0$, montrer que $a$ divise $f$ pour tout $f \in F[x]$.
(b) Si $p \in F[x]$ divise $f$ pour tout $f \in F[x]$, montrer que $p \in F$, $p \neq 0$.

2.2.5 ([Nic12, Ex. 4.2.2]). Si $f, g \in F[x]$ et $F$ est un corps, considerer les affirmations suivantes :

(a) il existe $0 \neq a \in F$ tel que $f = ag$ ;
(b) $f$ et $g$ ont les même racines dans $F$.

Démontrer que (a) $\implies$ (b). Est-ce que (b) $\implies$ (a) ? Justifier votre réponse.

2.2.6 ([Nic12, Ex. 4.2.3]). Dans chaque cas, expliquer pourquoi $f$ est réductible sur tout corps.

(a) $f = x^3 - 2x^2 + 3x - 2$
(b) $f = x^3 + x^2 + 4$

2.2.7 ([Nic12, Ex. 4.2.4]). Dans chaque cas, déterminer si le polynôme est irréductible. Justifier votre réponse.

(a) $x^3 + 5$ dans $\mathbb{Z}_7[x]$
(b) $x^2 - 2$ dans $\mathbb{R}[x]$
(c) $x^2 + 11$ dans $\mathbb{C}[x]$
(d) $x^3 - 4$ dans $\mathbb{Z}_{11}[x]$
(e) $x^3 + x + 1$ dans $\mathbb{Z}_5[x]$
(f) $x^2 + x + 1$ dans $\mathbb{Z}_{17}[x]$

2.2.8 ([Nic12, Ex. 4.2.5]). Dans chaque cas, déterminer si le polynôme est irréductible sur chaque des corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, et $\mathbb{Z}_7$.

(a) $x^2 - 3$
(b) $x^2 + x + 1$
(c) $x^3 + x + 1$
(d) $x^3 - 2$

2.2.9 ([Nic12, Ex. 4.2.6]). Soit $R$ un anneau intègre et soit $f \in R[x]$ un polynôme unitaire. Si $f$ se factorise dans $R[x]$, montrer qu'il a un décomposition $f = gh$, où $g$ et $h$ sont tous les deux unitaires (et de degré positif).

2.2.10 ([Nic12, Ex. 4.2.8]). (a) Si $x^2 + ax + b$ a des racines $u$ et $v$ dans un corps $F$, montrer que $b = uv$ et $a = -(u + v)$.

(b) Montrer que $1 + i$ est une racine de $x^2 + (1 - 2i)x - (3 + i) \in \mathbb{C}[x]$. Trouver l'autre racine.

2.2.11 ([Nic12, Ex. 4.2.9]). Montrer qu'un polynôme de degré impair dans $\mathbb{R}[x]$ a une racine réelle. (Il faut utiliser le calcul différentiel.)

2.2.12 ([Nic12, Ex. 4.2.10]). Trouver tous les polynômes cubiques, unitaires, et irréductibles dans $\mathbb{Z}_2[x]$.

2.2.13 ([Nic12, Ex. 4.2.12]). Soit $p(x)$ un polynôme unitaire de degré quatre dans $\mathbb{Z}_2[x]$. Montrer que $p(x)$ est irréductible dans $\mathbb{Z}_2[x]$ si et seulement si

(a) $p(x)$ n'a aucune racine dans $\mathbb{Z}_2$, et
(b) $p(x) \neq x^4 + x^2 + 1$.

*Indice* : l'exercice 2.2.8.

2.2.14 ([Nic12, Ex. 4.2.13]). Montrer qu'un polynôme unitaire $p(x)$ de degré 5 dans $\mathbb{Z}_2[x]$ est irréductible si et seulement si

(a) $p(x)$ n'a aucune racine dans $\mathbb{Z}_2$, et
(b) $p(x)$ n'est ni $x^5+x^4+1$ ni $x^5+x+1$.

*Indice* : l'exercice 2.2.12.

2.2.15 ([Nic12, Ex. 4.2.18]). Dans chaque cas, factoriser $f(x)$ comme produit des polynômes irréductibles dans $F[x]$.

(a) $f(x)=3x^4+2$, $F=\mathbb{Z}_5$
(b) $f(x)=3x^4+2$, $F=\mathbb{Z}_{11}$
(c) $f(x)=x^3+2x^2+2x+1$, $F=\mathbb{Z}_7$
(d) $f(x)=x^3+2x^2+2x+1$, $F=\mathbb{Z}_3$
(e) $f(x)=x^4-x^2+x-1$, $F=\mathbb{Z}_{13}$.
(f) $f(x)=x^4-x^2+x-1$, $F=\mathbb{Z}_{17}$.

2.2.16 ([Nic12, Ex. 4.2.19]). Factoriser $x^5+x^4+1$ comme produit des polynômes irréductibles dans $\mathbb{Z}_2[x]$.

2.2.17 ([Nic12, Ex. 4.2.20]). Factoriser $x^5+x^2-x+1$ comme produit des polynômes irréductibles dans $\mathbb{Z}_3[x]$.

2.2.18 ([Nic12, Ex. 4.2.21]). Montrer que chaque polynôme est irréductible dans $\mathbb{Q}[x]$.

(a) $3x^3+5x^2+x+2$
(b) $5x^3+2x+3$
(c) $x^3+9x^2+x+6$
(d) $x^3+x^2+10x+8$

2.2.19 ([Nic12, Ex. 4.2.22]). Montrer que chaque polynôme est irréductible dans $\mathbb{Q}[x]$.

(a) $x^5+6x^4+12x+15$
(b) $4x^5+28x^4+7x^3-28x^2+14$

2.2.20 ([Nic12, Ex. 4.2.24]). Montrer que $f(x)=x^4+4x^3+4x^2+4x+5$ est irréductible sur $\mathbb{Q}$ en considérant $f(x-1)$.

2.2.21 ([Nic12, Ex. 4.2.29]). Montrer que $x^n-p$ est irréductible dans $\mathbb{Q}[x]$ pour tout $n\geq 2$ et tout nombre premier $p\in\mathbb{Z}$. (Ainsi $\mathbb{Q}[x]$ a un nombre infini de polynômes irréductibles de chaque degré $\geq 2$.)

2.2.22 ([Nic12, Ex. 4.2.30]). Supposons que $p$ soit un nombre premier. Montrer que $x^p-a$ est réductible dans $\mathbb{Z}_p[x]$ pour tout $a\in\mathbb{Z}_p$.

2.2.23 ([Nic12, Ex. 4.2.31]). Soient $F\subseteq K$ des corps et $f,g\in F[x]$.

(a) Si $f$ est irréductible dans $K[x]$, montrer qu'il est irréductible dans $F[x]$.
(b) Si $f$ et $g$ sont premiers entre eux dans $F[x]$ (c.-à-d. les plus grand commun diviseur est 1), montrer qu'ils sont premiers entre eux dans $K[x]$. *Indice* : le théorème 2.2.24(d).

2.2.24 ([Nic12, Ex. 4.2.34]). Soit $f=x^3-42x^2+35x+m$. Montrer qu'il existe un nombre infini d'entiers $m$ pour lesquels $f$ est irréductible dans $\mathbb{Q}[x]$. *Indice* : le critère d'Eisenstein.

2.2.25 ([Nic12, Ex. 4.2.36]). Si $m$ et $p$ sont des entiers, avec $p$ premier, montrer que $x^4+mx+p$ est irréductible dans $\mathbb{Q}[x]$ si et seulement s'il n'aucune racine dans $\mathbb{Q}$.

2.2.26 ([Nic12, Ex. 4.2.39]). Dans chaque cas, calculer $d = \operatorname{pgcd}(f, g)$, et l'écrire dans $F[x]$ comme combinaison linéaire de $f$ et $g$.

(a) $f = x^2 + 2$, $g = x^3 + 4x^2 + x + 1$, $F = \mathbb{Z}_5$
(b) $f = x^2 + 1$, $g = x^5 + x^4 + x^3 + x^2 + x + 1$, $F = \mathbb{Z}_2$
(c) $f = x^2 - x - 2$, $g = x^5 - 4x^3 - 2x^2 + 7x - 6$, $F = \mathbb{Q}$
(d) $f = x^3 + x - 2$, $g = x^5 - x^4 + 2x^2 - x - 1$, $F \in \mathbb{Q}$

## 2.3 Anneaux quotients de polynômes sur un corps

Le résultat suivant indique que, si $F$ est un corps, tous les idéaux dans $F[x]$ sont principaux.

**Théorème 2.3.1.** *Soit $F$ un corps et soit $I$ un idéal non nul de $F[x]$. Alors il existe un polynôme unitaire unique $h(x) \in F[x]$ tel que $I = \langle h(x)\rangle = h(x)F[x] = \{h(x)g(x) : g(x) \in F[x]\}$.*

*Démonstration.* Soit $I$ un idéal non nul de $F[x]$. Alors $I$ contient des polynômes non nul et donc il contient des polynômes unitaires (puisqu'il est un idéal, on peut multiplier tout polynôme par l'inverse du coefficient dominant pour obtenir un polynôme unitaire dans $I$). Parmi tous les polynômes unitaires dans $I$, choisissons $h(x)$ de degré minimal. Alors $\langle h(x)\rangle \subseteq I$.

Maintenant supposons que $f(x) \in I$. D'après l'algorithme d'Euclide (l'algorithme 2.2.26), on a $f(x) = q(x)h(x) + r(x)$ avec $q(x), r(x) \in F[x]$ et $r(x) = 0$ ou $\deg r(x) < \deg h(x)$. Supposons que $r(x) \neq 0$ et soit $a$ le coefficient dominant de $r(x)$. Alors $a^{-1}r(x)$ est unitaire et

$$a^{-1}r(x) = a^{-1}(h(x) - q(x)f(x)) \in I.$$

Mais $\deg(a^{-1}r(x)) = \deg r(x) < \deg h(x)$, ce qui contredit notre choix de $h(x)$. Ainsi $r(x) = 0$ et donc $I = \langle h(x)\rangle$.

Pour démontrer l'unicité, supposons que $\langle h_1(x)\rangle = \langle h_2(x)\rangle \neq 0$, où $h_1(x)$ et $h_2(x)$ sont unitaires. Alors il existe $f_1(x), f_2(x) \in F[x]$ tel que

$$h_1(x) = f_1(x)h_2(x) \quad \text{et} \quad h_2(x) = f_2(x)h_1(x).$$

Ainsi $h_1(x) = f_1(x)f_2(x)h_1(x)$, ce qui implique que $\deg f_1(x) = \deg f_2(x) = 0$. Par conséquent, $f_1(x) \in F$. Puisque $h_1(x)$ et $h_2(x)$ sont tous les deux unitaires, on a $f_1(x) = 1$. Donc $h_1(x) = h_2(x)$. □

*Exemple* 2.3.2. Considérons l'anneau $\mathbb{R}[x]$ et soit $I = \langle x^2 + 1\rangle$. Nous pouvons diviser tout $f(x) \in \mathbb{R}[x]$ par $x^2+1$ pour obtenir $f(x) = q(x)(x^2+1)+(ax+b)$ pour un polynôme unique $q(x) \in \mathbb{R}[x]$ et $a, b \in \mathbb{R}$. Ainsi, tout élément de $\mathbb{R}[x]/I$ peut être écrit uniquement sous la

forme $(ax+b)+I$. On a $(ax+b)+I=(a'x+b')+I$ si et seulement si $a=a'$ and $b=b'$. De plus, on a

$$((ax+b)+I)+((a'x+b')+I)=((a+a')x+(b+b'))+I,$$
$$((ax+b)+I)((a'x+b')+I)=(aa'x^2+ab'x+a'bx+bb')+I=((a'b+ab')x+(bb'-aa'))+I.$$

Ainsi on a un isomorphisme $\mathbb{R}[x]/I\cong\mathbb{C}$, $ax+b\mapsto ai+b$.

L'exemple ci-dessus est un cas spécial du théorème suivant général. Vous pouvez trouver la démonstration dans [Nic12, §4.3].

**Théorème 2.3.3.** *Soient $F$ un corps, $h(x)\in F[x]$, et $I=\langle h(x)\rangle$. Supposons que $n=\deg h(x)$. Alors tout élément de $R=F[x]/I$ a une représentative unique de degré $\leq n-1$. Ainsi l'anneau quotient $R=F[x]/I$ est donné par*

$$R\cong\{a_0+a_1t+\cdots+a_{n-1}t^{n-1}:a_0,\ldots,a_{n-1}\in F\}$$

*(isomorphisme d'espaces vectoriels).*

Dans le théorème 2.3.3, $t$ correspond à $x+I$. L'addition dans la représentation de $R$ donné dans le théorème 2.3.3 est donnée par l'addition des coefficients. La multiplication est calculée en utilisant le fait que $h(t)=0$. Cela nous permet d'exprimer $t^n$ en termes des puissances inférieures de $t$.

*Exemple* 2.3.4. Considérons l'anneau quotient $\mathbb{Z}_2[x]/\langle x^2\rangle$. D'après le théorème 2.3.3, on a

$$\mathbb{Z}_2[x]/\langle x^2\rangle\cong\{at+b:a,b\in\mathbb{Z}_2\}=\{\bar{0},\bar{1},t,\bar{1}+t\}.$$

Quand on calcul dans cet anneau, on utilise le fait que $t^2=h(t)=0$. Ainsi on a les tables d'addition et de multiplication suivants.

| $+$ | $\bar{0}$ | $\bar{1}$ | $t$ | $\bar{1}+t$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $t$ | $\bar{1}+t$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ | $\bar{1}+t$ | $t$ |
| $t$ | $t$ | $\bar{1}+t$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}+t$ | $\bar{1}+t$ | $t$ | $\bar{1}$ | $\bar{0}$ |

| $\times$ | $\bar{0}$ | $\bar{1}$ | $t$ | $\bar{1}+t$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $t$ | $\bar{1}+t$ |
| $t$ | $\bar{0}$ | $t$ | $\bar{0}$ | $t$ |
| $\bar{1}+t$ | $\bar{0}$ | $\bar{1}+t$ | $t$ | $\bar{1}$ |

Notez que cet anneau n'est pas un corps puisque, par example, l'élément non nul $t$ n'est pas inversible.

*Exemple* 2.3.5. Considérez l'anneau quotient $\mathbb{Z}_2[x]/\langle x^2+x+\bar{1}\rangle$. D'après le théorème 2.3.3, on a un isomorphism d'espaces vectoriels

$$\mathbb{Z}_2[x]/\langle x^2+x+\bar{1}\rangle\cong\{at+b:a,b\in\mathbb{Z}_2\}.$$

Quand on calcule dans cet anneau, on utlise le fait que $h(t)=0$ et donc $t^2=-t-\bar{1}=t+\bar{1}$. La table de multiplication est donc le suivant :

| $\times$ | $\bar{0}$ | $\bar{1}$ | $t$ | $\bar{1}+t$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $t$ | $\bar{1}+t$ |
| $t$ | $\bar{0}$ | $t$ | $\bar{1}+t$ | $\bar{1}$ |
| $\bar{1}+t$ | $\bar{0}$ | $\bar{1}+t$ | $\bar{1}$ | $t$ |

C'est un corps avec quatre éléments. (Rappelons que $\mathbb{Z}_4$ n'est *pas* un corps, donc cet anneau quotient n'est pas isomorphe à $\mathbb{Z}_4$.)

**Théorème 2.3.6.** *Soient $F$ un corps et $h(x) \in F[x]$ avec $\deg h(x) \geq 1$. Alors les affirmations suivantes sont équivalentes :*

*(a) $h(x)$ est irréductible.*
*(b) $\langle h(x) \rangle$ est un idéal premier.*
*(c) $\langle h(x) \rangle$ est un idéal maximal.*

*Démonstration.* (a) $\Rightarrow$ (b) : C'est le corollaire 2.2.29.

(b) $\Rightarrow$ (c) : Supposons que $\langle h(x) \rangle$ est premier mais pas maximal. Alors il existe un idéal $I$ de $F[x]$ tel que $\langle h(x) \rangle \subsetneq I \subsetneq F[x]$. Maintenant, d'après le théorème 2.3.1, il existe $p(x) \in F[x]$ tel que $I = \langle p(x) \rangle$. Ainsi il existe $q(x) \in F[x]$ tel que $h(x) = p(x)q(x)$. Mais $p(x) \notin \langle h(x) \rangle$, et donc $q(x) \in \langle h(x) \rangle$, c.-à-d., il existe $r(x) \in F[x]$ tel que $q(x) = h(x)r(x)$. Cela implique que $h(x) = p(x)h(x)r(x)$, et donc $\deg p(x) = 0$, ce qui contredit le fait que $I \neq F[x]$.

(c) $\Rightarrow$ (a) : Si $h(x)$ n'est pas irréductible, alors il existe $h_1(x), h_2(x) \in F[x]$ avec $\deg h_1(x), \deg h_2(x) < \deg h(x)$ tels que $h(x) = h_1(x)h_2(x)$. Ainsi $\langle h(x) \rangle \subsetneq \langle h_1(x) \rangle \subsetneq F[x]$, ce qui implique que $\langle h(x) \rangle$ n'est pas maximal. □

Une des conséquences importantes du théorème 2.3.6 est que des corps d'ordre $p^m$ existent pour tout nombre premier $p$ et entier positif $m$. Nous explorons cela dans la section suivante.

---

## Exercices.

Pour tous ces exercices, $F$ est un corps.

2.3.1 ([Nic12, Ex. 4.3.1(b)]). Définir

$$A = \{f(x) \in F[x] : \text{la somme des coefficients de } f(x) \text{ est zéro}\}.$$

Trouver un polynôme unitaire $h(x) \in F[x]$ tel que $A = \langle h(x) \rangle$.

2.3.2 ([Nic12, Ex. 4.3.2]). Dans chaque cas, décrire $R = F[x]/\langle h \rangle$ comme dans le théorème 2.3.3 et écrire les tables d'addition et de multiplication pour $R$.

(a) $h = x^2 + 1$, $F = \mathbb{Z}_2$
(b) $h = x^2 + x$, $F = \mathbb{Z}_2$
(c) $h = x^3 + 1$, $F = \mathbb{Z}_2$
(d) $h = x^2 - 1$, $F = \mathbb{Z}_3$
(e) $h = x^2$, $F = \mathbb{Z}_3$
(f) $h = x^2 - x + 1$, $F = \mathbb{Z}_3$

2.3.3 ([Nic12, Ex. 4.3.3]). Construire un corps avec 8 éléments et écrire la table de multiplication.

2.3.4 ([Nic12, Ex. 4.3.4]). Construire un corps avec 9 éléments et écrire la table de multiplication.

2.3.5 ([Nic12, Ex. 4.3.5(b)]). Construire un corps avec 25 éléments.

2.3.6 ([Nic12, Ex. 4.3.6]). Dans chaque cas, déterminer tous les idempotents, éléments nilpotents, et unités de $R = F[x]/\langle h\rangle$ :

(a) $h = x^2 - x$
(b) $h = x^2$

2.3.7 ([Nic12, Ex. 4.3.7]). Dans chaque cas, montrer que $r$ est une unité dans $R = F[x]/\langle h\rangle$ et trouver l'inverse. Utiliser la notation du théorème 2.3.3.

(a) $r = 1 + t^2$, $F = \mathbb{Z}_{11}$, $h = x^3 + 1$
(b) $r = 1 + t - t^2$, $F = \mathbb{Z}_7$, $h = x^3 + x^2 - 1$

2.3.8 ([Nic12, Ex. 4.3.8]). Puisque $x - a$ est irréductible sur le corps $F$, le théoreme 2.3.6 et le corollaire 1.3.19 impliquent que $F[x]/\langle x - a\rangle$ est un corps. Décrire ce corps. Quel est le lien avec $F$ ?

2.3.9 ([Nic12, Ex. 4.3.9]). Trouver un sous-anneau de $\mathbb{R}$ qui est isomorphe à $\mathbb{Q}[x]/\langle x^3 - 2\rangle$.

2.3.10 ([Nic12, Ex. 4.3.10]). (a) Montrer que

$$F[x]/\langle x^2\rangle \cong \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in F \right\}, \text{ un sous-anneau de } \mathrm{Mat}_2(F).$$

(b) Montrer que

$$F[x]/\langle x^3\rangle \cong \left\{ \begin{bmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{bmatrix} : a, b \in F \right\}, \text{ un sous-anneau de } \mathrm{Mat}_3(F).$$

(c) Généraliser les résultats ci-dessus.

2.3.11 ([Nic12, Ex. 4.3.11]). Trouver un isomorphisme d'anneaux $F[x]/\langle x^2 - x\rangle \to F \times F$.

2.3.12 ([Nic12, Ex. 4.3.12]). Soit $R = F[x]/\langle x^2 - 1\rangle = \{a + bt : a, b \in F,\ t^2 = 1\}$. Montrer que $a + bt$ est une unité dans $R$ si et seulement si $a^2 \neq b^2$. *Indice* : Si $r = a + bt$, Soient $r^* = a - bt$, et $N(r) = rr^*$. Montrer que $(rs)^* = r^*s^*$, et donc que $N(rs) = N(r)N(s)$ pour tous $r, s \in R$.

2.3.13 ([Nic12, Ex. 4.3.18]). Soit $A$ l'ensemble des polynômes dans $\mathbb{Z}[x]$ avec coefficient constant pair. Montrer que $A$ est un idéal de $\mathbb{Z}[x]$ qui n'est pas principal. (*Remarque :* Il faut montrer que $A$ est un idéal.) Cela montre que le théorème 2.3.1 est faux si on remplace $F$ par un anneau intègre en général.

2.3.14 ([Nic12, Ex. 4.3.21]). (a) Supposons que $a, b \in F$ tels que $a^2 - 4b$ n'est pas le carré d'un élément de $F$. Montrer que $x^2 + ax + b$ est irréductible in $F[x]$.

(b) Montrer que l'implication réciproque de (a) est vraie si $2 \neq 0$ dans $F$.

2.3.15 ([Nic12, Ex. 4.3.22]). Soient $f$ et $g$ des polynômes non nuls dans $F[x]$.

(a) Montrer que $A = \{uf + vg : u, v \in F[x]\}$ est un idéal de $F[x]$.

(b) Expliquer comment le théoreme 2.3.1 est lié au théorème 2.2.24.

2.3.16 ([Nic12, Ex. 4.3.23]). Les polynômes $f_1, f_2, \ldots, f_m$ in $F[x]$ sont appelés *premiers entre eux* si 1 est le seul diviseur unitaire commun de tous les $f_i$ dans $F[x]$. Montrer que $f_1, f_2, \ldots, f_m$ sont premiers entre eux si est seulement s'il existe $q_1, q_2, \ldots, q_m \in F[x]$ tels que $1 = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$. *Indice* : le théorème 2.3.1.

2.3.17 ([Nic12, Ex. 4.3.26]). (a) Soit $A \neq F[x]$ un idéal de $F[x]$. Si $A \neq 0$, montrer que $A$ est premier si et seulement s'il est maximal.

(b) Que se passe-t-il si $A = 0$ ? Justifiez votre réponse.

2.3.18 ([Nic12, Ex. 4.3.27]). Soit $h$ un polynomial unitaire non constant dans $F[x]$. Montrer que $F[x]/\langle h\rangle$ n'a aucun élément nilpotent non nul si et seulement si $h = p_1 p_2 \cdots p_r$, où $p_1, p_2, \ldots, p_r$ sont des polynômes unitaires distincts. *Indice* : Utiliser le théorème 2.2.31.

2.3.19. Utiliser le premier théorème d'isomorphisme (le théorème 1.4.15) pour donner une démonstration alternative du fait que $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$ (voir l'exercice 2.3.2).

2.3.20 (Bonus). Démontrer que $\mathbb{C}[x]/\langle x^2 + 1\rangle \cong \mathbb{C} \times \mathbb{C}$ (en tant qu'anneaux).

## 2.4 Corps finis

Dans cette section, nous examinons les corps finis. Vous avez déjà vu les corps $\mathbb{Z}_p$, $p$ un nombre premier. Nous verrons ici qu'il existe d'autres corps finis. En fait, il est possible de classer complètement tous les corps finis, à isomorphisme près.

*Exemple* 2.4.1. Le polynôme $x^2 + x + 1$ n'a aucune racine dans $\mathbb{Z}_2$ est donc il est irréductible d'après le théorème 2.2.7. Ainsi

$$\mathbb{Z}_2[x]/\langle x^2 + x + \bar{1}\rangle = \{a + bt : a, b \in \mathbb{Z}_2,\ t^2 + t + \bar{1} = 0\}$$

est un corps avec quatre éléments. Nous l'avons vu par calcul direct dans l'exemple 2.3.5.

L'idée dans l'exemple 2.4.1 est la suivante : Si $h(x)$ est un polynôme unitaire irréductible dans $\mathbb{Z}_p[x]$ de degré $m$, alors, d'après le théorème 2.3.6, l'idéal $\langle h(x)\rangle$ est maximal et donc $\mathbb{Z}_p[x]/\langle h(x)\rangle$ est un corps d'après le corollaire 1.3.19. En utilisant le théorème 2.3.3, il n'est pas difficile à voir que ce corps a $p^m$ éléments. En fait, cette procédure produit *tous* le corps finis.

Supposons que $F$ soit un corps fini. Alors son groupe additif est fini et donc, d'après le lemme 1.1.19, sa caractéristique est positive. Ainsi d'après la proposition 1.2.12, sa caractéristique est un nombre premier $p$. Par conséquent, d'après le théorème 1.4.20, $\mathbb{Z}_p \subseteq F$ (l'application $\iota\colon \mathbb{Z}_p \hookrightarrow F$, $\iota(\bar{k}) = k \cdot 1$ est un morphisme d'anneaux injectif). On peut donc voir $F$ en tant qu'un espace vectoriel sur le corps $\mathbb{Z}_p$.

**Proposition 2.4.2.** *Si $F$ est un corps fini, alors il existe $n$ tel que $|F| = p^n$, où $p = \mathrm{car}(F)$.*

*Démonstration.* Puisque $F$ est un corp fini, il est de dimension finie en tant qu'espace vectoriel sur $\mathbb{Z}_p$. Si $n = \dim_{\mathbb{Z}_p} F$, alors $F \cong (\mathbb{Z}_p)^n$ en tant qu'espace vectoriel, et le résultat s'ensuit. □

**Théorème 2.4.3.** *Le nombre d'éléments d'un corps fini est une puissance d'un nombre premier. Pour toute puissance $q = p^n$ d'un nombre premier $p$, il existe un corps fini unique $F$ avec $q$ éléments, à isomorphisme près. Dans ces corps, tout élément $a$ satisfait $a^q = a$, et le polynôme $x^q - x$ se factorise en*

$$x^q - x = \prod_{a \in F} (x - a).$$

La preuve de ce théorème implique certains sujets de théorie des corps qui sortent du cadre de ce cours. (Ils sont traités dans MAT 4543.) Ainsi, nous ne donnons qu'un aperçu de la preuve.

*Aperçu de la preuve.* La première affirmation est la proposition 2.4.2. Le *corps de décomposition* d'un polynomial $f(x) \in F[x]$, où $F$ est un corps, est le plus petit corps qui contient $F$ et dans lequel on peut éctrire $f(x)$ comme produit des facteurs linéaires. On peut montrer qu'un corps de décomposition de $f(x)$ existe toujours, et qu'il est unique à isomorphisme près. Le corps avec $p^n$ éléments est le corps de décomposition du polynôme $x^{p^n} - x$. □

**Définition 2.4.4** (Corps de Galois)**.** Le corps unique avec $p^n$ éléments est appelé le *corps de Galois* à $p^n$ éléments, est il est noté $\mathrm{GF}(p^n)$ (pour *Galois field* en anglais).

**Théorème 2.4.5.** *Supposons que $F$ soit un corps. Si $G$ est un sous-groupe fini de $F^\times$, alors $G$ est cyclique.*

*Démonstration.* Soit $G$ un sous-groupe fini de $F^\times$ avec $n$ éléments. D'après le théorème de structure des groupes abéliens finis (de MAT 2543), il existe des nombres premiers $p_i$ tels que $n = p_1^{e_1} \cdots p_k^{e_k}$ (pas nécessairement distincts) tels que

$$G \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

Soit $m$ le plus petit commun multiple de $p_1^{e_1}, \ldots, p_k^{e_k}$. Alors $G$ contient un élément d'ordre $m$ (le produit des générateurs des facteurs cycliques ci-dessus). Puisque tout $\alpha$ dans $G$ satisfait $\alpha^m = 1$, nous voyons que chaque élément de $G$ est une racine de $x^m - 1$. Puisque $x^m - 1$ a au plus $m$ racines dans $F$, $n \leq m$. D'autre part, nous savons que $m \leq |G|$ ; par conséquent, $m = n$. Ainsi, $G$ contient un élément d'ordre $n$ et donc il faut que $G$ soit cyclique. □

**Corollaire 2.4.6.** *La groupe multiplicatif des éléments non nuls d'un corps fini est cyclique.*

**Définition 2.4.7** (Élément primitif, racine primitive de l'unité)**.** Si $F$ est un corps fini, alors un générateur pour $F^\times$ est appelé un *élément primitif* de $F$. Si un corps $F$ (possiblement infini) a un sous-groupe multiplicative $G$ avec $n$ éléments, alors un générateur de $G$ (ce qui existe d'après le théorème 2.4.5) est appelé une *racine primitive $n$-ième de l'unité* dans $F$. Par exemple, $e^{2\pi i/n}$ est une racine primitive $n$-ième de l'unité dans $\mathbb{C}$ pour tout $n \geq 2$.

## Exercices.

Pour toutes ces exercices, $F$ est un corps.

2.4.1. Trouver un élément primitif pour les corps suivants :

(a) $\mathbb{Z}_7$
(b) $\mathbb{Z}_{13}$
(c) Le corps de l'exemple 2.4.1.

2.4.2 ([Nic12, Ex. 6.4.3]). Expliquer pourquoi $\mathbb{Z}_2[x]/\langle p\rangle$ et $\mathbb{Z}_2[x]/\langle q\rangle$ sont isomorphes si $p = x^3 + x^2 + 1$ et $q = x^3 + x + 1$.

2.4.3. Soit $F$ un corps et supposons que $F^\times$ est un groupe cyclique. Prouver que $F$ est fini. Vous pouvez supposer que $\mathrm{car}(F) \neq 2$ (mais le résultat est aussi vrai dans ce cas où $\mathrm{car}(F) = 2$).

# Chapitre 3

# Anneaux intègres

Dans ce chapitre, nous abordons plus en détail les domaines intègres. En particulier, nous introduisons les anneaux factoriels, les anneaux principals, et les anneaux euclidiens. Une référence pour le matériel de ce chapitre est [Jud19, Ch. 18]. Tout au long de ce chapitre, sauf indication contraire, nous supposons que $R$ est un domaine intègre.

## 3.1 Anneaux factoriels

Rappelons que, pour $a, b \in R$, on dit que $a$ *divise* $b$, et on écrit $a|b$, s'il existe $c \in R$ tel que $b = ac$.

**Définition 3.1.1** (Décomposition, factorisation)**.** Une *décomposition* (ou un *factorisation*) d'un élément $a \in R$ est une façon d'écrire $a = bc$ avec $b, c \in R$. Une telle décomposition est *triviale* si $b$ ou $c$ est une unité dans $R$.

Les décomposition triviales ne sont pas très intéressantes. Nous considérons que deux décompositions $r = ab$ et $r = (ua)(u^{-1}b)$ pour une unité $u \in R^\times$ sont essentiellement les mêmes.

*Exemple* 3.1.2. Dans $\mathbb{Z}$ on a $8 = 4 \cdot 2 = (-4) \cdot (-2)$. Dans $\mathbb{R}[x]$ on a

$$(x^3 - 1) = (x - 1)(x^2 + x + 1) = (3x - 3)\left(\frac{1}{3}x^2 + \frac{1}{3}x + \frac{1}{3}\right).$$

**Théorème 3.1.3.** *Soient $a, b \in R$. Les affirmations suivantes sont équivalentes :*

*(a) $a|b$ et $b|a$,*
*(b) il existe $u \in R^\times$ tel que $a = ub$,*
*(c) $\langle a \rangle = \langle b \rangle$.*

*Démonstration.* La preuve de ce théorème est l'exercice 3.1.1. □

**Définition 3.1.4** (Éléments associés)**.** Deux éléments $a, b \in R$ sont *associés* si $a|b$ et $b|a$. Quand $a$ et $b$ sont associés, on écrit $a \sim b$.

**Lemme 3.1.5.** *La relation $\sim$ (c.-à-d. être associés) est un relation d'équivalence.*

*Démonstration.* La preuve de ce lemme est l'exercice 3.1.2. □

*Exemple* 3.1.6. Les classes d'équivalence de $\sim$ dans $\mathbb{Z}$ sont $\{0\}$, $\{\pm 1\}$ $\{\pm 2\}, \ldots$.

*Exemple* 3.1.7. Considérons l'anneau $\mathbb{Z}(\sqrt{3}) := \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$. Puisque $(2+\sqrt{3})(2-\sqrt{3}) = 1$, on voit que $2 + \sqrt{3} \in \mathbb{Z}(\sqrt{3})^\times$. Alors, puisque $\sqrt{3}(2+\sqrt{3}) = 3 + 2\sqrt{3}$, on voit que $\sqrt{3} \sim 3 + 2\sqrt{3}$.

Le concept suivant est utile quand on étudie les sous-anneaux de $\mathbb{C}$. Pour un nombre complexe $\omega \in \mathbb{C} \setminus \mathbb{Q}$ avec $\omega^2 \in \mathbb{Z}$, définissons la *norme* de $x = m + n\omega$, $m, n \in \mathbb{Z}$, par

$$N(x) = N(m + n\omega) = (m + n\omega)(m - n\omega) = m^2 - n^2\omega^2. \tag{3.1}$$

Alors $N(xy) = N(x)N(y)$ pour $x, y \in \mathbb{Z} + \omega\mathbb{Z} := \{m + n\omega : m, n \in \mathbb{Z}\}$. Notez aussi que $N(x) \in \mathbb{Z}$ pour tout $x \in \mathbb{Z} + \omega\mathbb{Z}$, et que $N(x) = 0$ si et seulement si $x = 0$ (exercice 3.1.3).

*Exemple* 3.1.8. Si $\omega$ est un nombre imaginaire (par ex. $\omega = \sqrt{-5}$), alors

$$N(x) = \bar{x}x = |x|^2.$$

On a $N(x) \in \mathbb{N}$ pour tout $x \in \mathbb{Z}(i)$.

*Exemple* 3.1.9. Trouvons toutes les unités dans $\mathbb{Z}(\sqrt{-5}) := \{a + b\sqrt{-5} : a, b \in \mathbb{C}\}$. On a

$$(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1 \implies N(a+b\sqrt{-5})N(c+d\sqrt{-5}) = 1 \implies (a^2+5b^2)(c^2+5d^2) = 1.$$

Puisque $a^2 + 5b^2$ et $c^2 + 5d^2$ sont des entiers non négatifs, il faut que $a^2 + 5b^2 = 1$ et donc $a = \pm 1$ et $b = 0$. Par conséquent, $\mathbb{Z}(\sqrt{-5})^\times = \{\pm 1\}$. Donc, les seuls éléments associés à $z \in \mathbb{Z}(\sqrt{-5})$ sont $\pm z$. D'autre part, rappelons que $\mathbb{Z}(i)^\times = \{\pm 1, \pm i\}$ (voir l'example 1.1.25).

La définition suivante généralise les concepts des éléments irréductibles et premiers aux anneaux intègres généraux.

**Définition 3.1.10** (Irréductible, premier)**.** Soit $r \in R$. On dit que $r$ est *irréductible* si les conditions suivantes sont satisfaites :

(a) $r \neq 0$,
(b) $r \notin R^\times$,
(c) si $r = ab$, alors $a \in R^\times$ ou $b \in R^\times$.

On dit que $r$ est *premier* si les conditions suivantes sont satisfaites :

(a) $r \neq 0$,
(b) $r \notin R^\times$,
(c) pour tous $a, b \in R$, si $r|ab$, alors $r|a$ or $r|b$.

*Exemple* 3.1.11. Tout nombre premier $p \in \mathbb{Z}$ est à la fois irréductible et premier.

*Exemple* 3.1.12. Tout polynôme irréductible dans $f(x) \in F[x]$ (où $F$ est un corps) et irréductible (par définition) et premier (d'après la proposition 2.2.28).

**Théorème 3.1.13.** *Tout élément premier d'un anneau intègre est irréductible.*

*Démonstration.* Supposons que $r \in R$ soit premier et qu'il existe $a, b \in R$ tels que $r = ab$. Alors $r|ab$ et donc $r|a$ ou $r|b$. Sans perte de généralité (c.-à-d. en échangeant $a$ et $b$ si nécessaire), on peut supposer que $r|a$. Alors il existe $c \in R$ tel que $a = rc$. Alors

$$r = ab = rcb \implies 1 = cb \implies b \text{ est une unité,}$$

où dans la première implication, on a utilisé la proposition 1.2.7. □

L'implication réciproque du théorème ci-dessus est fausse, comme l'illustre l'exemple suivant.

*Exemple* 3.1.14. On va montrer que $1 + \sqrt{-5}$ est un élément irréductible de $\mathbb{Z}(\sqrt{-5})$ qui n'est pas premier.

Supposons qu'on a une décomposition

$$1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5}).$$

Alors, en appliquant la norme $N$ de (3.1), on a

$$6 = N\left(1 + \sqrt{-5}\right) = N\left(a + b\sqrt{-5}\right) N\left(c + d\sqrt{-5}\right) = (a^2 + 5b^2)(c^2 + 5d^2).$$

Puisque chacun des facteurs à droite est postif, il faut que (en échangeant les deux facteurs si nécessaire)

— $a^2 + 5b^2 = 1$ et $c^2 + 5d^2 = 6$, et donc $a = 1$, $b = 0$ ; ou
— $a^2 + 5b^2 = 2$ et $c^2 + 5d^2 = 3$, ce qui est impossible.

Ainsi le décomposition est triviale.

Pour voir que $1 + \sqrt{-5}$ n'est pas premier, notez que $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$. Donc $1 + \sqrt{-5}$ divise $6 = 3 \cdot 2$. Cependant, on affirme que $1 + \sqrt{-5}$ ne divise ni 2 ni 3. S'il divise 2, on pouvait trouver $x \in \mathbb{Z}(i)$ tel que

$$2 = (1 + \sqrt{-5})x \implies 4 = N(2) = N\left(1 + \sqrt{-5}\right) N(x) \implies 4 = 6N(x),$$

ce qui est une contradiction puisque $N(x) \in \mathbb{Z}$. De même façon, si $1 + \sqrt{-5}$ divise 3, on pouvait trouver $x \in \mathbb{Z}$ tel que

$$3 = (1 + \sqrt{-5})x \implies 9 = N(3) = N\left(1 + \sqrt{-5}\right) N(x) \implies 9 = 6N(x),$$

ce qui est encore une contradiction. Par conséquent, $1 + \sqrt{-5}$ n'est pas premier.

**Définition 3.1.15** (Anneau factoriel)**.** Un anneau intègre $R$ est appelé un *anneau factoriel* s'il satisfait les conditions suivantes :

(a) Si $r \in R$ tel que $r \neq 0$ et $r \notin R^\times$, alors on peut écrire $r$ comme produit des éléments irréductibles.
(b) Si $r \in R$, $r \neq 0$ et $r \notin R^\times$ avec $r = p_1 \cdots p_s = q_1 \cdots q_t$ (où les éléments $p_i$ et $q_i$ sont irréductibles) alors $s = t$ et, après réétiqueter si nécessaire, $p_i \sim q_i$ pour $i = 1, \ldots, s$.

*Exemple* 3.1.16. L'anneau $\mathbb{Z}$ des entiers est un anneau factoriel. Aussi, d'après le théorème 2.2.31, l'anneau $F[x]$ est un anneau factoriel pour tout corps $F$.

**Lemme 3.1.17.** *Tout élément irréductible dans un anneau factoriel est premier.*

*Démonstration.* Supposons que $R$ soit un anneau factoriel, que $r \in R$ est irréductible, et qu'il existe $a, b \in R$ tel que $r|ab$. Alors il existe $s \in R$ tels que $ab = rs$. Puisque $R$ est un anneau factoriel, on peut factoriser $a, b, s$ comme produits d'irréductibles :

$$a = p_1 \cdots p_k, \quad b = q_1 \cdots q_\ell, \quad s = t_1 \cdots t_n.$$

Ainsi $p_1 \cdots p_k q_1 \cdots q_\ell = r t_1 \cdots t_n$. En utilisant l'unicité de décomposition dans un anneau factoriel, il existe $i = 1, \ldots, k$ tel que $r \sim p_i$ ou il existe $j = 1, \ldots, \ell$ tel que $r \sim q_j$. Par conséquent, $r|a$ ou $r|b$. □

*Exemple* 3.1.18. D'après l'exemple 3.1.14 et le lemme 3.1.17, on voit que $\mathbb{Z}(\sqrt{-5})$ n'est pas un anneau factoriel. Les décompositions

$$(1 + \sqrt{-5})(1 + \sqrt{-5}) = 6 = 3 \cdot 2$$

ne sont pas équivalents (c.-à-d. les facteurs à gauche et les facteurs à droite ne sont pas associés).

Dans un anneau factoriel, on peut utiliser la décomposition d'un élément pour trouver tous ses diviseurs (à multiplication près par une unité). Supposons que $R$ soit un anneau factoriel et que $a \in R$ soit un élément non nul qui n'est pas une unité. Alors on peut écrire uniquement

$$a \sim p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

où $a_i \geq 1$ et $p_i$ est un élément premier dans $R$ pour $i = 1, \ldots, r$ et les $p_i$ ne sont pas associés (c.-à-d. $p_i \not\sim p_j$ pour $i \neq j$). L'unicité ici veut dire que les éléments premiers sont détérminés uniquement à multiplication près par une unité (et réordonner) de même que les exposants $a_i$. Les diviseurs de $a$ sont alors déterminés uniquement (à multiplication près par une unité). Précisément, on a

$$d|a \iff d \sim p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}, \text{ pour } 0 \leq d_i \leq a_i, \ i = 1, \ldots, r.$$

La démonstration de ce fait est un exercice (ou voir [Nic12, §5.1, p. 258]).

**Définition 3.1.19** (Plus grand commun diviseur, plus petit commun multiple)**.** Supposons que $s_1, \ldots, s_n \in R$. Un élément $d \in R$ est appelé un *plus grand commun diviseur* (*pgcd*) de $s_1, \ldots, s_n$, et il est noté $\operatorname{pgcd}(s_1, \ldots, s_n)$, s'il satisfait les conditions suivantes :

(a) $d|s_i$ pour $i = 1, 2, \ldots, n$.
(b) Si $r \in R$ satisfait $r|s_i$ pour $i = 1, 2, \ldots, n$, alors $r|d$.

Un élément $m \in R$ est appelé un *plus petit commun multiple* (*ppcm*) de $s_1, \ldots, s_n$, est il est noté $\operatorname{ppcm}(s_1, \ldots, s_n)$ s'il satisfait :

(a) $s_i|m$ pour $i = 1, 2, \ldots, n$.

(b) Si $r \in R$ satisfait $s_i | r$ pour $i = 1, 2, \ldots, n$, alors $m | r$.

Notez que la définition de pgcd donné ci-dessus est en accord avec la définition habituelle d'un pgcd d'entiers et la définition 2.2.25 pour les polynômes, sauf qu'il faut que le pgcd dans $\mathbb{Z}$ soit positif et le pgcd dans $F[x]$ soit monique. Ces conditions supplémentaires garantissent l'unicité du pgcd. Dans un anneau factoriel général, on n'a aucune condition analogue pour garantir l'unicité. Ainsi, dans un anneau factoriel général, les plus grands communs diviseurs (et les plus petits communs multiples) ne sont définis qu'à multiplication près par une unité. Nous écrivons $\operatorname{pgcd}(s_1, \ldots, s_n)$ et $\operatorname{ppcm}(s_1, \ldots, s_n)$ pour désigner *n'importe quel* gcd et lcm. En particulier, on a :

$$\text{si } s_i \sim s_i' \text{ pour } i = 1, \ldots, n \quad \text{alors} \quad \operatorname{pgcd}(s_1, \ldots, s_n) \sim \operatorname{pgcd}(s_1', \ldots, s_n').$$

Notez qu'il est possible que les pgcd et les ppcm n'existe pas dans un anneau intègre général, comme l'illustre l'exemple suivant.

*Exemple* 3.1.20. Considérez les éléments $x^5, x^6$ dans le sous-anneau $\mathbb{Z}[x^2, x^3]$ de $\mathbb{Z}[x]$ de tous les sommes finis de la forme $\sum a_{ij}(x^2)^i(x^3)^j$, $a_{ij} \in \mathbb{Z}$. On voit que $x^2$ et $x^3$ sont tous deux des diviseurs communs de $x^5$ et $x^6$, mais aucun de $x^2$ ou $x^3$ divise l'autre (dans $\mathbb{Z}[x^2, x^3]$). Ainsi, le pgcd de $x^5$ et $x^6$ in $\mathbb{Z}[x^2, x^3]$ n'existe pas.

**Proposition 3.1.21.** *Les pgcd et les ppcm existent dans les anneaux factoriels. Supposons que $R$ soit un anneau factoriel et que $a, b, c, \ldots$ est une liste finie d'éléments non nuls dans $R$. Soient $p_1, \ldots, p_r$ les éléments premiers non associés qui divisent au moins un des éléments, et écrivez*

$$\begin{aligned} a &\sim p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, & a_i \in \mathbb{N}, \\ b &\sim p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}, & b_i \in \mathbb{N}, \\ c &\sim p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}, & c_i \in \mathbb{N}. \\ &\vdots \end{aligned}$$

*Pour tout $i = 1, 2, \ldots, r$, soient $d_i = \min(a_i, b_i, c_i, \ldots)$ et $m_i = \max(a_i, b_i, c_i, \ldots)$. Alors*

$$\operatorname{pgcd}(a, b, c, \ldots) \sim p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \quad \text{et} \quad \operatorname{ppcm}(a, b, c, \ldots) \sim p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}.$$

*Démonstration.* La démonstration quand $R = \mathbb{Z}$ s'applique au cas général. Les détailles sont laissés en l'exercice 3.1.7. □

**Définition 3.1.22** (Condition de chaîne ascendante sur des idéaux principals)**.** On dit qu'un anneau intègre $R$ satisfait la *condition de chaîne ascendante sur des idéaux principals* (ou *CCAP*) si $R$ ne contient aucune chaîne strictement ascendante infinie

$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \cdots$$

des idéaux principals.

*Exemple* 3.1.23. Supposons qu'on a une chaîne strictement ascendante des idéaux principals dans $\mathbb{Z}$ :

$$\{0\} \neq \langle m_1\rangle \subsetneq \langle m_2\rangle \subsetneq m_3\rangle \subsetneq \cdots .$$

Alors $|m_1| > |m_2| > |m_3| > \cdots$. Ainsi il faut que la chaîne se termine après un nombre fini d'idéaux. Par conséquent, $\mathbb{Z}$ satisfait la CCAP.

*Exemple* 3.1.24. Considérons une chaîne ascendante des idéaux principals dans $F[x]$, où $F$ est un corps :

$$\{0\} \neq \langle p_1(x)\rangle \subsetneq \langle p_2(x)\rangle \subsetneq p_3(x)\rangle \subsetneq \cdots .$$

Alors $\deg p_1(x) > \deg p_2(x) > \cdots$ est donc il faut que la chaîne soit finie. Par conséquent $F[x]$ satisfait la CCAP.

*Exemple* 3.1.25. Soit $R = \{n + xf(x) : n \in \mathbb{Z},\ f(x) \in \mathbb{Q}[x]\}$, l'ensemble des polynômes dans $\mathbb{Q}[x]$ dont la terme constante est un entier. Puisque $R$ est un sous-anneau de $\mathbb{Q}[x]$, il est un anneau intègre. Cependant,

$$\langle x\rangle \subsetneq \langle \tfrac{1}{2}x\rangle \subsetneq \langle \tfrac{1}{2^2}x\rangle \subsetneq \cdots$$

est une chaîne ascendante infinie des idéaux principals dans $R$. Ainsi $R$ ne satisfait pas la CCAP.

**Théorème 3.1.26.** *Supposons que $R$ soit un anneau intègre qui satisfait la CCAP. Alors tout élément non nul qui n'est pas une unité est un produit des éléments irréductibles.*

*Démonstration.* Supposons qu'un élément non nul $a \in R$ qui n'est pas une unité ne peut pas être écrit comme produit des irréductibles. Alors $a$ n'est pas irréductible et donc on a

$$a = r_1a_1, \quad a \not\sim r_1, \quad a \not\sim a_1.$$

Maintenant, au moins un des éléments $r_1, a_1$ ne peuvent pas être écrits comme produit d'éléments irréductibles (car s'ils le peuvent tous les deux, alors on peut écrire $a$ comme un tel produit). Sans perte de généralité, on peut supposer que $a_1$ ne peut pas être écrit come produit d'élément irréductibles. Alors on a à nouveau

$$a_1 = r_2a_2, \quad a_1 \not\sim r_2, \quad a_1 \not\sim a_2,$$

où $a_2$ ne peut pas être comme produit d'éléments irréductibles. Continuant de cette manière, on a

$$\langle a\rangle \subsetneq \langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \cdots .$$

Ainsi $R$ ne satisfait pas la CCAP. □

**Théorème 3.1.27.** *Les affirmations suivantes sont équivalentes :*

*(a) $R$ est un anneau factoriel.*

*(b) $R$ satisfait la CCAP et* $\operatorname{pgcd}(a, b)$ *existe pour tous $a, b \in R$.*

*(c) $R$ satisfait la CCAP et tout élément irréductible de $R$ est premier.*

*Démonstration.* (a) ⇒ (b) : Supposez que $R$ soit un anneau factoriel. Alors la proposition 3.1.21 montre que les pgcd existent dans $R$. Maintenant supposons qu'on a une chaîne ascendante des idéaux principals dans $R$ :

$$\{0\} \subsetneq \langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \cdots .$$

Considérons une décomposition $a_1 = p_1 \cdots p_m$ de $a$ avec $p_1, \ldots, p_m$ des éléments irréductibles. Puisque $\langle a_1\rangle \subsetneq \langle a_2\rangle$, on a $a_2 \sim p_{i_1} \cdots p_{i_k}$, où $\{i_1, \ldots, i_k\} \subsetneq \{1, \ldots, m\}$. De la même façon, on a $a_3 \sim p_{j_1} \cdots p_{j_\ell}$, où $\{j_1, \ldots, j_\ell\} \subsetneq \{i_1, \ldots, i_k\}$. Continuant dans cette manière, on voit que la chaîne est finie. Ainsi $R$ satisfait la CCAP.

(b) ⇒ (c) : Supposons que (b) est vraie. Supposons que $p \in R$ soit irréductible et que $p|ab$ in $R$. Soit $d = \operatorname{pgcd}(a, p)$. Alors $d|p$ et donc $d \sim p$ ou $d \sim 1$ (puisque $p$ est irréductible). Si $p \sim d$ alors, puisque $d|a$, on a $p|a$. D'autre part, si $d \sim 1$, alors $\operatorname{pgcd}(a, p) \sim 1$. On affirme que cela implique que $\operatorname{pgcd}(ab, pb) \sim b$. En supposant cette affirmation, on a $p|b$ puisque $p|ab$ et $p|pb$. Donc on a montré que $p|a$ ou $p|b$ et donc $p$ est premier.

Il reste a prouver l'affirmation. Soit $d' = \operatorname{pgcd}(ab, pb)$. On a $b|ab$ et $b|pb$. Ainsi $b|d'$. Supposons que $d' = bu$. On montre que $u$ est une unite. Écrivons $ab = d'x$ pour $x \in R$. Donc $ab = bux$. Ainsi $a = ux$, puisque $b \neq 0$. Par conséquent, $u|a$. De même, $u|p$. Donc $u|\operatorname{pgcd}(a, p) \sim 1$. Ainsi $u$ est une unité.

(c) ⇒ (a) : Supposons que (c) holds. D'après le théorème 3.1.26, tout élément est un produit des élément irréductibles. Donc il reste a montrer l'unicité de tels décompositions. Supposons que

$$p_1 p_2 \cdots p_r \sim q_1 q_2 \cdots q_s$$

sont des décomposition distinctes, où les éléments $p_i$ et $q_i$ sont irréductibles et $r + s$ est minimal. Si $r = 1$, alors on a $p_1 \sim q_1 \cdots q_s$. Puisque $p_1$ est irréductible, cela implique que $s = 1$, ce qui contredit l'hypothèse que les décompositions sont distinctes. Un argument analogue montre qu'on ne peut pas avoir $s = 1$. On peut donc supposer que $r, s \geq 2$. Puisque $p_1|q_1 \cdots q_s$, il faut qu'il existe $j$ tel que $p_1|q_j$ puisque $p_1$ est premier par notre supposition. En réordonnant si nécessaire, on peut supposer que $p_1|q_1$. Puisque $q_1$ est irréductible, cela implique que $p_1 \sim q_1$. Ainsi $p_2 \cdots p_r \sim q_2 \cdots q_s$ sont des décompositions distinctes, ce qui contredit notre supposition que $r + s$ est minimal. □

*Exemple* 3.1.28. L'anneau $R$ de l'exemple 3.1.25 n'est pas un anneau factoriel puiqu'il ne satisfait pas la CCAP.

Le reste de cette section est consacré à la preuve du résultat important que si $R$ est un anneau factoriel, alors $R[x]$ est aussi un anneau factoriel (voir le théorème 3.1.34). Avant de le prouver, on doit définir quelques termes et prouver quelques résultats préliminaires.

**Définition 3.1.29** (Contenu, polynôme primitif)**.** Supposons que $R$ soit un anneau factoriel et que $f(x) \in R[x] \setminus \{0\}$. Alors le *contenu* de $f(x)$ est le pgcd des coefficients non nuls de $f$ est il est noté $c(f(x))$. On dit que $f(x)$ est un *polynôme primitif* si $c(f(x)) \sim 1$.

*Exemple* 3.1.30. Dans $\mathbb{Z}[x]$, $c(12+6x+9x^4) = 3$. Cependant, dans $\mathbb{Q}[x]$, $c(12+6x+9x^4) = 1$ (bien sûr, il est aussi 3, puisque 1 et 3 sont associés dans $\mathbb{Q}$). Ainsi $12+6x+9x^4$ est primitif dans $\mathbb{Q}[x]$ mais pas dans $\mathbb{Z}[x]$.

**Lemme 3.1.31.** *Soit $R$ un anneau factoriel et soit $f(x) \in R[x] \setminus \{0\}$.*

*(a) On peut écrire $f(x)$ sous la forme $f(x) = c(f(x))f_1(x)$, où $f_1(x) \in R[x]$ est primitif.*
*(b) Si $a \in R \setminus \{0\}$, alors $c(a(f(x))) = ac(f(x))$.*
*(c) Si $f(x)$ est irréductible et $\deg f(x) \geq 1$, alors $f(x)$ est primitif.*

*Démonstration.* La démonstration de ce lemme est l'exercice 3.1.14. □

Le théorème suivant est un généralisation du théorème 2.2.15

**Théorème 3.1.32** (Lemme de Gauss)**.** *Supposons que $R$ soit un anneau factoriel et que $f(x), g(x) \in R[x] \setminus \{0\}$. Alors*

$$c(f(x)g(x)) = c(f(x))c(g(x)).$$

*En particulier, un produit de polynômes primitifs est primitif.*

*Démonstration.* Écrivons $f(x) = c(f(x))f_1(x)$ et $g(x) = c(g(x))g_1(x)$, où $f_1(x)$, $g_1(x)$ sont primitifs. Alors

$$c(f(x)g(x)) \sim c(c(f(x))c(g(x))f_1(x)g_1(x)) \sim c(f(x))c(g(x))c(f_1(x)g_1(x))$$

d'après le lemme 3.1.31. Ainsi, il suffit de prouver le résultat dans le cas où $f(x)$ et $g(x)$ sont primitifs.

Soient $f(x) = \sum_{i=0}^{m} a_i x^i$ et $g(x) = \sum_{i=0}^{n} b_i x^i$. Supposons que $p \in R$ soit un élément premier qui divise les coefficients de $f(x)g(x)$. Soit $r$ le plus petit entier tel que $p \nmid a_r$ et soit $s$ le plus petit entier tel que $p \nmid b_s$. Le coefficient de $x^{r+s}$ dans $f(x)g(x)$ est

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r+s-1} b_1 + a_{r+s} b_0.$$

Puisque $p$ divise $a_0, \ldots, a_{r-1}$ et $b_0, \ldots, b_{s-1}$, $p$ divise tout terme de $c_{r+s}$ sauf que le terme $a_r b_s$. Cependant, puisque $p | c_{r+s}$, soit $p$ divise $a_r$ soit $p$ divise $b_s$. Cette contradiction complète la preuve. □

**Proposition 3.1.33.** *Supposons que $R$ soit un anneau factoriel et que $F$ soit son corps des fractions. On considère $R$ comme sous-anneau de $F$ dans la manière naturelle (voir la section 1.2). Supposons que $p(x)$ soit un élément primitif de $R(x)$. Alors $p(x)$ est irréductible dans $R[x]$ si et seulement s'il est irréductible dans $F[x]$.*

*Démonstration.* Premièrement, supposons que $p(x)$ est irréductible dans $F[x]$. Soit $p(x) = f(x)g(x)$ un décomposition dans $R[x]$. Si $\deg f(x), \deg g(x) \geq 1$, alors c'est une décomposition non triviale dans $F[x]$, ce qui contredit le fait que $p(x)$ est irréductible dans $F[x]$. Ainsi on peut supposer, sans perte de généralité, que $\deg f(x) = 0$. Ainsi $f(x) = u \in R$. Alors, puisque $p(x)$ est primitif, on a

$$1 \sim c(p(x)) = c(f(x)g(x)) = c(f(x))c(g(x)) = uc(g(x)).$$

Ainsi $u$ est une unité dans $R$ et donc la décomposition $p(x) = f(x)g(x)$ est triviale dans $R[x]$. Par conséquent, $p(x)$ est irréductible dans $R[x]$.

Maintenant supposer que $p(x)$ soit primitive et irréductible dans $R[x]$ et que $p(x) = f(x)g(x)$ dans $F[x]$. Soient $a$ et $b$ les produits des dénominateurs des coefficients de $f(x)$ et $g(x)$ respectivement. Alors $f_1(x) := af(x)$ et $g_1(x) := bg(x)$ sont des éléments de $R[x]$ et

$$abp(x) = f_1(x)g_1(x)$$

est une décomposition dans $R[x]$. Ainsi, d'après le lemme de Gauss (le théorème 3.1.32), on a

$$ab \sim abc(p(x)) = c(abp(x)) = c(f_1(x)g_1(x)) \sim c(f_1(x))c(g_1(x)). \tag{3.2}$$

Maintenant écrivons $f_1(x) = c(f_1(x))f_2(x)$ et $g_1(x) = c(g_1(x))g_2(x)$, où $f_2(x)$ et $g_2(x)$ sont primitifs dans $R[x]$. Alors

$$abp(x) = f_1(x)g_1(x) = c(f_1(x))c(g_1(x))f_2(x)g_2(x).$$

Par conséquent, d'après (3.2), on a $p(x) \sim f_2(x)g_2(x)$ dans $R[x]$. Puisque $p(x)$ est irréductible dans $R[x]$, cela implique que soit $f_2(x)$ soit $g_2(x)$ est une unité dans $R[x]$ (d'où une unité dans $R$). Si $f_2(x) = u \in R^\times$, alors

$$af(x) = f_1(x) = c(f_1(x))f_2(x) = c(f_1(x))u \implies f(x) = a^{-1}c(f_1(x))u \in F[x]^\times.$$

De même façon, si $g_2(x) \in R^\times$, alors $g(x) \in F[x]^\times$. □

**Théorème 3.1.34.** *Si $R$ est un anneau factoriel, alors $R[x]$ l'est aussi.*

*Démonstration.* Soit $p(x)$ un polynôme non nul dans $R[x]$. Si $p(x)$ est un polynôme non constant, alors il faut que $p(x)$ ait un factorisation puisque $R$ est un anneau factoriel. Maintenant que $p(x)$ est un polynôme de degré positif dans $R[x]$. Soit $F$ le corps des fractions de $R$, et soit

$$p(x) = f_1(x)f_2(x)\cdots f_n(x)$$

une décomposition de $p(x)$ dans $F[x]$, où chaque $f_i(x)$ est irréductible dans $F[x]$. Choisissons $a_i \in R$ tels que $a_i f_i(x)$ est dans $R[x]$ (par ex. soit $a_i$ le produit des dénominateurs des coefficients de $f_i(x)$). Alors, pour $i = 1, \ldots, n$, soit $b_i = c(a_i f_i(x)) \in R$, pour que $a_i f_i(x) = b_i g_i(x)$, où $g_i(x)$ est un polynôme primitif dans $R[x]$. Puisque $g_i(x) = \frac{a_i}{b_i} f_i(x)$, les polynômes $f_i(x)$ et $g_i(x)$ sont associés dans $F[x]$. Ainsi, puisque $f_i(x)$ est irréductible dans $F[x]$, le polynôme $g_i(x)$ est aussi irréductible. Alors, d'après la proposition 3.1.33, chaque $g_i(x)$ est irréductible dans $R[x]$. Maintenant, on a

$$a_1 \cdots a_n p(x) = b_1 \cdots b_n g_1(x) \cdots g_n(x). \tag{3.3}$$

Puisque $g_1(x)\cdots g_n(x)$ est primitif, on a

$$a_1 \cdots a_n c(p(x)) = c(a_1 \cdots a_n p(x)) = c(b_1 \cdots b_n g_1(x) \cdots g_n(x)) = b_1 \cdots b_n.$$

Ainsi $a_1 \cdots a_n$ divise $b_1 \cdots b_n$. Par conséquent, en divisant les deux côtés de (3.3) par $a_1 \cdots a_n$, on a $p(x) = ag_1(x)\cdots g_n(x)$, où $a \in R$. Puisque $R$ est un anneau factoriel, on peut factoriser $a$ comme $c_1 \cdots c_k$, où chaque des éléments $c_i$ est irréductible dans $R$ (d'où dans $R[x]$ aussi). Ainsi on a démontré l'existence des factorisations en irréductibles.

Maintenant on va montrer l'unicité de tels factorisations. Soient

$$p(x) = a_1 \cdots a_m f_1(x) \cdots f_n(x) = b_1 \cdots b_r g_1(x) \cdots g_s(x)$$

deux décompositions de $p(x)$, où tous les facteurs sont irréductibles dans $R[x]$. D'après la proposition 3.1.33, chacun des $f_i(x)$ et $g_i(x)$ est irréductible dans $F[x]$. Les $a_i$ et les $b_i$ sont des unités dans $F$. Puisque $F[x]$ est un anneau factoriel d'après le théorème 2.2.31, on a $n = s$.

Maintenant, on réorganise les $g_i(x)$ tel que $f_i(x)$ et $g_i(x)$ sont associés dans $F[x]$ pour $i = 1, \ldots, n$. Alors il existe $c_1, \ldots, c_n$ et $d_1, \ldots, d_n$ dans $R$ tels que $(c_i/d_i)f_i(x) = g_i(x)$ ou, en d'autres termes, $c_i f_i(x) = d_i g_i(x)$. Les polynômes $f_i(x)$ et $g_i(x)$ sont primitifs ; donc $c_i$ et $d_i$ sont associés dans $R$. Ainsi, $a_1 \cdots a_m = u b_1 \cdots b_r$ dans $R$, où $u$ est une unité dans $R$. Puisque $R$ est un anneau factoriel, $m = s$. Finalement, on peut réordonner les $b_i$ tel que $a_i$ et $b_i$ sont associés pour chaque $i$. Ceci complète la partie unicité de la preuve. □

**Corollaire 3.1.35.** *Si $R$ est un anneau factoriel, alors $R[x_1, \ldots, x_n]$ l'est aussi.*

*Démonstration.* Ceci suit par une récurrence faciles en utilisant le théorème 3.1.34 et le fait que

$$R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n].$$ □

*Remarque* 3.1.36 (Des anneaux noethériens et artiniens). Un anneau commutatif qui satisfait la *condition de chaîne ascendante sur des idéaux* (l'analogue du CCAP, mais où nous ne spécifions pas que les idéaux sont principaux) est appelé un *anneau noethérien*. Un anneau commutatif qui satisfait la *condition de chaîne descendante sur des idéaux* est appelé un *anneau artinien*. Les anneaux artiniens sont également noéthériens (mais pas l'inverse). Les anneaux noéthériens et artiniens sont des classes d'anneaux importantes, mais nous n'étudierons pas ces classes d'anneaux dans ce cours. Dans les anneaux non commutatifs, on peut parler d'anneaux noéthériens (ou artiniens) à gauche et à droite.

---

## Exercices.

3.1.1. Démontrer le théorème 3.1.3.

3.1.2. Démontrer le lemme 3.1.5.

3.1.3. Avec $N(x)$ comme défini dans (3.1), prouver que $N(x) = 0$ si et seulement si $x = 0$.

3.1.4 ([Nic12, Ex. 5.1.3]). Dans l'anneau $\mathbb{Z}(i)$ des entiers de Gauss, montrer que

(a) $(2 + i) \sim (1 - 2i)$,
(b) $(1 + 2i) \not\sim (2 + i)$.

3.1.5 ([Nic12, Ex. 5.1.6]). Montrer qu'un anneau intègre est un corps si et seulement si $a \sim b$ pour tous $a \neq 0 \neq b$.

3.1.6 ([Nic12, Ex. 5.1.8]). Trouver les unités dans $\mathbb{Z}(\sqrt{-3})$. *Indice* : Utiliser $N(a+b\sqrt{-3}) = a^2+3b^2$ comme dans l'exemple 3.1.14.

3.1.7. Démontrer la proposition 3.1.21.

3.1.8 ([Nic12, Ex. 5.1.10]). Dans chaque cas, déterminer si $p$ est irréductible dans $\mathbb{Z}(i)$ :

(a) $p = 11$
(b) $p = 2 - i$
(c) $p = 5$
(d) $p = 7 - i$

3.1.9 ([Nic12, Ex. 5.1.12]). Dans chaque cas, déterminer si $p$ est irréductible dans $\mathbb{Z}(\sqrt{-5})$ :

(a) $p = 6 + \sqrt{-5}$
(b) $p = 7$
(c) $p = 29$
(d) $p = 2 - 3\sqrt{-5}$.

3.1.10 ([Nic12, Ex. 5.1.13]). Dans chaque cas, montrer que $p$ est irréductible dans $\mathbb{Z}(\sqrt{-5})$ mais qu'il n'est pas premier.

(a) $p = 2 + \sqrt{-5}$
(b) $p = 1 + 2\sqrt{-5}$

3.1.11 ([Nic12, Ex. 5.1.14]). Dans chaque cas, déterminer si $p$ est irréductible dans $\mathbb{Z}(\sqrt{-3})$. *Indice* : Utiliser la norme $N(m+n\sqrt{-3}) = m^2+3n^2$.

(a) $p = 3 + 2\sqrt{-3}$
(b) $p = 2 + 3\sqrt{-3}$
(c) $p = 5$
(d) $p = 7$

3.1.12 ([Nic12, Ex. 5.1.15]). Montrer que $1 + \sqrt{-3}$ est irréductible dans $\mathbb{Z}(\sqrt{-3})$ mais qu'il n'est pas premier.

3.1.13 ([Nic12, Ex. 5.1.16]). Soient $p \sim q$ dans l'anneau intègre $R$.

(a) Montrer que $p$ est irréductible si et seulement si $q$ est irréductible.
(b) Montrer que $p$ est premier si est seulement si $q$ est premier.

3.1.14. Démontrer le lemme 3.1.31.

3.1.15 ([Nic12, Ex. 5.1.19]). On dit qu'un anneau commutatif remplit la *condition de chaîne descendante sur des idéaux principals* (CCDP) si $\langle a_1\rangle \supseteq \langle a_2\rangle \supseteq \cdots$ dans $R$ implique qu'il existe $n \geq 1$ tel que $a_n \sim a_{n+1} \sim \cdots$. Montrer qu'un anneau intègre $R$ satisfait la CCDP si est seulement si $R$ est un corps.

3.1.16 ([Nic12, Ex. 5.1.23]). Si $S$ est un anneau factoriel et $R$ est un sous-anneau de $S$, l'anneau $R$ est-il nécessairement un anneau factoriel ? Justifier votre réponse.

3.1.17 ([Nic12, Ex. 5.1.27]). Montrer que

$$\operatorname{pgcd}(a, \operatorname{pgcd}(b, c)) \sim \operatorname{pgcd}(\operatorname{pgcd}(a, b), c)$$

chaque fois que tous les pgcd existent dans $R$. De plus, montrer que cette valeur commune est $\operatorname{pgcd}(a, b, c)$.

3.1.18 ([Nic12, Ex. 5.1.36]). Montrer que si un anneau intègre $R$ remplit la CCAP et $\operatorname{ppcm}(a, b)$ existe pour tous $a, b \neq 0$ dans $R$, alors $R$ est un anneau factoriel. *Indice :* Si $p|ab$, pour $p$ irréductible, considérer $m \sim \operatorname{ppcm}(a, p)$. Utiliser le fait que $m|ap$ et $m|ab$. (Bien sûr, il faut justifier ce fait avant de l'utiliser.)

## 3.2 Anneaux principals

**Définition 3.2.1** (Anneau principal)**.** Un anneau intègre $R$ est appelé un *anneau principal* si tout idéal de $R$ est principal (c.-à-d. engendré par un élément).

*Exemple* 3.2.2. D'après la proposition 1.3.6 et le théorème 2.3.1, les anneaux $\mathbb{Z}$ et $F[x]$ (où $F$ est un corps) sont principaux. Tout corps est aussi principal puisque ses seuls idéaux sont $\langle 0 \rangle$ et $\langle 1 \rangle$, qui sont tous deux principaux.

**Théorème 3.2.3.** *Tout anneau principal est un anneau factoriel.*

*Démonstration.* Supposons que $R$ soit un anneau principal. D'après le théorème 3.1.27, il suffit à montrer que chaque élément irréductible de $R$ est premier et que $R$ satisfait la CCAP.

Supposons que $p \in R$ soit irréductible et que $p|ab$ dans $R$. Soit $I$ l'idéal $Ra + Rp$. Alors, puisque $R$ est un anneau principal, il existe $d \in R$ tel que $I = \langle d \rangle$. Ainsi $d|a$ et $d|p$. Puisque $p$ est irréductible, cela implique que $d \sim p$ ou $d \sim 1$. Si $d \sim p$, alors $p|a$ (puisque $d|a$). D'autre part, si $d \sim 1$, alors $1 \in I$. Ainsi il existe $r, s \in R$ tels que $ra + sp = 1$. Alors $rab + spb = b$. Puisque $p|ab$, cela implique que $p|b$. D'où $p$ est premier.

Il reste à montrer que $R$ satisfait la CCAP. Supposons que

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots .$$

Soit $A = \bigcup_{i=1}^{\infty} \langle a_i \rangle$. Alors $A$ est un idéal de $R$ (exercise). Ainsi, puisque $R$ est un anneau principal, il existe $a \in R$ tel que $A = \langle a \rangle$. Alors il existe $i$ tel que $a \in \langle a_i \rangle$. Par conséquent, $\langle a_i \rangle = \langle a \rangle = A$ et donc $\langle a_n \rangle = A$ pour $n \geq i$. Ainsi $R$ satisfait la CCAP. □

L'implication réciproque du théorème 3.2.3 est fausse, comme on voit dans l'exemple suivant.

*Exemple* 3.2.4. L'anneau $\mathbb{Z}[x]$ est un anneau factoriel (d'après le théorème 3.1.34) mais il n'est pas un anneau principal puisque, par exemple, l'idéal

$$I = \langle 2, x \rangle := \{a_0 + a_1 x + \cdots + a_n x^n : a_0 \in 2\mathbb{Z},\ a_1, \ldots, a_n \in \mathbb{Z}\}$$

n'est pas un idéal principal (exercice 3.2.2).

*Remarque* 3.2.5. Le fait que $\mathbb{Z}$ est un anneau principal, mais $\mathbb{Z}[x]$ ne l'est pas, montre qu'une version du théorème 3.1.34 pour les anneaux principaux n'est pas vraie.

**Théorème 3.2.6.** *Si $R$ est un anneau principal, alors le pgcd des éléments non nuls $a_1, \ldots, a_n \in R$ existe et il existe $r_1, \ldots, r_n \in R$ tels que $d = r_1a_1 + \cdots + r_na_n$.*

*Démonstration.* Soit $I = \langle a_1, \ldots, a_n\rangle := \langle a_1\rangle + \cdots + \langle a_n\rangle$. Puisque $R$ est un anneau principal, il existe $d \in R$ tel que $I = \langle d\rangle$. Alors, d'après la définition de $I$, il existe $r_1, \ldots, r_n \in R$ tels que $d = r_1a_1 + \cdots + r_na_n$. Puisque $a_1, \ldots, a_n \in \langle d\rangle$, on a $d|a_i$ pour tout $i$. De plus, si $c|a_i$ pour tout $i$, alors $c|(r_1a_1 + \cdots + r_na_n)$ et donc $c|d$. Par conséquent, $d \sim \text{pgcd}(a_1, \ldots, a_n)$. □

**Théorème 3.2.7.** *Supposons que $R$ est un anneau principal et que $p \in R$, $p \neq 0$, $p \notin R^\times$. Alors les affirmations suivantes sont équivalentes :*

*(a) $p$ est un élément premier.*
*(b) $\langle p\rangle$ est un idéal premier.*
*(c) $\langle p\rangle$ est un idéal maximal.*

*Démonstration.* (a) ⇒ (b) : Supposons que $p$ soit un élément premier et que $ab \in \langle p\rangle$. Alors $p|ab$, ce qui implique que $p|a$ ou $p|b$. Ainsi $a \in \langle p\rangle$ ou $b \in \langle p\rangle$. Par conséquent, $\langle p\rangle$ est un idéal premier.

(b) ⇒ (c) : Supposons que $\langle p\rangle$ soit un idéal premier. Alors $p$ est premier puisque

$$p|ab \implies ab \in \langle p\rangle \implies a \in \langle p\rangle \text{ ou } b \in \langle p\rangle \implies p|a \text{ ou } p|b.$$

Ainsi $p$ est irréductible d'après le théorème 3.1.13. Maintenant supposons que $\langle p\rangle \subseteq \langle q\rangle \subsetneq R$. Alors $q|p$. Puisque $\langle q\rangle \neq R$, on a $q \not\sim 1$. Puisque $p$ est irréductible, cela implique que $p \sim q$. Ainsi $\langle p\rangle = \langle q\rangle$.

(c) ⇒ (a) : Supposons que $\langle p\rangle$ soit un idéal maximal. Alors il est un idéal premier d'après le corollaire 1.3.20. Ainsi, par ce qui précède, on voit que $p$ est premier. □

*Exemple* 3.2.8. Dans $\mathbb{Z}[x]$, l'idéal $\langle x\rangle$ est premier, mais $\langle x\rangle \subsetneq \langle 2, x\rangle \subsetneq \mathbb{Z}[x]$ et donc cet idéal n'est pas maximal. Par conséquent, $\mathbb{Z}[x]$ n'est pas un anneau principal (voir l'exemple 3.2.4).

*Exemple* 3.2.9. Soit $F$ un corps. Dans $F[x, y]$, l'idéal $\langle x\rangle$ est premier, mais $\langle x\rangle \subsetneq \langle x, y\rangle \subsetneq F[x, y]$. Ainsi $F[x, y]$ n'est pas un anneau principal. Cependant, $F[x, y]$ est un anneau factorial d'après le corollaire 3.1.35.

**Proposition 3.2.10.** *Supposons que $R$ soit un anneau principal et que $a_1, \ldots, a_n \in R \setminus \{0\}$.*

*(a) $d \sim \text{pgcd}(a_1, \ldots, a_n)$ si est seulement si $\langle a_1\rangle + \langle a_2\rangle + \cdots + \langle a_n\rangle = \langle d\rangle$.*
*(b) $m \sim \text{ppcm}(a_1, \ldots, a_n)$ si est seulement si $\langle a_1\rangle \cap \langle a_2\rangle \cap \cdots \cap \langle a_n\rangle = \langle m\rangle$.*

*Démonstration.* La partie (a) découle du théorème 3.2.6. La preuve de la partie (b) est l'exercice 3.2.9. □

## Exercices.

3.2.1. Montrer que si $I_1 \subseteq I_2 \subseteq \cdots$ est une chaîne d'idéaux dans un anneau $R$, alors $I := \bigcup_{i=1}^{\infty} I_i$ est un idéal de $R$.

3.2.2. Montrer que $\langle 2, x\rangle \subseteq \mathbb{Z}[x]$ n'est pas un idéal principal (voir l'exemple 3.2.4).

3.2.3 ([Nic12, Ex. 5.2.1]). Chaque sous-anneau d'un anneau principal est-il un anneau principal ? Justifiez votre réponse.

3.2.4 ([Nic12, Ex. 5.2.2]). Si $F$ est un corps, montrer que $F[x, y]$ est un anneau factoriel qui n'est pas un anneau principal. *Indice :* Considérer $\{f(x, y) : f(0, 0) = 0\}$.

3.2.5 ([Nic12, Ex. 5.2.4]). Est-ce $\mathbb{Z}(\sqrt{-5})$ un anneau principal ? Justifiez votre réponse.

3.2.6 ([Nic12, Ex. 5.2.5]). Si $R$ est un anneau principal et $A \neq 0$ est un idéal de $R$, montrer que $R/A$ a un nombre fini d'idéaux, qui sont tous principaux.

3.2.7 ([Nic12, Ex. 5.2.6]). (a) Est-ce que chaque idéal premier d'un anneau principal est maximal ? Justifiez votre réponse.

(b) Montrer que chaque idéal $A \neq R$ dans un anneau principal est contenu dans un idéal maximal de $R$.

3.2.8 ([Nic12, Ex. 5.2.8]). Soit $p \in \mathbb{Z}$ un nombre premier et définissons

$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \in \mathbb{Q} : p \text{ ne divise pas } n \right\}.$$

(a) Montrer que $\mathbb{Z}_{(p)}$ est un anneau intègre (appelé la *localisation* de $\mathbb{Z}$ à $p$) et trouver les unités.

(b) Si $A \neq 0$ est un idéal de $\mathbb{Z}_{(p)}$, montrer que $A = \langle p^k \rangle$, où $k \geq 0$ est le plus petit entier tel que $p^k \in A$. *Indice* : Si $0 \neq m \in \mathbb{Z}$, alors $m = p^r d$, où $r \geq 0$ et $p$ ne divise pas $d$.

(c) Montrer que $\mathbb{Z}_{(p)}$ est un anneau principal avec exactement un idéal maximal.

3.2.9. Démontrer la proposition 3.2.10(b).

3.2.10 ([Nic12, Ex. 5.2.10]). Soit $R$ un anneau tel que $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$. Montrer que $R$ est un anneau principal. *Indice :* Si $I$ est un idéal de $R$, considérer $A = \mathbb{Z} \cap I$.

3.2.11 ([Nic12, Ex. 5.2.12]). Supposons que $\omega \in \mathbb{C}$ satisfait $\omega^2 \in \mathbb{Z}$ et $\omega^2 < 0$. Montrer que $\mathbb{Z}(\omega) = \{a + b\omega : a, b \in \mathbb{Z}\}$ a un nombre fini d'unités.

3.2.12 (Problème de bonus). Supposons que $R$ soit un anneau intègre et que $a, b \in R \setminus \{0\}$. Montrer que les pgcds existent dans $R$ si et seulement si les ppcm existent. De plus, montrer que, s'ils existent, on a $\operatorname{pgcd}(a, b)\ \operatorname{ppcm}(a, b) \sim ab$ pour tous $a, b \in R$.

## 3.3 Anneaux euclidiens

**Définition 3.3.1** (Algorithme de division, fonction diviseur)**.** Si $R$ est un anneau intègre, on dit que $R$ a un *algorithme de division* s'il existe une fonction $\nu\colon R\setminus\{0\}\to\mathbb{N}$ (appelée une *fonction diviseur*) telle que, pour tous $a,b\in R$ où $b\neq 0$, il existe $q,r\in R$ tel que

$$a=qb+r \text{ et soit } r=0 \text{ soit } \nu(r)<\nu(b).$$

**Définition 3.3.2** (Anneau euclidien)**.** Un anneau intègre $R$ est appelé un *anneau euclidien* s'il a une fonction diviseur $\nu\colon R\setminus\{0\}\to\mathbb{N}$ qui satisfait la condition suivante :

$$a,b\in R\setminus\{0\}\implies \nu(ab)\geq\nu(a). \tag{3.4}$$

Un telle fonction diviseur est appelée un *stathme euclidien* (ou *fonction euclidienne*).

*Remarque* 3.3.3. La fonction

$$\nu\colon\mathbb{Z}\setminus\{0\}\to\mathbb{N},\quad \nu(k)=\begin{cases}k & \text{si } k>0,\\ 2|k| & \text{si } k<0.\end{cases}$$

est une fonction diviseur qui ne satisfait pas (3.4).

Cependant, la condition (3.4) est en fait superflue dans le sens suivant. Tout anneau intègre $R$ qui a un algorithme de division possède un stathme euclidien (c.-à-d. une fonction diviseur qui satisfait (3.4)). En effet, si $\nu$ est une fonction diviseur de $R$, alors

$$\nu'(a)=\min_{r\in R\setminus\{0\}}\nu(ra),\quad a\in R,$$

est un stathme euclidien sur $R$. Voir [Rog71] pour les détailles.

*Exemples* 3.3.4. (a) L'anneau $\mathbb{Z}$ est un anneau euclidien avec stathme euclidien $\nu\colon\mathbb{Z}\to\mathbb{N}$, $\nu(n)=|n|$.

(b) Pour tout corps $F$, l'anneau $F[x]$ est un anneau euclidien avec stathme euclidien $\nu\colon F[x]\setminus\{0\}\to\mathbb{N}$, $\nu(f(x))=\deg f(x)$ (voir le théorème 2.1.12).

**Théorème 3.3.5.** *Tout anneau euclidien est un anneau principal (et donc il est un anneau factoriel).*

*Démonstration.* Supposons que $R$ possède un stathme euclidien $\nu$, et soit $I$ un idéal de $R$. Si $I$ est l'idéal nul, alors il est clairement principal. Donc supposons que $I\neq\{0\}$. Choisissons $b\in I\setminus\{0\}$ avec $\nu(b)$ minimal. On affirme que $I=\langle b\rangle$. Puisque $b\in I$, on a $\langle b\rangle\subseteq I$. Donc il reste à montrer que $I\subseteq\langle b\rangle$. Supposons $a\in I$. Alors on a

$$a=qb+r\quad\text{où } r=0 \text{ ou } \nu(r)<\nu(b).$$

Alors $r=a-bq\in I$ et donc, par le fait que $\nu(b)$ est minimal, il faut que $r=0$. Ainsi $a=qb$ et donc $a\in\langle b\rangle$. □

**Lemme 3.3.6.** *L'anneau $\mathbb{Z}(i)$ des entiers de Gauss est un anneau euclidien, ainsi il est aussi un anneau principal et un anneau factoriel.*

*Démonstration.* (Voir [Jud19, Example 18.20].) Pour $a, b \in \mathbb{Z}$, définissons $\nu(a+bi) = a^2+b^2 = |a+bi|^2$. On affirme que $\nu$ est un stathme euclidien sur $\mathbb{Z}(i)$.

Soient $z, w \in \mathbb{Z}(i) \setminus \{0\}$. Alors $\nu(zw) = |zw|^2 = |z|^2|w|^2 = \nu(z)\nu(w)$. Puisque $\nu(z) \geq 1$ pour tout élément non nul $z \in \mathbb{Z}(i)$, on a $\nu(zw) \geq \nu(w)$.

Ensuite, on montre que pour tout $z = a + bi$ et $w = c + di$ dans $\mathbb{Z}(i)$ tel que $w \neq 0$, il existe des éléments $q$ et $r$ dans $\mathbb{Z}(i)$ tels que $z = qw + r$ et soit $r = 0$ soit $\nu(r) < \nu(w)$. On peut considérer $z$ et $w$ comme éléments de $\mathbb{Q}(i) = \{p + qi : p, q \in \mathbb{Q}\}$, l'anneau des fractions de $\mathbb{Z}(i)$. Notez que

$$\begin{aligned} zw^{-1} &= (a+bi)\frac{c-di}{c^2+d^2} \\ &= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \\ &= \left(m_1 + \frac{n_1}{c^2+d^2}\right) + \left(m_2 + \frac{n_2}{c^2+d^2}\right)i \\ &= (m_1 + m_2 i) + \left(\frac{n_1}{c^2+d^2} + \frac{n_2}{c^2+d^2}i\right) \\ &= (m_1 + m_2 i) + (s + ti) \end{aligned}$$

dans $\mathbb{Q}(i)$. Dans les dernières étapes, on écrit les parties réelles et imaginaire sous la forme d'un entier plus une fraction propre. C'est-à-dire, on prend l'entier le plus proche $m_i$ tel que la partie fractionnaire satisfait $|n_i/(c^2+d^2)| \leq 1/2$. Par exemple, on écrit

$$\begin{aligned} \frac{9}{8} &= 1 + \frac{1}{8} \\ \frac{15}{8} &= 2 - \frac{1}{8}. \end{aligned}$$

Ainsi, $s$ et $t$ sont les "parties fractionnaires" de $zw^{-1} = (m_1 + m_2 i) + (s + ti)$. On sait aussi que $s^2 + t^2 \leq 1/4 + 1/4 = 1/2$. En multipliant par $w$, on a

$$z = zw^{-1}w = w(m_1 + m_2 i) + w(s + ti) = qw + r,$$

où $q = m_1 + m_2 i$ et $r = w(s + ti)$. Puisque $z$ et $qw$ sont des éléments de $\mathbb{Z}(i)$, il faut que $r$ soit dans $\mathbb{Z}(i)$. Finalement, il faut montrer que soit $r = 0$ soit $\nu(r) < \nu(w)$. Cependant,

$$\nu(r) = \nu(w)\nu(s + ti) \leq \frac{1}{2}\nu(w) < \nu(w). \qquad \square$$

*Remarque* 3.3.7. Il n'est pas facile de trouver des exemples d'anneaux principaux qui ne sont pas des anneaux euclidiens, mais de tels anneaux existent. Le premier exemple de ce type a été donné par T. Motzkin en 1949 : $\mathbb{Z}\left(\frac{1}{2}\left(1 + \sqrt{-19}\right)\right)$ est un anneau principal non euclidien.

Résumant certains des résultats prouvés dans ce chapitre, on a la chaîne suivante d'inclusions de classes :

anneaux commutatifs $\supsetneq$ anneaux intègres $\supsetneq$ anneaux factoriels $\supsetneq$ anneaux principaux $\supsetneq$ anneaux euclidiens $\supsetneq$ corps.

## Exercices.

3.3.1 ([Nic12, Ex. 5.2.7]). Montrer que les conditions suivantes sont équivalents pour un anneau intègre $R$ :

(a) $R$ est un corps,
(b) $R[x]$ est un anneau euclidien,
(c) $R[x]$ est un anneau principal.

3.3.2 ([Nic12, Ex. 5.2.9]). Soit $\mathbb{Z}_{(p)}$ comme dans l'exercice 3.2.8. Montrer que $\mathbb{Z}_{(p)}$ est un anneau euclidien où, pour tout $a \neq 0$ in $R$, $\nu(a) = k$ où $\langle a \rangle = \langle p^k \rangle$. En effet, montrer que $\nu(ab) = \nu(a) + \nu(b)$ pour tous $a \neq 0$, $b \neq 0$ dans $\mathbb{Z}_{(p)}$ est que, si $a + b \neq 0$, alors $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$.

3.3.3 ([Nic12, Ex. 5.2.15]). (a) Montrer que $\mathbb{Z}(\sqrt{3})$ est un anneau euclidien avec $\nu(m + n\sqrt{3}) = |m^2 - 3n^2|$.
(b) Si $a = 4 + 5\sqrt{3}$ et $b = 1 + \sqrt{3}$, écrire $a = qb + r$, où $r = 0$ ou $\nu(r) < \nu(b)$.

3.3.4 ([Nic12, Ex. 5.2.16]). Montrer que $\mathbb{Z}(\sqrt{-3})$ n'est pas euclidien avec $\nu(m + n\sqrt{-3}) = m^2 + 3n^2$. En d'autres termes, montrer que $\nu$ n'est pas un stathme euclidien. *Indice :* Essayer $a = 1 + \sqrt{-3}$ et $b = 2$.

3.3.5 ([Nic12, Ex. 5.2.18]). (a) Si $F$ est un corps, montrer que $F$ est euclidien.
(b) Si la fonction $\nu$ est constante dans un anneau euclidien $R$, montrer que $R$ est un corps.

3.3.6 ([Nic12, Ex. 5.2.22]). Supposons que $R$ est un anneau euclidien dans lequel $\nu(a + b) \leq \max\{\nu(a), \nu(b)\}$ chaque fois que $a$, $b$, et $a+b$ sont non nuls. Montrer que $q$ et $r$ sont déterminés de manière unique dans l'algorithme de division.

3.3.7 ([Nic12, Ex. 5.2.23]). Supposons qu'un anneau euclidien $R$ a un idéal maximal unique $R$. D'après le théorème 3.3.5, il existe $p \in \mathbb{R}$ tel que $P = \langle p \rangle$.

(a) Montrer que $P$ est l'ensemble des éléments non-unités de $R$ ; c'est-à-dire, $a$ n'est pas une unité si est seulement si $p|a$. *Indice* : l'exercice 3.2.7.
(b) Montrer que tout idéal $A \neq \{0\}$ de $R$ peut être écrit sous la forme $A = \langle p^k \rangle$ pour un entier $k \geq 0$.

# Chapitre 4

# Modules

La notion de module est une extension naturelle de celle d'espace vectoriel. La différence est que les scalaires ne sont plus pris dans un corps mais plutôt dans un anneau. Cela permet d'englober davantage d'objets. Ainsi, on verra qu'un groupe abélien est un module sur l'anneau $\mathbb{Z}$ des entiers. On verra aussi que si $V$ est un espace vectoriel sur un corps $F$ muni d'un opérateur linéaire, alors $V$ est naturellement un module sur l'anneau $F[x]$ des polynômes à une variable sur $F$. Dans ce chapitre, on discute de manière générale la théorie des modules avec les notions de sous-module, de module quotient, de module libre, de somme directe, d'homomorphisme et d'isomorphisme de modules.

## 4.1 La notion d'un module

**Définition 4.1.1** (Module)**.** Un *module* sur un anneau $R$ (ou, un *$R$-module*) est un groupe abélien $(M, +)$, muni d'une application (appelée une *action*)

$$R \times M \mapsto M, \quad (r, u) \mapsto ru,$$

telle que

**(M1)** $r(u + v) = ru + rv$,
**(M2)** $(r + s)v = rv + sv$,
**(M3)** $r(sv) = (rs)v$,
**(M4)** $1v = v$,

pour tous $u, v \in M$, $r, s \in R$. (Ci-dessus, $1 = 1_R$ est l'élément neutre de l'anneau $R$.) On appelle $(M, +)$ le *groupe additif* (sous-jacent) de $M$.

Dans la définition 4.1.1, on a vraiment défini un *module à gauche*. Il existe une notion correspondante de *module à droite*. Cependant, dans ce cours, nous limiterons notre attention aux modules à gauche.

Si on compare la définition de module sur un anneau $R$ à celle d'un espace vectoriel sur un corps $F$, on reconnaît les mêmes axiomes. Comme un corps est un type particulier d'anneau, on en déduit :

*Exemple* 4.1.2. Un module sur un corps $F$ est simplement un espace vectoriel sur $F$.

Puisque $M$ est un group abélien, l'ordre dans laquel on additionne des éléments $v_1, \ldots, v_n$ de $M$ n'affecte pas leur somme, notée

$$v_1 + \cdots + v_n \quad \text{ou} \quad \sum_{i=1}^{n} v_i.$$

L'élément neutre de $(M, +)$ est noté 0, ou parfois $0_M$ quand on veut éviter la confusion avec l'élément zéro de l'anneau $R$. Il est appelé le *zéro* de $M$. On définit la soustraction dans $M$ par

$$u - v := u + (-v), \quad u, v \in M,$$

où $-v$ est l'opposé pour l'addition de of $v$ (ce qu'il existe d'après notre hypothèse que $(M, +)$ est un group abélien). On vérifie aussi, par récurrence sur $n$, que les axiomes de distributivité, (M1) et (M2), implique en général

$$\left(\sum_{i=1}^{n} r_i\right) v = \sum_{i=1}^{n} r_i v \quad \text{et} \quad r \sum_{i=1}^{n} v_i = \sum_{i=1}^{n} r v_i \tag{4.1}$$

pour tous $r, r_1, \ldots, r_n \in R$ et $v, v_1, \ldots, v_n \in M$.

**Lemme 4.1.3.** *Soit $M$ un module sur un anneau $R$. Pour tous $r \in R$ et $v \in M$, on a*

*(a)* $0v = 0$ *et* $r0 = 0$,

*(b)* $(-r)v = r(-v) = -(rv)$.

*Démonstration.* Dans $R$, on a $0 + 0 = 0$. L'axiome (M2) nous donne

$$0v = (0 + 0)v = 0v + 0v.$$

L'addition de $-(0v)$ aux deux côtés nous donne $0 = 0v$. Plus généralement, puisque $r + (-r) = 0$, l'axiome (M2) nous donne aussi

$$0v = (r + (-r))v = rv + (-r)v.$$

Puisque $0v = 0$, cela implique que $(-r)v = -(rv)$.

Les relations $a0 = 0$ et $a(-v) = -(av)$ sont démontrés dans un manière similaire, en utilisant (M1) au lieu de (M2). □

Supposons que $M$ est un $\mathbb{Z}$-module. Alors $M$ est un groupe abélien sous l'addition et, pour tout entier $n \geq 1$ et pour tout $v \in M$, (4.1) nous donne

$$nv = (\underbrace{1 + \cdots + 1}_{n \text{ termes}})v = \underbrace{1v + \cdots + 1v}_{n \text{ termes}} = \underbrace{v + \cdots + v}_{n \text{ termes}}.$$

Gràce au lemme 4.1.3, on trouve aussi

$$(-n)v = n(-v) = \underbrace{(-v) + \cdots + (-v)}_{n \text{ termes}} \quad \text{et} \quad 0v = 0.$$

Autrement dit, la multiplication par les entiers dans $M$ est entièrement déterminée par la loi d'addition dans $M$ et correspond à la notion naturelle de produit par un entier dans un groupe abélien. Réciproquement, si $M$ est un groupe abélien, la définition d'une action par $\mathbb{Z}$ comme ci-dessus satisfait les axiomes (M1)–(M3). Comme il satisfait clairement l'axiome (M4), on en déduit :

**Proposition 4.1.4.** *Un $\mathbb{Z}$-module est simplement un groupe abélien muni de la multiplication naturelle par les entiers.*

La proposition suivante fournit un troisième exemple de module.

**Proposition 4.1.5.** *Soit $V$ un espace vectoriel sur un corps $F$, et soit $T \in \mathrm{End}_F(V)$ un opérateur linéaire sur $V$. Alors $V$ est un $F[x]$-module pour l'addition de $V$ et la multiplication par les polynômes donnée par*

$$p(x)v := p(T)(v)$$

*pour tout $p(x) \in F[x]$ et tout $v \in V$.*

*Démonstration.* Puisque $V$ est un groupe abélien sous l'addition, il suffit à vérifier les axiomes (M1)–(M4). Soient $p(x), q(x) \in F[x]$ et $u, v \in V$. Il faut montrer :

— $1v = v$,
— $p(x)(q(x)v) = (p(x)q(x))v$,
— $(p(x) + q(x))v = p(x)v + q(x)v$,
— $p(x)(u + v) = p(x)u + p(x)v$.

En vertu de la définition de produit par un polynôme, cela revient à montrer

(a) $I_V(v) = v$,
(b) $p(T)(q(T)v) = (p(T) \circ q(T))v$,
(c) $(p(T) + q(T))v = p(T)v + q(T)v$,
(d) $p(T)(u + v) = p(T)u + p(T)v$,

car l'application

$$F[x] \to \mathrm{End}_F(V), \quad p(x) \mapsto p(T),$$

d'évaluation en $T$, étant un morphisme d'anneaux, elle applique 1 sur $I_V$, $p(x) + q(x)$ sur $p(T) + q(T)$ et $p(x)q(x)$ sur $p(T) \circ q(T)$. Les égalités (a), (b), et (c) découlent des définitions de $I_V$, $p(T) \circ q(T)$ et $p(T) + q(T)$ respectivement. Enfin, (d) découle du fait que $p(T)$ est une application linéaire. □

Dans le contexte de la proposition 4.1.5, on note aussi que, pour un polynôme constant $p(x) = a$ avec $a \in F$, on a

$$p(x)v = (aI)(v) = av$$

quel que soit $v \in V$. Donc la notation $av$ possède le même sens que l'on considère $a$ comme un polynôme de $F[x]$ ou comme un scalaire du corps $F$. On peut donc énoncer le complément suivant à la proposition 4.1.5.

**Proposition 4.1.6.** *Dans les notations de la proposition 4.1.5, la multiplication externe par les éléments de $F[x]$ sur $V$ étend la multiplication scalaire par les éléments de $F$.*

*Exemple* 4.1.7. Soit $V$ un espace vectoriel de dimension 2 sur $\mathbb{Q}$ muni d'une base $\mathcal{B} = \{v_1, v_2\}$ et soit $T\colon V \to V$ l'opérateur déterminé pas les conditions

$$T(v_1) = v_1 - v_2, \quad T(v_2) = v_1.$$

On munit $V$ de la structure de $\mathbb{Q}[x]$-module associée à cet endomorphisme $T$ et calcule

$$(2x-1)v_1 + (x^2+3x)v_2.$$

Par définition, on a

$$\begin{aligned}(2\,T - I)(v_1) + (T^2 + 3\,T)(v_2) &= 2\,T(v_1) - v_1 + T^2(v_2) + 3\,T(v_2)\\ &= 3\,T(v_1) - v_1 + 3\,T(v_2) \quad (\text{since } T^2(v_2) = T(T(v_2)) = T(v_1))\\ &= 3(v_1 - v_2) - v_1 + 3v_1\\ &= 5v_1 - 3v_2.\end{aligned}$$

Fixons un anneau $R$ quelconque. On conclut avec quatres exemples généraux de $R$-module. Les détails des preuves sont laissés en exercice.

*Exemple* 4.1.8 (Left regular module). L'anneau $R$ et un $R$-module pour son addition et l'action

$$R \times R \to R, \quad (r, v) \mapsto rv$$

donnée pas le produit dans $R$. Ce module est appelé le *module régulier gauche* pour $R$. Chaque fois qu'on réfère à $R$ comme un $R$-module, on utilise cette action.

*Exemple* 4.1.9. Soit $n \in \mathbb{N}_{>0}$. L'ensemble

$$R^n = \left\{ \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} : r_1, r_2, \ldots, r_n \in R \right\}$$

des $n$-tuples d'éléments de $R$ est un $R$-module pour les opérations

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} + \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} r_1 + s_1 \\ r_2 + s_2 \\ \vdots \\ r_n + s_n \end{pmatrix} \quad \text{et} \quad t \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} tr_1 \\ tr_2 \\ \vdots \\ tr_n \end{pmatrix}.$$

Pour $n = 1$, on retrouve la structure naturelle de $R$-module sur $R^1 = R$ décrite par l'exemple 4.1.8.

*Exemple* 4.1.10. Rappelons de l'exemple 1.1.5 que $\mathrm{Mat}_n(R)$ est un anneau, avec les règles naturelles d'addition et de multiplication des matrices. Alors $R^n$ est un $\mathrm{Mat}_n(R)$-module, avec l'action donnée par la multiplication matricielle à gauche.

*Exemple* 4.1.11. Soient $M_1, \ldots, M_n$ des $R$-modules. Leur produit cartésien

$$M_1 \times \cdots \times M_n = \{(v_1, \ldots, v_n) : v_1 \in M_1, \ldots, v_n \in M_n\}$$

est un $R$-module pour les opérations

$$\begin{aligned}(v_1, \ldots, v_n) + (y_1, \ldots, y_n) &= (v_1 + y_1, \ldots, v_n + y_n),\\ c(v_1, \ldots, v_n) &= (cv_1, \ldots, cv_n).\end{aligned}$$

*Remarque* 4.1.12. Si on applique la construction de l'exemple 4.1.11 avec $M_1 = \cdots = M_n = R$ pour la structure naturelle de $R$-module sur $R$ donnée dans l'exemple 4.1.8, on obtient une structure de $R$-module sur $R \times \cdots \times R = R^n$ qui est essentiellement celle de l'exemple 4.1.9 sauf que les éléments de $R^n$ sont présentés sous forme de lignes. Pour les applications ultérieures, il est cependant plus commode d'écrire les éléments de $R^n$ en colonnes.

*Remarque* 4.1.13. Parfois, on va écrire $M_1 \oplus \cdots \oplus M_n$ au lieu de $M_1 \times \cdots \times M_n$. Voir l'exemple 4.5.4.

---

## Exercices.

4.1.1. Compléter la preuve du lemme 4.1.3 en montrant que $a0 = 0$ et $a(-v) = -(av)$.

4.1.2. Soit $V$ un espace vectoriel de dimension 3 sur $\mathbb{Z}_5$ muni d'une base $\mathcal{B} = \{v_1, v_2, v_3\}$ et soit $T\colon V \to V$ l'opérateur linéaire déterminé par les conditions

$$T(v_1) = v_1 + \bar{2}v_2 - v_3, \quad T(v_2) = v_2 + \bar{4}v_3, \quad T(v_3) = v_3.$$

Pour la structure correspondante de $\mathbb{Z}_5[x]$-module sur $V$, calculer

(a) $xv_1$,
(b) $xv_1 - (x + \bar{1})v_2$,
(c) $(\bar{2}x^2 - \bar{3})v_1 + (\bar{3}x)v_2 + (x^2 + \bar{2})v_3$.

4.1.3. Soit $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ l'opérateur linéaire dont la matrice en base standard $\mathcal{E} = \{e_1, e_2\}$ est $[T]_{\mathcal{E}} = \begin{pmatrix} 2 & -1 \\ 3 & 0 \end{pmatrix}$. Pour la structure de $\mathbb{R}[x]$-module associée sur $\mathbb{R}^2$, calculer

(a) $xe_1$,
(b) $x^2e_1 + e_2$,
(c) $(x^2 + x + 1)e_1 + (2x - 1)e_2$.

4.1.4. Soit $n \in \mathbb{N}_{>0}$ et soit $R$ un anneau. Montrer que $R^n$ est un $R$-module pour les opérations définies dans l'exemple 4.1.9.

4.1.5. Soient $M_1, \ldots, M_n$ des modules sur un anneau $R$. Montrer que leur produit cartésien $M_1 \times \cdots \times M_n$ est un $R$-module pour les opérations définies dans l'exemple 4.1.11.

4.1.6. Soit $M$ un module sur l'anneau $R$ et soit $X$ un ensemble. Pour tout $r \in R$ et toute paire de fonctions $f\colon X \to M$ et $g\colon X\ toM$, on définit $f + g\colon X \to M$ et $af\colon X \to M$ en posant

$$(f + g)(x) = f(x) + g(x) \quad \text{et} \quad (af)(x) = af(x)$$

pour tout $x \in X$. Montrer que l'ensemble $\mathcal{F}(X, M)$ des fonctions de $X$ dans $M$ est un $R$-module pour ces opérations.

## 4.2 Sous-modules

Fixons un module $M$ quelconque sur un anneau $R$ quelconque.

**Définition 4.2.1** (Sous-module)**.** Un sous-$R$-module de $M$ est un sous-ensemble $N$ de $M$ qui remplit les conditions suivantes :

**(SM1)** $0 \in N$,
**(SM2)** Si $u, v \in N$, alors $u + v \in N$.
**(SM3)** Si $r \in R$ et $u \in N$, alors $ru \in N$.

On note que la condition (SM3) implique que $-v = (-1)v \in N$ pour tout $v \in N$ ce qui, joint aux conditions (SM1) et (SM2), signifie qu'un sous-$R$-module de $M$ est, en particulier, un sous-groupe de $M$.

Les conditions (SM2) et (SM3) demandent qu'un sous-$R$-module $N$ de $M$ soit invariant sous l'addition dans $M$ et l'action par les éléments de $R$. Par restriction, ces opérations fournissent donc une addition sur $N$ et une action par les éléments de $R$ sur $N$. On laisse en exercice le soin de vérifier que ces opérations satisfont les axiomes de la définition 4.1.1 requis pour faire de $N$ un $R$-module.

**Proposition 4.2.2.** *Un sous-$R$-module $N$ de $M$ est lui-même un $R$-module pour l'addition et la multiplication par les éléments de $R$ restreintes de $M$ à $N$.*

Tout $R$-module $M$ a le sous-module zéro (ou nul) $\{0\}$ et le sous-module $M$ lui-même. On dit qu'un sous-module $N$ de $M$ est *propre* si $N \neq M$.

**Définition 4.2.3** (Simple module)**.** Un $R$-module $M$ non nul est *simple* s'il n'a aucun sous-module propre non nul. Autrement dit, $M$ est simple si $M \neq \{0\}$ et les seuls sous-modules de $M$ sont $\{0\}$ et $M$.

*Exemple* 4.2.4. Soit $V$ un espace vectoriel sur un corps $F$. Un sous-$F$-module $V$ est simplement un sous-$F$-espace vectoriel de $V$. L'espace vectoriel $V$ est simple si et seulement s'il est de dimension 1.

*Exemple* 4.2.5. Soit $M$ un groupe abélien. Un sous-$\mathbb{Z}$-module de $M$ est simplement un sous-groupe de $M$. Un groupe abélien est un $\mathbb{Z}$-module simple si et seulement s'il est un group simple.

*Exemple* 4.2.6. Soit $R$ un anneau considéré comme module sur lui-même (c.-à-d. le module régulier gauche de l'exemple 4.1.8). Un sous-$R$-module de $R$ est simplement un idéal gauche de $R$.

Dans le cas d'un espace vectoriel $V$ muni d'un endomorphisme, le concept de sous-module se traduit ainsi :

**Proposition 4.2.7.** *Soit $V$ un espace vectoriel sur un corps $F$ et soit $T \in \mathrm{End}_F(V)$. Pour la structure correspondante de $F[x]$-module sur $V$, un sous-$F[x]$-module de $V$ est simplement un sous-espacce vectoriel $T$-*invariant *de $V$, c'est-à-dire, un sous-espace vectoriel $U$ de $V$ tel que $T(u) \in U$ pour tout $u \in U$.*

*Démonstration.* Comme l'action par les éléments de $F[x]$ sur $V$ étend la multiplication scalaire par les éléments de $F$ (voir la proposition 4.1.6), un sous-$F[x]$-module $U$ de $V$ est nécessairement un sous-espace vectoriel de $V$. Comme il satisfait aussi $xu \in U$ pour tout $u \in U$, et que $xu = T(u)$ (par définition), on obtient aussi que $U$ doit être $T$-invariant.

Réciproquement, si $U$est un sous-espace vectoriel $T$-invariant de $U$, on a $T(u) \in U$ pour tout $u \in U$. Par récurrence sur $n$, on en déduit que $T^n(u) \in U$ pour tout entier $n \geq 1$ et tout $u \in U$. Par suite, pour tout polynôme $p(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ et tout $u \in U$, on trouve

$$p(x)u = (a_0I + a_1T + \cdots + a_nT^n)(u) = a_0u + a_1T(u) + \cdots + a_nT^n(u) \ \in \ U.$$

Donc $U$ est un sous-$F[x]$-module de $V$ : on vient de montrer qu'il remplit la condition (SM3) et les autres conditions (SM1) et (SM2) sont satisfaites en vertu du fait que $U$ est un sous-espace de $V$. □

On conclut cette section avec quelques constructions générales valables pour un $R$-module quelconque.

**Proposition 4.2.8.** *Soit $S$ un sous-ensemble d'un $R$-module $M$. L'ensemble*

$$\{r_1u_1 + \cdots + a_ku_k : k \in \mathbb{N},\ a_1, \ldots, a_k \in A,\ u_1, \ldots, u_k \in S\}$$

*(on permet la possibilité que $k = 0$, auquel cas la somme ci-dessus est l'élément nul de $M$) est un sous-$R$-module de $M$ qui contient $S$ et il est le plus petit sous-$R$-module de $M$ avec cette propriété (c.-à-d. tout sous-$R$-module de $M$ qui contient $S$ contient ce sous-module).*

*Démonstration.* La démonstration de ce résultat est l'exercice 4.2.3. □

Le sous-$R$-module de la proposition 4.2.8 est appelé le sous-$R$-module de $M$ *engendré* par $S$. Il est noté

$$\langle S\rangle_R \quad \text{ou} \quad RS \quad \text{or} \quad \operatorname{Span}_R S.$$

Si $S = \{u_1, \ldots, u_k\}$, nous le désignons également par

$$\langle u_1, \ldots, u_k\rangle_R \quad \text{ou} \quad Ru_1 + \cdots + Ru_k \quad \text{ou} \quad \operatorname{Span}_R\{u_1, \ldots, u_k\}.$$

**Définition 4.2.9** (Module cyclique et module de type fini)**.** On dit qu'un $R$-module $M$ (ou un sous-$R$-module de $M$) est *cyclique* s'il est engendré par un seul élément. On dit qu'il est de *finite fini* s'il est engendré par un nombre fini d'éléments de $M$.

*Exemple* 4.2.10. Si $u_1, \ldots, u_k$ sont des éléments d'un groupe abélien $M$, alors $\langle u_1, \ldots, u_k\rangle_{\mathbb{Z}}$ est simplement le sous-groupe de $M$ engendré par $u_1, \ldots, u_k$. En particulier, In particular, $M$ est cyclique en tant que groupe abélien si et seulement s'il est cyclique en tant que $\mathbb{Z}$-module.

*Exemple* 4.2.11. Soit $V$ un espace vectoriel de dimension finie sur un corps $F$, soit $\{v_1, \ldots, v_k\}$ un système de générateurs de $V$, et soit $T \in \operatorname{End}_F(V)$. Comme la structure de $F[x]$-module sur $V$ associée à $T$ étend celle de $F$-module, on a

$$V = \langle v_1, \ldots, v_k\rangle_F \subseteq \langle v_1, \ldots, v_k\rangle_{F[x]},$$

donc $V = \langle v_1, \ldots, v_k\rangle_{F[x]}$ est aussi engendré par $v_1, \ldots, v_k$ en tant que $F[x]$-module. En particular, $V$ est un $F[x]$-module de type fini.

**Proposition 4.2.12.** *Soient $N_1, \ldots, N_k$ des sous-modules d'un $R$-module $M$. Leur* intersection $N_1 \cap \cdots \cap N_k$ *et leur* somme

$$N_1 + \cdots + N_k := \{u_1 + \cdots + u_k : u_1 \in N_1, \ldots, u_k \in N_k\}$$

*sont des sous-$R$-modules de $M$.*

*Preuve pour la somme.* On note d'abord que, puisque $0 \in N_i$ pour $i = 1, \ldots, s$, on a

$$0 = 0 + \cdots + 0 \in N_1 + \cdots + N_k.$$

Soient $u, u'$ des éléments quelconques de $N_1 + \cdots + N_k$, et soit $r \in R$. On peut écrire

$$u = u_1 + \cdots + u_k \quad \text{et} \quad u' = u'_1 + \cdots + u'_k$$

avec $u_1, u'_1 \in N_1, \ldots, u_k, u'_k \in N_k$. Par suite, on obtient

$$u + u' = (u_1 + u'_1) + \cdots + (u_k + u'_k) \in N_1 + \cdots + N_k,$$
$$ru = (ru_1) + \cdots + (ru_k) \in N_1 + \cdots + N_k.$$

Cela montre que $N_1 + \cdots + N_k$ est un sous-$R$-module de $M$. □

Notons que la notation $Ru_1 + \cdots + Ru_k$ pour le sous-$R$-module $\langle u_1, \ldots, u_k \rangle_R$ engendré par des éléments $u_1, \ldots, u_s$ de $M$ est consistante avec la notion de somme de sous-modules car, pour tout élément $u$ de $M$, on a

$$Ru = \langle u \rangle_R = \{au : a \in A\}.$$

Lorsque $R = F$ est un corps, on reconnaît les notions usuelles d'intersection et de somme de sous-espaces d'un espace vectoriel sur $F$. Lorsque $R = \mathbb{Z}$, on retrouve plutôt les notions d'intersection et de somme de sous-groupes d'un groupe abélien.

**Définition 4.2.13** (Annulateur)**.** Supposons que $M$ soit un $R$-module et que $S$ soit un sous-ensemble de $M$. L'*annulateur* de $S$ est

$$\mathrm{ann}(S) := \{r \in R : ru = 0 \text{ pour tout } u \in S\}.$$

Lorsqu'on considère $R$ comme module sur lui-même comme dans l'exemple 4.1.8, la notion ci-dessus d'annulateur coïcide avec celle de l'exercice 1.3.13.

---

# Exercices.

4.2.1. Démontrer la proposition 4.2.2.

4.2.2. Soit $M$ un groupe abélien. Expliquer pourquoi les sous-$\mathbb{Z}$-modules de $M$ sont simplement les sous-groupes de $M$. *Indice* : Montrer que tout sous-$\mathbb{Z}$-module de $M$ est un sous-group de $M$ et, réciproquement, que tous sous-groupe de $M$ est un sous-$\mathbb{Z}$-module de $M$.

4.2.3. Démontrer la proposition 4.2.8.

4.2.4. Soit $M$ un module sur un anneau $R$, et soit $u_1, \dots, u_k, v_1, \dots, v_m \in M$. Soient $L = \langle u_1, \dots, u_k \rangle_R$ et $N = \langle v_1, \dots, v_m \rangle_R$. Montrer que $L + N = \langle u_1, \dots, u_k, v_1, \dots, v_m \rangle_R$.

4.2.5. Démontrer qu'un $R$-module $M$ est simple si et seulement s'il est engendré par tout élément non nul. En d'autres termes, démontrer que $M$ est simple si et seulement si $\langle u \rangle_R = M$ pour tout $u \in M$, $u \neq 0$.

4.2.6. Soit $M$ un module sur un anneau $R$. On dit qu'un élément $u$ de $M$ est *torsion* s'il existe un élément non nul $r$ de $R$ tel que $ru = 0$. On dit que $M$ est un *$R$-module torsion* si tous ces élément sont torsions. On dit qu'il est *sans torsion* si zéro est son seul élément torsion. Supposons que $R$ est un anneau intègre.

(a) Montrer que l'ensemble $M_{\text{tor}}$ des éléments torsions de $M$ est un sous-$R$-module de $M$.
(b) Montrer que, si $M$ est de type fini et tous ces éléments sont torsions, alors il existe un élément non nul $r$ de $R$ el que $ru = 0$ pour tout $u \in M$.

4.2.7. Supposons que $M$ soit un $R$-module et que $S$ soit un sous-ensemble de $M$.

(a) Montrer que $\operatorname{ann}(S)$ est un idéal gauche de $R$. Il s'ensuit que, si $R$ est commutatif, alors $\operatorname{ann}(S)$ est un idéal bilatère de $R$.
(b) Donner un exemple qui montre que $\operatorname{ann}(S)$ n'est pas toujours un idéal bilatère de $R$.
(c) Montrer que, si $R$ est commutatif, alors $\operatorname{ann}(S) = \operatorname{ann}(RS)$.
(d) Donner un exemple où $\operatorname{ann}(S) \neq \operatorname{ann}(RS)$.

## 4.3 Modules quotients

Si $N$ est un sous-module d'un $R$-module $M$, alors on peut considérer le quotient $M/N$ des groupes additifs correspondants.

**Théorème 4.3.1.** *Si $N$ est un sous-module d'un $R$-module $M$, alors $M/N$ est un $R$-module avec l'action déterminée par*

$$r(u + N) = ru + N, \quad r \in R,\ u \in M.$$

*Démonstration.* On le laisse en exercice (l'exercice 4.3.1) de vérifier que l'action est bien définie (c.-à-d. indépendante de le représentative $u$) et qu'elle satisfait les conditions de la définition 4.1.1. □

*Exemple* 4.3.2. Si $M$ est un groupe abélien, alors un sous-$\mathbb{Z}$-module est simplement un sous-groupe $N$. (Rappelons que, pour les groupes abéliens, tout sous-groupe est normal.) Alors la notion de module quotient coïncide avec la notion de groupe quotient.

*Exemple* 4.3.3. Comme dans l'exemple 4.2.6, les sous-modules du module régulier gauche de $R$ sont les idéaux gauches de $R$. Ainsi, pour tout idéal gauche $I$ de $R$, on a le $R$-module quotient $R/I$.

*Exemple* 4.3.4. Si $V$ est un espace vectoriel sur un corps $F$, alors les sous-$F$-modules sont simplement les sous-espace vectoriels. Pour tout sous-espace vectoriel $U$ de $V$ on a donc l'espace vectoriel quotient $V/U$.

---

## Exercices.

4.3.1. Démontrer le théorème 4.3.1.

4.3.2. Supposons que $M$ soit un $R$-module. Rappelons la définition du module torsion $M_{\text{tor}}$ de $M$ (l'exercise 4.2.6). Montrer que $M/M_{\text{tor}}$ est sans torsion.

## 4.4 Modules libres

**Définition 4.4.1** (Indépendance linéaire, base, module libre)**.** Soient $u_1, \dots, u_n$ des éléments d'un $R$-module $M$.

(a) On dit que $u_1, \dots, u_n$ sont *linéairement indépendant* sur $R$ si les seules valeurs des éléments $r_1, \dots, r_n$ de $R$ tels que

$$r_1 u_1 + \cdots + r_n u_n = 0$$

sont $r_1 = \cdots = r_n = 0$.

(b) On dit que $\{u_1, \dots, u_n\}$ est une *base* de $M$ si $u_1, \dots, u_n$ sont linéairement indépendants sur $R$ et ils engendrent $M$ en tant que $R$-module.

(c) On dit que $M$ est un $R$-module *libre* s'il admet une base.

Par convention le module $\{0\}$ constitué d'un seul élément est un $R$-module libre qui admet l'ensemble vide comme base.

*Exemple* 4.4.2. Soit $n \in \mathbb{N}_{>0}$. Le $R$-module $R^n$ introduit dans l'exemple 4.1.9 admet la base

$$\left\{ e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\}.$$

En effet, on a

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = r_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + r_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + r_n \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \tag{4.2}$$

pour tous $r_1, \ldots, r_n \in R$. Ainsi $e_1, \ldots, e_n$ engendrent $R^n$ en tant que $R$-module. De plus, si $r_1, \ldots, r_n \in A$ satisfait $r_1 e_1 + \cdots + r_n e_n = 0$, alors l'égalité (4.2) nous donne

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

et donc $r_1 = r_2 = \cdots = r_n = 0$. Ainsi $e_1, \ldots, e_n$ sont aussi linéairement indépendant sur $R$.

**Lemme 4.4.3.** *Toute base d'un $R$-module libre $M$ est un ensemble engendrant minimal.*

*Démonstration.* Supposons que $B$ soit une base de $M$ et que $B_0$ est un sous-ensemble propre de $B$. Soit $b \in B \setminus B_0$. Si $b$ était contenu dans $\langle B_0 \rangle_R$, alors $b$ on pouvait l'exprimer comme combinaison $R$-linéaire des éléments de $B_0$, ce qui contredirait l'indépendance linéaire de $B$. Par conséquent, $b \notin \langle B_0 \rangle_R$, et $B_0$ n'engendre pas $M$. □

**Lemme 4.4.4.** *Toute base d'un $R$-module libre de type fini est finie.*

*Démonstration.* Supposons que $M$ soit un $R$-module avec une base (peut-être infinie) $B$ et un ensemble fini de générateurs $S$. Chaque élément de $S$ est un combinaison linéaire d'un nombre fini d'éléments de $B$. Puisque $S$ est fini, il est contenu dans le sous-module de $B$ engendré par un sous-ensemble fini $B_0$. Mais alors $M = \langle S \rangle_R \subseteq \langle \langle B_0 \rangle_R \rangle_R = \langle B_0 \rangle_R$. Ainsi $B_0$ engendre $M$. D'après le lemme 4.4.3, $B = B_0$. □

En algèbre linéaire, vous avez appris que chaque espace vectoriel a une base et que toutes les bases ont la même cardinalité. Vous définissez ensuite la dimension d'un espace vectoriel comme étant la cardinalité de n'importe quelle base. Lorsque vous travaillez avec le concept plus général des modules, vous devez être plus prudent. Tout d'abord, il existe des modules qui ne sont pas libres, et donc qui ne possède aucune base. Voir, par exemple, l'exercice 4.4.1. Deuxièmement, même si un $R$-module $M$ est libre, il peut avoir des bases de cardinalités différentes ! Voir, par exemple, l'exercice 4.8.2.

---

## Exercices.

4.4.1. Montrer qu'un group abélien fini $M$ admet une basis en tant que $\mathbb{Z}$-module si et seulement si $M = \{0\}$ (auquel cas l'ensemble vide est, par convention, une base de $M$).

4.4.2. En général, montrer que, si $M$ est un module fini sur un anneau infini $R$, alors $M$ est un module libre si et seulement si $M = \{0\}$.

4.4.3. Soit $V$ un espace vectoriel de type fini sur un corps $F$ et soit $T \in \mathrm{End}_F(V)$. Montrer que, pour la structure de $F[x]$-module correspondante, $V$ admet une base si et seulement si $V = \{0\}$.

4.4.4. Soient $m$ et $n$ des entiers positifs est soit $R$ un anneau. Montrer que $\mathrm{Mat}_{m\times n}(R)$, l'ensemble des matrices de type $m \times n$ avec coefficients dans $R$, est un $R$-module libre pour les operations naturelles d'addition et de multiplication par des éléments de $R$.

## 4.5 Somme directe

**Définition 4.5.1** (Somme directe)**.** Soient $M_1, \ldots, M_k$ des sous-modules d'un $R$-module $M$. On dit que leur somme est *directe* si le seul choix de $u_1 \in M_1, \ldots, u_k \in M_k$ tels que

$$u_1 + \cdots + u_k = 0$$

est $u_1 = \cdots = u_k = 0$. Lorsque cette condition est remplie, on écrit le somme $M_1 + \cdots + M_k$ comme $M_1 \oplus \cdots \oplus M_k$. On dit que $M$ est la *somme directe* de $M_1, \ldots, M_k$ si $M = M_1 \oplus \cdots \oplus M_k$.

Les propositions suivantes qui généralisent les résultats analogues pour les sommes directes des espaces vectoriels sont laissées en exercice. La première justifie l'importance de la notion de somme directe.

**Proposition 4.5.2.** *Soient $M_1, \ldots, M_k$ des sous-modules d'un $R$-module $M$. Alors, on a $M = M_1 \oplus \cdots \oplus M_k$ si et seulement si, pour tout $u \in M$, il existe un et un seul choix de $u_1 \in M_1, \ldots, u_k \in M_k$ tels que $u = u_1 + \cdots + u_k$.*

**Proposition 4.5.3.** *Soient $M_1, \ldots, M_k$ des sous-modules d'un $R$-module $M$. Les conditions suivantes sont équivalentes :*

*(a) la somme de $M_1, \ldots, M_k$ est directe ;*
*(b) $M_i \cap (M_1 + \cdots + \widehat{M_i} + \cdots + M_k) = \{0\}$ pour $i = 1, \ldots, s$ ;*
*(c) $M_i \cap (M_{i+1} + \cdots + M_k) = \{0\}$ pour $i = 1, \ldots, k-1$.*

*(La notation $\widehat{M_i}$ veut-dire qu'on omet le terme $M_i$ de la somme.)*

*Exemple* 4.5.4. Supposons que $M_1, \ldots, M_k$ sont des $R$-modules, et considérons leur produit cartésien

$$M = M_1 \times \cdots \times M_k$$

comme dans l'exemple 4.1.11. Pour $1 \leq i \leq k$, soit

$$M_i' = \{(0, \ldots, 0, u, 0, \ldots, 0) : 0 \in M_i\},$$

où $u$ est dans la $i$-ième place. Alors $M_i'$ est un sous-module de $M$, et on a un isomorphisme de $R$-modules

$$M_i \to M_i', \quad u \mapsto (0, \ldots, 0, u, 0, \ldots, 0), \tag{4.3}$$

et

$$M_1 \times \cdots \times M_k = M_1' \oplus \cdots \oplus M_k'.$$

Si on utilise (4.3) pour identifier $M_i$ et $M_i'$, on a donc $M = M_1 \oplus \cdots \oplus M_k$. Pour cette raison, on utiliser parfois la notation $\oplus$ pour le produit cartésien, et on l'appelle la "somme directe" ; voir la remarque 4.1.13.

*Exemple* 4.5.5. Soit $V$ un espace vectoriel sur un corps $F$ et soit $T \in \mathrm{End}_F(V)$. Pour la structure correspondante d'un $F[x]$-module sur $V$, on sait que les sous-modules de $V$ sont simplement lest sous-espaces $T$-invariantes de $V$. Puisque la notion de somme directe implique seulement l'addition, $V$ est une somme directe, en tant que $F[x]$-module, des sous-$F[X]$-modules $V_1, \ldots, V_k$ si et seulement s'il est une somme directe, en tant qu'espace vectoriel, des sous-espaces $T$-invariantes $V_1, \ldots, V_k$.

**Définition 4.5.6** (Module indécomposable)**.** Un $R$-module non nul est *indécomposable* s'il ne peut pas être écrit comme somme directe de deux sous-modules non nuls.

**Proposition 4.5.7.** *Tout module simple est indécomposable.*

*Démonstration.* On démontre la proposition contraposée. Supposons que $M$ n'est pas indécomposable. Alors il existe des sous-modules non nuls $M_1$ et $M_2$ de $M$ tels que $M = M_1 \oplus M_2$. Alors $M_1$ est un sous-module non nul de $M$ qui est aussi propre puisque $M_1 = M$ impliquerait que $M_2 = \{0\}$. Ainsi $M$ n'est pas simple. □

La proposition 4.5.7 nous donne de nombreux exemples de modules indécomposables. Par exemple, tout espace vectoriel de dimension un sur un corps $F$ est un $F$-module indécomposable (voir l'exemple 4.2.4) et tout groupe abélien simple est un $\mathbb{Z}$-module indécomposable (voir l'exemple 4.2.5). Cependant, l'inverse de la proposition 4.5.7 est faux, comme l'illustre l'exemple suivant.

*Exemple* 4.5.8. En tant que module sur lui-même, $\mathbb{Z}$ est un $\mathbb{Z}$-module indécomposable qui n'est pas simple. En effet, puisque $\mathbb{Z}$ a de nombreux idéaux propres non nuls, ce n'est clairement pas un $\mathbb{Z}$-module simple. Il reste donc à montrer qu'il est indécomposable. Supposons qu'il existe des sous-modules $M, N$ tels que $\mathbb{Z} = M \oplus N$. Comme noté dans l'exemple 4.2.6, cela signifie que $M$ et $N$ sont des idéaux de $\mathbb{Z}$. D'après la proposition 1.3.6, il existe des éléments $m, n \in \mathbb{Z}$ non nuls tels que $M = m\mathbb{Z}$ et $N = n\mathbb{Z}$. Mais alors $mn \in M \cap N$, et donc la somme $M + N$ n'est pas directe, ce qui est une contradiction.

---

## Exercices.

4.5.1. Démontrer la proposition 4.5.2.

4.5.2. Soit $M$ un $R$-module et soit $u_1, \ldots, u_n \in M$. Montrer que $\{u_1, \ldots, u_n\}$ est une base de $M$ si et seulement si $M = Ru_1 \oplus \cdots \oplus Ru_n$ et aucun des éléments $u_1, \ldots, u_n$ est torsion. (Voir l'exemple 4.2.6 pour la définition de *torsion*.)

4.5.3. Soit $F$ un corps. Montrer que le $F$-module quotient $F[x]/x^2F[x]$ (voir l'exemple 4.3.3) est indécomposable, mais qu'il n'est pas simple.

4.5.4. Supposons que $F$ soit un corps. Montrer qu'un $F$-module est simple si et seulement s'il est indécomposable.

4.5.5. Un $R$-module $P$ est *projectif* s'il est facteur direct dans un module libre. En d'autres terms, $P$ est projectif s'il existe un autre $R$-module $M$ tel que $P \oplus M$ est un $R$-module libre. Il est claire que chaque module libre est projectif. (On peut prendre $M = \{0\}$.) Montrer que le $\mathrm{Mat}_n(\mathbb{C})$-module $\mathbb{C}^n$ (action par multiplication matricielle à gauche) est projectif mais qu'il n'est pas libre.

## 4.6 Morphismes de modules

Fixons un anneau $R$.

**Définition 4.6.1.** Soient $M$ et $N$ des $R$-modules. Un *morphisme* de $R$-modules (ou *homomorphisme* de $R$-modules) de $M$ dans $N$ est une application $\varphi\colon M \to N$ qui remplit les conditions suivantes :

**(HM1)** $\varphi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2)$ pour tous $u_1, u_2 \in M$ (c.-à-d. $\varphi$ est un morphisme de groupes additifs) ;

**(HM2)** $\varphi(ru) = r\varphi(u)$ pour tous $r \in R$ et $u \in M$.

*Exemple* 4.6.2. Si $R = F$ est un corps, alors des $F$-modules $M$ et $N$ sont simplement des espace vectoriels sur $F$ est un morphisme de $F$-modules $\varphi\colon M \to N$ est simplement une application linéaire de $M$ dans $N$.

*Exemple* 4.6.3. Rappelons que si $A = \mathbb{Z}$, alors des $\mathbb{Z}$-modules $M$ et $N$ sont simplement les groups abéliens équipés de la multiplication naturelles par des entiers. Si $\varphi\colon M \to N$ est un morphisme de $\mathbb{Z}$-modules, la condition (HM1) montre que c'est un morphisme de groupes. Réciproquement si $\varphi\colon M \to N$ est un morphisme de groupes abéliens, on a

$$\varphi(nu) = n\varphi(u)$$

pour tout $n \in \mathbb{Z}$ et tout $u \in M$ (exercice), donc $\varphi$ remplit les conditions (HM1) et (HM2) de la définition 4.6.1. Donc, *un homomorphisme de $\mathbb{Z}$-modules est simplement un morphisme de groupes abéliens.*

*Exemple* 4.6.4. Si $N$ est un sous-module d'un $R$-module $M$, alors l'*application quotient*

$$M \to M/N, \quad m \mapsto m + N,$$

est un morphisme de $R$-modules surjectif. Voir l'exercice 4.6.1.

*Exemple* 4.6.5. Soit $V$ un espace vectoriel sur un corps $F$ et soit $T \in \mathrm{End}_F(V)$. Pour la structure correspondante de $F[x]$-module sur $V$, un morphisme de $F[x]$-modules $S\colon V \to V$est simplement une application linéaire telle que $S \circ T = T \circ S$ (exercice).

*Exemple* 4.6.6. Soient $m, n \in \mathbb{N}_{>0}$, et soit $P \in \mathrm{Mat}_{m\times n}(A)$. Pour tout choix de $u, u' \in R^n$ et $r \in R$, on a :

$$P(u + u') = Pu + Pu' \quad \text{et} \quad P(ru) = rPu.$$

Donc la fonction

$$R^n \to R^m, \quad u \mapsto Pu,$$

est un morphisme de $R$-modules.

Le résultat suivant montre qu'on obtient ainsi tous les morphismes de $R$-modules de $R^n$ dans $R^m$.

**Proposition 4.6.7.** *Soient $m, n \in \mathbb{N}_{>0}$ et soit $\varphi\colon R^n \to R^m$ un morphisme de $R$-modules. Il existe une et une seule matrice $P \in \mathrm{Mat}_{m\times n}(R)$ telle que*

$$\varphi(u) = Pu \quad \textit{pour tout } u \in R^n. \tag{4.4}$$

*Démonstration.* Soit $\{e_1, \dots, e_n\}$ la base «canonique» de $R^n$ définie dans l'exemple 4.4.2 et soit $P$ la matrice $m \times n$ dont les colonnes sont $C_1 := \varphi(e_1), \dots, C_n := \varphi(e_n)$. Pour tout $u = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in R^n$, on a :

$$\varphi(u) = \varphi(r_1e_1 + \cdots + r_ne_n) = r_1C_1 + \cdots + r_nC_n = \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = Pu.$$

Donc $P$ satisfait la condition (4.4). C'est la seule matrice qui remplisse cette condition car si une matrice $P' \in \mathrm{Mat}_{m\times n}(R)$ satisfait aussi $\varphi(u) = P'u$ pour tout $u \in R^n$, alors sa $j$-ième colonne est $P'e_j = \varphi(e_j) = C_j$ pour tout $j = 1, \dots, n$. □

On reprend la théorie générale avec le résultat suivant.

**Proposition 4.6.8.** *Soient $\varphi\colon M \to N$ et $\psi\colon N \to P$ des morphismes de $R$-modules.*

*(a) La composée $\psi \circ \varphi\colon M \to P$ est aussi un morphisme de $R$-modules.*

*(b) Si $\varphi\colon M \to N$ est bijective, son inverse $\varphi^{-1}\colon N \to M$ est un morphisme de $R$-modules.*

*Démonstration.* La partie (a) est laissé en exercice. Pour démontrer (b), supposons que $\varphi$ soit bijectif. Soient $v, v' \in N$ et $r \in R$. On pose

$$u := \varphi^{-1}(v) \quad \text{et} \quad u' := \varphi^{-1}(v').$$

Comme $u, u' \in M$ et $\varphi$ est un morphisme de $R$-modules, on trouve

$$\varphi(u + u') = \varphi(u) + \varphi(u') = v + v' \quad \text{et} \quad \varphi(ru) = r\varphi(u) = rv.$$

Par conséquent,

$$\varphi^{-1}(v + v') = u + u' = \varphi^{-1}(v) + \varphi^{-1}(v') \quad \text{et} \quad \varphi^{-1}(rv) = ru = r\varphi^{-1}(v).$$

Cela montre bien que $\varphi^{-1}\colon N \to M$ est un morphisme de $R$-modules. □

**Définition 4.6.9** (Isomorphisme)**.** Un morphisme de $R$-modules qui est bijectif est appelé un *isomorphisme* de $R$-modules. On dit qu'un $R$-module $M$ est *isomorphe* à un $R$-module $N$ s'il existe un isomorphisme de $R$-modules $\varphi\colon M \to N$. On écrit alors $M \simeq N$.

En vertu de ces définitions, la proposition 4.6.8 admet pour conséquence immédiate :

**Corollaire 4.6.10.** *Soient $\varphi\colon M \to N$ et $\psi\colon N \to P$ des isomorphismes de $R$-modules. Alors $\psi \circ \varphi\colon M \to P$ et $\varphi^{-1}\colon N \to M$ sont aussi des isomorphismes de $R$-modules.*

On en déduit encore que l'isomorphisme est une relation d'équivalence sur la classe des $R$-modules. De plus, l'ensemble des isomorphismes de $R$-modules d'un $R$-module $M$ dans lui-même, appelés *automorphismes* de $M$, forment un sous-groupe du groupe des bijections de $M$ dans lui-même. On l'appelle le *groupe des automorphismes* de $M$.

**Définition 4.6.11.** Soit $\varphi\colon M \to N$ un morphisme de $R$-modules. Le *noyau* de $\varphi$ est

$$\ker(\varphi) := \{u \in M : \varphi(u) = 0\}$$

et l'*image* de $\varphi$ est

$$\mathrm{im}(\varphi) := \{\varphi(u) : u \in M\}.$$

Le noyau et l'image d'un homomorphisme de $R$-modules $\varphi\colon M \to N$ sont donc simplement le noyau et l'image de $\varphi$ considéré comme morphisme de groupes abéliens. Le résultat suivant est laissé en exercice.

**Proposition 4.6.12.** *Soit $\varphi\colon M \to N$ un morphisme de $R$-modules.*

*(a)* $\ker(\varphi)$ *est un sous-$R$-module de $M$.*

*(b)* $\mathrm{im}(\varphi)$ *est un sour-$R$-module of $N$.*

*(c) Le morphisme $\varphi$ est injectif si et seulement si* $\ker(\varphi) = \{0\}$. *Il est surjectif si et seulement si* $\mathrm{im}(\varphi) = N$.

*Exemple* 4.6.13. Soit $M$ un $R$-module et soit $r \in Z(R)$ (voir la définition 1.1.26). L'application

$$\varphi\colon M \to M, \quad u \to ru$$

est un momorphisme de $R$-modules (exercice). Son noyau est

$$M_r := \{u \in M : ru = 0\}$$

et son image est

$$rM := \{ru : u \in M\}.$$

Donc, en vertu de la proposition 4.6.12, $M_a$ et $aM$ sont des sous-$R$-modules de $M$.

*Exemple* 4.6.14. Considérons $R$ comme module sur lui-même, comme dans l'exemple 4.1.8. Tout $s \in R$ détermine un morphisme de $R$-modules

$$\rho_s\colon R \to R, \quad \rho_s(r) = rs.$$

En fait, *tout* morphisme de $R$-modules $R \to R$ est de cette forme. Voir l'exercice 4.6.7.

**Proposition 4.6.15.** *Tout $R$-module $M$ de type fini est l'image d'un morphisme d'anneaux $\varphi\colon N \to M$ avec $N$ un $R$-module libre de type fini.*

*Démonstration.* Supposons que $M$ ait une liste finie $v_1, \dots, v_n$ de générateurs. On le laisse en exercice (l'exercice 4.6.9) à vérifier que

$$\varphi\colon R^n \to M, \quad \varphi(r_1, \dots, r_n) \mapsto \sum_{i=1}^{n} r_i v_i. \tag{4.5}$$

est un morphisme de $R$-modules surjectif. □

On conclut cette section par le résultat suivant.

**Proposition 4.6.16.** *Soit $\varphi\colon M \to N$ un morphisme de $R$-modules. Supposons que $M$ soit libre avec base $\{u_1, \dots, u_n\}$. Alors $\varphi$ est un isomorphisme si et seulement si $\{\varphi(u_1), \dots, \varphi(u_n)\}$ est une base de $N$.*

*Démonstration.* On va montrer plus précisément que

(a) $\varphi$ est injectif si et seulement si $\varphi(u_1), \dots, \varphi(u_n)$ sont linéairement indépendants sur $R$, et

(b) $\varphi$ est surjectif si est seulement si $\varphi(u_1), \dots, \varphi(u_n)$ engendrent $N$.

Par conséquent, $\varphi$ est bijectif si et seulement si $\{\varphi(u_1), \dots, \varphi(u_n)\}$ est une base de $N$.

Pour démontrer (a), on utilise le fait que $\varphi$ est injectif si et seulement si $\ker(\varphi) = \{0\}$ (proposition 4.6.12(c)). On note que, pour tout choix de $r_1, \dots, r_n \in R$, on a

$$\begin{aligned} r_1\varphi(u_1) + \cdots + r_n\varphi(u_n) = 0 &\iff \varphi(r_1u_1 + \cdots + r_nu_n) = 0 \\ &\iff r_1u_1 + \cdots + r_nu_n \in \ker(\varphi). \end{aligned} \tag{4.6}$$

Si $\ker(\varphi) = \{0\}$, la dernière condition devient $r_1u_1 + \cdots + r_nu_n = 0$ qui implique $r_1 = \cdots = r_n = 0$ puisque $u_1, \dots, u_n$ sont linéairement indépendants sur $R$. Dans ce cas, on conclut que $\varphi(u_1), \dots, \varphi(u_n)$ sont linéairement indépendants sur $R$. Réciproquement, si $\varphi(u_1), \dots, \varphi(u_n)$ sont linéairement indépendants, les équivalences (4.6) nous apprennnent que le seul choix de $r_1, \dots, r_n \in R$ tel que $r_1u_1 + \cdots + r_nu_n \in \ker(\varphi)$ est $r_1 = \cdots = r_n = 0$. Comme $u_1, \dots, u_n$ engendrent $M$, cela implique que $\ker(\varphi) = \{0\}$. Ainsi $\ker(\varphi) = \{0\}$ si et seulement si $\varphi(u_1), \dots, \varphi(u_n)$ sont linéairement indépendants. Pour démontrer (b), on utilise le fait que $\varphi$ est surjectif si et seulement si $\mathrm{im}(\varphi) = N$. Comme $M = \langle u_1, \dots, u_n\rangle_R$, on a

$$\begin{aligned} \mathrm{im}(\varphi) &= \{\varphi(r_1u_1 + \cdots + r_nu_n) : r_1, \dots, r_n \in R\} \\ &= \{r_1\varphi(u_1) + \cdots + r_n\varphi(u_n) : r_1, \dots, r_n \in R\} \\ &= \langle \varphi(u_1), \dots, \varphi(u_n)\rangle_R. \end{aligned}$$

Donc $\mathrm{im}(\varphi) = N$ si et seulement si $\varphi(u_1), \dots, \varphi(u_n)$ engendrent $N$. □

## Exercices.

4.6.1. Prouver que l'application de l'exemple 4.6.4 est un morphisme de $R$-modules.

4.6.2. Démontrer la proposition 4.6.8(a).

4.6.3. Démontrer la proposition 4.6.12.

4.6.4. Prouver que l'application $\varphi$ de l'exemple 4.6.13 est un morphisme de $R$-modules.

4.6.5. Soit $\varphi\colon M \to M'$ un morphisme de $R$-modules et soit $N$ un sous-$R$-module de $M$. On définit l'*image* de $N$ sous $\varphi$ par

$$\varphi(N) := \{\varphi(u) : u \in M\}.$$

Montrer que

(a) $\varphi(N)$ est un sous-$R$-module de $M'$ ;
(b) si $N = \langle u_1, \ldots, u_m\rangle_R$, alors $\varphi(N) = \langle \varphi(u_1), \ldots, \varphi(u_m)\rangle_R$ ;
(c) si $N$ admet une base $\{u_1, \ldots, u_m\}$ et si $\varphi$ est injective, alors $\{\varphi(u_1), \ldots, \varphi(u_m)\}$ est une base de $\varphi(N)$.

4.6.6. Soit $\varphi\colon M \to M'$ un morphisme de $R$-modules et soit $N'$ un sous-$R$-module de $M'$. On définit l'*image réciproque* de $N'$ sous $\varphi$ par

$$\varphi^{-1}(N') := \{u \in M : \varphi(u) \in N'\}.$$

(On ne suppose pas que $\varphi^{-1}$ existe.) Montrer que $\varphi^{-1}(N')$ est un sous-$R$-module de $M$.

4.6.7. Démontrer que l'application $\rho_s$ de l'exemple 4.6.14 est un morphisme de $R$-modules et que tout morphisme de $R$-modules $R \to R$ est de cette forme.

4.6.8. Soit $M$ un $R$-module libre avec base $\{u_1, \ldots, u_n\}$, soit $N$ un $R$-module quelconque, et soient $v_1, \ldots, v_n$ des éléments quelconques de $N$. Montrer qu'il existe un et un seul morphisme de $R$-modules $\varphi\colon M \to N$ tel que $\varphi(u_i) = v_i$ pour $i = 1, \ldots, n$.

4.6.9. Montrer que (4.5) est un morphisme de $R$-modules surjectif. *Indice* : Utiliser l'exercice 4.6.8.

4.6.10. Soit $N$ un $R$-module de type fini engendré par $n$ éléments. Montrer qu'il existe un morphisme surjectif de $R$-modules $\varphi\colon A^n \to N$. *Indice* : Utiliser le résultat de l'exercice 4.6.8.

## 4.7 Théorèmes d'isomorphisme

Dans cette section, on démontre quelques théorèmes d'isomorphismes importants concernant les modules. Dans cette section, $R$ est un anneau quelconque.

Rappelons, de la proposition 4.6.12, que si $\varphi\colon M \to N$ est un morphisme de $R$-modules, alors $\ker(\varphi)$ est un sous-module de $M$ et $\operatorname{im}(\varphi)$ est un sous-module de $N$.

**Théorème 4.7.1** (Premier théorème d'isomorphisme de modules)**.** *Soient $M$ et $N$ les $R$-modules, et soit $\varphi\colon M \to N$ un morphisme de $R$-modules. Alors on a un isomorphisme de $R$-modules*

$$\operatorname{im}(\varphi) \cong M/\ker(\varphi).$$

*Démonstration.* Considérons l'application

$$\bar{\varphi}\colon M/\ker(\varphi) \to \operatorname{im}(\varphi), \quad \bar{\varphi}(u + \ker(\varphi)) = \varphi(u).$$

D'après le premier théorème d'isomorphisme pour les groupes (MAT 2143), cette fonction est bien définie et elle est un morphisme de groupes additifs. Il reste à vérifier qu'elle est un morphisme de $R$-modules. On le laisse en exercice (l'exercice 4.7.1). □

Rappelons, de la proposition 4.2.12, que les sommes et les intersections de $R$-modules sont des $R$-modules.

**Théorème 4.7.2** (Deuxième théorème d'isomorphisme de modules)**.** *Supposons que $M$ soit un $R$-module, et soient $S$ et $T$ des sous-modules de $M$. Alors les modules quotients $(S+T)/T$ et $S/(S \cap T)$ sont isomorphes.*

*Démonstration.* Considérons l'application

$$\varphi\colon S \mapsto (S+T)/T, \quad u \mapsto u + T.$$

Puisque $\varphi$ est la composition de l'inclusion de $R$-modules $S \hookrightarrow S + T$ et la projection $S + T \to (S + T)/T$ (voir l'exemple 4.6.4), elle est un morphisme de $R$-modules. On a

$$\varphi(u) = 0 \iff u + T = 0 + T \iff u \in T.$$

Donc $\ker(\varphi) = T$. De plus, pour $u \in S$ et $v \in T$, on a

$$(u + v) + T = u + T \in \operatorname{im}(\varphi).$$

Ainsi $\varphi$ est surjectif. Le résultat maintenant découle de premier théorème d'isomorphisme de modules (le théorème 4.7.1). □

**Théorème 4.7.3** (Troisième théorème d'isomorphisme de modules)**.** *Si $N \subseteq L \subseteq M$ sont des $R$-modules (c.-à-d. $L$ est un sous-module de $M$ et $N$ est un sous-module de $L$), alors*

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

*Démonstration.* Considérons l'application

$$\varphi\colon M/N \to M/L, \quad \varphi(u+N) = u+L.$$

Cette application est bien définie puisque

$$u+N = v+N \implies u-v \in N \subseteq L \implies \varphi(u+N) = u+L = v+L = \varphi(v+N).$$

Puisque

$$\varphi(u+N) = 0+L \iff u \in L,$$

on a $\ker(\varphi) = L/N$. C'est claire qu'on a aussi $\mathrm{im}(\varphi) = M/L$. Alors le résultat découle du premier théorème d'isomorphisme de modules (le théorème 4.7.1). □

Quand $R = F$ est un corps, les théorèmes ci-dessus donnent des théorèmes d'isomorphisme importants pour les espace vectoriels que vous n'avez peut-être pas vu dans vos cours d'algèbre linéaire.

*Exemple* 4.7.4. Soit $\mathcal{F}(\mathbb{R})$ le espace vectoriel sur $\mathbb{R}$ des fonctions $\mathbb{R} \to \mathbb{R}$. Soit

$$W = \{f \in \mathcal{F}(\mathbb{R}) : f(0) = 0\}.$$

Il est simple à vérifier que $W$ est un sous-espace de $\mathcal{F}(\mathbb{R})$. Maintenant considérons l'application

$$\varphi\colon \mathcal{F}(\mathbb{R}) \to \mathbb{R}, \quad \varphi(f) = f(0).$$

Il n'est pas difficile à vérifier que $\varphi$ est une application linéaire (c.-à-d. un morphisme de $R$-modules). C'est clairement surjectif, et on a $W = \ker(f)$. Ainsi, le premier théorème d'isomorphisme de modules (le théorème4.7.1) implique que

$$\mathcal{F}(\mathbb{R})/W \cong \mathbb{R}$$

en tant qu'espaces vectoriels sur $\mathbb{R}$. Cela serait difficile à prouver sans le premier théorème d'isomorphisme, puisque l'espace $\mathcal{F}(\mathbb{R})$ est énorme. (Par exemple, il n'a même pas de base comptable.)

---

## Exercices.

4.7.1. Démontrer que l'application $\bar{\varphi}$ dans la preuve du théorème 4.7.1 est un morphisme de $R$-modules.

4.7.2. Démontrer que le module $W$ de l'exemple 4.7.4 est un sous-espace de $\mathcal{F}(\mathbb{R})$. Montrer aussi que $\varphi$ est une application linéaire surjective.

4.7.3. Supposons que $M = M_1 \oplus M_2$ pour des sous-modules $M_1, M_2$ d'un $R$-module $M$. Montrer que $R/M_1 \cong M_2$ en tant que $R$-modules.

4.7.4. Rappelons qu'une fonction $R \to R$ est *impaire* si $f(x) = f(-x)$ pour tout $x \in \mathbb{R}$. Considérons les sous-espaces suivants de $\mathcal{F}(\mathbb{R})$ (notation de l'exemple 4.7.4) :

$$\begin{aligned} U &= \{f \in \mathcal{F}(\mathbb{R}) : f \text{ est continue}\},\\ V &= \{f \in \mathcal{F}(\mathbb{R}) : f \text{ est impaire}\},\\ W &= \{f \in \mathcal{F}(\mathbb{R}) : f \text{ est continue } \textit{et} \text{ impaire}\},\\ X &= \{f \in \mathcal{F}(\mathbb{R}) : f \text{ est la somme d'une fonction impaire et une fonction continue}\}. \end{aligned}$$

Démontrer que $X/V \cong U/W$.

4.7.5. Supposons que $m, n \in \mathbb{Z}$, $m, n \geq 2$. Soit

$$M = \{ma + mn\mathbb{Z} : a \in \mathbb{Z}\} \subseteq \mathbb{Z}_{mn}.$$

(a) Vérifier que $M$ est un sous-groupe de $\mathbb{Z}_{mn}$.
(b) Montrer que $\mathbb{Z}_m \cong \mathbb{Z}_{mn}/M$ en tant que $\mathbb{Z}$-modules (c.-à-d. en tant que groupes abélliens).

4.7.6. Supposons que $M$ est un module cyclique sur un anneau $R$. Montrer que $M \cong R/\operatorname{ann}(M)$ en tant que $R$-modules.

## 4.8 Modules sur les anneaux commutatifs

Dans cette section $R$ est un *anneau commutatif*. À un moment donné, nous commencerons aussi à supposer que $R$ soit un anneau principal.

Supposons que $M$ soit un $R$-module. Alors on peut noté les coefficients de

$$M^n := \underbrace{M \times M \times \cdots \times M}_{n \text{ facteurs}}$$

sous forme de matrices $1 \times n$ à coefficients dan $M$, qu'on écrit comme des «vecteur ligne» $(v_1, \ldots, v_n)$, $v_1, \ldots, v_n \in M$. Si $C \in \operatorname{Mat}_{n\times s}(R)$, alors la multipliation à droite par $C$ donne un morphisme de $R$-modules de $M^n$ dans $M^s$. Plus précisément, si $C = (c_{i,j})$, alors

$$(v_1, \ldots, v_n)C = \left( \sum_{i=1}^{n} c_{i,1}v_i, \ldots, \sum_{i=1}^{n} c_{i,s}v_i \right).$$

Si $B \in \operatorname{Mat}_{s\times t}(R)$, alors la multiplication à droite par $CB$ correspond à la composition de la multiplication à droite par $C$ suivie de la multiplication à droite par $B$ :

$$(v_1, \ldots, v_n)(CB) = ((v_1, \ldots, v_n)C)B.$$

Si $\{v_1, \ldots, v_n\}$ est linéairement indépendant sur $R$ et $(v_1, \ldots, v_n)C = 0$, alors $C$ est la matrice zéro. Voir l'exercice 4.8.1.

Vous avez appris en algèbre linéaire que deux bases quelconques d'un espace vectoriel de dimension finie ont la même cardinalité (c.-à-d. le même nombre d'éléments). La même chose est vraie pour les modules libres de type fini sur un anneau commutatif.

**Lemme 4.8.1.** *Soit $R$ un anneau commutatif. Deux bases quelconques d'un $R$-module de type fini ont la même cardinalité.*

*Démonstration.* D'après le lemme 4.4.4, on sait que toute base d'un $R$-module de type fini est finie. Soit $M$ un $R$-module avec base $\{v_1, \ldots, v_n\}$ et ensemble de générateurs $\{w_1, \ldots, w_m\}$. On va montrer que $m \geq n$. Le lemme découle de ce fait puisque toute base est un ensemble de générateurs.

Pour tout $j = 1, \ldots, m$, on peut écrire $w_j$ de façon unique comme une combinaison $R$-linéaire des éléments $v_i$ de la base :

$$w_j = a_{1,j}v_1 + a_{2,j}v_2 + \ldots a_{n,j}v_n. \tag{4.7}$$

Soit $A \in \mathrm{Mat}_{n\times m}(R)$ une matrice $A = (a_{i,j})$. Alors les $m$ equations (4.7) peuvent être écrites comme une seule equation matricielle :

$$(v_1, \ldots, v_n)A = (w_1, \ldots, w_m). \tag{4.8}$$

Puisque $\{w_1, \ldots, w_m\}$ engendre $M$, on peut aussi écrire chaque $v_j$ comme une combinaison $R$-linéaire des éléments $w_i$. Comme ci-dessus, cela implique qu'on a une matrice $B \in \mathrm{Mat}_{m\times n}(R)$ telle que

$$(w_1, \ldots, w_m)B = (v_1, \ldots, v_n). \tag{4.9}$$

Il s'ensuit de (4.8) et (4.9) que

$$(v_1, \ldots, v_n)AB = (w_1, \ldots, w_m)B = (v_1, \ldots, v_n),$$

ce qui est équivalent à

$$(v_1, \ldots, v_n)(AB - I_n) = 0,$$

où $I_n$ est la matrice identité $n\times n$. Puisque l'ensemble $\{v_1, \ldots, v_n\}$ est linéairement indépendant, cela implique que $AB = I_n$.

Maintenant supposons, vers une contradiction, que $m < m$. Alors on ajoute à $A$ $n - m$ colonnes de zéros sur le côté droit pour obtenir une matrice $A' \in \mathrm{Mat}_{n\times n}(R)$. De même, nous ajoutons $n - m$ lignes de zéros au bas de $B$ pour obtenir une matrice $B' \in \mathrm{Mat}_{n\times n}(R)$. Alors on a $A'B' = AB = E_n$. En prenant déterminants, [1] on obtient

$$1 = \det(I_n) = \det(A'B') = \det(A')\det(B').$$

Mais $\det(A') = 0$, puisque la matrice $A'$ a une colonne de zéros. Cette contradiction implique que $m \geq n$, comme on veut. □

**Attention !** Sur un anneau non commutatif, un module libre peut avoir deux bases des cardinalités différentes. Voir l'exercice 4.8.2.

**Définition 4.8.2** (Rang d'un module)**.** Soit $R$ un anneau commutatif. Le *rang* d'un $R$-module libre de type fini est la cardinalité de toute base.

Notez qu'il découle de la définition que le $R$-module nul est libre de rang zéro, avec l'ensemble vide comme base.

1. Nous n'avons pas discuté des propriétés des déterminants pour les matrices avec des coefficients dans un anneau commutatif quelconque $R$. Mais la preuve que vous avez vue en algèbre linéaire montre que le déterminant, calculé de la manière naturelle, a la propriété multiplicative utilisée ici.

## Exercices.

4.8.1. Supposons que $R$ soit un anneau commutatif, $M$ soit un $R$-module, et $A \in \mathrm{Mat}_{n\times m}$. Montrer que si $\{v_1, \ldots, v_n\}$ est un sous-ensemble linéairement indépendant de $M$ et $(v_1, \ldots, v_n)A = 0$, alors $A = 0$.

4.8.2. Soit $R$ l'ensemble de matrices infini-par-infini $(a_{i,j})_{i,j\in\mathbb{Z}}$, $a_{i,j} \in \mathbb{C}$, telles que chaque ligne et chaque colonne a un nombre fini de coefficients non nuls. Montrer que $R$ est un anneau non commutatif. (La supposition de finitude est ici cruciale.) Montrer aussi que $R \cong R \oplus R$ en tant que $R$-modules. En particulier, cela implique que $R$ a une bases avec un élément *et* une base avec deux éléments ! Par conséquent, il n'a pas de rang bien défini !

4.8.3. Soient $V$ et $W$ des modules libres sur un anneau commutatif $R$, avec des bases ordonnés $(v_1, \ldots, v_n)$ et $(w_1, \ldots, w_m)$, respectivement. Soit $\varphi\colon V \to W$ un morphisme de $R$-modules. Soit $A = (a_{i,j}) \in \mathrm{Mat}_{m\times n}(R)$ la matrice définie par

$$\varphi(v_j) = \sum_{i=1}^{m} a_{i,j} w_i.$$

Montrer que pour tout élément $\sum_{j=1}^{n} r_j v_j$ de $V$, on a

$$\varphi\left(\sum_{j=1}^{n} r_j v_j\right) = (w_1, \ldots, w_m)A \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}.$$

4.8.4. Soit $R$ un anneau commutatif et soit $N$ un $R$-module. Supposons que $\{w_1, \ldots, w_k\}$ engendre $N$ en tant que $R$-module. Soit $D \in \mathrm{Mat}_s(R)$ et définissons $\{w'_1, \ldots, w'_k\}$ par

$$(w'_1, \ldots, w'_k) = (w_1, \ldots, w_k)D.$$

Montrer que si $D$ est inversible dans $\mathrm{Mat}_s(R)$, alors $\{w'_1, \ldots, w'_k\}$ engendre $N$.

## 4.9 Modules sur des anneaux principals

Dans cette section, $R$ est un anneau principal.

**Lemme 4.9.1.** *Soit $M$ un module libre de rang fini $n$ sur un anneau principal $R$. Tous sous-module de $M$ a un ensemble de générateurs avec au plus $n$ elements.*

*Démonstration.* Nous prouvons le résultat par récurrence sur $n$. Si $n = 1$, alors $M \cong R$. Dans ce cas, les sous-$R$-modules correspondent à des idéaux de $R$, générés par un seul élément, puisque $R$ est un anneau principal. Ceci démontre le cas de base.

Supposons maintenant que $M$ soit de rang $n > 1$ et que l'affirmation est vraie pour les modules libres de rang inférieur à $n$. Soit $\{v_1, \ldots, v_n\}$ une base pour $M$, et soit $M' =$

$\langle v_1, \dots, v_{n-1} \rangle_R$. Soit $N$ un sous-module de $M$, et soit $N' = N \cap M'$. Par l'hypothèse de récurrence, $N'$ a un ensemble de générateurs avec au plus $n-1$ éléments.

Tout élément $u \in M$ peut être écrit sous la forme

$$u \in \sum_{i=1}^{n} \alpha_i(u) v_i, \quad \alpha_i(u) \in R.$$

L'application $u \mapsto \alpha_n(u)$ est un morphisme de $R$-modules de $M$ dans $R$. Si $\mathrm{im}(\alpha_n) = \{0\}$, alors $N = N'$, et donc $N$ est engendré par au plus $n-1$ éléments. Autrement, $\mathrm{im}(\alpha_n)$ est un idéal non nul de $R$, donc il existe $d \in R$ non nul tel que $\mathrm{im}(\alpha_n) = dR$. Choisissons $h \in N$ tel que $\alpha_n(h) = d$.

Si $u \in N$, alors il existe $r \in R$ tel que $\alpha_n(u) = rd$. Alors $y = x - rh$ remplit la condition $\alpha_n(y) = 0$, et donc $y \in N \cap M' = N'$. Ainsi $u = y + rh \in N' + Rh$. Donc $N = Rh + N'$.

Puisque $N'$ possède un ensemble de générateurs avec au plus $n-1$ elements, $N$ est engendré par au plus $n$ elements. □

**Corollaire 4.9.2.** *Si $M$ est un module de type fini sur un anneau principal, alors tout sous-module de $M$ est de type fini.*

*Démonstration.* Supposons que $M$ a un ensemble fini de générateurs $v_1, \dots, v_n$. Considérons le morphisme de $R$-modules

$$\varphi \colon R^n \to M, \quad \varphi(r_1, \dots, r_n) \mapsto \sum_{i=1}^{n} r_i v_i,$$

de l'exercice 4.6.9. Soit $N$ un sous-module de $M$ et soit $N = \varphi^{-1}(N)$. D'après le lemme 4.9.1, $N$ est engendré pas un ensemble $S$ avec au plus $n$ éléments. Alors $\varphi(S)$ est un ensemble de générateurs pour $N$ avec au plus $n$ éléments. □

Vous avez appris en algèbre linéaire que si $U$ est un sous-espace d'un espace vectoriel $V$ de dimension $n$, alors vous pouvez trouver une base $\{v_1, \dots, v_n\}$ de $V$ et $m \leq n$ telle que $\{v_1, \dots, v_m\}$ est un base de $U$. Cependant, ceci n'est *pas* vrai pour les modules généraux, même pour les modules libres sur un anneau principal. Par exemple, en tant que $\mathbb{Z}$-module, $\mathbb{Z}$ est libre avec base $\{1\}$ ou $\{-1\}$. Considérez le sous-module $2\mathbb{Z}$. C'est libre avec base $\{2\}$ ou $\{-2\}$. Ainsi, il n'y a pas de sous-ensemble d'une base de $\mathbb{Z}$ qui soit une base de $2\mathbb{Z}$.

Le théorème suivant est la bonne généralisation de cette propriété des bases de modules libres et de leurs sous-modules.

**Théorème 4.9.3.** *Supposons que $R$ soit un anneau principal. Soit $M$ un $R$-module libre de rang $m$, et soit $N$ un sous-module de $M$. Alors il existe une base $\{v_1, \dots, v_m\}$ de $M$ et des éléments $d_1, \dots, d_n \in R$, $n \leq m$, tels que $d_i$ divise $d_j$ si $i \leq j$ et $\{d_1 v_1, \dots, d_n v_n\}$ est une base de $N$. En particulier, $N$ est un $R$-module libre de rang $n$.*

La démonstration du théorème 4.9.3 n'est pas conceptuellement difficile, mais elle est un peu longue, et nous ne la couvrirons donc pas dans ce cours. Cela implique le type d'opérations sur les lignes et les colonnes que vous avez appris en algèbre linéaire, sauf que vous devez faire attention car vous travaillez sur un anneau principal quelconque. Pour plus de détails sur la preuve, voir la preuve de [Goo15, Th. 8.4.2].

**Lemme 4.9.4.** *Soient $A_1, \dots, A_n$ des $R$-modules, et soient $B_i \subseteq A_i$ des sous-modules. Alors*

$$(A_1 \oplus \cdots \oplus A_n)/(B_1 \oplus \cdots \oplus B_n) \cong A_1/B_1 \oplus \cdots \oplus A_n/B_n.$$

*Démonstration.* Le morphisme de $R$-modules

$$\varphi\colon A_1 \oplus \cdots \oplus A_n \to A_1/B_1 \oplus \cdots \oplus A_n/B_n, \quad (a_1, \dots, a_n) \mapsto (a_1 + B_1, \dots, a_n + B_n).$$

est surjectif, avec $\ker(\varphi) = B_1 \oplus \cdots \oplus B_n$. Ainsi le résultat découle de théorème 4.7.1. □

**Théorème 4.9.5** (Théorème des facteurs invariants)**.** *Soit $R$ un anneau principal, et soit $M$ un $R$-module non nul de type fini.*

*(a) Le module $M$ est une somme directe de modules cycliques,*

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k) \oplus R^n,$$

*où les éléments $a_i \in R$ sont non nuls et non unités, et $a_i$ divise $a_j$ pour $i \leq j$.*

*(b) La décomposition dans la partie (a) est unique dans le sens suivant : Supposons que*

$$M \cong R/(b_1) \oplus R/(b_2) \oplus \cdots \oplus R/(b_l) \oplus R^m,$$

*où les éléments $b_i \in R$ sont non nul et non unités, et $b_i$ divise $b_j$ pour $i \leq j$. Alors $k = l$, $m = n$, et $(a_i) = (b_i)$ pour tout $i$.*

*Démonstration.* On va démonter la partie (a). Vous pouvez trouver la preuve de la partie (b) dans [Goo15, §8.5]. Soit $\{v_1, \dots, v_m\}$ un ensemble de générateurs de $M$ de cardinalité minimale. D'après la propsotion 4.6.15, il exist un module libre $L$ de rang $m$ et un morphisme de $R$-module surjectif

$$\varphi\colon L \to M.$$

Soit $N = \ker(\varphi)$. D'après le théorème 4.9.3, $N$ est libre de rang $k \leq m$, et il existe une base $\{v_1, \dots, v_m\}$ de $L$ est des éléments non nuls $d_1, \dots, d_k$ de $R$ tels que $\{d_1 v_1, \dots, d_k v_k\}$ est une base de $N$ et $d_i$ divise $d_j$ pour $i \leq j$. Par conséquent,

$$\begin{aligned} M \cong L/N &= (Rv_1 \oplus \cdots \oplus Rv_m)/(Rd_1v_1 \oplus \cdots \oplus Rd_kv_k) \\ &\cong Rv_1/Rd_1v_1 \oplus \cdots \oplus Rd_kv_k \oplus Rv_{k+1} \oplus \cdots \oplus Rv_m. \end{aligned} \tag{4.10}$$

Maintenant, l'application

$$R \to Rv_i/Rd_iv_i, \quad r \mapsto rv_i + Rd_iv_i,$$

est un morphisme de $R$-modules surjectif avec noyau $(d_i)$. Ainsi $Rv_i/Rd_iv_i \cong R/(d_i)$ d'après le théorème 4.7.1. Ainsi, (4.10) nous donne

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_k) \oplus R^{m-k}.$$

Si un des éléments $d$ était inversible, alors $R/(d_i)$ serrait le module zéro, et donc on pouvait le supprimer de la somme. Mais alors $M$ serait engendré par moins que $m$ elements, ce qui contredit le fait que $m$ est minimal. □

Comme conséquence immédiate du théorème 4.9.5, nous récupérons l'un des théorèmes importants que vous avez vus dans MAT 2543.

**Théorème 4.9.6** (Théorème de structure des groups abéliens de type fini)**.** *Soit $G$ un groupe abélien de type fini. Alors $G$ est un produit direct des groupes cycliques,*

$$G \cong \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_k\mathbb{Z} \times \mathbb{Z}^n,$$

*où les éléments $a_i \geq 2$, et $a_i$ divise $a_j$ pour $i \leq j$. Les éléments $a_i$ et les valeurs $k$ et $n$ sont déterminées de façon unique par $G$.*

*Démonstration.* Cela découle du théorème 4.9.5, avec $R = \mathbb{Z}$. □

Si $F$ est un corps algébriquement clos, alors le théorème 4.9.5 appliqué à l'anneau $R = F[x]$ donne la forme canonique de Jordan d'une transformation linéaire d'un espace vectoriel de dimension finie sur $F$. Pour plus de détails, voir [Goo15, §8.7]. La forme canonique de Jordan est couverte dans MAT 3741.

---

## Exercices.

Rappelons la définition de *torsion* de l'exercice 4.2.6.

4.9.1. Soit $R$ un anneau intègre avec idéal non principal $J$.

(a) Montrer que $J$ est sans torsion en tant que $R$-module.
(b) Montrer que chaque deux éléments de $J$ sont linéairement dépendants.
(c) Montrer que $J$ n'est pas un $R$-module libre.

4.9.2. Supposons que $R$ soit un anneau principal. Utiliser le théorème 4.9.5 pour montrer que, si $M$ est un module de type fini, alors $M/M_{\text{tor}}$ est un $R$-module libre.

4.9.3. Montrer que $M = \mathbb{Q}/\mathbb{Z}$ est un $\mathbb{Z}$-module torsion, que $M$ n'est pas de type fini, et que $\text{ann}(M) = \{0\}$.

# Index

# Bibliographie


[Goo15] Frederick M. Goodman. *Abstract : abstract and concrete*. 2.6 edition, 2015. URL : http://homepage.math.uiowa.edu/~goodman/algebrabook.dir/algebrabook.html.

[Jud19] Thomas W. Judson. *Abstract algebra*. 2019 annual edition, 2019. URL : http://abstract.ups.edu/index.html.

[Nic12] W. Keith Nicholson. *Introduction to abstract algebra*. Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, fourth edition, 2012.

[Rog71] Kenneth Rogers. The axioms for Euclidean domains. *Amer. Math. Monthly*, 78 :1127–1128, 1971. URL : https://doi.org/10.2307/2316324.

[Roy] Damien Roy. MAT 3141 – Linear Algebra II, Lecture notes (translated by A. Savage). URL : http://alistairsavage.ca/mat3141/notes/MAT3141-LinearAlgebraII.pdf.