Université Mohammed V
Faculté des Sciences
Rabat, Maroc

Polycopié du cours d'Algèbre 2

Structures algébriques, Polynômes et Fractions Rationnelles

Filière : Sciences Mathématiques, Informatique et Applications (**SMIA**)

2020-2021

Professeur Driss Bennis

Ce polycopié est juste un outil complémentaire aux cours et travaux dirigés où nous présontons plus de détails.

Table des matières

Introduction

En algèbre, une structure algébrique est un ensemble sur lequel une opération ou plusieurs opérations (dites lois), respectant certaines règles (appelées axiomes), ont été définies.
Dans ce cours, nous introduisons les structures algébriques de bases suivantes : les groupes, les anneaux et les corps.

Chapitre 1

Groupes

1.1 Vocabulaire des lois de composition interne

Dans cette section, E désigne un ensemble non vide.

Définition 1.1.1 (Loi de composition interne)

Toute application $*$ de $E \times E$ dans E est appelée une **loi de composition interne** ou une **opération dans** E.
On dit que E est muni de la loi de composition interne $*$.

Notation et vocabulaire.

1. Il y a certainement des lois externe, comme le produit d'un vecteur par un réel ou aussi le produit d'une fonction par un réel. Mais, souvent le contexte nous indique qu'on travaille avec quelle type de lois (interne ou externe). C'est pour cela, on convient de dire simplement "une loi sur E" pour indiquer "une loi de composition interne sur E".
2. Dans un magma $(E, *)$, on utilise la notation opératoire au lieu de la notation fonctionnelle pour désigner l'image d'un couple $(x, y) \in E^2$. Ainsi, $*(x, y)$ sera notée $x * y$ et appelée le **composé** de x par y par la loi $*$.
3. Les lois de composition internes sont souvent notées avec l'un des symboles suivants : $*, \cdot, +, T, \perp, \times, \circ$. Cependant, le choix du symbole pour noter une loi est complètement arbitraire. On signale, à titre d'exemple, que même le choix du symbole $+$ pour l'addition de nombres réels remonte juste au 15ème siècle, remplaçant le symbole p précédemment utilisé.

Exemple 1.1.2 (Premiers exemples)

1. *La multiplication et l'addition usuelles sont des lois sur* $\mathbb{R}$.
2. *L'union et l'intersection des parties d'un ensemble* A *sont des lois sur l'ensemble* $P(A)$ *des parties de* A.
3. *La division (des nombres) peut être ou non une loi selon l'ensemble de nombres considéré : Elle n'est pas une loi de composition interne dans* $\mathbb{Z}^*$*, mais elle l'est dans* $\mathbb{R}^*$ *(ensemble des réels non nuls).*

4. *Aussi, la soustraction n'est pas une loi de composition interne dans* $\mathbb{N}$*, mais elle l'est dans* $\mathbb{Z}$*.*
5. *La composition des applications* $\circ$ *est une loi dans l'ensemble* E^E *des applications de* E *dans* E*.*
6. min *et* max *sont deux lois dans* $\mathbb{R}$*.*
   Remarquer qu'ici, ces deux lois ont une notation fonctionnelle ; mais on emploie parfois une notation opératoire :
$$\min(x, y) = x \wedge y, \quad \max(x, y) = x \vee y$$
7. *pgcd et ppcm sont deux lois dans* $\mathbb{Z}$*.*
   On rappelle :
$$d = pgcd(a, b) \Leftrightarrow \begin{cases} d \in \mathbb{N} \\ d \text{ divise } a \text{ et } b \\ \text{si } d' \text{ divise } a \text{ et } b, \text{ alors } d' \text{ divise } d \end{cases}$$
$$m = ppcm(a, b) \Leftrightarrow \begin{cases} m \in \mathbb{N} \\ a \text{ et } b \text{ divisent } m \\ \text{si } a \text{ et } b \text{ divisent } m', \text{alors } m \text{ divise } m' \end{cases}$$
   On emploie aussi une notation opératoire : $pgcd(a, b) = a \wedge b$ *et* $ppcm(a, b) = a \vee b$ *(s'il n'y a pas de confusion possible avec min et max).*

Définition 1.1.3 (Magma)

Si un ensemble E est muni d'une loi $*$, le couple $(E, *)$ est appelé un **magma**.

Convention. Par abus de langage, on peut dire simplement "le magma E" au lieu de dire "le magma $(E, *)$" lorsqu'il n'y a pas d'ambiguïté sur la loi $*$.

Définition 1.1.4 (Associativité)

Soit $(E, *)$ un magma. La loi $*$ est dite **associative** si, pour tout $(x, y, z) \in E^3$,
$$(x * y) * z = x * (y * z).$$
On dit aussi que le magma $(E, *)$, ou simplement E, est associatif.

Définition 1.1.5 (Commutativité)

Soit $(E, *)$ un magma. La loi $*$ est dite **commutative** si, pour tout $(x, y) \in E^2$, $x * y = y * x$.
On dit aussi que le magma $(E, *)$, ou simplement E, est commutatif.

Exemple 1.1.6

1. *La multiplication et l'addition usuelles dans* $\mathbb{R}$ *sont des lois à la fois associatives et commutatives .*
2. *L'union et l'intersection des parties d'un ensemble* A *sont des lois commutatives et associatives sur l'ensemble* $P(A)$ *des parties de* A*. Cependant, la différence est une loi sur* $P(A)$ *qui n'est ni associative, ni commutative.*
3. *La soustraction est une loi dans* $\mathbb{Z}$ *qui n'est ni commutative, ni associative.*
4. *La composition des applications* $\circ$ *est une loi dans l'ensemble* E^E *des applications de* E *dans* E *qui est associative mais pas commutative en générale.*
5. min *et* max *sont des lois commutatives et associatives dans* $\mathbb{R}$*.*
6. *pgcd et ppcm sont deux lois commutatives et associatives dans* $\mathbb{Z}$*.*

Proposition et Définition 1.1.7 (Magma produit)

Soit $((E_i, \perp_i))_{1\leq i\leq n}$ (où $n \in \mathbb{N}^*$) une famille finie de magmas. On munit le produit cartésien $E = E_1 \times \cdots \times E_n$ de la loi suivante :

$$(a_i)_{1\leq i\leq n} \perp (b_i)_{1\leq i\leq n} = (a_i \perp_i b_i)_{1\leq i\leq n}$$

pour tous $(a_i)_i$ et $(b_i)_i$ dans E. Le magma $(E, \perp)$ ainsi défini est appelé le **magma produit** des magmas $(E_1, \perp_1)$,...,$(E_n, \perp_n)$. Et on a :

1. $(E, \perp)$ est commutatif si et seulement si E_i est commutatif pour tout $i \in \{1, ..., n\}$.
2. $(E, \perp)$ est associatif si et seulement si E_i est associatif pour tout $i \in \{1, ..., n\}$.

Preuve. On notera simplement $(a_i)_i$ tout élément $(a_i)_{1\leq i\leq n}$ de E.
On montre la première assertion. La deuxième peut être montrée de la même façon.
On suppose que $(E, \perp)$ est commutatif et on montre que E_k est commutatif pour un certain $k \in \{1, ..., n\}$. Soit $(a, b) \in E_k^2$. On choisit deux élément $(a_i)_i$ et $(b_i)_i$ de E tels que $a_k = a$ et $b_k = b$. Puisque E est commutatif, on a $(a_i)_i(b_i)_i = (b_i)_i(a_i)_i$, c'est-à-dire $(a_ib_i)_i = (b_ia_i)_i$. En particulier, $a_kb_k = b_ka_k$, c'est-à-dire $ab = ba$. Par suite, E_k est commutatif.
Montrons l'implication réciproque. Supposons que E_i est commutatif pour tout $i \in \{1, ..., n\}$. Soit $(a_i)_i$ et $(b_i)_i$ deux élément de E. On a $(a_i)_i(b_i)_i = (a_ib_i)_i$ et $(b_i)_i(a_i)_i = (b_ia_i)_i$. Et puisque E_i est commutatif pour tout $i \in \{1, ..., n\}$, on a $(a_ib_i)_i = (b_ia_i)_i$. D'où, $(a_i)_i(b_i)_i = (b_i)_i(a_i)_i$. Ce qui montre que $(E, \perp)$ est commutatif. **(c.q.f.d)**

Exemple 1.1.8
En utilisant les notations de la proposition 1.1.7, si les magmas $(E_i, \perp_i)$ coïncident avec un magma $(\mathbb{E}, *)$, alors, lorsqu'il n'y a pas d'ambiguïté sur la loi, on convient de noter la loi du magma produit $\mathbb{E}^n := E_1 \times \cdots \times E_n$ par le même symbole que celui de $\mathbb{E}$. Ainsi, on écrit

$$(a_i)_i * (b_i)_i = (a_i * b_i)_i$$

pour tous $(a_i)_i$ et $(b_i)_i$ dans $\mathbb{E}^n$.
Sur $\mathbb{Z}^n$ ($\mathbb{Q}^n$, $\mathbb{R}^n$ et aussi $\mathbb{C}^n$), on définit les deux lois additive et multiplicative suivantes :

$$(a_i)_{1\leq i\leq n} + (b_i)_{1\leq i\leq n} = (a_i + b_i)_{1\leq i\leq n} \quad \text{et} \quad (a_i)_{1\leq i\leq n}(b_i)_{1\leq i\leq n} = (a_i b_i)_{1\leq i\leq n}$$

Notamment, $(\mathbb{Z}^n, +)$, $(\mathbb{Q}^n, +)$, $(\mathbb{R}^n, +)$, et $(\mathbb{C}^n, +)$ sont les magmas produits multiplicatifs usuels. Aussi, $(\mathbb{Z}^n, \times)$, $(\mathbb{Q}^n, \times)$, $(\mathbb{R}^n, \times)$, et $(\mathbb{C}^n, \times)$ sont les magmas produits multiplicatifs usuels.
Noter que, dans $\mathbb{R}^2$ (resp. $\mathbb{R}^3$), la somme définie ci-dessous corresponds à l'addition des vecteurs (géométriques) du plan (resp. de l'espace).

Notation. Ainsi, comme on a vu dans l'exemple 1.1.8, il est parfois commaude d'utiliser la notation additive (resp., multiplicative) quand on définit une nouvelle loi à partir d'une autre loi additive (resp., multiplicative). En général, lorsqu'il n'y a pas d'ambiguïté sur la loi, on préfère d'utiliser les notations usuelles $+$ ou . ou $\times$. Dans ces cas :

— Si on utilise $+$, la loi est appelée **addition**. On dit que la loi de E est notée **additivement**. Dans ce cas, "$x + y$" s'appelle la **somme** de x et de y.
— Si on utilise . ou $\times$, la loi est appelée **multiplication**. On dit que la loi de E est notée **multiplicativement**. Dans ce cas, "$x \times y = x.y$" s'appelle le produit de x et de y. Parfois, il convient d'omettre les symboles . et $\times$ (i.e., on utilise simplement xy pour désigner "$x \times y$").

Exemple 1.1.9
1. *On considère l'ensemble $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}$.*
   On définit une addition $+$ sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{a} + \overline{b} := \overline{a+b}$ pour tout $(a, b) \in \mathbb{Z}^2$, est une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ qui est à la fois associative et commutative.
   De même on définit un produit $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{a} \times \overline{b} := \overline{a \times b}$ pour tout $(a, b) \in \mathbb{Z}^2$, est une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ qui est à la fois associative et commutative.
   Noter qu'on peut aussi écrire $\overline{a}\,\overline{b} = \overline{a} \times \overline{b} = \overline{a \times b} = \overline{ab}$.
2. *L'ensemble des fonctions réelles $\mathcal{F}(\mathbb{R})$ muni de l'une des deux lois usuelles, l'addition et la multiplication des fonctions réelles, est un magma commutatif et associatif.*

Exemple 1.1.10 (Magma des matrices carrées)
Soit $\mathbb{K}$ l'un des ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. On appelle une ***matrice carrée*** *d'**ordre** $n \in \mathbb{N}^*$ (ou de **taille** n) à **coefficients** dans $\mathbb{K}$, tout tableau carré de n^2 nombres dans $\mathbb{K}$, rangés ligne par ligne (de n éléments de $\mathbb{K}$). Il y a donc n lignes et n colonnes, et dans chaque ligne et chaque colonnes il y a n éléments de $\mathbb{K}$. Comme dans le cas des produits cartésiens des ensembles, une matrice carrée d'ordre n est notée brièvement*

$$A = (a_{i,j})_{1\leq i\leq n, 1\leq j\leq n} \qquad (avec \quad a_{i,j} \in \mathbb{K})$$

ou plus simplement $(a_{i,j})$ lorsqu'il n'y a pas d'ambiguïté sur l'ordre de la matrice, ou elle est explicitement représentée sous la forme d'un tableau carré. Par exemple, une matrice carrée M d'ordre 3 est représentée comme suit :

$$M = \begin{pmatrix} 0 & \pi & 33 \\ \sqrt{3} & e^2 & 1 \\ 3,3 & 0 & 0 \end{pmatrix}$$

L'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ est souvent notée par $\mathcal{M}_n(\mathbb{K})$. En particulier, $\mathcal{M}_n(\mathbb{R})$ est l'ensemble des matrices réelle. On définit sur $\mathcal{M}_n(\mathbb{K})$ deux lois, l'addition et la multiplication, comme suit :

— *L'addition sur $\mathcal{M}_n(\mathbb{K})$ est définie comme suit :*

$$(a_{i,j}) + (b_{i,j}) := (a_{i,j} + b_{i,j}).$$

— *La multiplication sur $\mathcal{M}_n(\mathbb{K})$ est définie comme suit :*
Le produit des deux matrices $(a_{i,j})$ et $(b_{i,j})$, noté multiplicativement $(a_{i,j}) \times (b_{i,j})$ ou simplement $(a_{i,j})(b_{i,j})$, est une matrice $(c_{i,j})$ telle que $c_{i,j} = \Sigma a_{i,k} b_{k,j}$.

Par exemple, le produit de deux matrices d'ordre 2 est comme suit :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{pmatrix}$$

En plus, les magmas $(\mathcal{M}_n(\mathbb{K}), +)$ et $(\mathcal{M}_n(\mathbb{K}), \times)$ sont associatifs.
Aussi, le magma $(\mathcal{M}_n(\mathbb{K}), +)$ est commutatif, cependant le magma $(\mathcal{M}_n(\mathbb{K}), \times)$ ne l'est pas.

L'utilisation des opérations des matrices et leurs propriétés est appelé habituelement "le calcul matriciel". Il appertient principalement à une partie d'algèbre dite "Algèbre linéare". Les matrices sont en fait des représentations de cas particulier d'application, appelées "applications linéaire". Les lois sur les matrices définies ci-dessous correspondent bien à l'addition et la composition des applications linéaires.

L'exercice suivant présente quelques particularités du calcul matriciel.

Exercice 1.1.11

Calculer les produit suivants dans $(\mathcal{M}_2(\mathbb{R}), \times)$:

$$\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}; \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix};$$

$$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}; \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$$

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}; \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}; \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}; \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}^2$$

Exercice 1.1.12

Calculer les produit suivants dans $(\mathcal{M}_3(\mathbb{R}), \times)$:

$$\begin{pmatrix}0 & 0 & 0\\ 1 & 1 & 1\\ 0 & 0 & 0\end{pmatrix}\begin{pmatrix}a_{1,1} & a_{1,2} & a_{1,3}\\ a_{2,1} & a_{2,2} & a_{2,3}\\ a_{3,1} & a_{3,2} & a_{3,3}\end{pmatrix}; \quad \begin{pmatrix}a_{1,1} & a_{1,2} & a_{1,3}\\ a_{2,1} & a_{2,2} & a_{2,3}\\ a_{3,1} & a_{3,2} & a_{3,3}\end{pmatrix}\begin{pmatrix}0 & 0 & 0\\ 1 & 1 & 1\\ 0 & 0 & 0\end{pmatrix}$$

$$\begin{pmatrix}0 & 0 & 0\\ 1 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}\begin{pmatrix}a_{1,1} & a_{1,2} & a_{1,3}\\ a_{2,1} & a_{2,2} & a_{2,3}\\ a_{3,1} & a_{3,2} & a_{3,3}\end{pmatrix}; \quad \begin{pmatrix}a_{1,1} & a_{1,2} & a_{1,3}\\ a_{2,1} & a_{2,2} & a_{2,3}\\ a_{3,1} & a_{3,2} & a_{3,3}\end{pmatrix}\begin{pmatrix}0 & 0 & 0\\ 1 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}$$

$$\begin{pmatrix}0 & 1 & 1\\ 0 & 0 & 1\\ 0 & 0 & 0\end{pmatrix}^2; \quad \begin{pmatrix}0 & 1 & 1\\ 0 & 0 & 1\\ 0 & 0 & 0\end{pmatrix}^3; \quad \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{pmatrix}^2$$

Pour les ensembles finis on peut définir une loi à partir d'une table définie comme suit :

Définition 1.1.13

Etant donné un magma fini $(E, *)$ de cardinal $n \in \mathbb{N}^*$, disons $E = \{x_1, ..., x_n\}$, on appelle **table de Cayley** de $(E, *)$ (ou simplement de E) le tableau carré de n lignes et n colonnes obtenu en inscrivant à la i-ème ligne et à la j-ième colonne l'élément $x_i * x_j$ du magma E.

Exemple 1.1.14
La table de Cayley du magma $(\mathbb{Z}/2\mathbb{Z}, \times)$ est la suivante :

$\times$	0	1
0	0	0
1	0	1

Exercice 1.1.15

1. Dresser la table de Cayley de $(\mathbb{Z}/4\mathbb{Z}; +)$.
2. On considère le magma $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}; +)$ défini, comme dans l'exemple 1.1.6 (4), par $(x, y) + (x', y') := (x + x', y + y')$ pour tout $(x, y, x', y') \in (\mathbb{Z}/2\mathbb{Z})^4$. Dresser la table de Cayley de $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}; +)$.

Définition 1.1.16 (Elément neutre)

Soit $(E, *)$ un magma. On appelle **élément neutre** de $(E, *)$ tout élément $e \in E$ vérifiant $x * e = e * x = x$ pour tout $x \in E$.

Il est claire que si $(E, *)$ est un magma commutatif, alors $e \in E$ est un élément neutre de E si seulement $x * e = x$ pour tout $x \in E$.

Exercice 1.1.17

Donner un exemple d'un magma $(E, *)$ qui admet un élément $f \in E$ vérifiant $x * f = x$ pour tout $x \in E$ sans qu'il soit un élément neutre.

Proposition 1.1.18

Si un magma admet un élément neutre, alors il est unique.

Preuve. Supposons q'un un magma $(E, *)$ admet deux éléments neutres e et e'. Alors, $e = e' * e$ (car e' est un élément neutre). Or e est aussi un élément neutre de E, donc $e * e' = e'$. Par suite, $e = e'$. **(c.q.f.d)**

Exemple 1.1.19

1. *Soit $(E_1, \perp_1), ..., (E_n, \perp_n)$ (où $n \in \mathbb{N}^*$) des magmas d'éléments neutres, respectivement, $e_1, ..., e_n$. Alors, il est facile de montrer que $(e_1, ..., e_n)$ est l'élément neutre du magma produit $E = E_1 \times \cdots \times E_n$.*
2. *Pour tout $n \in \mathbb{N}$, il est facile de voir que $\overline{0}$ (resp., $\overline{1}$) est l'élément neutre du magma $(\mathbb{Z}/n\mathbb{Z}, +)$ (resp., $(\mathbb{Z}/n\mathbb{Z}, \times)$).*
3. *Il est claire que la fonction constante $x \mapsto 0$ (resp., $x \mapsto 1$) est l'élément neutre du magma des fonctions réelles $(\mathcal{F}(\mathbb{R}), +)$ (resp.,*

$(\mathcal{F}(\mathbb{R}), \times)$.

4. *L'application identité de E, $\mathrm{id}_E : x \mapsto x$, est l'élément neutre du monoïde $(E^E, \circ)$.*

Selon le contexte on choisit une notation pour désigner l'élément neutre d'un magma. Par exemple, l'élément neutre pour l'addition des vecteurs du plan (et de l'espace) est le vecteur nul, il est habituelement noté $\overrightarrow{0}$. Aussi, nous avons l'exemple suivant sur le magma des matrices.

Exemple 1.1.20
on peut voir facilement que le magma $(\mathcal{M}_n(\mathbb{R}), +)$ admet un élément neutre ; c'est la matrice nulle dont dont tous les coefficients valent 0. Cette matrice est souvent notée 0_n. Ainsi, la matrice nulle d'ordre 2 est :

$$0_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Pour le magma multiplicatif $(\mathcal{M}_n(\mathbb{R}), \times)$, on montre qu'il admet aussi un élément neutre, noté souvent I_m et appelée la matrice identité de taille n. C'est la matrice carrée de taille n dont les coefficients diagonaux sont égaux à 1 et dont les autres coefficients sont nuls :

$$I_n = (\delta_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$$

où $\delta_{i,j}$ désigne le symbole de Kronecker qui vaut 1 si $i = j$ et 0 sinon. En particulier,

$$I_1 = \begin{pmatrix} 1 \end{pmatrix}, \quad I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Quand on note une loi additivement ou multiplicativement, on a l'habitude d'utiliser les notations usuelles 0 et 1.

Notation. Soit E un magma admettant un élément neutre.

— Si la loi de E est notée multiplicativement, alors l'élément neutre de E est parfois noté 1_E ou simplement 1.
— Si la loi de E est notée additivement, alors l'élément neutre de E est parfois noté 0_E ou simplement 0.

Noter, qu'en général, un magma n'admet pas un élément neutre (par exemple $(\mathbb{N}^*, +)$). Mais, lorsqu'il l'admet, on peut donc parler de la notion d'un élément symétrisable définie comme suit.

Définition 1.1.21 (Symétrique d'un élément)

Soit $(E, *)$ un magma admettant un élément neutre e.
Un élément x est dit **symétrisable** dans E, s'il existe un élément $y \in E$ vérifiant : $x * y = y * x = e$. Dans ce cas, y est appelé un **symétrique** de x dans E.

Il est claire que si $(E, *)$ est un magma commutatif, alors $x \in E$ est symétrisable dans E s'il existe un élément $y \in E$ vérifiant seulement l'un des égalités $x * y = e$ ou $y * x = e$.

Exercice 1.1.22

On muni $\mathbb{R}$ de loi de composition interne $*$ définie par : $\forall (x, y) \in \mathbb{R}^2$, $x * y = xy + (x^2 - 1)(y^2 - 1)$.

1. Montrer que $\mathbb{R}$ muni de la loi $*$ admet un élément neutre que l'on déterminera.
2. Montrer que la loi $*$ est commutative.
3. Montrer que la loi $*$ n'est pas associative.
4. Déterminer l'ensemble S des éléments symétrisables dans $(\mathbb{R}, *)$. Et montrer qu'en particulier tout élément $a \in \mathbb{R}$ avec $|a| > 1$ admet deux symétriques.

Pour garentir l'unicité du symétrique, on a besoin que la loi soit associative.

Définition 1.1.23

Un magma associatif $(E, *)$ admettant un élément neutre sera appelé un **monoïde**.

Par abus de langage, on peut dire simplement "le monoïde E" au lieu de "le monoïde $(E, *)$" lorsqu'il n'y a pas d'ambiguïté sur la loi $*$.

Voir parmi les exemples de magmas donnés dans Exemples 1.1.6 et 1.1.9 ceux qui sont des monoïdes. Aussi, en utlisant l'exemple 1.1.19, l'assertion (2) de la proposition et définition 1.1.7 peut être reformuler en termes de monoïde comme suit :

Proposition et Définition 1.1.24 (Monoïde produit)

Soit $((M_i, \perp_i))_{1 \leq i \leq n}$ (où $n \in \mathbb{N}^*$) une famille finie de monoïdes. Alors, le magma produit $M = M_1 \times \cdots \times M_n$ est un monoïde. Il est appelé le **monoïde produit** des monoïdes $(M_1, \perp_1)$,...,$(M_n, \perp_n)$.

De même en utlisant l'exemple 1.1.20, l'assertion (2) de la proposition et définition 1.1.10 peut être reformuler en termes de monoïde comme suit :

Proposition et Définition 1.1.25 (Monoïdes des matrices carrées)

Le magmas $(\mathcal{M}_n(\mathbb{K}), +)$ (resp., $(\mathcal{M}_n(\mathbb{K}), \times)$) est un monoïde appelé le **monoïde produit (additif) des matrices carrées** (resp., **monoïde produit (multiplicatif) des matrices carrées**).

Proposition 1.1.26

Dans un monoïde, tout élément symétrisable admet un unique symétrique.

Preuve. Soit x un élément symétrisable d'un monoïde $(E, *)$ d'élément neutre e. Supposons qu'il admet deux symétriques x' et x''. Alors, en utilisant l'associativité de loi de E, on obtient

$$x' = e * x' = (x'' * x) * x' = x'' * (x * x') = x'' * e = x''.$$

D'où le résultat. **(c.q.f.d)**

D'après l'exercice 1.1.22, si à chaque élément symétrisable on fait correspondre un symétrique, on ne peut pas dire que cette correspondance est une application car on aura pas l'unicité de l'image. Cependant, si on travaille dans un monoïde, dans ce cas on parle d'une application. Ainsi, on peut adopter la notation suivante :

Notation. Le symétrique d'un élément symétrisable x dans un monoïde $(E, *)$ sera noté $sym_*(x)$ ou simplement $sym(x)$ lorsqu'il n'y a pas d'ambiguïté sur la loi $*$.
En particulier, si la loi de E est notée :

— multiplicativement, les éléments symétrisables seront dits **inversibles**. Dans ce cas, le symétrique d'un élément inversible x sera appelé **l'inverse** de x et noté x^{-1}.
— additivement, le symétrique de x sera noté $-x$ et appelé **l'opposé** de x.

Exemple 1.1.27

1. *Soit $(E_1, \perp_1), ..., (E_n, \perp_n)$ (où $n \in \mathbb{N}^*$) des monoïdes. Soit $(x_1, ..., x_n)$ un élément du monoïde produit $E = E_1 \times \cdots \times E_n$. Alors, on montre facilement que $(x_1, ..., x_n)$ est symétrisable si et seulement si, pour chaque $i \in \{1, ..., n\}$, x_i est symétrisable dans E_i. Dans ce cas,*

$$sym(x_1, ..., x_n) = (sym(x_1), ..., sym(x_n)).$$

En particulier, si les lois des E_i sont tous notées :

– *multiplicativement, alors la loi du monoïde E sera notée multiplicativement et on écrit* $(x_1, ..., x_n)^{-1} = ((x_1)^{-1}, ..., (x_n)^{-1})$..
– *additivement, alors la loi du monoïde E sera notée additivement et on écrit* $-(x_1, ..., x_n) = (-x_1, ..., -x_n)$.

2. *Toute matrice $A = (a_{i,j})$ dans le monoïde $(\mathcal{M}_n(\mathbb{K}), +)$ admet une opposée qui est $-A = (-a_{i,j})$.*
3. *Il existe des matrices dans $(\mathcal{M}_n(\mathbb{K}), \times)$ qui ne sont pas inversible. Notemment, dans $(\mathcal{M}_2(\mathbb{K}), \times)$, on peut montrer facilement l'équivalence suivant :*
une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible si et seulement si $ad - bc \neq 0$.

Le nombre $ad - bc$ est appelé le ***déterminant*** *de la matrice M et noté $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ ou aussi $det(M)$. On écrit alors :*

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \quad ou \quad det(M) = ad - bc.$$

Si $det(M) = ad - bc \neq 0$, l'inverse de M est $M^{-1} = \begin{pmatrix} \frac{d}{det(M)} & \frac{-b}{det(M)} \\ \frac{-c}{det(M)} & \frac{a}{det(M)} \end{pmatrix}$.
Avec le produit externe introduit à la fin de cette section on écrit simplement : $M^{-1} = \frac{1}{det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Si on pose $SYM(E)$ l'ensemble des éléments symétrisables dans E, alors l'application

$$\begin{array}{rccc} sym: & SYM(E) & \longrightarrow & SYM(E) \\ & x & \longmapsto & sym(x) \end{array}$$

est bien définie.
Il claire d'après la définition de l'élément symétrisable, si un élément x de E est symétrisable, alors son symétrique est de même symétrisable de symétrique x. On écrit, $sym(sym(x)) = x$; autrement dit, l'application sym est involutive [1].
En particulier, si la loi de E est notée :
– multiplicativement, on écrit pour un élément inversible x : $(x^{-1})^{-1} = x$.
– Si la loi de E est notée additivement, on écrit pour un élément x qui admet un opposé : $-(-x) = x$.

On montre qu'en plus l'application sym est anti-involutive [2].

1. Une application $f : E \to E$ est dite **involutive** ou une **involution** lorsqu'on l'applique deux fois on se ramène au point de départ ; i.e., $(f \circ f)(x) = x$ pour tout $x \in E$.
2. Une involution $f : E \to E$, où $(E, *)$ est un monoïde, est dite anti-involutive si elle vérifie $f(xy) = f(y)f(x)$ pour tout $x, y \in E$.

Proposition 1.1.28

Soit $(E, *)$ un monoïde. Soit $(x, y) \in E^2$. Si x et y sont symétrisables, alors xy est symétrisable de symétrique $sym(y) * sym(x)$. On écrit, $sym(x * y) = sym(y) * sym(x)$.

Preuve. On a

$$\begin{aligned}(x * y) * (sym(y) * sym(x)) &= x * (y * (sym(y) * sym(x))) \\ &= x * ((y * (sym(y)) * sym(x)) \\ &= x * (e * sym(x)) \\ &= x * sym(x) = e.\end{aligned}$$

De même on montre $(sym(y) * sym(x)) * (x * y) = e$. D'où, xy est symétrisable de symétrique $sym(y) * sym(x)$. **(c.q.f.d)**

Ainsi, la proposition 1.1.28 peut être reformuler dans le cas des notations additive et multiplicative comme suit :

Notation. Soit E un monoïde.
– Si la loi de E est notée multiplicativement, alors pour deux éléments inversibles x et y de E, xy est inversible et on a : $(xy)^{-1} = y^{-1}x^{-1}$.
– Si la loi est notée additivement, alors si x et y admettent des opposés, il en est de même de $x + y$, et on a : $-(x + y) = (-y) + (-x)$.

Avec l'élément symétrisable on peut simplifier des égalités, autrement dit, si x est un élément symétrisable de symétrique x' dans un monoïde $(E, *)$, alors si pour un couple $(y, z) \in E^2$, on a $x * y = x * z$, alors $y = z$. En effet, on multipliant les deux membres de cette égalité par le symétrique de x, on obtient $x' * (x * y) = x' * (x * z)$. Or la loi de E est associative, alors $(x' * x) * y = (x' * x) * z)$. Et puisque, $x' * x = e$, on obtient $y = z$.
Cela souligne une des utilités de l'élément symétrisable, mais on a des situations que même l'élément n'est pas symétrisable et on peut simplifier une égalité de genre $x * y = x * z$, comme il est le cas pour tous les éléments du monoïde multiplicatif $(\mathbb{Z}^*, \times)$ où seuls 1 et -1 sont inversibles (i.e. symétrisables). Cela donne lieu à la notion suivante :

Définition 1.1.29

Un élément x d'un monoïde $(E, *)$ est dit **régulier** (ou aussi **simplifiable**) s'il vérifie les deux assertions suivantes :
— Pour tout $(y, z) \in E^2$, $x * y = x * z \Rightarrow y = z$ (simplification à gauche).
— Pour tout $(y, z) \in E^2$, $y * x = z * x \Rightarrow y = z$ (simplification à droite).

Proposition 1.1.30

Dans un monoïde tout élément symétrisable est régulier.

Noter qu'un élément régulier n'est pas nécessairement symétrisable. Par exemple, dans $(\mathbb{Z}, \times)$, tout élément non nul est régulier, alors que seuls 1 et -1 sont inversibles dans $(\mathbb{Z}, \times)$.

Exercice 1.1.31

On pose $H = (\mathbb{Z}/n\mathbb{Z})\backslash\{\overline{0}\}$, où $n \in \mathbb{N}\backslash\{0, 1\}$, et on considère le monoïde $(H, \times)$.

1. Soit $m \in \{0, ..., n-1\}$. Montrer que $\overline{m}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si m et n sont premier entre eux.
2. En déduire que n est premier si et seulement si tout élément de H est inversible.
3. Montrer qu'un élément de $(H, \times)$ est régulier si et seulement s'il est inversible.

Exercice 1.1.32

Soit $(G, *)$ un monoïde fini.

1. Soit $g \in G$. On considère l'application $d_g : G \to G$ définie par $d_g(x) = g * x$ pour tout $x \in G$.
   Montrer que d_g est bijective si et seulement si g est symétrisable.
2. On suppose que tout élément de G est régulier. Montrer que tout élément de G est symétrisable.
3. Montrer qu'on obtient le même résultat de la question précédente si on suppose que $(G, *)$ est seulement un magma associatif fini.
4. Donner un exemple d'un monoïde dont tout élément est régulier mais pas tout élément est symétrisable.

L'associativité de la loi d'un monoïde permet d'étendre le composé de deux éléments au composé de plusieurs éléments comme suit :

Définition 1.1.33

Soit $(E, *)$ un monoïde d'élément neutre e.
Le composé d'un nombre fini d'éléments de E se définit par récurrence comme suit : Considérons une suite $(x_i)_i$ d'éléments de E. Pour tout entier $n \geq 2$, on écrit :

$$x_1 * \cdots * x_n * x_{n+1} := (x_1 * \cdots * x_n) * x_{n+1}.$$

En particulier, si $x = x_1 = \cdots = x_n$, alors $x_1 * \cdots * x_n$ sera noté x^{*n}.
Pour $n = 1$, on convient de poser $x^{*1} = x$.
Pour $n = 0$, on convient de poser $x^{*0} = e$.

Notation. Soit x un élément d'un monoïde $(E, *)$. Si on note la loi de E :
— multiplicativement, alors x^{*n} sera simplement noté x^n et appelé la **puissance n-ième** de x. On lit x exposant n ou x puissance n.
— additivement, alors x^{*n} sera simplement noté nx. Dans ce cas, nx est dit un **multiple** de x.

Proposition 1.1.34

Soient a et b deux éléments d'un monoïde $(E, *)$. Alors, pour tout $(p, q) \in \mathbb{N}^2$, on a les assertions suivantes :

1. $a^{*p} * a^{*q} = a^{*(p+q)}$.
2. $(a^{*p})^{*q} = a^{*qp} = (a^{*q})^{*p}$.
3. Si a et b commutent, alors $(ab)^{*p} = a^{*p} b^{*p}$.

Dans les cas additif et multiplicatif, la proposition 1.1.34 peut être reformuler comme suit :

Notation. Si on note la loi de E :
— multiplicativement, on écrit :
1. $a^p a^q = a^{(p+q)}$.
2. $(a^p)^q = a^{qp} = (a^q)^p$.
3. $(ab)^p = a^p b^p$ si a et b commutent.

— additivement, on écrit :
1. $pa + qa = (p + q)a$.
2. $q(pa) = (qp)a = pq)a = p(qa)$.
3. $p(a + b) = pa + pb$ si a et b commutent.

Pour étendre l'utilisation de la notation x^{*n} à tout entier relatif n, on a besoin du résultat suivant :

Proposition 1.1.35

Soit $(E, *)$ un monoïde. Soient $x \in E$ et n un entier naturel. Si x est symétrisable, alors x^{*n} est symétrisable de symétrique $(sym(x))^{*n}$. On écrit, $sym(x^{*n}) = (sym(x))^{*n}$.

Notation. Soit x un élément symétrisable d'un monoïde $(E, *)$. Si on note la loi de E :
— multiplicativement, on écrit : $(x^n)^{-1} = (x^{-1})^n$.
— additivement, on écrit : $-(nx) = n(-x)$.

La proposition précédente nous permet d'étendre l'utilisation de la notation x^{*n} à tout entier relatif comme suit :

Définition 1.1.36 (Puissances généralisées)

Soient $(E, *)$ un monoïde d'élément neutre e et x un élément symétrisable de E. Pour tout entier négatif n, on pose :

$$x^{*n} = (sym(x))^{*(-n)}.$$

Corollaire 1.1.37

Soient $(E, *)$ un monoïde d'élément neutre e et x un élément symétrisable de E. Alors, pour tout entier $n \in \mathbb{Z}$, on a :

$$x^{*n} = (sym(x))^{*(-n)} = sym(x^{*(-n)}).$$

Notation. Soit x un élément symétrisable d'un monoïde $(E, *)$. Si on note la loi de E :
— multiplicativement, on écrit $x^n = (x^{-1})^{-n} = (x^{-n})^{-1}$.
— additivement, on écrit $nx = (-n)(-x) = -((-n)x)$.

Noter que na, où $n \in \mathbb{N}$ et a un élément d'un monoïde additif M, exprime en général la somme de a répété n fois. Dans certain cas, na est exprimé par une autre loi de M. Par exemple, si $M = \mathbb{Z}$, donc na n'est que le produit (interne) de n par a. Aussi, si $M = \mathbb{Z}/m\mathbb{Z}$ (où $m \in \mathbb{N}$), alors na n'est que le produit (interne) de $\overline{n}$ par a. En effet, si $a = \overline{b}$, pour un certain entier b, alors $na = n\overline{b} = \overline{nb} = \overline{n}\overline{b}$.

Il arrive des fois qu'on a $a * b = b * a$ pour deux éléments a et b d'un monoïde E sans qu'il soit nécessairement commutatif. On dit que les deux éléments a et b **commutent** si $a * b = b * a$.

Proposition 1.1.38

Soient a et b deux éléments symétrisables d'un monoïde $(E, *)$. Alors, pour tout $(p, q) \in \mathbb{Z}^2$, on a les assertions suivantes :

1. $a^{*p} * a^{*q} = a^{*(p+q)}$.
2. $(a^{*p})^{*q} = a^{*qp} = (a^{*q})^{*p}$.
3. Si a et b commutent, alors $(ab)^{*p} = a^{*p}b^{*p}$.

Dans les cas additif et multiplicatif, la proposition 1.1.38 peut être reformuler comme suit :

Notation. Soient a et b deux éléments symétrisables d'un monoïde $(E, *)$. Si on note la loi de E :

— multiplicativement, on écrit :

1. $a^p a^q = a^{(p+q)}$.
2. $(a^p)^q = a^{qp} = (a^q)^p$.
3. Si a et b commutent, alors $(ab)^p = a^p b^p$.

— additivement, on écrit :

1. $pa + qa = (p + q)a$.
2. $q(pa) = (qp)a = pq)a = p(qa)$.
3. Si a et b commutent, alors $p(a + b) = pa + pb$.

Noter que la condition «a et b commutent» est nécessaire pour que $(ab)^{*p} = a^{*p}b^{*p}$. Voir l'exercice suivant :

Exercice 1.1.39

Soient a et b deux éléments symétrisables d'un monoïde $(E, *)$. Montrer que si $(ab)^{*2} = a^{*2}b^{*2}$, alors a et b commutent.

Proposition 1.1.40

Soit $(E_1, \perp_1), ..., (E_n, \perp_n)$ (où $n \in \mathbb{N}^*$) des monoïdes et on considère le monoïde produit $E = E_1 \times \cdots \times E_n$. Alors, $(a_i)_i \in E$ et pour tout $n \in \mathbb{Z}$, $n(a_i)_i = (na_i)_i$.

Preuve. Par récurrence sur n. **(c.q.f.d)**

Produit externe sur les monoïdes produits usuels. Dans le résultat ci-dessus, il claire que le produit $n(a_i)_i$ d'un élément $(a_i)_i \in E$ par un entier

$n \in \mathbb{Z}$ est externe de E. Dans le cas où $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, ce produit peut être étendu à $\mathbb{K}$ comme suit :

$$\forall \lambda \in \mathbb{K}, \forall (a_i)_i \in \mathbb{K}^n, \qquad \lambda (a_i)_i = (\lambda a_i)_i.$$

On peut facilement montrer les propriétés suivantes :
$\forall x, y \in \mathbb{K}, \forall u, v \in \mathbb{K}^n$,

$$\begin{cases} x(u+v) = xu + xv \\ (x+y)u = xu + yv \end{cases} \quad \begin{cases} x(uv) = (xu)v = u(xv) \\ (xy)u = x(yu) \end{cases}$$

Proposition 1.1.41

On considère le monoïde des matrices carrées $\mathcal{M}_n(\mathbb{K})$ d'ordre un entier $n \geq 1$ à coefficients dans $\mathbb{K}$ (où $K = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$). Montrer que, pour tout $n \in \mathbb{Z}$ et tout $(a_{i,j}) \in M_n(\mathbb{K})$, $n(a_{i,j}) = (na_{i,j})$.

Produit externe sur le monoïde des matrices carrées. Il claire que le produit $n(a_{i,j})$ est externe. Comme dans le cas du monoïde produit, ce produit peut être étendu à $\mathbb{K}$ comme suit :

$$\forall \lambda \in \mathbb{K}, \forall (a_{i,j}) \in \mathcal{M}_n(\mathbb{K}), \qquad \lambda (a_{i,j}) = (\lambda a_{i,j}).$$

Par exemple,

$$\lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$$

On peut facilement montrer les propriétés suivantes :
$\forall x, y \in \mathbb{K}, \forall A, B \in \mathcal{M}_n(\mathbb{K})$,

$$\begin{cases} x(A+B) = xA + xB \\ (x+y)A = xA + yA \end{cases} \quad \begin{cases} x(AB) = (xA)B = A(xB) \\ (xy)A = x(yA) \end{cases}$$

1.2 Groupes

Dans la suite, sauf mention contraire, on utilisera la notation multiplicative.

Définition 1.2.1 (Groupe)

On appelle **groupe** tout monoïde $(G, *)$ tel que tout élément est inversible.

Par abus de langage , on peut dire simplement "le groupe G" au lieu de "le groupe $(G, *)$" lorsqu'il n'y a pas d'ambiguïté sur la loi $*$.

Notation et vocabulaire.

— Si la loi de G est commutative, G est dit un **groupe commutatif** ou un **groupe abélien**.
— Si G est fini, on dit que G est **d'ordre fini** et son cardinal sera noté par $|G|$ et appelé **l'ordre** de G.

Exemple 1.2.2

1. $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Z},+)$ *et* $(\mathbb{Q},+)$ *sont des groupes abéliens.*
2. $(\mathbb{R}^*,\times)$, $(\mathbb{C}^*,\times)$ *et* $(\mathbb{Q}^*,\times)$ *sont des groupes abéliens.*
3. *Pour tout* $n\in\mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe abélien.*
4. $(\mathbb{Z}^*,\times)$ *n'est pas un groupe car, par exemple,* 2 *n'est pas inversible (en fait, seuls* 1 *et* -1 *sont inversibles).*
5. $(\mathbb{R},\times)$ *n'est pas un groupe car, par exemple,* 0 *n'est pas inversible.*
6. $(\mathbb{N},+)$ *n'est pas un groupe. En effet, aucun élément non nul n'est inversible.*
7. *Soit* E *un ensemble. Si on note* $\mathfrak{S}(E)$ *l'ensemble des bijections de* E *dans* E*, alors l'ensemble* $\mathfrak{S}(E)$ *muni de la comoposition des applications* $\circ$ *est un groupe appelé* ***groupe symétrique*** *de* E*. En particulier,* S_n *est l'ensemble des permutations de* $\mathbb{N}_n=\{1,2,...,n\}$ *où* $n\geq 1$*. Rappelons que* $Card(S_n)=n!$*.*
8. *L'ensemble des isométries du plan (i.e., des applications qui préservent les distances) muni de la comoposition des applications est un groupe.*
9. *L'ensemble* $\{0,1\}$ *muni de la loi définie par la table de Cayley suivante*

$+$	0	1
0	0	1
1	1	0

est un groupe.

Proposition et Définition 1.2.3 (Groupe produit)

Soit $(G_1,...,G_n)$ (où $n\in\mathbb{N}^*$) une famille finie de groupes. Alors, le monoïde produit est un groupe qui est commutatif si et seulement si G_i est commutatif pour tout $i\in\{1,...,n\}$.
Le groupe G est appelé le **groupe produit** des groupes G_i. Dans le cas où $G_1=\cdots=G_n=G$, le groupe produit sera noté simplement G^n.

Exercice 1.2.4

Soit $n\in\mathbb{N}^*$. On désigne par $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble $(\mathbb{Z}/n\mathbb{Z})\backslash\{\overline{0}\}$. Montrer que $((\mathbb{Z}/n\mathbb{Z})^*,\times)$ est un groupe si et seulement si n est premier.

Exercice 1.2.5

Soit G un magma associatif vérifiant les deux assertions suivantes :

1. $\exists\, e \in G,\ \forall\, x \in G,\ x\,e = x$ (autrement dit, G possède un élément neutre à droite e).
2. $\forall\, x \in G,\ \exists\, x' \in G,\ x\,x' = e$ (autrement dit, x admet possède un inverse à droite x').

Montrer que G est un groupe.

Exercice 1.2.6

On considère l'ensemble E des matrices carrées à coefficients réels de la forme

$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}$$

tel que $x \in \mathbb{R}^*$ et $y \in \mathbb{R}$, muni du produit des matrices.

1. Montrer que E est une partie stable pour le produit des matrices carrées à coefficients réels.
2. Déterminer tous les éléments neutres à droite de E.
3. Montrer que E n'admet pas d'élément neutre à gauche.
4. Soit e un élément neutre à droite. Montrer que tout élément de E possède un inverse à gauche pour cet élément neutre, i.e. $\forall\, g \in E$, $\exists\, h \in E,\ hg = e$.

Exercice 1.2.7

Soit G un groupe d'élément neutre e.

1. Montrer que si G est d'ordre pair, alors il existe un élément $x \in G$ tel que $x^2 = e$.
2. On suppose que, pour tout $x \in G$, $x^2 = e$. Montrer que G est commutatif.
3. Soit $n \geq 2$ un entier positif. On considère le groupe produit H^n, où H est le groupe additif $\mathbb{Z}/2\mathbb{Z}$. Montrer que le groupe H^n vérifie bien la condition de la dernière question.

1.3 Sous-groupes

Pour aborder la notion de sous-groupe, il faut d'abord savoir ce qu'est une partie stable d'une loi.

Définition 1.3.1

Une partie non vide H d'un magma $(E, *)$ est dite **stable** pour la loi de E si, pour tout $(x, y) \in H^2$, $x * y \in H$. Dans ce cas, la restriction de la loi de E à H est une loi de composition interne sur H appelée **la loi induite** sur H. Cette loi sera notée par le même symbole que celui de la loi de E.

Exemple 1.3.2

1. *L'ensemble des entiers naturels pairs est stable pour l'addition, cependant l'ensemble des entiers naturels impairs n'est pas stable pour l'addition. Les deux ensembles sont stables pour la multiplication.*
2. *Soit $n \in \mathbb{N}\backslash\{0, 1\}$. On considère l'ensemble $\mathcal{Z}_n$ des éléments $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ (avec $k \in \mathbb{Z}$) tels qu'il existe $\overline{k'} \in \mathbb{Z}/n\mathbb{Z}$ (avec $k' \in \mathbb{Z}$) avec $\overline{kk'} = 0$. Par exemple, $\mathcal{Z}_4 = \{\overline{0}, \overline{2}\}$ et $\mathcal{Z}_/= \{\overline{0}, \overline{2}, \overline{3}, \overline{4}\}$. On peut voir, en utilisant l'exercice 1.1.31, que $\mathcal{Z}_n = \{\overline{0}\}$ si et seulement si n est premier. En général, l'ensemble $\mathcal{Z}_n$ est stable pour la multiplication mais n'est pas, en général, stable pour l'addition.*
3. *L'ensemble des matrices triangulaires supérieures à diagonale unité est stable pour le produit mais pas pour la somme.*
4. *L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est stable pour le produit.*
5. *L'ensemble $\mathbb{U}_n \subset \mathbb{C}$ des racines n-ièmes de l'unité est stable pour le produit des nombres complexes.*

Pour un monoïde $(M, *)$, la partie des éléments inversibles dans M est évidemment non vide, elle sera notée $U(M, *)$ ou simplement $U(M)$.

Proposition 1.3.3

Si $(M, *)$ est un monoïde, alors $U(M)$ est stable pour la loi de M. En plus, muni de la loi induite, $U(M)$ est un groupe.

Il facile de voir que $U(M) = M$ si et seulement si M est un groupe.

Exemple 1.3.4

1. $U(\mathbb{Z}, \times) = \{-1, 1\}$.
2. *$U(\mathbb{Z}/4\mathbb{Z}, \times) = \{\overline{1}, \overline{3}\}$ et $U(\mathbb{Z}/12\mathbb{Z}, \times) = \{\overline{1}, \overline{5}, \overline{Z}, \overline{11}\}$. D'après l'exercice 1.1.31, on peut déduire qu'en général : $U(\mathbb{Z}/n\mathbb{Z}, \times) = \{\overline{k};\ k \in \mathbb{Z}$ premier avec $n\}$.*

Définition 1.3.5 (Sous-groupe)

Soit H une partie d'un groupe G. On dit que H est un **sous-groupe** de G si les assertions suivantes sont vérifiées :

1. $H \neq \emptyset$,
2. H est stable pour la loi de G, et
3. H muni de la loi induite est un groupe.

Exemple 1.3.6

1. *Pour tout groupe G d'élément neutre e, les deux ensembles G et $\{e\}$ sont des sous-groupes de G, appelés* ***sous-groupes triviaux*** *de G.*
2. *$(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$.*
3. *$(\mathbb{Q}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.*
4. *Pour tout $n \in \mathbb{N}$, $n\mathbb{Z} := \{nk | k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$. On verra que seuls les $n\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$.*
5. *L'ensemble des rotations du plan est un sous-groupe du groupe des isométries du plan.*

Proposition 1.3.7

Soit H un sous-groupe d'un groupe G. Alors,

1. l'élément neutre de H est celui de G.
2. L'inverse d'un élément $a \in H$ dans H est celui de a dans G.

En pratique, pour montrer qu'une partie non vide est un sous-groupe on utilise le résultat important suivant :

Théorème 1.3.8 (Caractérisation des sous-groupes)

Soit H une partie **non vide** d'un groupe G. Alors, les assertions suivantes sont équivalentes :

1. H est un sous-groupe de G.
2. Les assertions suivantes sont vérifiées :
   (a) H est stable pour la loi de G.
   (b) H est stable par passage à l'inverse (i.e., pour tout $x \in H$, $x^{-1} \in H$).
3. Pour tout $(x, y) \in H^2$, $xy^{-1} \in H$.

Exercice 1.3.9

Montrer que l'ensemble $\{1+2m/1+2n|n,m\in\mathbb{Z}\}$ est un sous-groupe multiplicatif de $\mathbb{Q}^*$.

Exercice 1.3.10

On munit $E=\mathbb{R}^*\times\mathbb{R}$ de la loi de composition interne $\star$ définie par : $(a,e)\star(b,f)=(ab,af+e)$ pour tout $((a,e),(b,f))\in E^2$.

1. Montrer que $(E,\star)$ est un groupe non commutatif.
2. Soit H un sous-groupe de $(\mathbb{R}^*,\times)$. Montrer que $H\times\mathbb{R}$ est un sous-groupe de E.

Exercice 1.3.11

Soit G un groupe. Montrer que l'ensemble $Z(G):=\{g\in G|\forall x\in G,\ gx=xg\}$ est un sous-groupe de G.

Proposition 1.3.12

Les sous-groupes de $(\mathbb{Z},+)$ sont tous de la forme $n\mathbb{Z}$ où $n\in\mathbb{N}$.

Nous allons voir à travers l'exercice 1.4.18 comment déterminer l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1.3.13

Soit $(n,m)\in\mathbb{Z}^2$.

1. Montrer que $m\mathbb{Z}\subset n\mathbb{Z}$ si et seulement si n divise m.
2. En déduire les sous-groupes du groupe additif $(n\mathbb{Z},+)$.

Exercice 1.3.14

Soit G un sous-groupe additif de $(\mathbb{R},+)$. On pose a la borne inférieure de $G\cap]0,+\infty[$. Alors,

— si $a\neq 0$, alors $G=a\mathbb{Z}:=\{ka|k\in\mathbb{Z}\}$ (dit le sous-groupe discert de $\mathbb{R}$ engendré par a).

— Si $a=0$, alors G est dense dans $\mathbb{R}$ (on rappelle qu'une partie D de $\mathbb{R}$ est dite dense dans $\mathbb{R}$ si pour tout $x<y$ dans $\mathbb{R}$ il existe $d\in D$ tel que $x<d<y$).

Proposition 1.3.15

Toute intersection de sous-groupes d'un groupe G est un sous-groupe de G.

Exercice 1.3.16

Soient n et m deux entiers naturels. Déterminer l'intersection $n\mathbb{Z} \cap m\mathbb{Z}$.

L'union de deux sous-groupes d'un groupe G n'est pas, en général, un sous-groupes de G. Par exemple, $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$ (voir aussi 2 de l'exercice 1.3.31). En particulier, nous avons le résultat suivant :

Proposition 1.3.17

Soient H et K deux sous-groupes d'un groupe G. Alors, $H \cup K$ est un sous-groupe de G si et seulement si $H \subseteq K$ ou $K \subseteq H$.

Soient H et K deux sous-groupes d'un groupe G abélien. Supposons que la loi de G est notée additivement. L'ensemble $H + K := \{h + k | h \in H, k \in K\}$ est appelé la **somme des sous-groupes** H et K.

Proposition 1.3.18

La somme des deux sous-groupes d'un groupe abélien G est un sous-groupe de G.

La notion de somme de deux idéaux peut s'étendre d'une manière naturelle à la somme d'une famille finie de sous-groupes.

Exercice 1.3.19

Montrer que, pour deux entiers naturels n et m, $n\mathbb{Z} + m\mathbb{Z} = \text{pgcd}(m, n)\mathbb{Z}$.

Maintenant, nous introduisons l'un des concepts importants de la théorie des groupes : "L'engendrement". En fait, nous allons nous limiter cette année au cas des sous-groupes (groupes) monogènes : sous-groupes (groupes) engendrés (ou générés) par un seul élément. L'idée d'engendrement est basée sur la question suivante :

Etant donné un élément a dans un groupe G, quel genre de sous-groupes pouvons-nous construire en utilisant seulement a ?

En fait, en utilisant la stabilité de ce sous-groupe, il contiendra toutes les puissances de a. En d'autres termes, il contiendra l'ensemble $\{a^n | n \in \mathbb{Z}\}$. Nous montrons dans le résultat suivant que cet ensemble est en fait un sous-groupe de G. Donc, l'ensemble $\{a^n | n \in \mathbb{Z}\}$ est un sous-groupe de G engendré par a, et en fait, d'après le raisonnement ci-dessus, il est le plus petit sous-groupe de G contenant a. D'où le théorème fondamental suivant :

Théorème et Définition 1.3.20

Soient G un groupe et $a \in G$. L'ensemble $\{a^n | n \in \mathbb{Z}\}$ est un sous-groupe de G, dit **engendré** par a et noté $< a >$. On dit aussi que a est un **générateur** du sous-groupe $< a >$.
En plus, pour tout sous-groupe H de G, si $a \in H$, alors $< a > \subset H$. On dit que le sous-groupe engendré par a est le plus petit sous-groupe de G, au sens de l'inclusion, contenant a.

Preuve. On pose $K = \{a^n | n \in \mathbb{Z}\}$. Montrons que K est un sous-groupe de G. Il claire que K est non vide. En effet, $1 = a^0 \in K$. Considère maintenant deux élément $x = a^m$ et $y = a^n$ de K, où $m, n \in \mathbb{Z}$. Alors,

$$xy^{-1} = a^m(a^n)^{-1} = a^{m-n}.$$

D'où, $xy^{-1} \in K$. Par suite, K est un sous-groupe de G.
Enfin, il est claire que si un sous-groupe H de G contient a, alors, $a^n \in H$ pour tout $n \in \mathbb{Z}$. D'où, $< a > \subset H$. **(c.q.f.d)**

Définition 1.3.21

Soit G un groupe. Tout sous-groupe de G de la forme $< a >$ (i.e., engendré par a), pour certain $a \in G$, est dit **monogène**.

En particulier, si $G =< g >= \{g^n | n \in \mathbb{Z}\}$, pour un certain $g \in G$, on dit aussi que G est un groupe **monogène** engendré par g.

Remarque 1.3.22

1. *Il importe de noter que si la loi de G est notée additivement, alors on écrit $< a >= \{na | n \in \mathbb{Z}\}$.*
2. *Il est claire que pour tout groupe G d'élément neutre e, $< e >= \{e\}$. En fait, c'est le seul sous-groupe de G d'ordre 1.*

Exemple 1.3.23

1. *Il est évident que $\mathbb{Z}$ est un groupe monogène engendré par 1. Nous avons vu à partir de la proposition 1.3.12 que en fait tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ (pour un certain $n \in \mathbb{N}$) qui est bien le sous-groupe monogène de $\mathbb{Z}$ engendré par n (i.e., $n\mathbb{Z} =< n >$). D'où les sous-groupes de $(\mathbb{Z}, +)$ sont tous monogènes.*

2. *Cependant, le groupe produit $\mathbb{Z}^2$ n'est pas monogène. Car si on suppose qu'il est monogène, alors il existe $(a,b) \in \mathbb{Z}^2$, tel que $\mathbb{Z}^2 =< (a,b) >$. Cela veut dire que pour tout $(x,y) \in \mathbb{Z}^2$, il existe $k \in \mathbb{Z}$ tel que $(x,y) = k(a,b)$. Alors, en particulier, pour $(x,y) = (0,1)$, il existe $k \in \mathbb{Z}$ tel que $(0,1) = k(a,b)$. Alors, d'après la proposition 1.1.40, $(0,1) = (ka,kb)$, c'est-à-dire $ka = 0$ et $kb = 1$. L'entier k ne peut pas être nul car sinon $1 = kb = 0$. Alors, $ka = 0$ nous donne $a = 0$. De même on montre que $b = 0$ en utilisant $(1,0)$ à la place de $(0,1)$. Mais, on sait que $< (0,0) >= \{(0,0)\}$. Ce qui est absurde.*
3. *Le groupe additif $\mathbb{Q}$ n'est pas monogène. En fait, si on suppose qu'il est monogène, alors il existe $\frac{a}{b} \in \mathbb{Q}$ (avec $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ et on peut supposer que a et b sont premiers entre eux). Cela veut dire que pour tout $x \in \mathbb{Q}$, il existe $k \in \mathbb{Z}$ tel que $x = k\frac{a}{b}$. Alors, en particulier, pour tout $x \in \mathbb{Z}$, il existe $k \in \mathbb{Z}$ tel que $x = k\frac{a}{b}$. Alors, $xb = ka$, en particulier a divise xb, mais comme $\text{pgcd}(p,q) = 1$, a divise x. Cela pour tout $x \in \mathbb{Z}$, absurde.*
4. *De même, le groupe additif $\mathbb{R}$ n'est pas monogène.*

Exercice 1.3.24

On pose $H = \{(6n, 4m); (n,m) \in \mathbb{Z}^2\}$ et $K = \{(12k, 12k); k \in \mathbb{Z}\}$.

1. Montrer que H est un sous-groupe du groupe produit $\mathbb{Z}^2$. Est-il monogène ?
2. Montrer que n'est pas contenu dans aucun sous-groupe monogène de $\mathbb{Z}^2$.
3. Montrer que K est un sous-groupe monogène de $\mathbb{Z}^2$ contenu dans H.
4. Soit G est un sous-groupe monogène de $\mathbb{Z}^2$. Montrer que si $G \subset H$, alors G est contenu dans un sous-groupe monogène de $\mathbb{Z}^2$ de la forme $< (3\alpha, 2\beta) >$ pour certain $(\alpha, \beta) \in \mathbb{Z}^2$.

Proposition 1.3.25

Pour tout élément g d'un groupe G, le sous-groupe monogène $< g >$ est commutatif.

On considère, pour $n \in \mathbb{N}^*$ le groupe symétrisue S_n (i.e., l'ensemble des permutations de $\mathbb{N}_n = \{1, 2, ..., n\}$ muni de la composition des applications). On sait que S_n n'est pas commutatif sauf si $n = 2$, cependant S_n contient des sous-groupes commutatifs non-triviaux. Il suffit de considèrer un sous-groupe engendré par l'une des permutations (voir aussi l'exercice 1.3.38).

Proposition 1.3.26

Pour tout groupe G, le sous-groupe de G engendré par un élément $g \in G$ est le même le sous-groupe engendré par l'inverse de g. On écrit, $< g >=< g^{-1} >$.

Si la loi de G est notée additivement, alors on écrit $< g >=< -g >$.
En particulier, dans le groupe additif $\mathbb{Z}$, on a le résultat suivant :

Proposition 1.3.27

Pour tous deux entiers n et m dans le groupe additif $\mathbb{Z}$, on a $< m >=< n >$ si et seulement si $|n| = |m|$.

Remarque 1.3.28
Noter qu'il se peut que $< g >=< g' >$, pour deux éléments g et g' d'un groupe G, sans qu'il soit g l'inverse de g' (ou bien, dans le cas additif, g l'opposé de g'). On prend, par exemple, le groupe additif $\mathbb{Z}/21\mathbb{Z}$, on peut voir que : $< \overline{3} >=< \overline{15} >$ (car $\overline{15} = 5\,\overline{3}$ et $\overline{3} = 3\,\overline{15}$). Mais, $\overline{3} \neq -\overline{15} = \overline{6}$.

Définition 1.3.29

Soit H un sous-groupe monogène engendré par un élément a d'un groupe G. Si H est d'ordre fini, il sera dit **cyclique**. Dans ce cas, l'ordre de H est dit aussi **l'ordre de a** et noté simplement par $|a|$ (au lieu de $| < a > |$).

En particulier, si $G = \{g^n | n \in \mathbb{Z}\}$, pour un certain $g \in G$, et il est d'ordre fini, alors on dit aussi que G est un groupe **cyclique** engendré par g.

Exemple 1.3.30

1. *Pour tout entier n, le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par $\overline{1}$. En fait, on peut montrer que tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique (voir Exercice 1.4.18).*
2. *Les sous-groupes (cycliques) du groupe additif $\mathbb{Z}/6\mathbb{Z}$ sont : $< \overline{0} >= \{\overline{0}\}$; $< \overline{2} >= \{\overline{0}, \overline{2}, \overline{4}\}$ et $< \overline{3} >= \{\overline{0}, \overline{3}\}$ et $\mathbb{Z}/6\mathbb{Z} =< \overline{1} >$. Noter aussi que $< \overline{2} >=< -\overline{2} >=< \overline{4} >$ et que $\mathbb{Z}/6\mathbb{Z} =< \overline{1} >=< -\overline{1} >=< \overline{5} >$. Ainsi, par exemple, $\overline{2}$ est d'ordre 3, $\overline{3}$ est d'ordre 2 et $\overline{5}$ est d'ordre 6.*
3. *Les sous-groupes (cycliques) du groupe multiplicatif $(\mathbb{Z}/5\mathbb{Z})^*$ sont : $< \overline{1} >= \{\overline{1}\}$; $< \overline{2} >=< \overline{3} >= (\mathbb{Z}/5\mathbb{Z})^*$; $< \overline{4} >= \{\overline{1}, \overline{4}\}$.*
4. *L'ensemble $\mathbb{U}_n \subset \mathbb{C}$ des racines n-ièmes de l'unité muni de la mul-*

tiplication des nombres complexes est groupe cyclique engendré par $\omega_1 = e^{\frac{2i\pi}{n}}$.

Exercice 1.3.31

1. Montrer que l'ensemble $\{\overline{0}, \overline{9}, \overline{6}, \overline{3}\}$ est un sous-groupe de $\mathbb{Z}/12\mathbb{Z}$.
2. Déterminer les sous-groupes $< \overline{2} >$, $< \overline{3} >$ et $< \overline{6} >$ du groupe multiplicatif $(\mathbb{Z}/7\mathbb{Z})^*$. Noter que $< \overline{2} > \cup < \overline{6} >$ n'est pas un sous-groupe de $(\mathbb{Z}/7\mathbb{Z})^*$.

Exercice 1.3.32

Soient $n \neq 0$ un entier positif et $k \in \mathbb{Z}$. Alors, $\mathbb{Z}/n\mathbb{Z} =< \overline{k} >$ si et seulement si $\text{pgcd}(k, n) = 1$.

Théorème 1.3.33 (Ordre d'un groupe cyclique ; I)

Soit $G =< a >$ un groupe monogène. Alors, G est d'ordre fini (i.e., G est cyclique) si et seulement s'il existe $k \in \mathbb{N}^*$ tel que $a^k = 1$.

Théorème 1.3.34 (Ordre d'un groupe cyclique ; II)

Si $G =< a >$ un groupe cyclique d'ordre fini n, alors on a les assertions suivantes :

1. $n = \min\{k \in \mathbb{N}^* | a^k = 1\}$.
2. $G = \{1, a, a^2, ..., a^{n-1}\}$.
3. Si $k \in \mathbb{Z}^*$ vérifie $a^k = 1$, alors n divise k. Autrement dit, $\{k \in \mathbb{Z} | a^k = 1\} = n\mathbb{Z}$.

Exercice 1.3.35

Soit G un groupe d'élément neutre e.

1. Soit $g \in G\backslash\{e\}$. Montrer que les assertions suivantes sont équivalentes :
   (a) $|g| = 2$.
   (b) $g = g^{-1}$.
   (c) $< g >= \{e, g\}$.
2. On suppose que $|G| = 3$. Montrer que tout élément $a \in G\backslash\{e\}$ engendre G.
3. Montrer que le groupe additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique.

Exercice 1.3.36

Montrer que dans tout groupe G les ordres de ab et ba sont égaux pour tout $(a, b) \in G^2$.

Exercice 1.3.37

1. Soient x et y deux éléments d'un groupe G d'ordres respectifs p et q. On suppose que $xy = yx$ et que p et q sont premiers entre eux. Démontrer que xy est d'ordre pq.
2. On considère dans le groupe linéaire $GL_2(\mathbb{R})$ les deux matrices $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Vérifier que A et B sont d'ordre fini, mais que AB n'est pas d'ordre fini.

Exercice 1.3.38

Pour un entier n, on considère le groupe symétrisue S_n. Une permutation f est souvent représentée comme suit :

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

On considère dans le groupe symètrique S_5, les permutations :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}; \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} \text{ et } h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}.$$

1. Montrer que f et g sont d'ordres respectifs 2 et 3.
2. En déduire l'ordre de h (remarquez que $h = f \circ g = g \circ f$).

Exercice 1.3.39

Soit G un groupe fini d'élément neutre e vérifiant $x^2 = e$ pout $x \in G$. Alors, G est commutatif d'après l'exercice 1.2.7.

1. Soient H un sous-groupe de G et $g \in G \backslash H$. On pose $gH = \{gh/h \in H\}$.
   (a) Montrer que $H \cup gH$ est un sous-groupe de G.
   (b) Montrer que $card(gH) = |H|$.
   (c) En déduire $|H \cup gH| = 2|H|$.
2. On pose $H =< a >$ pour un élément $a \in G$. On considère $g \in G \backslash H$. Déterminer $|H \cup gH|$.
3. Montrer que l'ordre de G est une puissance de 2.

1.4 Morphismes de groupes

Définition 1.4.1 (Morphisme de groupes)

Soient $(G, *)$ et (G', T) deux groupes. On appelle **morphisme de groupes** ou **homomorphisme de groupes** de G dans G' toute application $\phi : G \longrightarrow G'$ vérifiant : pour tout $(x, y) \in G^2$, $\phi(x * y) = \phi(x) T \phi(y)$.

Notation et vocabulaire.
Soit $\phi : G \longrightarrow G'$ un morphisme de groupes.
— Lorsque les lois de G et G' sont notées multiplicativement on écrit simplement $\phi(xy) = \phi(x)\phi(y)$.
— L'ensemble $\phi(G)$ est appelé l'**image** de ϕ et il sera noté $\mathrm{Im}(\phi)$.
— Si $G = G'$, alors le morphisme ϕ est appelé **endomorphisme** de G.
— Si ϕ est bijectif, il sera appelé un **isomorphisme** de groupes. Dans ce cas, on dit que G et G' sont **isomorphes** et on écrit $G \cong G'$.
— Si $G = G'$ et ϕ est un isomorphisme, alors ϕ est appelé un **automorphisme** de G.

Exemple 1.4.2
1. *L'application identité d'un groupe G est un automorphisme de G. Rappelons l'application identité d'un ensemble E (ou application identique de E) est l'application de E dans E, notée Id_E, définie par $\mathrm{Id}_E(x) = x$ pour tout $x \in E$.*
2. *Soit $(G, *)$ un groupe d'élément neutre e. L'application $\phi : x \mapsto e$ est un endomorphisme de G.*
   En particulier, si la loi de G est notée additivement, alors on écrit

$\phi(x) = 0$ *pour tout* $x \in G$ *et dans ce cas,* ϕ *est appelé l'****endomorphisme nul*** *de* G.

3. *L'application exponentielle est un isomorphisme de* $(\mathbb{R}, +)$ *dans* $(\mathbb{R}^{+*}, \times)$.
4. *L'application logarithme est un isomorphisme de* $(\mathbb{R}^{+*}, \times)$ *dans* $(\mathbb{R}, +)$.

Exercice 1.4.3

Soient G un groupe et $g \in G$.

1. Montrer que l'application $f : \mathbb{Z} \mapsto G$ définie par $f(p) = g^p$ pour tout $p \in \mathbb{Z}$, est un morphisme de groupes.
2. Montrer que l'application $\phi : G \longrightarrow G'$, $x \mapsto gxg^{-1}$ est un automorphisme de G. Le morphisme ϕ est appelé un **automorphisme intérieur**.

Proposition 1.4.4

Pour tout morphisme de groupes $\phi : G \longrightarrow G'$, on a :

1. $\phi(1_G) = 1_{G'}$.
2. Pour tout $p \in \mathbb{Z}$ et tout $x \in G$, $\phi(x^p) = \phi(x)^p$.
   En particulier, $\phi(x^{-1}) = \phi(x)^{-1}$.
3. Pour tout sous-groupe H de G, $\phi(H)$ est un sous-groupe de G'.
   Autrement dit, toute image directe d'un sous-groupe de G est un sous-groupe de G'.
   En particulier, $\mathrm{Im}(\phi)$ est un sous-groupe de G'.
4. Pour tout sous-groupe K de G', $\phi^{-1}(K)$ est un sous-groupe de G.
   Autrement dit, toute image inverse d'un sous-groupe de G' est un sous-groupe de G.

Proposition 1.4.5

1. La composée de deux morphismes de groupes est un morphisme de groupes.
2. L'inverse d'un isomorphisme de groupes est un isomorphisme de groupes.
3. La relation d'isomorphisme de groupes est une relation d'équivalence.

Il est facile de noter qu'un homomorphisme de groupes $f : G \longrightarrow G'$ est surjectif si et seulement si $Im(f) = G'$ (ce qui est en fait vrai pour n'importe quelle application). Nous allons voir que dans le cas des homomorphismes de groupes, l'injectivité est peut être étudiée en utilisant aussi un ensemble particulier défini comme suit.

Définition 1.4.6 (Noyau)

Soit $f : G \longrightarrow G'$ un homomorphisme de groupes. L'ensemble $f^{-1}(\{1_{G'}\})$ est appelé le **noyau** de f et noté $\mathrm{Ker}(f)$.

Proposition 1.4.7

Pour tout homomorphisme de groupes $f : G \longrightarrow G'$, le noyau de f est un sous-groupe de G.

Preuve. Puisque $\{1_{G'}\}$ est un sous-groupe de G', $\mathrm{Ker}(f) = f^{-1}(\{1_{G'}\})$ est un sous-groupe de G (d'après la proposition 1.4.4). **(c.q.f.d)**

Parfois pour montrer qu'une partie d'un groupe est un sous-groupe il suffit de le montrer un noyau d'un homomorphisme de groupes. Par exemple, pour un groupe G, le fait que l'ensemble $Z(G) := \{g \in G | \forall x \in G,\ gx = xg\}$ est un sous-groupe de G (voir Exercice 1.3.11), peut être déduit de la question 2.b de l'exercice 1.4.13.

Le noyau d'un homomorphisme de groupes est une notion très importante. Il permet entre autres à "mesurer" l'injectivité des homomorphisme.

Proposition 1.4.8

Soit $f : G \longrightarrow G'$ un homomorphisme de groupes. Alors, f est injectif si et seulement si $\mathrm{Ker}(f) = \{1_G\}$.

Preuve. $\Rightarrow$. Supposons que f est injectif et montrons que $\mathrm{Ker}(f) = \{1_G\}$. Puisque $\mathrm{Ker}(f)$ est un sous-groupe de G, $\{1_G\} \subset \mathrm{Ker}(f)$. Alors, il reste à montrer l'inclusion inverse. Soit $g \in \mathrm{Ker}(f)$. Alors, $f(g) = 1_{G'}$. Puisque, f est un homomorphisme de groupes, $f(1_G) = 1_{G'}$, en particulier $f(g) = f(1_G)$. Or, f est injectif, donc $g = 1_G$. D'où la deuxième inclusion et par suite le résultat. $\Leftarrow$. On suppose que $\mathrm{Ker}(f) = \{1_G\}$ et on montre que f est injectif. Soit $(a, b) \in G^2$ tel que $f(a) = f(b)$. Alors,

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = 1_{G'}$$

Alors, $ab^{-1} \in \mathrm{Ker}(f) = \{1_G\}$, c'est-à-dire $ab^{-1} = 1_G$, et par suite $a = b$. Cela montre que f est injectif. **(c.q.f.d)**

Remarque 1.4.9

Noter bien que, d'après (1) de la proposition 1.4.4, on a $\{1_G\} \subset \mathrm{Ker}(f)$ *pour tout homomorphisme de groupes* $f : G \longrightarrow G'$. *Ainsi, pour montrer que* f *est injectif, il suffit de montrer l'autre inclusion* $\mathrm{Ker}(f) \subset \{1_G\}$ *; autrement dit, il suffit de montrer l'implication suivante :*

Pour tout $x \in G$, *si* $f(x) = 1_{G'}$, *alors* $x = 1_G$.

En notation additive, l'implication est écrite comme suit :

$$\boxed{\textit{Pour tout } x \in G, \textit{ si } f(x) = 0_{G'}, \textit{ alors } x = 0_G.}$$

Exercice 1.4.10

1. Justifier que $exp : \mathbb{C} \to \mathbb{C}^*$ est un homomorphisme du groupe $(\mathbb{C}, +)$ vers $(\mathbb{C}, \times)$.
2. En déterminer l'image et le noyau.

Exercice 1.4.11

On considère le groupe produit $G = \mathbb{Z}^2$. On définit l'application $f : G \to \mathbb{Z}$ par $f(n, m) = 3n + 2m$.

1. Montrer que f est un homomorphisme de groupes.
2. Déterminer l'image et le noyau de f.

Exercice 1.4.12

On considère le groupe produit $G = \mathbb{Z}^2$ et on définit l'application $g : G \to G$ par $g(n, m) = (2n - m, 3n - m)$.
Montrer que g est un automorphisme.

Exercice 1.4.13

Soit G un groupe. Pour tout $g \in G$, on considère l'application

$$\begin{array}{rccc} I_g : & G & \longrightarrow & G \\ & x & \longmapsto & gxg^{-1} \end{array}$$

1. Montrer que I_g est un automorphisme de G pour tout $g \in G$.
2. On considère l'application

$$\begin{array}{rccc} I : & G & \longrightarrow & Aut(G) \\ & g & \longmapsto & I_g \end{array}$$

   (a) Montrer que I est un homomorphisme de groupes.
   (b) Montrer que $\mathrm{Ker}(I) = \{g \in G | \forall x \in G,\ gx = xg\}$.

Théorème 1.4.14

1. Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.
2. Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Autrement dit, tout groupe monogène est isomorphe à $(\mathbb{Z}, +)$ ou à $(\mathbb{Z}/n\mathbb{Z}, +)$ pour un certain entier n.

Exercice 1.4.15

Soient H et K deux groupes et f un homomorphisme de H dans K. Montrer que pour tout $a \in H$, $f(< a >) =< f(a) >$.

Exercice 1.4.16 (Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$)

On considère l'application surjective $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ (où $n \in \mathbb{N}$) définie par $\pi(k) = \overline{k}$ pour $k \in \mathbb{Z}$.

1. Montrer que π est un homomorphisme de groupes additifs.
2. Déterminer le noyau de π.
3. Montrer que l'image réciproque par π de tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $m\mathbb{Z}$ où m est un entier naturel qui divise n.
4. Déduire que l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ est cyclique de la forme $< \overline{m} >$, où m est un entier naturel qui divise n.

Proposition 1.4.17

Une partie non vide H du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ (où $n \in \mathbb{N}$) est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $H = m\mathbb{Z}$ où m est un entier naturel qui divise n.

Il ne faut pas confondre entre la forme des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ Remarquons que, par exemple, que dans le groupe additif $\mathbb{Z}/6\mathbb{Z}$, on a $< \overline{4} >$ est un sous-groupe de $\mathbb{Z}/6\mathbb{Z}$ bien que 4 ne divise pas 6, mais on sait $< \overline{4} >=< \overline{2} >$ ce qui correspond bien à la proposition 1.4.17.

Exercice 1.4.18

Déterminer les sous-groupes du groupe multiplicatif $\mathbb{U}_n \subset \mathbb{C}$ des racines n-ièmes de l'unité. (Rappellons qu'il est un groupe cyclique engendré par $\omega_1 = e^{\frac{2i\pi}{n}}$).

Chapitre 2

Anneaux et corps

2.1 Définitions et propriétés des anneaux et corps

Définition 2.1.1 (Anneau)

Soit A un ensemble muni des deux lois internes Δ et $*$ (addition et multiplication). Le triplet $(A, \Delta, *)$ (ou simplement A) est dit un **anneau** si les assertions suivantes sont vérifiées :

1. (A, Δ) est un groupe abélien.
2. $(A, *)$ est un monoïde.
3. **Distributivité.** Pour tout $(x, y, z) \in A^3$,

$$\begin{cases} x * (y \Delta z) = (x * y) \Delta (x * z) \\ (x \Delta y) * z = (x * z) \Delta (y * z) \end{cases}$$

On dit que la loi $*$ est distributive par rapport à loi Δ.

Si de plus la loi $*$ est commutative, alors l'anneau A est dit **commutatif**.

On convient souvent de noter la première loi d'un anneau additivement et la deuxème loi multiplicativement. Ainsi, dans la suite, lorsqu'il n'y a pas d'ambiguïté sur les lois, on adopte cette convention. Dans ce cas, l'élément neutre pour la addition sera noté 0_A ou simplement 0 et l'élément neutre pour la multiplication sera noté 1_A ou simplement 1.
Aussi, la distributivité s'écrira simplement comme suit :

$$\begin{cases} x(y+z) = xy + xz \\ (x+y)z = xz + yz \end{cases}$$

Exemple 2.1.2

1. *Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, muni des lois d'addition et de multiplication usuelles, sont des anneaux commutatifs.*
2. *L'ensemble des entiers naturels $\mathbb{N}$ n'est pas un anneau.*

3. *On montre facilement que, pour tout $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$, muni des lois d'addition et de multiplication usuelles, est un anneau commutatif.*
4. *L'ensemble des fonctions réelles (resp., complexes) muni de l'addition et de la multiplication usuelles est un anneau commutatif appelé* ***l'anneau des fonctions réelles*** *(resp.,* ***l'anneau des fonctions complexes****) et noté $(\mathcal{F}(\mathbb{R}), +, \times)$ (resp., $(\mathcal{F}(\mathbb{C}), +, \times)$) ou simplement $\mathcal{F}(\mathbb{R})$ (resp., $(\mathcal{F}(\mathbb{C}))$).*

Remarque 2.1.3

1. *Noter que dans certains cas un anneau A est réduit à un seul élément (jouant à la fois le rôle du 1 et du 0). Dans ce cas, A est dit* ***l'anneau nul****. Par exemple, pour tout entier $n \in \mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'anneau nul si et seulement si $n = 1$.*
2. *Certains auteurs excluent la condition qu'un anneau contient l'élément neutre pour la deuxième loi et les anneaux qui en possèdent sont dits unitaires.*

Proposition et Définition 2.1.4 (Anneau produit des anneaux)

Soit $(A_1, ..., A_n)$ (où $n \in \mathbb{N}^*$) une famille finie d'anneaux. On munit le produit cartésien $A = A_1 \times \cdots \times A_n$ des deux lois des monoïdes produits $(A, +)$ et $(A, \times)$. Alors, muni de ces lois, A est un anneau qui est commutatif si et seulement si A_i est commutatif pour tout $i \in \{1, ...n\}$.
L'anneau $(A, +, \times)$ est appelé **l'anneau produit** des anneaux A_i.

Noter que l'anneau produit $A = A_1 \times \cdots \times A_n$ est nul si et seulement si A_i est nul pour tout $i \in \{1, ...n\}$.

On appelle une **matrice carrée** d'**ordre** $n \in \mathbb{N}^*$ (ou de **taille** n) à **coefficients** dans un anneau non nul A, comme elle est définie dans l'exemple 1.1.10. L'ensemble des matrices carrées d'ordre n à coefficients dans A est aussi notée $\mathcal{M}_n(A)$. Noter que, pour $n = 1$, les matrices de $\mathcal{M}_n(A)$ ne contiennent qu'un seul coefficient. Dans ce cas, $\mathcal{M}_1(A)$ est identifié avec A.

Proposition et Définition 2.1.5 (Anneau des matrices carrées)

Soit A un anneau non nu et $n \geq 2$ un entier naturel. On définit sur $\mathcal{M}_n(A)$ deux lois, l'addition et la multiplication, comme elle sont définies dans l'exemple 1.1.10. Muni de ces deux lois, $\mathcal{M}_n(A)$ est un anneau qui n'est pas commutatif.

Exercice 2.1.6

Montrer que l'ensemble $P(E)$ des parties d'un ensemble E muni de la différence symétrique Δ et de l'intersection est un anneau commutatif (On rappelle que la différence symétrique $A\Delta B$ des deux parties A et B de E est définie par : $A\Delta B := (A\backslash B)\cup(B\backslash A) = (A\cup B)\backslash(A\cap B)$).

Exercice 2.1.7

Soient E un ensemble non vide et A un anneau non nul. On munit l'ensemble $\mathcal{F}(E,A)$ des applications de E dans A des lois d'addition et de multiplication suivantes : Soit $(f;g)\in\mathcal{F}(E,A)^2$.

— L'addition $f+g$ est définie par : $(f+g)(x) = f(x)+g(x)$ pour tout $x\in E$.

— Le produit fg est définie par : $(fg)(x) = f(x)g(x)$ pour tout $x\in E$.

1. Montrer que $(\mathcal{F}(E,A),+,\times)$ est un anneau.
2. Montrer que $\mathcal{F}(E,A)$ est commutatif si et seulement si A est commutatif.

Exercice 2.1.8

On définit deux nouvelles lois $\oplus$ et $\otimes$ sur $\mathbb{R}$ de la manière suivante : $\forall(x,y)\in\mathbb{R}^2$, on pose

$$x\oplus y = x+y-2 \quad \text{et} \quad x\otimes y = xy-2x-2y+6.$$

1. Montrer que $(\mathbb{R},\oplus)$ est un groupe abélien.
2. Montrer que $(\mathbb{R},\oplus,\otimes)$ est un anneau commutatif.

Proposition 2.1.9 (Règles de calcul dans un anneau)

Soit A un anneau.

1. Pour tout $a\in A$, $0\times a = a\times 0 = 0$ (on dit que 0 est un élément absorbant pour la loi $\times$).
2. Pour tout $(a,b)\in A^2$, $(-a)b = -(ab) = a(-b)$.
3. Soit $(a,b,c)\in A^3$. On pose $a-b := a+(-b)$. Alors, $a(b-c) = ab-ac$ et $(b-c)a = ba-ca$.
4. (**Transformation de somme en produit**) Pour tout $(a,b)\in A^2$ et tout $n\mathbb{Z}$, $n(ab) = (na)b = a(nb)$.
   En particulier, $na = (n1_A)a$ et $(nm)a = (n\,1_A)(m\,a)$ pour tout $a\in A$ et tout $(n,m)\in\mathbb{Z}^2$.

Remarque 2.1.10
En utilisant l'assertion (1) *de la proposition précédente, on remarque que si, dans un anneau* A, $1 = 0$, *alors* $A = \{0\}$ *(i.e., A est l'anneau nul).*

Noter bien que, contrairement au cas habituel des nombres entiers (rationnels, réels et complexes), il se peut que le produit de deux éléments non nuls dans un anneau soit nul. Par exemple, dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}\,\overline{3} = \overline{0}$. Aussi, dans un anneau produit de deux anneaux A et B, $(1_A, 0_B)(0_A, 1_B) = (0_A, 0_B)$. Cela donne lieu aux notions de diviseurs de zéro et d'intégrité des anneaux commutatifs définies comme suit :

Définition 2.1.11 (Diviseurs de zéro et anneaux intègres)

Soit A un anneau non nul et commutatif. Un élément x de A est dit un **diviseur de zéro** s'il existe $y \in A$ tel que $y \neq 0$ et $xy = 0$. L'ensemble des diviseur de zéro dans A sera noté $Z(A)$.
Si $Z(A) = \{0\}$, alors A est dit **intègre**.
Autrement dit, A est intègre si, pour tout $(x, y) \in A^2$, $xy = 0$ implique $x = 0$ ou $y = 0$.
Autrement dit, par la contraposée de l'implication précédente, A est intègre si l'ensemble $A^* := A\backslash\{0\}$ est stable pour la multipilication.

Exercice 2.1.12

Soit $n \in \mathbb{N}\backslash\{0, 1\}$. Alors, tout élément $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ et soit inversible soit un diviseur de zéro.

Solution. On peut supposer que $m \in \{0, ..., n-1\}$. Si $\overline{m}$ n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$. Alors, d'après l'exercice 1.1.31, m et n ne sont pas premier entre eux. On pose $d = \text{pgcd}(m, n)$, $m_0 = \dfrac{m}{d}$ et $n_0 = \dfrac{n}{d}$. Alors,

$$\overline{m}\,\overline{n_0} = \overline{m_0 d n_0} = \overline{m_0 n} = \overline{0}$$

Evidement $\overline{n_0} \neq \overline{0}$, alors $\overline{m}$ est bien un diviseur de zéro. **(c.q.f.d)**

Exercice 2.1.13

Montrer que $Z(A)$, l'ensemble des diviseurs de zéro d'un anneau non nul et commutatif A, est stable pour la multiplication mais pas nécessairement pour l'addition.

Définition 2.1.14 (Anneau intègre)

Soit A un anneau non nul et commutatif. L'anneau A est dit **intègre** si $Z(A) = \{0\}$. Autrement dit, si, pour tout $(x, y) \in A^2$, $xy = 0$ implique $x = 0$ ou $y = 0$.

Remarque 2.1.15

Par la contraposée de l'implication précédente, on peut voir qu'un anneau non nul et commutatif A est intègre si l'ensemble $A^* := A\backslash\{0\}$ est stable pour la multipilication.

Exemple 2.1.16

1. *Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, muni des lois d'addition et de multiplication usuelles, sont des anneaux commutatifs et intègres.*
2. *On montre facilement que, pour tout $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$, muni des lois d'addition et de multiplication usuelles, est un anneau intègre si et seulement si n est un nombre premier.*

On a vu dans le chapitre des groupes, que tout élément symétrisable est régulier. Dans les anneaux, l'intégrité d'un anneau suffira pour que tout élément non nul soit régulier.

Proposition 2.1.17

Si A est un anneau intègre, alors tout élément non nul de A est régulier pour la multiplication.

Proposition 2.1.18 (Deux identités remarquables)

Soient a et b deux éléments d'un anneau A. Si a et b commutent (i.e., $ab = ba$), alors, pour tout $n \in \mathbb{N}^*$, on a les deux identités remarquables suivantes :

$$(a+b)^n = \sum_{k=0}^{n} C_n^k \, a^k b^{n-k} \qquad \textbf{(Formule du binôme de Newton)}$$

$$a^n - b^n = (a-b)\Big(\sum_{k=0}^{n-1} a^{n-1-k} b^k\Big).$$

Exercice 2.1.19 (Eléments nilpotents)

Soient $(A, +, \times)$ un anneau commutatif et $a \in A$. On dit que a est nilpotent s'il existe $n \in N^*$ tel que $a^n = 0$. On pose $N(A)$ l'ensemble des éléments nilpotents de A.

1. Déterminer $N(\mathbb{Z})$, $N(\mathbb{Z}/4\mathbb{Z})$ et $N(\mathbb{Z}/63\mathbb{Z})$.
2. Montrer que l'ensemble $N(A)$ est un sous-groupe additif de $(A, +)$.
3. Montrer que, pour tout $a \in A$ et tout $\alpha \in N(A)$, $a\alpha \in N(A)$.

Soit A un anneau. Un élément x de A est dit idempotent s'il vérifie $x^2 = x$. Par exemple, 0 et 1 sont des idempotents (appelés les idempotents triviaux de A). Pour donner un exemple d'un idempotent non trivial, on considère l'anneau produit $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Alors, $(\overline{1}, 0)$ et $(0, \overline{1})$ sont des idempotents non triviaux.

Exercice 2.1.20 (Eléments idempotents I)

1. Déterminer les éléments idempotents de $\mathbb{Z}/6\mathbb{Z}$.
2. En déduire que la somme de deux idempotents n'est pas nécessairement idempotent.
3. Montrer que si e est idempotent alors $1 - e$ est aussi idempotent.

Exercice 2.1.21 (Eléments idempotents II)

Soit A un anneau commutatif.

1. Montrer que le produit de deux idempotents est idempotent.
2. Soient e et f deux idempotents de A. Montrer que $e + f - ef$ est aussi idempotent.
3. On considère $E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $E_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, et $B = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ dans l'anneau des matrices $\mathcal{M}_2(\mathbb{R})$.
   (a) Calculer E_1E_2, E_1B, et $E_1 + B$.
   (b) En déduire que le produit de deux idempotents n'est pas nécessairement idempotent.
4. Déterminer les idempotents de l'anneau des matrices $\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})$.

Définition 2.1.22

Un élément x d'un anneau A est dit **inversible** s'il est inversible pour la loi $\times$ (i.e., s'il existe $y \in A$ tel que $xy = yx = 1$).
L'ensemble des éléments inversibles de A est noté par $U(A)$ (qui est bien un groupe multiplicatif) est appelé le groupe des inversibles (ou parfois, des unités) de A.

Exemple 2.1.23

1. *Pour les anneaux* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *et* $\mathbb{C}$, *on a* $U(\mathbb{Z}) = \{-1; 1\}$, $U(\mathbb{Q}) = \mathbb{Q}^*$, $U(\mathbb{R}) = \mathbb{R}^*$ *et* $U(\mathbb{C}) = \mathbb{C}^*$.
2. *Dans un anneau non nul l'élément* 0 *n'est pas inversible.*

Proposition 2.1.24

Soit $n \in \mathbb{N}$. Alors, $U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{k} | \text{pgcd}(k, n) = 1\}$.

Proposition 2.1.25

On considère l'anneau produit $A \times B$ des deux anneaux A et B. Alors, $U(A \times B) = U(A) \times U(B)$.

Exercice 2.1.26

1. Montrer que les éléments nilpotents d'un anneau non nul ne sont pas inversibles.
2. Montrer que les éléments idempotents non triviaux d'un anneau non nul ne sont pas inversibles.

Exercice 2.1.27 (Suite de l'exercice 2.1.19)

Soit $(A, +, \times)$ un anneau commutatif.

1. Soit $a \in N(A)$. Montrer que $1 - a$ est inversible.
2. Soient $a \in N(A)$ et $b \in U(A)$. Montrer que $a + b$ est inversible.

Exercice 2.1.28

Soit A un anneau commutatif non nul. On pose $B = A \times A$. On munit B des lois suivantes : pour tout $((x,e),(y,f)) \in B^2$, on pose

$$\begin{cases} (x,e)+(y,f) = (x+y, e+f) \\ (x,e)(y,f) = (xy, xf+ey) \end{cases}$$

1. Montrer que B est un anneau commutatif.
2. Montrer que B n'est pas intègre.
3. Déterminer l'ensemble des éléments inversibles de B.
4. Soient $(x,e) \in B$ et $n \in \mathbb{N}^*$. Montrer que $(x,e)^n = (x^n, na^{n-1}e)$.
5. Déduire que $N(B) = N(A) \times A$ où $N(A)$ (resp., $N(B)$) est l'ensemble des élément nilpotents de A (resp., de B).

Définition 2.1.29 (Corps)

Un anneau commutatif et non nul K est dit un **corps** si tout élément non nul de K est inversible (i.e., $A^* = U(A)$).

Exemple 2.1.30

1. *L'anneau $\mathbb{Z}$ n'est pas un corps.*
2. *Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.*
3. *Pour tout $n \in \mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

De la définition on déduit facilement la caractérisation suivante des corps.

Proposition 2.1.31

Un ensemble K muni des deux lois internes $+$ et $\times$ est un corps si et seulement s'il satisfait les trois assertions suivantes :

1. $(K,+)$ est un groupe abéliens.
2. $(K^*,\times)$ est un groupe abéliens.
3. la loi $\times$ est distributive par rapport à $+$.

Corollaire 2.1.32

Tout corps est un anneau intègre.

Exercice 2.1.33

Montrer que tout anneau intègre, commutatif et fini est un corps.

Exercice 2.1.34

Soient $n \in \mathbb{Z}$ et A un anneau commutatif non nul. On définit sur A les deux lois suivantes : pour tous (a_1, a_2) et (b_1, b_2) dans A, on pose

$$\begin{cases} (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \\ (a_1, a_2)(b_1, b_2) = (a_1 b_1 + n a_2 b_2, a_1 b_2 + a_2 b_1) \end{cases}$$

Déterminer selon les valeurs de n la structure de A muni de ces deux lois (i.e., $(A, +, \times)$ est-t-il un anneau (un corps) ?).

Exercice 2.1.35 (Suite de l'exercice 2.1.7)

On uilise les notations de l'exercice 2.1.7. Soit $f \in \mathcal{F}(E, A)$ non nulle.

1. Montrer que f est inversible dans $\mathcal{F}(E, A)$ si, et seulement si, pour tout $x \in E$, $f(x)$ est inversible dans A.
2. Montrer que f est un diviseur de zéro si, et seulement si, il existe $x \in E$ tel que $f(x) = 0_A$.
3. L'anneau $\mathcal{F}(E, A)$ est-il intègre ? Est-ce un corps ?

2.2 Sous-anneaux et sous-corps

Définition 2.2.1 (Sous-anneau)

1. Une partie B non vide d'un anneau A est dit un **sous-anneau** de A si les assertions suivantes sont vérifiées :
   (a) B est stable pour les deux lois $+$ et $\times$.
   (b) $(B, +, \times)$ est un anneau.
   (c) $1_A \in B$ (i.e., $1_B = 1_A$).

Définition 2.2.2 (Sous-corps)

Uun sous-anneau K' d'un corps K est dit un **sous-corps** de K si, pour tout $x \in K' \backslash \{0\}$, $x^{-1} \in K'$ (i.e., $(K', +, \times)$ est un corps).

Exemple 2.2.3

1. *$\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ (et ainsi de $\mathbb{R}$ et de $\mathbb{C}$).*
2. *$\mathbb{Q}$ est un sous-corps du corps $\mathbb{R}$.*
3. *$\mathbb{R}$ est un sous-corps du corps $\mathbb{C}$.*
4. *Pour tout anneau A, l'ensemble $B := \{k.1_A | k \in \mathbb{Z}\}$ est un sous-anneau de A. C'est pour cette raison, s'il n'y a pas d'ambiguïté, qu'on convient parfois de représenter l'élément $k.1_A$ simplement par k. Par exemple :*
   (a) *Dans l'anneau des fonctions réelles $(\mathcal{F}(\mathbb{R}), +, \times)$, la fonction constante $1_{\mathcal{F}(\mathbb{R})} : x \mapsto 1$ est l'élément neutre pour la multiplication. Donc, $\{k.1_{\mathcal{F}(\mathbb{R})} | k \in \mathbb{Z}\}$ est exactement l'ensemble des fonctions constantes. Ainsi, souvent on note simplement $k.1_{\mathcal{F}(\mathbb{R})}$ par k pour tout $k \in \mathbb{Z}$. En fait, il est connu qu'on peut définir une multiplication (externe), λf, d'une fonction réelle f par un scalaire (i.e., réel) λ rcomme suit : $(\lambda f)(x) = \lambda f(x)$ (pour tout $x \in \mathbb{R}$). Il est claire que l'ensemble $\{\lambda 1_{\mathcal{F}(\mathbb{R})} | \lambda \in \mathbb{R}\}$ est l'ensemble de toutes les fonctions constantes. Souvent, s'il n'y a pas d'ambiguïté, la fonction $\lambda 1_{\mathcal{F}(\mathbb{R})}$ est simplement notée λ. On peut voir aussi que l'ensemble des fonctions constante, muni des lois induites de l'addition et de la multiplication usuelles des fonctions réelles, est un corps et c'est aussi un sous-anneau de $(\mathcal{F}(\mathbb{R}), +, \times)$.*
   (b) *Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ (où $n \in \mathbb{N}$), on convient de représenter une calsse par un de ces représentants, souvent l'entier compris entre 0 et $n-1$. On convient donc d'écrire, dans $\mathbb{Z}/6\mathbb{Z}$, $2.5 = 10 = 4$.*
5. *On considère l'anneau produit $A \times B$ des deux anneaux non nuls A et B. Alors, $A \times \{0\}$ muni des lois induites de celle de $A \times B$ est un anneau d'élément neutre $(1_A, 0)$. Cependant, il n'est pas un sous-anneau de $A \times B$, car $1_{A\times B} \neq 1_{A\times\{0\}}$.*

Proposition 2.2.4

Une partie B non vide d'un anneau A est un sous-anneau de A si et seulement si les assertions suivantes sont vérifiées :

1. $(B, +)$ est un sous-groupe de $(A, +)$,
2. B est stable pour la loi $\times$.
3. $1_A \in B$.

Exercice 2.2.5 (Suite des exercices 2.1.7 et 2.1.35)

On uilise les notations de l'exercice 2.1.7. Soit B un sous-anneau de A. Montrer que l'ensemble C des fonctions $F : E \to B$ est un sous-anneau de $\mathcal{F}(E, A)$.

Exercice 2.2.6

Soit $a \in \mathbb{N}$ avec $\sqrt{a} \notin \mathbb{Q}$. Montrer que l'ensemble $\mathbb{Z}[i\sqrt{a}] := \{x + i\sqrt{a}y | (x, y) \in \mathbb{Z}^2\}$ est le plus petit sous-anneau de $\mathbb{C}$, au sens de l'inclusion, contenant $\mathbb{Z}$ et $i\sqrt{a}$.

Exercice 2.2.7

On considère l'ensemble

$$Rot_2(\mathbb{R}) := \{\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \in \mathcal{M}_2(\mathbb{R});\ \alpha^2 + \beta^2 = 1\}$$

1. Montrer que $Rot_2(\mathbb{R})$, muni de la multiplication des matrices, est un groupe.
2. Rot_2 est-il un groupe commutatif ?
3. Pourquoi $Rot_2(\mathbb{R})$ n'est-il pas un sous-anneau de $\mathcal{M}_2(\mathbb{R})$?

Remarque 2.2.8
Soit K une partie stable pour l'addition et la multiplication d'un anneau A. Pour montrer que K, muni des lois induites, est un corps, il suffit de montrer les assertions suivantes :

1. *K est un sous-anneau de A,*
2. *le monoïde $(K, \times)$ est commutatif (autrement dit, K est un sous-anneau commutatif de A), et*
3. *tout élément non nul de K est inversible (autrement dit, le monoïde $(K\backslash\{0_A\}, \times)$ est un groupe ou aussi $U(K) = K\backslash\{0_A\}$).*

Exercice 2.2.9

On considère les matrices $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Soit l'ensemble $K = \{aI_2 + bJ; a, b \in \mathbb{R}\}$.

1. Calculer J^2. En déduire que K est stable dans $(\mathcal{M}_2(\mathbb{R}), \times)$.
2. Montrer que $(K, +, \times)$ est un corps

Exercice 2.2.10

On appelle centre d'un anneau $(A, +, \times)$ l'ensemble $C(A) := \{x \in A; \forall y \in A, xy = yx\}$.

1. Montrer que $C(A)$ est un sous-anneau de A.
2. On considère $A = C(\mathcal{M}_2(\mathbb{R}))$, l'anneau des matrices carrées de taille 2.
   (a) Déterminer l'ensemble des matrices dans $C(\mathcal{M}_2(\mathbb{R}))$ qui commutent avec la matrice $J = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.
   (b) Déterminer l'ensemble des matrices dans $C(\mathcal{M}_2(\mathbb{R}))$ qui commutent avec la matrice $K = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
   (c) Déterminer l'ensemble des matrices dans $C(\mathcal{M}_2(\mathbb{R}))$ qui commutent avec la matrice $K = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
   (d) En déduire $C(\mathcal{M}_2(\mathbb{R}))$.
   (e) Déduire que $C(\mathcal{M}_2(\mathbb{R}))$ est un corps.

2.3 Idéaux d'un anneau commutatif

Définition 2.3.1 (Idéal d'un anneau)

Soit A un anneau commutatif. Une partie non vide I de A est dit un **idéal** de A si les assertions suivantes sont vérifiées :

1. I est un sous-groupe additif de A.
2. Pour tout $a \in A$ et tout $x \in I$, $ax \in I$.

Exemple 2.3.2

1. *Tout anneau commutatif non nul A contient au moins deux idéaux, l'idéal nul $0 := \{0\}$ et A. Ces deux idéaux sont appelés les idéaux triviaux de A. Les idéaux qui sont inclus strictement dans A sont dit **propre**.*
2. *On sait que les sous-groupes additifs de $\mathbb{Z}$ sont tous de la forme $n\mathbb{Z}$ ($n \in \mathbb{N}$). Donc, si I est un idéal de $\mathbb{Z}$, alors, en tant qu'un sous-groupe du groupe additif $(\mathbb{Z}, +)$, il est de la forme $n\mathbb{Z}$ pour certain entier n. Et puisque, pour tout élément $k \in \mathbb{Z}$ et tout élément $a \in n\mathbb{Z}$, évidement ka reste dans $n\mathbb{Z}$, on conclut que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Par suite, les "$n\mathbb{Z}$" sont les seuls idéaux de l'anneau $\mathbb{Z}$.*
3. *On a vu, d'après l'exercice 1.3.24, que $K = \{(12k, 12k); k \in \mathbb{Z}\}$. est*

un sous-groupe du groupe produit $\mathbb{Z}^2$. Mais, on peut montrer qu'il n'est pas un idéal de l'anneau produit $\mathbb{Z}^2$.

4. *D'après l'exercice 2.1.19, l'ensemble $N(A)$ des éléments nilpotents d'un anneau commutatif A est un idéal de A.*

Proposition 2.3.3 (Caractérisation des idéaux)

Une partie I non vide d'un anneau commutatif A est un idéal de A si et seulement si les assertions suivantes sont vérifiées :

1. I est stable pour la loi $+$.
2. Pour tout $a \in A$ et tout $x \in I$, $ax \in I$.

Preuve. Il suffit de vérifier l ?implication inverse. Et pour cela, seule la stabilité par passage à l'opposé qui reste à vérifier. Donc, considère $a \in I$. On a $-a = (-1_A).a$ (voir Proposition 2.1.9). Cela montre que $-a \in I$. Ainsi, I est bien un idéal. **(c.q.f.d)**

Exercice 2.3.4

On considère l'anneau produit $A \times B$ des deux anneaux A et B. Montrer qu'une partie I de $A \times B$ est un idéal de $A \times B$ si et seulement s'il existe deux idéaux J et K de A et B, respectivement, tels que $I = J \times K$.

Exercice 2.3.5 (Suite des exercices 2.1.7, 2.1.35 et 2.2.5)

On uilise les notations de l'exercice 2.1.7. Soit I un idéal de A. Montrer que l'ensemble J des fonctions $f : E \to I$ est un idéal de $\mathcal{F}(E, A)$.

Maintenant, on introduit l'analogue de la notion des sous-groupes monogènes (voir Théorème 1.3.20) dans le contexte des idéaux.

Théorème et Définition 2.3.6 (Idéal principal)

Soit a un élément d'un anneau commutatif A. Toute partie de A de la forme $\{\alpha a | \alpha \in A\}$ est un idéal de A, appelé l'idéal **principal** de A **engendré** par a et noté aA. On dit aussi que a est un **générateur** de l'idéal aA.
En plus, pour tout idéal J de A, si $a \in J$, alors $aA \subset J$. on dit que aA est le plus petit idéal de A, au sens de l'inclusion, contenant a.

Preuve. On pose $K = \{\alpha a | \alpha \in A\}$. Montrons que K est un idéal de A. Il claire que K est non vide. En effet, $0 = 0 \times a \in K$. Considère maintenant deux élément $x = ab$ et $y = ac$ de K, où $b, c \in \mathbb{A}$. Alors,

$$x + y = ab + ac = a(b + c).$$

D'où, $x + y \in K$.
Aussi, si on considère $x = ab \in K$ avec $b \in \mathbb{A}$, alors pour tout $c \in A$, $cx = c(ab) = a(cb) \in K$. Par suite, d'après la proposition 2.3.3, K est un idéal de A.
Enfin, il est claire que si un idéal J de A contient a, alors, $ab \in J$ pour tout $b \in A$. D'où, $aA \subset J$. **(c.q.f.d)**

Exemple 2.3.7

1. *Tout idéal de $\mathbb{Z}$ est principal (d'après (2) de l'exemple 2.3.2).*
2. *En utilisant l'exercice 1.4.18, on montre facilement que tout idéal de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (où $n \geq 2$) est principal de la forme $\overline{m}(\mathbb{Z}/n\mathbb{Z})$, où m est un entier naturel qui divise n.*

Proposition 2.3.8

Soit a un élément d'un anneau commutatif A. Alors, pour tout élément inversible u dans A, $(ua)A = aA$. Autrement dit, l'idéal principal engendré par ua est le même l'idéal principal engendré par a.

Preuve. Il suffit d'applique le théorème 2.3.6 en remarquant que $ua \in aA$, alors $(ua)A \subset aA$. Et aussi que $a = (ua)u^{-1}$ et alors $a \in (ua)A$. Ce qui implique d'après, le théorème 2.3.6, que $aA \subset (ua)A$. **(c.q.f.d)**

Exemple 2.3.9

1. *Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z} = (-n)\mathbb{Z}$.*
2. *Dans l'anneau $\mathbb{Z}/12\mathbb{Z}$, $\overline{5}$ est inversible et on a $\overline{5}\,\overline{4} = \overline{8}$, alors $\overline{5}(\mathbb{Z}/12\mathbb{Z}) = \overline{8}(\mathbb{Z}/12\mathbb{Z})$. On peut remarquer aussi $\overline{8} = -\overline{5}$ et c'est claire que $\overline{5}(\mathbb{Z}/12\mathbb{Z}) = -\overline{5}(\mathbb{Z}/12\mathbb{Z})$.*

Exercice 2.3.10 (Suite de l'exercice 2.3.4)

On considère l'anneau produit $A \times B$ des deux anneaux A et B.

1. On pose $A = B = \mathbb{Z}$.
   (a) Déterminer les idéaux de $\mathbb{Z}^2$.
   (b) Est-ce que les idéaux de $\mathbb{Z}^2$ sont tous principaux ?
2. On pose $A = \mathbb{Z}$ et $B = \mathbb{Q}$.
   (a) Déterminer les idéaux de $\mathbb{Z} \times \mathbb{Q}$.
   (b) Est-ce que les idéaux de $\mathbb{Z} \times \mathbb{Q}$ sont tous principaux ?

Solution. 1.a. Soit I un idéal de $\mathbb{Z}^2$. Alors, d'après l'exercice 2.3.4, il existe deux idéaux J et K de $\mathbb{Z}$ tels que $I = J \times K$. Alors, d'après Exemples 2.3.2, il existent $n, m \in \mathbb{N}$ tels que $J = n\mathbb{Z}$ et $K = m\mathbb{Z}$. Ainsi, $I = n\mathbb{Z} \times m\mathbb{Z}$.
1.b. Les idéaux de $\mathbb{Z}^2$ sont tous principaux. Notamment, on montre que $n\mathbb{Z} \times m\mathbb{Z} = (n, m)(\mathbb{Z}^2)$. En effet, il est claire que $(n, m) \in n\mathbb{Z} \times m\mathbb{Z}$, d'où $(n, m)(\mathbb{Z}^2) \subset n\mathbb{Z} \times m\mathbb{Z}$ (d'après l le théorème 2.3.6). Pour l'inclusion inverse, on considère $(na, mb) \in n\mathbb{Z} \times m\mathbb{Z}$ (avec $(a, b) \in \mathbb{Z} \times \mathbb{Z}$). On a $(na, mb) = (a, b)(n, m)$. D'où $(na, mb) \in (n, m)(\mathbb{Z}^2)$ ce qui doone la deuxième inclusion.
2.a. Soit I un idéal de $\mathbb{Z}^2$. Alors, d'après l'exercice 2.3.4, il existe deux idéaux J et K de $\mathbb{Z}$ tels que $I = J \times K$. Alors, d'après Exemples 2.3.2, il existent $n \in \mathbb{N}$ tels que $J = n\mathbb{Z}$. Et puisque $\mathbb{Q}$ est un corps, $K = \{0\}$ soit $K = \mathbb{Q}$. Ainsi, $I = n\mathbb{Z} \times \{0\}$ ou $I = n\mathbb{Z} \times \mathbb{Q}$.
1.b. Comme dans le cas de l'anneau $\mathbb{Z}^2$, les idéaux de $\mathbb{Z} \times \mathbb{Q}$ sont aussi tous principaux. Notamment, on montre que, comme pour $(1.b.)$, $n\mathbb{Z} \times \{0\} = (n, 0)(\mathbb{Z} \times \mathbb{Q})$ et $n\mathbb{Z} \times \mathbb{Q} = (n, 1)(\mathbb{Z} \times \mathbb{Q})$. **(c.q.f.d)**

Remarque 2.3.11
Soit a un élément d'un anneau commutatif A. On remarque que le sous-groupe monogène $< a >$ de $(A, +)$ est inclus dans l'idéal principal aA de A engendré par a (i.e., $< a > \subset aA$). En effet, on sait que, pour tout $k \in \mathbb{Z}$, $ka = (k.1_A).a$, ce qui implique que $ka \in aA$. Il faut noter que dans le cas où $A = \mathbb{Z}$, évidemment $< a >= aA$, mais en général, l'inclusion $< a > \subset aA$ est stricte. Par exemple, pour $A = \mathbb{Z} \times \mathbb{Z}$, le sous-groupe monogène de $(\mathbb{Z} \times \mathbb{Z}, +)$ engendré par $(2, 3)$ est de la forme :

$$< (2, 3) >= \{k(2, 3); k \in \mathbb{Z}\} = \{(2k, 3k); k \in \mathbb{Z}\}.$$

Mais l'idéal de $\mathbb{Z} \times \mathbb{Z}$ engendré par $(2, 3)$ est de la forme :

$$(2, 3)(\mathbb{Z} \times \mathbb{Z}) = \{(2, 3)(h, k); (h, k) \in \mathbb{Z} \times \mathbb{Z}\} = \{(2h, 3k); (h, k) \in \mathbb{Z} \times \mathbb{Z}\}.$$

Il faut aussi noter que l'idéal $(2, 3)(\mathbb{Z} \times \mathbb{Z})$ est un produit cartésien, cependant le sous-groupe $< (2, 3) >$ ne l'est pas.

Définition 2.3.12 (Anneau principal)

Un anneau intègre A est dit principal si tout idéal de A est **principal**.

Exemple 2.3.13
1. *L'anneau $\mathbb{Z}$ est principal.*
2. *Rappelons que, pour un entier $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ est intègre (et donc un corps) si et seulement si n est premier. Donc, si n n'est premier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal bien que tous ces idéaux sont principaux.*

Exercice 2.3.14 (Anneau des entiers de Gauss)

On pose $\mathbb{Z}[i] = \{a + bi \in \mathbb{C}; a, b \in Z\}$.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
2. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
3. Soient $u, v \in \mathbb{Z}[i]$ avec $v \neq 0$. Montrer qu'il existe $q, r \in \mathbb{Z}[i]$ tels que $u = qv + r$ et $|r| < |v|$. A-t-on unicité ?
4. Montrer que $\mathbb{Z}[i]$ est un anneau principal.

Exercice 2.3.15

Soit A un sous-anneau non nul du corps $\mathbb{Q}$.

1. Montrer que A contient $\mathbb{Z}$.
2. Soit I un idéal de A. Montrer que $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$.
3. Soit $x = \frac{p}{q}$ un élément d'un idéal I de A, où p et q sont deux entier relatifs premier entre eux et $q \neq 0$.
   (a) Montrer que $\frac{k}{q} \in A$ pour tout $k \in \mathbb{Z}$. (vous pouvez utiliser l'égalité de Bezout)
   (b) En déduire que, si I un idéal principal de A engendré par $\frac{p}{q}$, alors il engendré simplement par p (i.e., $I = pA$).
4. En déduire que A est un anneau principal.

Exercice 2.3.16

On pose $\mathbb{Z}_p := \{\frac{a}{b} | a \in \mathbb{Z}; b \in \mathbb{N}^* \text{ } et \text{ } p \text{ ne divise pas } b\}$, où $p \in \mathbb{N}$ est un nombre premier.

1. Montrer que $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}$.
2. Montrer que, pour tout élément $x \in \mathbb{Q}^*$, on a soit $x \in \mathbb{Z}_p$, soit $x^{-1} \in \mathbb{Z}_p$.
3. Montrer que $U_p = \{\frac{a}{b} | a \in \mathbb{Z}; b \in \mathbb{N}^* \text{ } et \text{ } p \text{ ne divise ni } a \text{ ni } b\}$ où U_p désigne l'ensemble des éléments inversibles de $\mathbb{Z}_p$.
4. On pose $M_p = \{\frac{a}{b} | a \in \mathbb{Z}; b \in \mathbb{N}^* \text{ } et \text{ } p \text{ divise } a \text{ mais ne divise pas } b\}$. Montrer que M_p est un idéal principal de $\mathbb{Z}_p$ engendré par p.
5. Montrer que tout idéal propre de $\mathbb{Z}_p$ (i.e. idéal différent de $\mathbb{Z}_p$) est inclus dans M_p.
   Indication : vous pouvez utiliser le fait qu'un idéal contenant un élément inversible coïncide avec l'anneau.

On va montrer qu'un corps n'a que les idéaux triviaux. En fait, la deuxième propriété dans la définition d'un idéal montre que contrairement au sous-anneaux, les idéaux propres d'un anneau ne doivent pas contenir l'identité. En général nous avons le résultat suivant :

Proposition 2.3.17

Si un idéal I d'un anneau commutatif A contient un élément inversible, alors $I = A$.

Preuve. Soit $u \in I$ un élément inversible dans A. Alors, pour tout $a \in A$, $ua \in I$ car I est un idéal de A et $u \in I$. Alors, de même $a = u^{-1}(ua) \in I$. D'où, $A \subset I$ et par suite $I = A$. **(c.q.f.d)**

Corollaire 2.3.18

Un anneau commutatif A est un corps si et seulement si A ne possède que les idéaux triviaux.

Preuve. $\Rightarrow$. Si A est un corps, alors tout élément non nul est inversible. Donc, si I est un idéal non nul, donc il contient un élément non nul qui est donc inversible. Donc, d'après la proposition 2.3.17, $I = A$.
$\Leftarrow$. Supposons que A ne possède que les idéaux triviaux. Soit a un élément non nul de A. On montre que a est inversible. En effet, considère l'idéal principal aA. Il est non nul (car $a \in aA$), donc par hypothèse $aA = A$. En particulier, $1 \in aA$. Cela veut dire qu'il existe $b \in A$ tel que $1 = ab$ et par suite a est inversible dans A. **(c.q.f.d)**

On termine cette partie par deux résultats sur les opérations sur les idéaux dans un anneau commutatif.

Proposition 2.3.19

L'intersection d'une famille quelconque d'idéaux d'un anneau commutatif A est un idéal de A.

Exercice 2.3.20

Soit a un élément d'un anneau commutatif A. Montrer que l'idéal principal aA est l'intersection de tous les idéaux de A contenant a.

Exercice 2.3.21

Soit a un élément d'un anneau commutatif A. Montrer que a est nilpotent si et seulement si l'interection de tous les idéaux de la forme a^nA (avec $n \in \mathbb{N}$) est non nul.

Soit $(I_1, ..., I_n)$, où $n \in \mathbb{N}^*$, une famille finie d'idéaux d'un anneau commutatif A. On définit l'ensemble $I_1 + \cdots + I_n$, la **somme des idéaux** $I_1, ..., I_n$, comme suit :

$$I_1 + \cdots + I_n := \{a_1 + \cdots + a_n | a_i \in I_i \text{ pour tout } 1 \leq i \leq n\}.$$

Proposition 2.3.22

La somme d'une famille finie d'idéaux d'un anneau commutatif A est un idéal de A.

Il est claire que $I_1 + \cdots + I_n$ contient tous les idéaux $I_1, ..., I_n$. Ainsi, $\cup I_i \subset I_1 + \cdots + I_n$. En fait, on peut montrer que $I_1 + \cdots + I_n$ est le plus petit idéal, au sens de l'inclusion, contenant tous les idéaux $I_1, ..., I_n$.

Proposition 2.3.23

Soit $(I_1, ..., I_n)$, où $n \in \mathbb{N}^*$, une famille finie d'idéaux d'un anneau commutatif A.

1. Soit K un idéal de A contenant tous les les idéaux $I_1, ..., I_n$ (i.e., $\cup I_i \subset K$). Montrer que $I_1 + \cdots + I_n \subset K$.
2. En déduire que $I_1 + \cdots + I_n$ est l'intersection de tous les idéaux contenant $\cup I_i$.

Exercice 2.3.24

Soit I et J deux idéaux d'un anneau commutatif A.

1. Montrer que $I + J = I$ si et seulement si $J \subset I$.
2. Soit K un idéal tel que $I \subset K \subset I + J$. Montrer que $K = I + (K \cap J)$.
3. Donner un contre exemple montrant que si on ne suppose pas que $I \subset K \subset I + J$, alors le résultat précédent tombe en défaut.

Exercice 2.3.25

Soient a et b deux éléments d'un anneau commutatif A.

1. Montrer que l'intersection de tous les idéaux de la forme A contenant a et b est exactement l'idéal $aA + bA$.
2. Généraliser ce dernier résultat.

Exercice 2.3.26

On considère l'anneau produit $A = (\mathbb{Z}/2\mathbb{Z})^3$. Montrer que la somme de toute famille finie d'idéaux de A est principal.

2.4 Morphismes d'anneaux

Définition 2.4.1

Soient A et B deux anneaux. Une application $f : A \longrightarrow B$ est dite un **morphisme ou homomorphisme d'anneaux**, si les assertions suivantes sont vérifiées :

1. $f(1_A) = 1_B$.
2. Pour tout $(x, y) \in A^2$, $f(x + y) = f(x) + f(y)$.
3. Pour tout $(x, y) \in A^2$, $f(xy) = f(x)f(y)$.

Notation et vocabulaire.
Soit $\phi : A \longrightarrow B$ un morphisme d'anneaux.

— L'ensemble $\phi(A)$ est appelé l'**image** de ϕ et il sera noté $\mathrm{Im}(\phi)$.
— Si $A = B$, alors le morphisme ϕ est appelé **endomorphisme** de A.
— Si ϕ est bijectif, il sera appelé un **isomorphisme** d'anneaux. Dans ce cas, on dit que A et B sont **isomorphes** et on écrit $A \cong B$.
— Si $A = B$ et ϕ est un isomorphisme, alors ϕ est appelé un **automorphisme** de A.

Exemple 2.4.2

1. *Soit B un sous-anneau d'un anneau A. La restriction de l'application identité Id_A à B est un homomorphisme injectif d'anneaux appelé l'**injection canonique** de B dans A.*
2. *Soit A un anneau. L'application*

$$\begin{array}{rccc} \pi : & \mathbb{Z} & \longrightarrow & A \\ & k & \longmapsto & k1_A \end{array}$$

est un homomorphisme d'anneaux. En particulier, si $A = \mathbb{Z}/n\mathbb{Z}$ (où

$n \in \mathbb{N}$), alors π est appelé la ***surjection canonique*** *de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

3. *Soient A et B deux anneaux non nuls. Alors, l'application $\theta : A \to B$ définie par $\theta(a) = 0_B$ (pour tout $a \in A$) est un homomorphisme de groupes additifs, mais ce n'est pas un homomorphisme d'anneaux car $\theta(1_A) = 0_B \neq 1_B$.*

Remarque 2.4.3
Par définition, un homomorphisme d'anneaux $f : A \longrightarrow A'$ est un homomorphisme du groupe additif $(A, +)$ dans le groupe additif $(A', +)$. Ainsi, f possède, en particulier toutes les propriétés d'un morphisme de groupes abéliens. Par exemple, pour montrer que f est injectif, on montre simplement $\mathrm{Ker}(f) = \{0\}$. *Pour montrer que f est surjectif, on montre* $\mathrm{Im}(f) = A'$. *Aussi, pour tout $x \in A$ et tout $n \in \mathbb{Z}$, $f(nx) = nf(x)$. En particulier, $f(0_A) = 0_{A'}$ et $f(-x) = -f(x)$.*

Proposition 2.4.4

Soit $f : A \longrightarrow A'$ un morphisme d'anneaux commutatifs.

1. Pour tout $x \in A$ et tout $n \in \mathbb{N}$, $f(x^n) = f(x)^n$.
2. Si x est un élément inversible dans A, alors $f(x)$ est inversible dans A' et on a $f(x^{-1}) = f(x)^{-1}$. Ainsi, $f(x^n) = f(x)^n$ pour tout $n \in \mathbb{Z}$.
3. L'image directe d'un sous-anneau de A est un sous-anneau de A'. En particulier, l'image de f, $\mathrm{Im}(f)$, est un sous-anneau de A'.
4. L'image réciproque d'un sous-anneau de A' est un sous-anneau de A.
5. Si f est surjectif, alors l'image directe d'un idéal de A est un idéal de A'.
6. L'image réciproque d'un idéal de A' est un idéal de A. En particulier, $\mathrm{Ker}(f)$ est un idéal de A.
7. Si f est un isomorphisme, alors f^{-1} est aussi un isomorphisme d'anneaux.

Preuve. 1. Par récurrence sur n.
2. C'est claire, car $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_A) = 1'_A$.
Alors, si $n < 0$, alors $f(x^n) = f((x^{-n})^{-1}) = f(x^{-n})^{-1}$. Et d'après l'assertion 1, $f(x^{-n}) = f(x)^{-n}$, d'où le résultat.
Les assertions (3) et (4) sont
5. Soit I un idéal de A'. Alors, $f(I)$ est un sous-groupe de $(A', +)$ (d'après la proposition 1.4.4). Soient $b \in f(I)$ et $y \in A'$. Alors, il existe $a \in I$ tel que $b = f(a)$, et puisque, f est surjectif, il existe $x \in A$ tel que $y = f(x)$. Alors, $by = f(a)f(x) = f(ax)$. Puisque $a \in I$ et I un idéal de A, $ax \in I$. D'où, $f(ax) \in f(I)$. Par suite, $f(I)$ est un idéal de A'.
6. Soit J un idéal de A. Alors, $f^{-1}(J)$ est un sous-groupe de $(A, +)$ (d'après

la proposition 1.4.4). Soient $a \in f^{-1}(J)$ et $x \in A$. Alors, $f(a) \in J$. Puisque J est un idéal de A', $f(a)f(x) \in J$, c'est-à-dire $f(ax) \in J$. Donc, $ax \in f^{-1}(J)$ et par suite $f^{-1}(J)$ est un idéal de A.
7. Facile à montrer. **(c.q.f.d)**

Remarque 2.4.5

1. *En utilisant (1) de la proposition 2.4.4, on peut montrer facilement que l'image d'un élément nilpotent (resp. idempotent) est aussi nilpotent (resp. idempotent).*
2. *En général, l'image directe d'un idéal par un homomorphisme d'anneaux n'est pas nécessairement un idéal. Par exemple, si on considère i l'injection canonique de $\mathbb{Z}$ dans $\mathbb{Q}$. Alors, l'image de l'idéal $\mathbb{Z}$ de l'anneau $\mathbb{Z}$ par i est $\mathbb{Z}$ lui même, mais il n'est pas un idéal du corps $\mathbb{Q}$.*
3. *Il faut noter qu'on peut définire deux structures (i.e., anneaux) sur le même ensemble qui ne sont pas isomorphes. Par exemple, si on considère l'anneau $B = A \times A$ défini dans l'exercice 2.1.28 et on pose $A = \mathbb{Z}/2\mathbb{Z}$, alors B n'est pas isomorphe à l'anneau produit $T = (\mathbb{Z}/2\mathbb{Z})^2$. En effet, B contient un élément nilpotent non nul (voir $(\overline{0}, \overline{1})^2 = (\overline{0}, \overline{0})$), cependant on peut voir facilement que, dans T, seul l'élément nul est nilpotent. Alors, si $f : T \to B$ est un homomorphisme d'anneaux, alors $f(\overline{0}, \overline{1})$ est nilpotent dans B, d'où $f(\overline{0}, \overline{1}) = (\overline{0}, \overline{0})$. Donc, f n'est pas injectif et en particulier n'est pas bijectif.*

Corollaire 2.4.6

Soit K un corps et A un anneau commutatif non nul.

1. Tout homomorphisme $f : K \longrightarrow A$ est injectif.
2. Si A et K sont isomorphes, alors A est un corps.

Preuve. 1. Puisque $f : K \longrightarrow A$ est un homomorphisme d'anneaux, le noyau $\mathrm{Ker}(f)$ de f est un idéal de K. Or K est un corps, donc $\mathrm{Ker}(f)$ est trivial (d'après le corollaire 2.3.18). Si on suppose que $\mathrm{Ker}(f) = K$, alors en particulier $f(1_K) = 0_A \neq 1_A$, absurde. Alors, $\mathrm{Ker}(f)$ est l'idéal nul et ainsi f est injectif.
2. Découle de l'assertion 2 de la proposition 2.4.4. **(c.q.f.d)**

Exercice 2.4.7

Soit $(A, +, \times)$ un anneau. On définit deux lois $\oplus$ et $\otimes$ sur A de la manière suivante : pour tout $(a, b) \in A$, on pose

$$\begin{cases} a \oplus b = a + b + 1 \\ a \otimes b = ab + a + b \end{cases}$$

1. Montrer que $(A, \oplus, N)$ est un anneau.
2. Montrer que l'application $f : (A, +, \times) \to (A, \oplus, \otimes)$ définie par $f(a) = a - 1$ est un isomorphisme d'anneaux.
3. Résoudre dans $(\mathbb{C}, \oplus, \otimes)$ l'équation $X^{\otimes 3} = 1$.

Exercice 2.4.8

1. Soit $(A_1, ..., A_n)$ (où $n \in \mathbb{N}^*$) une famille finie d'anneaux non nuls. On considère $A = A_1 \times \cdots \times A_n$ l'anneau produit des anneaux A_i. Pour tout $i \in \{1, ..., n\}$, on considère les deux applications :

$$f_i : \begin{array}{ccc} A & \longrightarrow & A_i \\ (x_j)_j & \longmapsto & x_i \end{array} \quad \text{et} \quad g_i : \begin{array}{ccc} A_i & \longrightarrow & A \\ x & \longmapsto & (\delta_{i,j}x)_j \end{array}$$

   où $\delta_{i,j}$ est le symbole de kronecker qui vaut 1 si $i = j$ et 0 sinon (i.e., $(\delta_{i,j}x)_j$ est l'élément de A dont toutes les composantes sont nules sauf la i-ième qui vaut x).

   (a) Montrer que, pour tout $i \in \{1, ..., n\}$, l'application f_i est un homomorphisme d'anneaux. Elle est appelée la projection de A dans A_i.

   (b) Montrer que, pour tout $i \in \{1, ..., n\}$, l'application g_i est un homomorphisme de groupes additifs mais pas des homomorphismes d'anneaux.

2. Montrer que les projections de $\mathbb{Z}^n$ dans $\mathbb{Z}$ sont les seuls homomorphismes d'anneaux de $\mathbb{Z}^n$ dans $\mathbb{Z}$.

Exercice 2.4.9 (Anneau des endomorphismes)

Soit G un groupe additif et commutatif. On considère $(E(G), +, \circ)$ l'ensemble des endomorphismes de G muni de l'addition usuelles et de la composition.

1. Montrer que $(E(G), +, \circ)$ est un anneau.
2. On prend $G = \mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}$.
   (a) Montrer que A est l'ensemble des applications de la forme f_a : $x \mapsto xa$ pour certain $a \in G$.
   (b) En déduire que A est isomorphe à l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Dans la définition suivante on considère, on considère le morphisme d'anneaux commutatifs $f : \mathbb{Z} \to A$ défini par : $f(k) = k.1_A$ (pour tout $k \in \mathbb{Z}$). Alors, le noyau $\mathrm{Ker}(f)$ de f est un idéal de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$ pour certain $d \in \mathbb{N}$. Ainsi,

$$\mathrm{Ker}(f) = d\mathbb{Z} = \{k \in Z;\ k.1_A = 0\}.$$

Dans la théorie des anneaux commutatifs, la nature de cet entier d a une grande influence sur l'étude de plusieur propriétés et notions liées à l'anneau.

Définition 2.4.10 (Caractéristique d'un anneau)

Soit A un anneau commutatif. L'entier $d \in \mathbb{N}$ tel que $\mathrm{Ker}(f) = d\mathbb{Z}$ est appelé la **caractéristique** de l'anneau A et on écrit $car(A) = d$.

En général, on distingue les deux cas suivants :

1. L'homomorphisme f est injectif, ce qui veut dire que $d = 0$. On dit que l'anneau A est de caractéristique nul et on écrit $car(A) = 0$.
2. L'homomorphisme f n'est pas injectif, ce qui veut dire que $d \neq 0$. Dans ce cas, tout multiple de d annule 1_0. Notamment, on a le résultat suivant :

Proposition 2.4.11

Soit A un anneau commutatif de caractéristique d.

1. Pour tout $x \in A$, $dx = 0$. En général, $nx = 0$ pour tout n multiple de d.
2. Soit un entier $n \in \mathbb{N}$. Alors, $n.1_A = 0$ si et seulement si d divise n.
3. $d \neq 0$ si et seulement s'il existe un entier $k \neq 0$ tel que $k.1_A = 0$.
4. Si $d \neq 0$, alors d est le plus petit entier naturel non nul k vérifiant $k1_A = 0$.

Preuve. 1. Noter simplement que $dx = (d.1_A)x$ (d'après (4) de la proposition 2.1.9). Puisque, $car(A) = d$, $d.1_A = 0_A$ et par suite, $dx = 0$. Alors, si n est un multiple de d ; c'est-à-dire, $n = kd$ (pour $k \in \mathbb{Z}$). Alors, d'après (4) de la proposition 2.1.9, $nx = (kd)x = k(dx) = k.0 = 0$
2. C'est trivial, car : $n.1_A = 0$ si et seulement si $n \in \text{Ker}(f) = d\mathbb{Z}$ si et seulement si d divise n.
3. L'implication directe est évidente car on prend $k = d$.
Réciproquement, s'il existe un entier $k \neq 0$ tel que $k.1_A = 0$. Cela veut dire que le noyau de $f : \mathbb{Z} \to A$ défini par $f(k) = k.1_A$ (pour tout $k \in \mathbb{Z}$) n'est pas injectif. Donc, l'idéal $\text{Ker}(f) = d\mathbb{Z}$ est non nul. Et par suite, $d \neq 0$.
4. C'est trivial, d'après ce qui précède. **(c.q.f.d)**

La caractéristique d'un anneau commutatif nous donne également des informations sur l'anneau.

Proposition 2.4.12

Soit A un anneau commutatif.

1. Si $car(A) = 0$, alors A est infini.
2. Si $car(A) = d$ avec $d \in \mathbb{N}^*$, alors $\overline{f} : \mathbb{Z}/d\mathbb{Z} \to A$ définie par $f(\overline{k}) = k.1_A$ (pour tout $k \in \mathbb{Z}$) est un homomorphisme injectif d'anneaux.

Preuve. 1. Si $car(A) = 0$, alors par définition, l'homomorphisme $f : \mathbb{Z} \to A$ défini par $f(k) = k.1_A$ (pour tout $k \in \mathbb{Z}$) est injectif. D'où, $\mathbb{Z}$ et $f(\mathbb{Z})$ sont isomorphes. En particulier, $f(\mathbb{Z})$ est infini. Donc, A contient une partie infini et alors il est infini aussi.
2. Il faut d'abord montrer que $\overline{f}$ est une application bien définie. Soit donc $a, b \in \mathbb{Z}$ tels que $\overline{a} = \overline{b}$. Alors, $b - a = kn$ pour certain $k \in \mathbb{Z}$. Alors,

$$\overline{f}(\overline{b}) - \overline{f}(\overline{a}) = b.1_A - a.1_A = (b-a).1_A = (kn).1_A = k(n.1_A) = k.0_A = 0_A$$

D'où, $\overline{f}(\overline{b}) = \overline{f}(\overline{a})$, ce qui montre que $\overline{f}$ est une application bien définie.
Il est facile de montrer que $\overline{f}$ est un homomorphisme d'anneaux. Il reste à montrer qu'il est injectif. Soit $a \in \mathbb{Z}$ tel que $\overline{f}(\overline{b}) = 0_A$. Alors, $a.1_A = 0_A$. **(c.q.f.d)**

Il existe des anneaux infinis mais de caractéristique non nul.

Exercice 2.4.13 (Anneau infini de caractéristique non nul)

Soit A un anneau commutatif non nul. On pose B l'ensemble des suites à termes dans A. On note simplement (a_n) un élément $(a_n)_{n\in\mathbb{N}}$ de B. On munit B des lois suivantes : pour tout $((a_n),(b_n)) \in B^2$

$$\begin{cases} (a_n)+(b_n) = (a_n+b_n) \\ (a_n)(b_n) = (a_n b_n) \end{cases}$$

1. Montrer que B, muni de ces deux lois, est un anneau commutatif avec 0_B est la suite nulle et 1_B est la suite constante dont tous les termes égale à 1_A.
2. Montrer que, pour tout $(a_n) \in B$ et tout $k \in \mathbb{N}$, $k\,(a_n) = (k\,a_n)$.
3. Montrer que A et B ont la même caractéristique.

Preuve. 1. Preuve similaire au cas d'un anneau produit.
2. Par récurrence sur n.
3. Pour tout $k \in \mathbb{N}$, les équivalences suivantes sont vraies :

$$k.1_B = 0_B \Leftrightarrow (k\,1_A) = (0_A) \Leftrightarrow k.1_A = 0_A.$$

Donc, si $car(B) = d$, alors $d.1_B = 0_B$. Donc, $d.1_A = 0_A$. Ce qui emplique que $car(A)$ divise $d = car(B)$. De même on montre $car(B)$ divise $car(A)$ et puisque la caractéristique d'un anneau commutatif est un entier naturel, $car(B) = car(A)$. **(c.q.f.d)**

Exercice 2.4.14

Soient D un anneu intègre et a un élément non nul de D. Montrer que si $na = 0$ pour certain entier naturel non nul n, alors D est de caractéristique non nulle.

Solution. Simplement, on $na = (n.1_A)a$. Alors, si $na = 0$, de même $(n.1_A)a = 0$. Or $a \neq 0$ et A est intègre, alors $n.1_A = 0$. Donc, d'après la proposition 2.4.11, la caractéristique de D est non nulle. **(c.q.f.d)**

Proposition 2.4.15

La caractéristique d'un anneau commutatif et intègre est soit nulle soit un nombre premier.

Preuve. Soit A un anneau commutatif et intègre de caractéristique d. On suppose que $d \neq 0$. S'il n'est pas premier, alors il existe deux entier $0 < a < d$

et $0 < b < d$ tels que $d = ab$. Alors, puisque $d1_A = 0$, $(ab)1_A = 0$. Et comme $(ab)1_A = (a1_A)(b1_A)$, on déduit que $(a1_A)(b1_A) = 0$. Puisque A est intègre, $a1_A = 0$ ou $b1_A = 0$. Cela est absurde car , d'après la proposition 2.4.11, d est le plus petit entier naturel non nul k vérifiant $k1_A = 0$. **(c.q.f.d)**

Exercice 2.4.16 (Endomorphisme de Frobenius)

Soit A un anneau commutatif de caractéristique un nombre premier p. Soit $F_A : A \longrightarrow A$ l'application définie par $F_A(x) = x^p$ (pour tout $x \in A$).

1. Montrer que F_A est un homomorphisme d'anneaux. Il est appelé **l'endomorphisme de Frobenius**.
2. Déterminer F_A quand $A = \mathbb{Z}/p\mathbb{Z}$.
3. On munit $K = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ des lois suivantes : pour tout $((x, e), (y, f)) \in K^2$, on pose

$$\begin{cases} (x, e) + (y, f) = (x + y, e + f) \\ (x, e)(y, f) = (xy + ef, xf + ey + ef) \end{cases}$$

   (a) Montrer que K, muni de ces deux lois, est un anneau commutatif avec $0_K = (\overline{0}, \overline{0})$ et $1_K = (\overline{1}, \overline{0})$.

   (b) Dresser la table de multiplication dans K. En déduire que K est un corps.

   (c) Déterminer la caractéristique de K.

   (d) Déterminer F_K.

Preuve. 1. On a bien $F_A(1) = 1^p = 1$.
Soient a et b deux éléments de A. Alors, $f(ab) = (ab)^p = a^p b^p$ (car $ab = ba$). D'où, $f(ab) = f(a)f(b)$.
On a aussi

$$\begin{aligned} F_A(a + b) &= (a + b)^p \\ &= \sum_{k=0}^{p} C_p^k \, b^k a^{p-k} \qquad \text{(Formule du binôme de Newton)} \\ &= a^p + \sum_{k=1}^{p-1} C_p^k \, b^k a^{p-k} + b^p. \end{aligned}$$

Puisque p est premier, $p \in C_p^k$ pour tout $k \in \{1, ..., p - 1\}$. Donc, puisque $car(A) = p$, $C_p^k \, b^k a^{p-k} = 0_A$ (d'après (1) de la proposition 2.4.11). Alors, $F_A(a + b) = a^p + b^p = F_A(a) + F_A(b)$.
Par suite, F_A est un endomorphisme de A. **(c.q.f.d)**

Problème 2.4.17
On munit $T = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ des lois suivantes : pour tout $((x,\overline{e}),(y,\overline{f})) \in T^2$, on pose

$$\begin{cases} (x,\overline{e}) + (y,\overline{f}) = (x+y, \overline{e}+\overline{f}) \\ (x,\overline{e})(y,\overline{f}) = (xy, x\overline{e} + y\overline{f}) \end{cases}$$

On considère les deux applications $f : \mathbb{Z} \to T$ et $g : T \to \mathbb{Z}$ définies par $f(a) = (a,0)$ $(\forall a \in \mathbb{Z})$ et $g(x,\overline{e}) = x$ $(\forall (x,\overline{e}) \in T)$.

1. *Montrer que T, muni de ces deux lois, est un anneau commutatif.*
2. *Montrer que f est un homomorphisme injectif d'anneaux.*
3. *Montrer que g est un homomorphisme surjectif d'anneaux.*
4. *Déterminer $Ker(g)$.*
5. *En déduire que $\{0\} \times \mathbb{Z}/2\mathbb{Z}$ est un idéal de T.*
6. *Soit $n \in \mathbb{N}$.*
   (a) *Montrer que $2n\mathbb{Z} \times \{0\}$ est un idéal principal de T.*
   (b) *Montrer que $n\mathbb{Z} \times \{0\}$ est un idéal de T si et seulement si n est pair.*
   (c) *Montrer que $n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un idéal principal de T.*
   (d) *Montrer que $\{(2a,\overline{a}) \in Z \times \mathbb{Z}/2\mathbb{Z}; a \in \mathbb{Z}\}$ est un idéal principal de T qui n'est pas un produit cartésien.*
7. *Déterminer la caractéristique de T.*

2.5 Construction de corps usuels

Dans cette partie, nous allons présenter la construction des corps usuels $\mathbb{C}$ et $\mathbb{Q}$. Commençons d'abord par la remarque importante suivante :

Remarque 2.5.1
*Si $f : A \longrightarrow A'$ est un morphisme d'anneaux injectif, alors A est isomorphe à $f(A)$. Ainsi, on convient d'**identifier** A à $f(A)$ et, pour tout $x \in A$, $f(a)$ sera noté simplement a.*
*On dit qu'on **a injecté** A **dans** A' (via l'homomorphisme f) ou A est **injecté** (ou plongé) dans A'. On dit aussi que A' est une **extension** de A.*

On donne ci-dessous, deux exemples d'extensions classiques. Commençons par la construction de $\mathbb{C}$ et l'injection de corps des réels $\mathbb{R}$ dans $\mathbb{C}$.

Théorème et Définition 2.5.2

On munit $\mathbb{R}^2$ des deux lois suivantes : pour tous (a_1,a_2) et (b_1,b_2) dans $\mathbb{R}^2$,

$$\begin{cases} (a_1,a_2) + (b_1,b_2) = (a_1+b_1, a_2+b_2) \\ (a_1,a_2)(b_1,b_2) = (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1) \end{cases}$$

Muni de ces deux loi, $\mathbb{R}^2$ est un corps d'élément neutre pour la multiplication $(1,0)$. Il sera noté $\mathbb{C}$ et appelé **corps des nombres complexes.**

Noter que, avec la loi $+$, $\mathbb{C}$ n'est que le groupe produit additif d'élément neutre $(0,0)$.
Noter aussi que, pour tout $(x,y) \in \mathbb{R}^2$, $(x,0)(y,0) = (xy,0)$. D'où le résultat suivant :

Proposition 2.5.3

L'application $i_{rc} : \mathbb{R} \to \mathbb{C}\,; x \mapsto (x,0)$ est un homomorphisme de corps injectif.

Par conséquent, on convient d'identifier x à $(x,0)$ pour tout $x \in \mathbb{R}$.
Remarquons aussi que, pour tout $(x,y) \in \mathbb{C}$, $(0,y) = (0,1)(y,0)$. Ainsi, en notant $(0,1)$ par i, tout nombre complexe $(x,y) \in \mathbb{C}$ aura l'écriture simplifiée suivante :

$$\begin{aligned}(x,y) &= (x,0) + (0,y)\\ &= (x,0) + (0,1)(y,0)\\ &= x + iy\end{aligned}$$

Cette expression est appelée **l'écriture algèbrique** du nombre complexe (x,y).

Exercice 2.5.4

Soit $n \geq 2$ un entier naturel et on pose $A = (\mathbb{Z}/n\mathbb{Z})^2$. On définit sur A les deux lois suivantes (similaires à celles de $\mathbb{C}$) : pour tous (a_1,a_2) et (b_1,b_2) dans A,

$$\begin{cases}(a_1,a_2)+(b_1,b_2) = (a_1+b_1, a_2+b_2)\\ (a_1,a_2)(b_1,b_2) = (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1)\end{cases}$$

Déterminer la structure de A muni de ces deux lois (i.e., $(A,+,\times)$ est-t-il un anneau (un corps) ?).

Il est claire que $\mathbb{Q} = \{ab^{-1} \in \mathbb{R} | (a,b) \in (\mathbb{Z}^2)^*\}$. Cette relation entre $\mathbb{Z}$ et $\mathbb{Q}$ en tant que sous-anneaux de $\mathbb{R}$ peut être étendre de la manière suivante.

Proposition et Définition 2.5.5

Soit A un sous-anneau d'un corps K. Alors, l'ensemble $k = \{ab^{-1} | (a,b) \in A \times A^*\}$ est un sous-corps de K. C'est le plus petit sous-corps de K, au sens de l'inclusion, contenant A. On l'appelle le **corps des fractions** de A et noté par $Frac(A)$.

Il est à noter qu'il existe une construction plus générale (et abstraite) du corps des fractions de tout anneau intègre. Cependant, cette construction dépasse les limites de ce cours.

Exemple 2.5.6

1. *Le corps $\mathbb{Q}$ est le corps des fractions de l'anneau $\mathbb{Z}$.*
2. *Le corps des fractions de n'importe quel corps est lui même.*

Exercice 2.5.7

Le corps des fractions de l'anneau des entiers de Gauss $\mathbb{Z}[i]$ est l'ensemble $\mathbb{Q}[i] = \{x + iy | (x, y) \in \mathbb{Q}^2\}$. Ainsi, $\mathbb{Q}[i]$ est un sous-corps de $\mathbb{C}$.

Solution. Le corps des fractions de $\mathbb{Z}[i]$ est par définition

$$Frac(\mathbb{Z}[i]) = \{ab^{-1} | (a, b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*\}.$$

Montrons que $Frac(\mathbb{Z}[i]) = \mathbb{Q}[i]$.
Si $Z \in Frac(\mathbb{Z}[i])$, alors il existe $(X, Y) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*$ tel que $Z = XY^{-1}$. Puisque $(X, Y) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*$, il existe $(a, b, c, d)) \in \mathbb{Z}^4$ tel que $X = a + ib$ et $Y = x + iy$. D'autre part, $x^2 + y^2 \neq 0$, car sinon $x = y = 0$ et ainsi $Y = x + iy = 0$, ce qui est absurde. Alors,

$$\begin{aligned} Z &= \frac{a + ib}{x + iy} = \frac{(a + ib)(x - iy)}{x^2 + y^2} \\ &= \frac{(ax + by) + i(-ay + bx)}{x^2 + y^2} \\ &= \frac{ax + by}{x^2 + y^2} + i\frac{-ay + bx}{x^2 + y^2} \end{aligned}$$

Il est claire que $\dfrac{ax + by}{x^2 + y^2}$ et $\dfrac{-ay + bx}{x^2 + y^2}$ sont des nombres rationnels. D'où $Z \in \mathbb{Q}[i]$. Cela montre la première inclusion $Frac(\mathbb{Z}[i]) \subset \mathbb{Q}[i]$. Pour l'inclusion inverse, on considère un élément $x + iy \in \mathbb{Q}[i]$. Alors, $x = \dfrac{p}{q}$ et $x = \dfrac{p'}{q'}$ pour certains $p, q, p', q' \in \mathbb{Z}$ avec $q \neq 0$ et $q' \neq 0$. Alors,

$$x + iy = \frac{p}{q} + i\frac{p'}{q'} = \frac{pq' + iqp'}{qq'} = (pq' + iqp')(qq')^{-1}$$

Il est claire que $pq' + iqp' \in \mathbb{Q}[i]$ et de même $qq' \in \mathbb{Q}[i]$ (car $p, q, p', q' \in \mathbb{Z}$). Alors, $x + iy \in Frac(\mathbb{Z}[i])$. Cela montre l'inclusion inverse et par suite donne le résultat. **(c.q.f.d)**

Problème 2.5.8
Soit $a \in \mathbb{N}$. On pose $\mathbb{Z}[\sqrt{a}] = \{x + y\sqrt{a} | (x, y) \in \mathbb{Z}^2\}$ et $\mathbb{Q}[\sqrt{a}] = \{x + y\sqrt{a} | (x, y) \in \mathbb{Q}^2\}$.

1. *Montrer que si $\sqrt{a} \in \mathbb{Q}$, alors $\mathbb{Z}[\sqrt{a}] = \mathbb{Z}$ et $\mathbb{Q}[\sqrt{a}] = \mathbb{Q}$. dans la suite, on suppose que $\sqrt{a} \notin \mathbb{Q}$.*

2. *Démontrer que, dans l'écriture $z = x + y\sqrt{a}$ d'un élément $z \in \mathbb{Z}[\sqrt{a}]$ (avec $(x, y) \in \mathbb{Z}^2$), les entiers x et y sont uniques.*
3. *Montrer que $\mathbb{Z} \subset \mathbb{Z}[\sqrt{a}]$ et $\mathbb{Q} \subset \mathbb{Q}[\sqrt{a}]$.*
4. *Montrer que $\mathbb{Z}[\sqrt{a}]$ est stable dans $(\mathbb{R}, \times)$.*
5. *Montrer que $\mathbb{Z}[\sqrt{a}]$ est un sous-groupe de $(\mathbb{R}, +)$.*
6. *Montrer que $\mathbb{Z}[\sqrt{a}]$, muni des deux lois induites de l'addition et de la multiplication, est un anneau commutatif.*
7. *Montrer que $\mathbb{Q}[\sqrt{a}]$ est le corps des fractions de l'anneau $\mathbb{Z}[\sqrt{a}]$.*
8. *Montrer que $\mathbb{Q}[\sqrt{a}]$ est le plus petit sous-corps de $\mathbb{R}$, au sens de l'inclusion, contenant $\mathbb{Z}$ et $\sqrt{a}$.*
9. ***Les éléments inversibles de** $\mathbb{Z}[\sqrt{\mathbf{a}}]$. Pour tout $z = x + y\sqrt{a} \in \mathbb{Z}[\sqrt{a}]$, on pose : $\overline{z} = x - y\sqrt{a}$.*
   - 9.1 *Montrer que l'application $\phi : \mathbb{Z}[\sqrt{a}] \to \mathbb{Z}[\sqrt{a}]$ telle que $\phi(z) = \overline{z}$ est un automorphisme de l'anneau $\mathbb{Z}[\sqrt{a}]$*
   - 9.2 *Pour tout $z \in \mathbb{Z}[\sqrt{a}]$, on pose : $N(z) = z\overline{z}$. Montrer que $N(zz') = N(z)N(z')$ pour tout z et z' de $\mathbb{Z}[\sqrt{a}]$.*
   - 9.3 *En déduire qu'un élément $z \in \mathbb{Z}[\sqrt{a}]$ est inversible dans $\mathbb{Z}[\sqrt{a}]$ si et seulment si $N(z) = 1$ ou $N(z) = -1$.*

Chapitre 3

Fonctions polynomiales et fractions rationnelles

3.1 Anneau des fonctions polynomiales

Dans ce chapitre $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

Définition 3.1.1 (Fonctions polynomiales)

Soient $n \in \mathbb{N}$ et $\{a_0, ..., a_n\}$ une ensemble d'éléments de $\mathbb{K}$. Toute application de la forme

$$\begin{aligned} P : \quad \mathbb{K} &\longrightarrow \mathbb{K} \\ x &\longmapsto \sum_{k=0}^{n} a_k x^k \end{aligned}$$

sera appelée une **fonction polynomiale** (ou simplement un polynôme) à coefficients dans $\mathbb{K}$.

Notation.

1. On note un polynôme $P : x \mapsto \sum_{k=0}^{n} a_k x^k$ simplement par $\sum_{k=0}^{n} a_k x^k$ et on écrit $P = \sum_{k=0}^{n} a_k x^k$. Des fois, il est pratique d'écrire simplement $P = \sum a_k x^k$. Cependant, quand on utilise cette dernière notation, on doit comprendre que la suite $(a_k)_{k\in\mathbb{N}}$ s'annule à partir d'un certain rang[1] (i.e., il existe $n \in \mathbb{N}$ tel que $a_k = 0$ pour tout $k \geq n$).
2. L'ensemble de polynômes à coefficients dans $\mathbb{K}$ sera noté $\mathbb{K}[x]$.

1. A ne pas confondre : si nous disons que $(a_k)_{k\in\mathbb{N}}$ s'annulle à partir d'un rang $n \in \mathbb{N}$, cela ne veut pas dire qu'elle ne l'est pas avant n. Dans certains cas, on s'intéresse au plus petit entier k tel que $a_k = 0$. Dans ce cas, nous parlons de la notion du degré d'un polynôme que nous introduirons par la suite.

Vocabulaire.
Soit $P = \sum a_k x^k$ un polynôme.

— Le coefficient a_k est appelé le **k-ième coefficient de** P. En particulier, a_0 est appelé le **coefficient constant** (ou le **terme constant**) de P. Il est claire que $P(0) = a_0$.
— Un terme $a_k x^k$ est appelé un **monôme de degré** k.
— Si tous les coefficients a_k, pour $k \geq 1$, sont nuls, alors P est dit un **polynôme constant**. On écrit simplement, $P = a_0$. Si, en plus, a_0 est aussi nul, alors P est dit un **polynôme nul** et noté 0.
— Si $\mathbb{K} = \mathbb{R}$, P est dit un **polynôme réel** et si $\mathbb{K} = \mathbb{C}$, P est dit un **polynôme complexe**.

Dans cette partie, on s'interesse en premier lieu à présenter quelques propriétés principales de l'ensemble de polynômes à coefficients dans $\mathbb{K}$.

Notation. L'ensemble de polynômes à coefficients dans $\mathbb{K}$ sera noté $\mathbb{K}[x]$.

Rappellons que $\mathcal{F}(\mathbb{K})$, l'ensemble des fonctions de $\mathbb{K}$ dans $\mathbb{K}$, muni des deux lois usulles est un anneau (voir Exercice 2.1.7). On montre facilement que $\mathbb{K}[x]$ est stable pour l'addition et la multiplication dans $\mathcal{F}(\mathbb{K})$. En effet, considère deux polynômes $P = \sum a_k x^k \in \mathbb{K}[x]$, et $Q = \sum b_k x^k \in \mathbb{K}[x]$. Alors, la somme de P et Q est un polynôme de la forme :

$$P + Q = \sum (a_k + b_k) x^k$$

Il est claire que si (a_k) et (b_k) s'annulent à partir des entiers n et m respectivement, alors $(a_k + b_k)$ s'annule forcement à partir de $\max(n, m)$.
Pour déterminer le produit de P et Q, il est claire qu'en utilisant la distributivité, qu'il est une somme de monômes de la forme $a_i b_j x^{i+j}$. Alors, le produit PQ est aussi un polynôme. Après qu'on réduit le polynôme PQ sous sa forme canonique, on obtient :

$$PQ = \sum c_k x^k \quad \textit{tel que} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

En particulier, $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, ...
Il est claire que si (a_k) et (b_k) s'annulent à partir des entiers n et m respectivement, alors (c_k) s'annule forcement à partir de $n + m$. Notamment, si $n \neq 0$ et $m \neq 0$, alors $c_{n+m-2} = a_{n-1} b_{m-1}$.

Théorème 3.1.2

L'ensemble des fonctions polynomiales $\mathbb{K}[x]$, muni des deux lois induites de l'addition et de la multiplication des fonctions est un anneau commutatif.

Preuve. Il suffit de noter que l'opposé d'un polynôme $P = \sum a_k x^k \in \mathbb{K}[x]$ est aussi un polynôme. Notamment, $-P = \sum -a_k x^k \in \mathbb{K}[x]$. Aussi, il est évident que la fonction constante 1, l'identité pour la multiplication dans $\mathcal{F}(\mathbb{K})$, est aussi un polynôme dans $\mathbb{K}[x]$. Par suite, $\mathbb{K}[x]$ est un sous-anneau de $\mathcal{F}(\mathbb{K})$. **(c.q.f.d)**

Produit externe sur $\mathbb{K}[x]$.
Il est aussi claire de voir que le produit d'un polynôme par un scalaire est un polynôme. Précisément, on a : $\forall \lambda \in \mathbb{K}, \forall\, P = \sum a_k x^k \in \mathbb{K}[x]$,

$$\lambda P = \lambda \sum a_k x^k = \sum \lambda a_k x^k.$$

On a aussi les propriétés suivantes :
$\forall x, y \in \mathbb{K}, \forall P, Q \in \mathbb{K}[x]$,

$$\begin{cases} x(P+Q) = xP + xQ \\ (x+y)P = xP + yP \end{cases} \quad \begin{cases} x(PQ) = (xP)Q = P(xQ) \\ (xy)P = x(yP) \end{cases}$$

Il est claire qu'un un polynôme $P = \sum a_k x^k$ est nul si et seulement si $a_n = 0$ pour tout $n \in \mathbb{N}$. En général, on a le "principe d'identification des coefficients" suivant :

Proposition 3.1.3 (Principe d'identification des coefficients)

Deux polynômes $P = \sum a_k x^k$ et $Q = \sum b_k x^k$ sont égaux si et seulement si $a_n = b_n$ pour tout $n \in \mathbb{N}$.

Preuve. Remarquer que $P - Q = \sum (a_k - b_k) x^k$. **(c.q.f.d)**

Définition 3.1.4 (Degré d'un polynôme)

Soit $P = \sum a_k x^k$ un polynôme dans $\mathbb{K}[x]$. Si P est non nul, l'entier $d = \max\{n \in \mathbb{N} | a_n \neq 0\}$ est appelé le **degré** de P et noté $\deg(P)$.

Convention, notation et vocabulaire.
- Si d est le degré d'un polynôme non nul P, alors le coefficient a_d est appelé le **coefficient dominant** de P. Si en plus, $a_d = 1$, P est dit un polynôme **unitaire**.
- On convient d'étendre la relation d'ordre usuelle à $\overline{\mathbb{R}}_- = \mathbb{R} \cup \{-\infty\}$ de sorte que $-\infty < n$ pour tout entier $n \in \mathbb{N}$ et $-\infty \leq -\infty$.
- Par convention, **le degré du polynôme nul vaut** $-\infty$.
- L'ensemble de polynômes de degré au plus un entier n sera noté $\mathbb{K}_n[x]$. En particulier, $\mathbb{K}_0[x]$, est l'ensemble des polynômes constants.

D'après la discussion sur la forme de la somme de deux polynômes (voir le paragraphe précédant le théorème 3.1.2), on obtient facilement le résultat suivant qui determine le degré d'une somme de deux polynômes.

Proposition 3.1.5

Soient P et Q deux polynômes dans $\mathbb{K}[x]$.

$$\deg(P+Q) \leq \max(\deg(P), \deg(Q)).$$

En particulier,

1. Si $\deg(P) \neq \deg(Q)$, alors $\deg(P+Q) = \max(\deg(P)\ ,\ \deg(Q))$.
2. Si $\deg(P) = \deg(Q)$, alors $\deg(P+Q) = \deg(Q)$ si et seulement si les coefficients dominants de P et Q ne sont pas opposés.

Aussi, d'après la discussion sur la forme du produit de deux polynômes, on obtient le résultat suivant :

Lemme 3.1.6

Si P et Q deux polynômes non nuls, alors le coefficient dominant de PQ est le produit des coefficients dominants de P et de Q.

Par conséquent, on obtient le résultat important suivant :

Proposition 3.1.7

Si P et Q deux polynômes non nuls, alors

$$\deg(PQ) = \deg(P) + \deg(Q).$$

Il faut noter que l'anneau $\mathcal{F}(\mathbb{K})$ n'est pas intègre. En fait, on peut construire facilement deux fonctions (même (réelles) continues) non nulles avec un produit nul. Cependant, en utilisant le lemme 3.1.6, on déduit le résultat suivant :

Corollaire 3.1.8

L'anneau $\mathbb{K}[x]$ est intègre.

La proposition 3.1.7 nous permet de déterminer les éléments inversibles de $\mathbb{K}[x]$.

Corollaire 3.1.9

Les éléments inversibles de $\mathbb{K}[x]$ sont les polynômes constants non nuls.

Preuve. Il est claire que tout polynôme constant $\lambda \neq 0$ est inversible d'inverse le polynôme constant $\frac{1}{\lambda}$.
Réciproquement, si P est inversible, alors il existe un polynôme Q tel que $PQ = 1$. Alors, $\deg(P) + \deg(Q) = \deg(1) = 0$. Alors, $\deg(P) = \deg(Q) = 0$. Ce qui veut dire que P est un polynôme constant. **(c.q.f.d)**

Rappelons que la dérivée d'un polynôme $P = \sum a_k x^k$ est aussi un polynôme. Notamment, le **polynôme dérivé** est : $P' = \sum k a_k x^{k-1}$. On notera également P'' le polynôme dérivé de P', et $P^{(n)}$ le polynôme dérivé n fois du polynôme P.

Proposition 3.1.10

Soit P un polynôme dans $\mathbb{K}[x]$ et soit n un entier naturel non nul. Si $\deg(P) \geq n$, alors $\deg(P^{(n)}) = \deg(P) - n$.
Par conséquent, $P \in \mathbb{K}_n[x]$ si et seulement si $P^{(n+1)} = 0$.
En particulier, P est un polynôme constant si et seulement si son polynôme dérivé P' est nul (i.e., $P' = 0$).

Preuve. La preuve se fait par réccurence sur n. **(c.q.f.d)**

Nous allons voir le long de ce chapitre que l'anneau de polynômes et l'anneau des entiers relatifs partagent plusieurs proprités. En fait, nous allons montrer que l'anneau de polynômes est doté d'une division euclidienne qui lui confère une structure similaire à celles de $\mathbb{Z}$. Présisèment, la division euclidienne permet de montrer que l'anneau de polynôme est principal. En général, en théorie des anneaux commutatifs, l'étude des anneaux principaux s'inspire principalement des propriétés de l'anneau $\mathbb{Z}$.

Théorème et Définition 3.1.11 (Division euclidienne)

Pour tout $A \in \mathbb{K}[x]$ et tout $B \in \mathbb{K}[x]\backslash\{0\}$, il existe un unique couple $(Q, R) \in \mathbb{K}[x]^2$ tel que

$$A = QB + R \quad \text{et} \quad (R = 0 \quad \text{ou} \quad 0 \leq \deg(R) < \deg(B)).$$

— Le polynôme Q (resp., R) est appelé le **quotient** (resp., le **reste**) de la division euclidienne de A par B.
— Le polynôme A (resp., B) est appelé le **dividende** (resp., le **diviseur**) de la division euclidienne de A par B.

Preuve. On note que $\deg(B) \neq -\infty$ car $B \neq 0$. Posons $m = \deg(B) \in \mathbb{N}$. Alors, $B = \sum_{k=0}^{m} b_k x^k$ pour cetains $b_i \in \mathbb{K}$ avec $b_m \neq 0$.
- Si $\deg(A) < m$, on pose $Q = 0$ et $R = A$. On obtient $A = BQ + R$ avec $\deg(R) < \deg(B)$.
- Si $m = 0$ (B est une constante non nulle). Posons $B = b_0$. Alors, $A = QB+R$ où $Q = \frac{1}{b_0}A$ et $R = 0$.
- Maintenant, on suppose que $m > 1$.
Montrons par récurrence que : $\forall n > m$, si $\deg(A) \leq n$, alors il existe $(Q, R) \in \mathbb{K}[x]^2$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$.

— Soit A est un polynôme de degré m (le cas où $\deg(A) < m$ a été discuté avant). Posons $A = \sum_{k=0}^{m} a_k x^k$ puis $Q = \frac{a_m}{b_m}$ (Q est un polynôme de degré 0) et $R = A - BQ$. Alors,

$$R = \sum_{k=0}^{m} a_k x^k - \frac{a_m}{b_m}\sum_{k=0}^{m} b_k x^k = \sum_{k=0}^{m}(a_k - \frac{a_m}{b_m}b_k)x^k = \sum_{k=0}^{m-1}(a_k - \frac{a_m}{b_m}b_k)x^k$$

et donc $\deg(R) < m$. Donc l'affirmation est vraie pour $n = m$.

— Soit $n \geq m$. Supposons que pour tout polynôme A de degré inférieur ou égal à n, il existe $(Q, R) \in \mathbb{K}[x]^2$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$.
Soit A un polynôme de degré $n+1$. Posons $A = \sum_{k=0}^{n+1} a_k x^k$. Alors

$A - \frac{a_{n+1}}{b_m}x^{n+1-m}B = \sum_{k=0}^{n+1} a_k x^k - \frac{a_{n+1}}{b_m}x^{n+1-m}\sum_{k=0}^{m} b_k x^k = a_{n+1}x^{n+1} + \sum_{k=0}^{n} a_k x^k - \frac{a_{n+1}}{b_m}b_m x^{n+1} + \sum_{k=0}^{m-1}\frac{a_{n+1}}{b_m}b_k x^{n+1-m+k}$. Ainsi,

$$A - \frac{a_{n+1}}{b_m}x^{n+1-m}B = \sum_{k=0}^{n} a_k x^k - \sum_{k=n+1-m}^{n}\frac{a_{n+1}}{b_m}b_{n+1-m+k}x^k$$

Par suite,

$$\deg(A - \frac{a_{n+1}}{b_m}b_k x^{n+1-m}B) \leq n$$

Par hypothèse de récurrence, il existe $(Q_1, R) \in \mathbb{K}[x]^2$ tel que

$$A - \frac{a_{n+1}}{b_m}b_k x^{n+1-m}B = BQ_1 + R$$

et $\deg(R) < \deg(B)$. Mais alors,

$$A = B(\frac{a_{n+1}}{b_m}x^{n+1-m} + Q_1) + R$$

et les polynômes $Q = \frac{a_{n+1}}{b_m}x^{n+1-m} + Q_1$ et R conviennent.

Le résultat est ainsi démontré par récurrence.
Montrons maintenant l'unicité. Soit $(Q_1, Q_2, R_1, R_2) \in \mathbb{K}[x]^4$ tel que $A = BQ_1 + R_1 = BQ_2 + R_2$ et $\deg(R_1) < \deg(B)$ et $\deg(R_2) < \deg(B)$. On a donc $B(Q_1 - Q_2) = R_2 - R_1$ avec

$$\deg(R_2 - R_1) \leq \max\{deg(R_1), \deg(R_2)\} < \deg(B)$$

Si $Q_1 \neq Q2$, alors $Q_1 - Q_2$ a un degré entier, et on a

$$\deg(R_2 - R_1) = \deg(B(Q_1 - Q_2)) = \deg(B) + \deg(Q_1 - Q_2) > \deg(B)$$

ce qui est faux. Donc, $Q_1 = Q_2$ puis $R_1 = R_2$. **(c.q.f.d)**

Remarque 3.1.12

1. *Noter que, si* $\deg(B) \geq 1$, *la condition* ($R = 0$ *ou* $0 \leq \deg(R) < \deg(B)$) *est équivalente à* $R \in \mathbb{K}_n[x]$, *où* $n = \deg(B) - 1$.
2. *Noter aussi qu'en utilisant la convention* $-\infty < n$ *pour tout entier* n, *la condition* ($R = 0$ *ou* $0 \leq \deg(R) < \deg(B)$) *peut s'écrire simplement* $\deg(R) < \deg(B)$.

Il est claire que la démonstration du théorème 3.1.11 offre un algorithme de calcul similaire à celui de la division euclidienne dans les entiers. Ainsi, en pratique, nous calculons le quotient et le reste comme indiqué dans l'exemple suivant :

$$A = x^5 - x^4 - x^3 + 3x^2 - 2X \quad \text{et} \quad B = x^2 - x + 1.$$

$$\begin{array}{cccccc|c}
x^5 & -x^4 & -x^3 & +3x^2 & -2X & +0 & x^2 - x + 1 \\
\cline{7-7}
-x^5 & +x^4 & -x^3 & & & & x^3 - 2x + 1 \\
 & & -2X^3 & +3X^2 & -2X & & \\
 & & +2x^3 & -2X^2 & +2X & & \\
 & & & +x^2 & & & \\
 & & & -x^2 & +x & -1 & \\
 & & & & +x & -1 &
\end{array}$$

D'où, on trouve l'identité de la division euclidienne suivante :

$$x^5 - x^4 - x^3 + 3x^2 - 2X = (x^2 - x + 1)(x^2 - x + 1) + (x^3 - 2x + 1).$$

Dans des cas particuliers, on peut calculer le reste et ainsi le quotient d'une division euclidienne en utilsant des proprités du diviseur. Par exemple, si le diviseur est de degré 1, on a le résultat suivant :

Proposition 3.1.13

Pour tout $P \in \mathbb{K}[x]$ et tout $a \in \mathbb{K}$, il existe un unique polynôme $Q \in \mathbb{K}[x]$ tel que $P = Q(x - a) + P(a)$.

Preuve. On effectuant la division euclidienne de P par $(x-a)$, on trouve un unique couple $(Q,R) \in \mathbb{K}[x]^2$ tel que $P = Q(x-a)+R$ et $\deg(R) < \deg(x-a) = 1$. Donc, $R = \lambda$ est un polyôme constant avec $\lambda \in \mathbb{K}$. Par suite, $P(a) = \lambda$. **(c.q.f.d)**

Définition 3.1.14

Un élément $a \in \mathbb{K}$ est dit une **racine** d'un polynôme $P \in \mathbb{K}[x]$ si $P(a) = 0$.

Corollaire 3.1.15

Pour tout $P \in \mathbb{K}[x]$, un élément $a \in \mathbb{K}$ est une racine de P si et seulement le reste la division euclidienne de P par $(x-a)$ est nul.

Dans le cas où le diviseur possède deux racines et de degré 2, on peut déterminer le reste facilement comme montre l'exemple suivant :

Exemple 3.1.16
Déterminons R, le reste de la division euclidienne de $P = (x+1)^n - x^n - 1$ (où $n \in \mathbb{N}^*$) par le polynôme $B = x^2 - 3x + 2$.

On $P = BQ+R$ où Q est le quotient de la division euclidienne de P par Q. Puisque $\deg(R) < \deg(B) = 2$, R est de la forme $R = ax+b$ pour certains $a, b \in \mathbb{R}$. Puisque $Q(1) = Q(2) = 0$, on trouve : $P(1) = R(1)$ et $P(2) = R(2)$, c'est-à-dire :

$$\begin{cases} 2^n - 2 = a + b \\ 3^n - 2^n - 1 = 2a + b \end{cases}$$

Par suite,

$$\begin{cases} a = 3^n - 2^{n+1} + 1 \\ b = -3^n + 2^{n+1} + 2^n - 3 \end{cases}$$

Exercice 3.1.17

Calculer le reste de la division euclidienne du polynôme $P = (x+1)^n - x^n - 1$ (où $n \in \mathbb{N}^*$) par le polynôme $B = x^2 + x + 1$.

Exercice 3.1.18

On considère les deux polynômes $P = \prod_{k=1}^{n} \left(x \sin \frac{k\pi}{n} + \cos \frac{k\pi}{n} \right)$ (où $n \geq 2$) et $Q = x^2 + 1$. Calculer le reste de la division euclidienne du polynôme P par Q.

Exercice 3.1.19

On considère les deux polynômes $x^n + x + 1$ (où $n \geq 2$) et $(x-1)^2$. Calculer le reste de la division euclidienne du polynôme P par Q.

Théorème 3.1.20

Tout idéal de l'anneau $\mathbb{K}[x]$ est principal. Autrement dit, l'anneau $\mathbb{K}[x]$ est principal.

Preuve. Soit I un idéal de $\mathbb{K}[x]$. Montrons que I est principal.
Si I est nul, alors il est claire qu'il est principal engendré par le polynôme nul.
Supposons que I est non nul.
On considère E l'ensemble des degrés des polynômes non nuls appartenants à I. Comme I n'est pas nul, E est une partie non vide de $\mathbb{N}$. Donc, E possède un minimum, soit n_0 ce minimum. Alors, il existe $P \in I$ tel que $\deg(P) = n_0$.
On montre que $I = P\mathbb{K}[x]$.
Soit maintenant Q un élément de I. En effectuant la division euclidienne de Q par P, on trouve $(A, R) \in \mathbb{K}[x]^2$ tel que

$$Q = AP + R \quad \text{avec} \quad (R = 0 \quad \text{ou} \quad 0 \leq \deg(R) < \deg(P) = n_0).$$

Comme I est un idéal de $\mathbb{K}[x]$ et $P \in I$, $AP \in I$ et par conséquent $R = Q - AP \in I$. Alors, si on suppose que R est non nul, on obtient, d'après la définition de E et par minimalité de n_0, que $\deg(R) \geq n_0$. Ce qui est donc une contradiction avec le fait que $\deg(R) < \deg(P) = n_0$ (car $R \neq 0$). D'où, $R = 0$ et par suite $Q = AP$, en particulier $Q \in P\mathbb{K}[x]$. Cela montre que I est inclus dans l'idéal principal $P\mathbb{K}[x]$. L'inclusion inverse est aussi vraie car $P \in I$. Par suite, I est un idéal principal. **(c.q.f.d)**

Exercice 3.1.21

Dans cet exercice, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$. Soit $\mathbb{A}$ un sous-anneau de $\mathbb{K}$. On pose $\mathbb{A}[x] = \{\sum a_n x^n \in \mathbb{K}[x] / a_n \in \mathbb{A}, \forall n \in \mathbb{N}\}$.

1. Montrer que $\mathbb{A}[x]$ est un sous-anneau de $\mathbb{K}[x]$.
2. Déterminer l'ensemble des éléments inversibles de $\mathbb{A}[x]$.
3. Soit $P \in \mathbb{A}[x]$. Montrer que $P\mathbb{A}[x] = \mathbb{A}[x]$ si et seulement si P est un polynôme constant non nul.
4. Montrer que l'idéal principal $2\mathbb{Z}[x]$ de $\mathbb{Z}[x]$ est propre, bien que dans $\mathbb{Q}[x]$, $2\mathbb{Q}[x] = \mathbb{Q}[x]$.
5. Montrer que l'idéal $2\mathbb{Z}[x] + x\mathbb{Z}[x]$ de $\mathbb{Z}[x]$ n'est pas principal.

Nous avons montré que l'anneau $\mathbb{K}[x]$ de polynômes à coefficients dans un sous-corps $\mathbb{K}$ de $\mathbb{C}$ est principal (Théorème 3.1.20), mais d'après la question (5) de l'exercice 3.1.21, ce résultat tombe en défaut si l'on considère l'anneau de polynômes à coefficients dans l'anneau $\mathbb{Z}$. En général, nous avons le résultat classique suivant :

Exercice 3.1.22 (Suite de l'exercice 3.1.21)

Soit $\mathbb{A}$ un sous-anneau de $\mathbb{C}$. Montrer que $\mathbb{A}[x]$ est principal si et seulement si $\mathbb{A}$ est un corps.

Exercice 3.1.23 (Suite de l'exercice 3.1.21)

Soient $\mathbb{A}$ un sous-anneau de $\mathbb{C}$ et $a \in \mathbb{C}$. On pose

$$\mathbb{A}[a] = \{P(a)/P \in \mathbb{A}[x]\}.$$

1. Montrer que $\mathbb{A} \subset \mathbb{A}[a]$ et $a \in \mathbb{A}[a]$.
2. Montrer que si $a \in \mathbb{A}$, alors $\mathbb{A}[a] = \mathbb{A}$.
3. Montrer que $\mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2}; a, b \in \mathbb{Z}\}$.
4. On considère $j = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.
   Montrer que $\mathbb{Z}[j^2] = \{a + bj + cj^2; a, b \in \mathbb{Z}\}$.
5. On considère l'application $\Phi : \mathbb{A}[x] \to \mathbb{C}$ définie par $\Phi(P) = P(a)$ pour $P \in \mathbb{A}[x]$.
   (a) Montrer que Φ est un homomorphisme d'anneaux.
   (b) Montrer que $\mathrm{Im}(\Phi) = \mathbb{A}[a]$.
   (c) Montrer que $\mathbb{A}[a]$ est le plus petit sous-anneau de $\mathbb{C}$ (au sens de l'inclusion) contenant a et $\mathbb{A}$.

Exercice 3.1.24 (Suite de l'exercice 3.1.23)

On considère l'application $\Phi : \mathbb{R}[x] \to \mathbb{R}$ définie par $\Phi(P) = P(\sqrt{2})$ pour $P \in \mathbb{R}[x]$.

1. Montrer que Φ est un homomorphisme d'anneaux surjectif.
2. En déduire que $I = \{P \in \mathbb{R}[x]; P(\sqrt{2}) = 0\}$ est un idéal de $\mathbb{R}[x]$.
3. Rappelons que $\mathbb{R}[x]$ est un anneau principal. Déterminer le générateur unitaire de l'idéal principal I.

3.2 Arithmétique dans $\mathbb{K}[x]$

Dans la section précédente, nous avons présenté quelques propriétés de $\mathbb{K}[x]$ qui montrent une certaine similitude avec $\mathbb{Z}$. Nous verrons que nous pouvons également définir des concepts similaires à ce que nous avons dans l'arithmétique dans $\mathbb{Z}$.

3.2.1 Divisibilité dans $\mathbb{K}[x]$

Définition 3.2.1

Soient A et B deux polynômes dans $\mathbb{K}[x]$. On dit que **A divise B** et on note A/B, s'il existe $Q \in \mathbb{K}[x]$ tel que $B = QA$. On dit aussi que B est un **multiple** de A.

En terme de divisibilité, le corollaire 3.1.15 est reformulé comme suit :

Proposition 3.2.2

Un élément $a \in \mathbb{K}$ est une racine d'un polynôme $P \in \mathbb{K}[x]$ si et seulement si $x - a/P$.

Comme dans le cas de $\mathbb{Z}$, la divisibilité peut être exprimée en termes d'idéaux. Cela facilitera l'étude de certaines propriétés d'autant plus que l'on pourra utiliser le fait que l'anneau de polynômes $\mathbb{K}[x]$ est principal.

Proposition 3.2.3

Soient A et B deux polynômes. Alors, les assertions suivantes sont équivalentes :

1. A/B.
2. $B \in A\mathbb{K}[x]$.
3. $B\mathbb{K}[x] \subset A\mathbb{K}[x]$.

Preuve. $1 \Leftrightarrow 2$. Par définition, A/B si et seulement s'il existe $Q \in \mathbb{K}[x]$ tel que $B = QA$. Cela est équivaut à $B \in A\mathbb{K}[x]$.
$2 \Rightarrow 3$. Conséquence du théorème 2.3.6.
$3 \Rightarrow 2$. Cette implication est triviale car $B \in B\mathbb{K}[x]$. **(c.q.f.d)**

Nous donnons maintenant quelques propriétés principales de la divisibilité qui sont très utiles dans ce qui suit.

Proposition 3.2.4

1. Pour tout polynôme P, P/P. On dit que la relation de divisibilité dans $\mathbb{K}[x]$ est réflexive.
2. Soient A, B et C dans $\mathbb{K}[x]$.
   Si A/B et B/C, alors A/C. On dit que la relation de divisibilité dans $\mathbb{K}[x]$ est transitive.
3. Pour tout $A \in \mathbb{K}[x]$, $A/0$.
4. Pour tous $A, B \in \mathbb{K}[x]$, A/B si et seulement si $\alpha A/\beta B$ pour tous $\alpha, \beta \in \mathbb{K}^*$.
   En particulier, pour tous $\lambda, \beta \in \mathbb{K}^*$ et tout $A \in \mathbb{K}[x]$, λ/A et $\lambda A/\beta A$.
5. Soient A, B et C dans $\mathbb{K}[x]$.
   Si A/B et A/C, alors $A/P_1B + P_2C$ pour tous P_1 et P_2 dans $\mathbb{K}[x]$.
6. Soient A et B deux polynômes dans $\mathbb{K}[x]$ avec $B \neq 0$.
   Si A/B, alors $\deg(A) \leq \deg(B)$.

Exercice 3.2.5

Montrer que si un polynôme $P \in \mathbb{K}[x]$ divise deux polynômes de la forme $x^n + a$ et $x^n - a$ (avec $n \in \mathbb{N}^*$ et $a \in \mathbb{R}$), alors $P = \lambda$ pour un certain $\lambda \in \mathbb{K}^*$.

Preuve. Remarquer que $(x^n + a) - (x^n - a) = a$. **(c.q.f.d)**

Noter que bien que la relation de divisibilité dans $\mathbb{K}[x]$ est réflexive et transitive, elle n'est pas une relation antisymétrique, et donc elle n'est pas une relation d'ordre. En fait, on peut voir facilement que, par exemple, $3x-5/6x-10$ et $6x-10/3x-5$, mais $6x-10 \neq 3x-5$. Cela a donné lieu à la notion suivante.

Définition 3.2.6

Soient A et B deux polynômes dans $\mathbb{K}[x]$. On dit que les deux polynômes A et B sont **associés** si A/B et B/A.

Il est facile de voir, d'après l'assertion 6 de la proposition 3.2.4, que, si deux polynômes non nuls A et B dans $\mathbb{K}[x]$ sont associés, alors ils ont le même degré. En fait, nous montrons qu'ils sont simplement égaux à un facteur près. Notamment on a la caractérisation suivante :

Proposition 3.2.7

Soient A et B deux polynômes dans $\mathbb{K}[x]$. Alors, les assertions suivantes sont équivalentes :

1. A et B sont associés.
2. Il existe $\lambda \in K^*$ tel que $A = \lambda B$.
3. $A\mathbb{K}[x] = B\mathbb{K}[x]$.
4. A/B et $\deg(B) \leq \deg(A)$

Preuve. $1 \Rightarrow 2$. Puisque A et B sont associés, il existe deux polynômes Q et P tels que $A = QB$ et $B = PA$. Alors, $A = QPA$. Si $A = 0$, alors de même B et on a rien à montrer. Sinon, $QP = 1$ (car l'anneau $\mathbb{K}[x]$ est intègre). Cela veut dire que P et Q sont inversibles et ainsi le résultat découle du corollaire 3.1.9.
$2 \Rightarrow 3$. Par double inclusions en utilisant la proposition 3.2.3.
$3 \Rightarrow 1$. C'est aussi d'après la proposition 3.2.3 en exprimant les deux inclusions en termes de divisibilité.
Il reste à montrer qu'équivalence avec la dernière assertion. L'implication ($1 \Rightarrow 4$) est triviale. On montre $4 \Rightarrow 2$. En effet, puisque A/B, il existe $P \in \mathbb{K}[x]$ tel que $B = PA$. Alors, $\deg(B) = \deg(P) + \deg(A)$, en particulier $\deg(B) \geq \deg(A)$. Par hypothèse, on a $\deg(B) \leq \deg(A)$. D'où, $\deg(B) = \deg(A)$ et alors $\deg(P) = 0$. Ce qui montre que P est constant. **(c.q.f.d)**

Il est claire maintenant que tout polynôme admet une infinité d'associés. Cependant, dans certaines situations la propriété d'unicité facilite la tâche. D'où l'importance du résultat suivant :

Corollaire 3.2.8

Pour tout polynôme non nul A de $\mathbb{K}[x]$, il existe un unique polynôme unitaire ω associé à A.
Autrement dit, il existe un unique polynôme unitaire ω tel que $A\mathbb{K}[x] = \omega\mathbb{K}[x]$.
Par conséquent, deux polynômes unitaires sont associés si et seulement si sont égaux.

Preuve. Soit A un polynôme non nul de coefficient dominant $\lambda \neq 0$. Alors, $\frac{1}{\lambda}A$ est un polynôme unitaire associé à A (d'après la proposition 3.2.7). Supposons qu'il existe un autre polynôme unitaire B associé à A. Alors $A = \eta B$ pour certain $\eta \in \mathbb{K}$. Mais B est unitaire, alors η est le coefficient dominant de $\eta B = A$. D'où $\eta = \lambda$. **(c.q.f.d)**

Noter qu'avec le corollaire 3.2.8 et le théorème 3.1.20 on conclut que, pour tout idéal I non nul de $\mathbb{K}[x]$, il existe un unique polynôme unitaire ω tel que $I = \omega\mathbb{K}[x]$.

Exemple 3.2.9
Dans $\mathbb{R}[x]$, *on a* $(4x^2 - 3x + 2)\mathbb{R}[x] = (x^2 - \frac{3}{4}x + \frac{1}{2})\mathbb{R}[x]$.

3.2.2 PGCD et ces applications

Nous introduisons dans cette partie le pgcd de deux polynômes et nous donnons certaines de ces propriétés. Nous allons voir aussi son rôle dans la décomposition des polynômes. A la fin de cette partie nous parlons du ppcm de deux polynômes et en donnons quelques propriétés.

Il est à noter que la définition du pgcd de deux entiers utilise la relation d'ordre naturelle qui existe sur les entiers, en prenant le pgcd le plus grand diviseur parmi les diviseurs communs. Cependant, nous ne pouvons pas définir le pgcd des polynômes de cette manière, car simplement l'anneau de polynômes $\mathbb{K}[x]$ n'a pas de relation d'ordre naturelle. Mais, on sait que le pgcd peut être aussi caractérisé de la façon suivante : Soit $(n, m) \in \mathbb{Z}^2$ et $d \in \mathbb{N}$. Alors les assertions suivantes sont équivalentes :

1. $\text{pgcd}(m, n) = d$.
2. d vérifie les deux assetrions suivantes :
   (a) d est un diviseur commun de m et n.
   (b) Si k est un diviseur commun de m et n, alors k divise d.
3. $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$.

Cela signifie que le pgcd dans $\mathbb{Z}$ garde également sa valeur comme le plus grand élément mais cette fois pour la relation de divisibilité (entre nombres naturels). Avant de définir le pgcd de deux polynômes, on montre que l'analogue du résultat ci-dessus existe dans $\mathbb{K}[x]$.

Théorème 3.2.10

Soient A et B deux polynômes dans $\mathbb{K}[x]$. On suppose que l'un au moins A ou B est non nul. Alors, pour un diviseur commun $D \in \mathbb{K}[x]$ de A et B, les assertions suivantes sont équivalente :

1. $A\mathbb{K}[x] + B\mathbb{K}[x] = D\mathbb{K}[x]$.
2. Si Δ est un diviseur commun de A et B, alors Δ divise D.
3. D est de plus grand degré parmi les diviseurs communs de A et B.

Preuve. $1 \Rightarrow 2$. Puisque $A\mathbb{K}[x]+B\mathbb{K}[x] = D\mathbb{K}[x]$; en particulier, $D \in A\mathbb{K}[x]+B\mathbb{K}[x]$, il existe alors deux polynômes U et V tels que $D = UA + VB$. Maintenant, si Δ est un diviseur commun de A et B, alors Δ divise $UA+VB = D$ d'après la proposition 3.2.4.
$2 \Rightarrow 1$. Puisque l'anneau $\mathbb{K}[x]$ est principal, il existe un polynôme $\Delta \in \mathbb{K}[x]$ tel que $A\mathbb{K}[x] + B\mathbb{K}[x] = \Delta\mathbb{K}[x]$. En particulier, A et B sont des éléments de

$\Delta\mathbb{K}[x]$, c'est-à-dire Δ est un diviseur commun de A et B. D'où, par (2), Δ divise D et ainsi $D\mathbb{K}[x] \subset \Delta\mathbb{K}[x]$.
Réciproquement, puisque D est un diviseur commun de A et B, $A\mathbb{K}[x] \subset D\mathbb{K}[x]$ et $B\mathbb{K}[x] \subset D\mathbb{K}[x]$ (d'après la proposition 3.2.3). Alors, $A\mathbb{K}[x]+B\mathbb{K}[x] \subset D\mathbb{K}[x]$ (car $D\mathbb{K}[x]$ est un idéal de $\mathbb{K}[x]$). Alors, $\Delta\mathbb{K}[x] \subset D\mathbb{K}[x]$.
Par suite, $D\mathbb{K}[x] = \Delta\mathbb{K}[x] = A\mathbb{K}[x] + B\mathbb{K}[x]$.
$2 \Rightarrow 3$. Si Δ un diviseur commun de A et B, alors Δ divise D. En particulier, $\deg(\Delta) \leq \deg(D)$ (car $D \neq 0$ car $B \neq 0$). D'où $\deg(D)$ est le plus grand degré parmi les degrés des diviseurs communs de A et B.
$3 \Rightarrow 1$. Puisque l'anneau $\mathbb{K}[x]$ est principal, il existe un polynôme $\Delta \in \mathbb{K}[x]$ tel que $A\mathbb{K}[x] + B\mathbb{K}[x] = \Delta\mathbb{K}[x]$. En particulier, Δ est un diviseur commun de A et B. Donc, par (3), $\deg(\Delta) \leq \deg(D)$. D'autre part, comme dans $2 \Rightarrow 1$, $\Delta\mathbb{K}[x] \subset D\mathbb{K}[x]$. Alors, D divise Δ. Donc, d'après la proposition 3.2.7, D et Δ sont associés et ainsi $\Delta\mathbb{K}[x] = D\mathbb{K}[x]$ (d'après la proposition 3.2.7). D'où le résultat. **(c.q.f.d)**

Soient A et B deux polynômes dans $\mathbb{K}[x]$. On suppose que l'un au moins A ou B est non nul. Alors, il existe une infinité de diviseurs communs de A et B qui vérifient l'une des assertions équivalentes du théorème 3.2.10. En fait, puisque l'anneau $\mathbb{K}[x]$ est principal, il existe un polynôme $D \in \mathbb{K}[x]$ tel que $A\mathbb{K}[x] + B\mathbb{K}[x] = D\mathbb{K}[x]$. Ainsi, tout polynôme Δ associé à D vérifie bien les trois assertions équivalentes du théorème 3.2.10, car

$$\Delta\mathbb{K}[x] = D\mathbb{K}[x] = A\mathbb{K}[x] + B\mathbb{K}[x].$$

On peut appeler chacun de ces polynômes **un** plus grand commun diviseur de A et B (un PGCD, en bref). Mais, avec cette définition, il y'aura une infinité de PGCD de A et B qui sont tous associés. Cependant, on préfère comme il est le cas pour $\mathbb{Z}$ de choisir un polynôme particulier parmi ces polynômes qui garantit l'unicité, utile dans certains contextes. Notant que dans le cas de $\mathbb{Z}$, il n'y a que deux entiers d vérifiant $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ pour un couple d'enteirs $(n, m) \in \mathbb{Z}^2$. En fait, ils sont justes opposés. Donc le pgcd de n et m est choisi comme étant le positif des deux entiers. Dans le cas de polynômes, on se base sur le corollaire 3.2.8 pour garentir l'unicité.

Théorème et Définition 3.2.11

Soient A et B deux polynômes dans $\mathbb{K}[x]$. On suppose que l'un au moins A ou B est non nul. Alors, il existe un unique diviseur commun unitaire $D \in \mathbb{K}[x]$ de A et B qui vérifie l'une des assertions équivalentes du théorème 3.2.10. Il sera appelé **le plus grand commun diviseur** (PGCD, en bref) de A et B et noté $\text{PGCD}(A, B)$.
Si $A = B = 0$, alors nous convenons d'écrire $\text{PGCD}(0, 0) = 0$.

Preuve. En utilisant le corollaire 3.2.8 et le fait que l'anneau $\mathbb{K}[x]$ est principal, il existe un unique polynôme unitaire $D \in \mathbb{K}[x]$ tel que $A\mathbb{K}[x] + B\mathbb{K}[x] = D\mathbb{K}[x]$. En particulier, D est un diviseur commun A et B. D'où le résultat. **(c.q.f.d)**

Proposition 3.2.12

Soient A, B, C trois polynômes dans $\mathbb{K}[x]$.

1. $\text{PGCD}(A, B) = \text{PGCD}(B, A)$ (commutativité du PGCD).
2. $\text{PGCD}(A, \text{PGCD}(B, C)) = \text{PGCD}(\text{PGCD}(A, B), C)$ (associativité du PGCD).
3. Pour tout $\lambda \in \mathbb{K}^*$, $\text{PGCD}(\lambda, A) = 1$.
4. Si C est unitaire, alors $\text{PGCD}(CA, CB) = C.\text{PGCD}(A, B)$.

Preuve. Seule la quatrième assertion mérite une démonstration. Notons $D = \text{PGCD}(A, B)$ et $\Delta = \text{PGCD}(CA, CB)$. Montrons que $CD = \Delta$.
On a D/A et D/B, donc CD/CA et CD/CB. Par suite, CD/Δ.
D'autre part, C/CA et C/CB, donc C/Δ et on peut écrire $\Delta = CE$. Comme Δ/CA et Δ/CB, on peut aussi écrire $CA = \Delta A_0$ et $CB = \Delta B_0$. On a alors $CA = CA_0E$ et $CB = CB_0E$. Donc, $A = A_0E$ et $B = B_0E$. Par suite, E divise A et B, donc E divise D. Alors, $CE = \Delta$ divise donc CD.
En conclusion CD/Δ et Δ/CD et les deux polynômes CD et Δ sont unitaires donc $\Delta = CD$. **(c.q.f.d)**

D'après le théorème 3.2.10, le PGCD D de deux polynômes A et B vérifie $D\mathbb{K}[x] = A\mathbb{K}[x] + B\mathbb{K}[x]$. En particulier, D est une combinaison de A et B. D'où le résultat suivant :

Corollaire 3.2.13

Si un polynôme D est le PGCD de deux polynômes A et B, alors il existe deux polynômes U et V tels que $D = UA + VB$.

Exercice 3.2.14

Soit D le PGCD de deux polynômes A et B dans $\mathbb{K}[x]$. Montrer qu'il existe deux polynômes uniques U_0 et V_0 tels que $D = U_0A + V_0B$ avec $\deg(U_0) < B$ et $\deg(V_0) < A$.

La réciproque de l'implication du corollaire 3.2.15 n'est pas vraie en général. En fait, en utilisant le théorème 3.2.10 et la définition du pgcd de deux polynômes, on obtient le résultat suivant :

Corollaire 3.2.15

Soient un polynôme Δ et D le PGCD de deux polynômes A et B. S'il existe deux polynômes U et V tels que $\Delta = UA + VB$, alors D divise Δ.

Preuve. Puisque D est le PGCD de deux polynômes A et B, alors $A\mathbb{K}[x] + B\mathbb{K}[x] = D\mathbb{K}[x]$. On a $\Delta = UA + VB$, alors $\Delta \in A\mathbb{K}[x] + B\mathbb{K}[x] = D\mathbb{K}[x]$. Donc, D divise Δ. **(c.q.f.d)**

il l'est dans le cas des polynômes premiers entre eux définis comme suit.

Définition 3.2.16

Soient A et B deux polynômes. On dit que les deux polynômes A et B sont **premiers entre eux**, si $\text{PGCD}(A, B) = 1$. Autrement dit, si seuls les polynômes constants sont des diviseurs communs de A et B.

Théorème 3.2.17 (Théorème de Bézout)

Deux polynômes A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $UA + VB = 1$.

Preuve. $\Rightarrow$. Cas particulier du corollaire 3.2.15.
$\Leftarrow$. Si $UA + VB = 1$, alors $1 \in A\mathbb{K}[x] + B\mathbb{K}[x]$. Donc, l'idéal $A\mathbb{K}[x] + B\mathbb{K}[x]$ coïncide avec l'anneau $\mathbb{K}[x]$ qui est un idéal principal engendré par le polynôme constant 1. Par suite, $\text{PGCD}(A, B) = 1$. **(c.q.f.d)**

Exemple 3.2.18
Soient a et b deux éléments différents de $\mathbb{K}$. Alors, $x - a$ et $x - b$ sont premiers entre eux.
En effet, puisque $b \neq a$, $b - a \neq 0$. Alors, $b - a$ est inversible dans $\mathbb{K}$. Maintenant, on a

$$(b - a)^{-1}(x - a) + (a - b)^{-1}(x - b) = 1.$$

Alors, d'après le théorème de Bézout, $x - a$ et $x - b$ sont premiers entre eux.

Pour déterminer le PGCD de deux polynômes, on utilise le résultat suivant :

Proposition 3.2.19

Soient A et B deux polynômes non nuls. Si R est le reste de la division euclidienne de A par B, alors $\text{PGCD}(A, B) = \text{PGCD}(B, R)$.

Preuve. On pose $\text{PGCD}(A, B) = D$ et $\text{PGCD}(B, R) = D_0$. Montrons que $D = D_0$.
On $A = BQ + R$ où Q est le quotient de la division euclidienne de P par Q. Donc, D_0 divise A (en utilisant la proposition 3.2.4 puisque D_0 divise B et R). Ainsi, D_0/D.
De même, puisque on a $R = A - BQ$, on conclut que D divise R aussi et ainsi D/D_0. Cela montre que D et D_0 sont associés. Or en tant que PGCD, ils sont unitaires, d'où ils sont égaux. **(c.q.f.d)**

Comme il est le cas dans $\mathbb{Z}$, le résultat ci-dessus permet de déterminer le PGCD de deux polynômes comme suit :

L'algorithme d'Euclide. Pour déterminer le PGCD de deux polynômes non nuls A et B, on procède comme suit : On peut supposer que $\deg(B) \leq \deg(A)$.

— Si B divise A, alors $\text{PGCD}(A, B) = \frac{1}{\alpha}B$, où α est le coefficient dominant de B.

— Sinon, on effectue une suite des divisions euclidiennes successives comme suit :

$$A = Q_1B + R_1;\ B = Q_2R_1 + R_2;\ R_1 = Q_3R_2 + R_3;\ \cdots$$

dont la condition d'arrêt est "le reste est nul". En effet, Puisque, pour tout $k \in \mathbb{N}^*$, $\deg(R_{k+1}) < \deg(R_k)$, il existe un entier $m \geq 1$ tel que $R_m = 0$. Donc la condition d'arrêt est atteinte au bout d'un nombre fini d'itérations. Soit R_n le dernier reste non nul ; autrement dit,

$$\forall k \leq n,\ R_k \neq 0 \quad \text{et} \quad R_{n+1} = 0.$$

En particulier, on a

$$\text{PGCD}(R_n, R_{n+1}) = \text{PGCD}(R_n, 0) = \frac{1}{\alpha}R_n,$$

où α est le coefficient dominant de R_n. Donc, d'après la proposition 3.2.19,

$$\text{PGCD}(A, B) = \text{PGCD}(B, R_1) = \cdots = \text{PGCD}(R_n, R_{n+1}) = \frac{1}{\alpha}R_n.$$

Alors, $\frac{1}{\alpha}R_n$ est le PGCD de A et B. Cette méthode est appelé l'**algorithme d'Euclide**.

Remarque 3.2.20

Des fois on n'a pas besoin d'arriver jusqu'au dernier reste nul. Par exemple,

— *lorsqu'on trouve un reste non nul R_m un polynôme constant, donc c'est claire que $\text{PGCD}(R_{m-1}, R_m) = 1$. Et par suite, les deux polynômes A et B sont premiers entre eux.*

— *lorsqu'on trouve un reste non nul R_m de degré 1, donc de la forme $R_m = ax + b$. Dans ce cas il suffit de voir est ce que $-\frac{b}{a}$ est une racine de R_{m-1} (i.e., R_m divise R_{m-1}). Car dans ce cas c'est claire que $\text{PGCD}(R_{m-1}, R_m) = \frac{1}{a}R_m = x + \frac{b}{a}$. Sinon, on déduit que les deux polynômes A et B sont premiers entre eux. En fait, le reste de la division euclidienne de R_{m-1} par R_m ne peut être qu'un polynôme constant non nul.*

Exemple 3.2.21
Trouvons le PGCD de $A = x^4 - x^3 + 2x^2 - x + 1$ *et* $B = x^3 + 1$ *dans* $\mathbb{R}[x]$.

Par division euclidienne de A *par* B, *on trouve que*

$$A = (x-1)B + (2x^2 - 2x + 2).$$

Posons $R_1 = 2x^2 - 2x + 2$.
Par division euclidienne de B *par* R_1, *on trouve que*

$$B = (\frac{1}{2}x + \frac{1}{2})R_1.$$

Ainsi, $\text{PGCD}(A, B) = \frac{1}{2}R_1 = x^2 - x + 1$.

L'agorithme d'Euclide nous aide aussi à determiner les polynôme U et V dans l'identité de Bézout.

Exercice 3.2.22

Déteminer l'ensemble des couples $(U, V) \in \mathbb{R}[x]^2$ vérifiant l'égalité suivante : $(*)$ $(x^7 - x - 1)U + (x^5 + 1)V = 1$.

Solution. On pose $A = x^7 - x - 1$ et $B = x^5 + 1$. On pose S l'ensemble des couples $(U, V) \in \mathbb{R}[x]^2$ vérifiant l'égalité $(*)$. On vérifie d'abord que S est non vide.
On effectue des divisions euclidiennes successives et on trouve :

$$\begin{array}{ll} (1) & A = x^2B - (x^2 + x + 1) \\ (2) & B = (x^3 - x^2 + 1)(x^2 + x + 1) - x \\ (3) & x^2 + x + 1 = (-x)(-x - 1) + 1 \end{array}$$

Donc A et B sont premier entre eux, ce qui garentie, d'près le théorème de Bézout, que S n'est pas vide.
Maintenant déterminons un élément de S.
De l'égalité (3), on déduit :

$$1 = (x^2 + x + 1) + (-x)(x + 1).$$

Donc avec (2), on touve :

$$1 = (x^2 + x + 1) + (B - (x^3 - x^2 + 1)(x^2 + x + 1))(x + 1).$$

Ce qui donne :

$$1 = B(x + 1) + (x^2 + x + 1)[1 - (x^3 - x^2 + 1)(+x + 1)]$$

Maintenant, on utilise (2) pour touver :

$$1 = B(x + 1) + (x^2B - A)(x^4 + x^2 - x).$$

On trouve enfin,

$$1 = (x^4 - x^2 + x)A + (x^6 + x^4 - x^3 + x + 1)B.$$

On pose $U_0 = x^4 - x^2 + x$ et $V_0 = x^6 + x^4 - x^3 + x + 1$. Alors, $(U_0, V_0) \in S$.
Maintenant, déterminons S.
On considère un couple $(U, V) \in S$, c'est-à-dire vérifiant l'égalité $(*)$. Alors, $A(U-U_0)+B(V-V_0) = 0$, d'où $(**)$ $A(U-U_0) = -B(V-V_0)$. En particulier, $A/B(V - V_0)$. Or PGCD$(A, B) = 1$, donc d'après le lemme de Gauss, $A/(V - V_0)$. Alors, il existe un polynôme Q tel que $V - V_0 = QA$, et par suite, $V = V_0 - QA$. En remplaçant dans l'égalité $(**)$, on trouve aussi $U = U_0 + QB$. Cela montre que $S \subset \{(U_0 + QB, V_0 - QA); Q \in \mathbb{K}[x]\}$.
Réciproquement, on considère un couple de la forme $(U_0 + QB, V_0 - QA)$. On montre facilement qu'il vérifie l'égalité $(*)$.
Par suite, $S = \{(U_0 + QB, V_0 - QA); Q \in \mathbb{K}[x]\}$. **(c.q.f.d)**

Maintenant donnons quelques conséquences importantes du Théorème de Bézout 3.2.17.

Corollaire 3.2.23 (Lemme de Gauss)

Soient A, B et C trois polynômes. Si A divise BC et PGCD$(A, B) = 1$, alors A divise C.

Preuve. Puisque A et B sont premiers entre eux, on peut écrire $AU + BV = 1$ pour certains polynômes U et V (d'après le théorème de Bezout 3.2.17). Alors, $ACU + BCV = C$. Or A/A et A/BC. Donc, A/ACU et A/BCV et par suite $A/ACU + BCV = C$. **(c.q.f.d)**

Corollaire 3.2.24

Soient A, B et C trois polynômes. Si B et C divisent A, et PGCD$(B, C) = 1$, alors BC divise A.

Preuve. Puisque B/A, on peut écrire $A = BB_1$. Comme $C/A = BB_1$ et PGCD$(B, C) = 1$, le lemme de Gauss (Corollaire 3.2.23) montre que C/B_1 et par suite $BC/BB_1 = A$. **(c.q.f.d)**

Corollaire 3.2.25

Soient A, B et C trois polynômes. Si PGCD$(A, B) = 1$ et PGCD$(A, C) = 1$, alors PGCD$(A, BC) = 1$.

Preuve. Puisque $\text{PGCD}(A, B) = 1$ et $\text{PGCD}(A, C) = 1$, on peut écrire $AU_B + BV_B = 1$ et $AU_C + CV_C = 1$ pour certains polynômes U_B, V_B, U_C et V_C (d'après le théorème de Bezout 3.2.17). Alors,

$$A(AU_BU_C + U_BCV_C + BV_BU_C) + BC(V_BV_C) = 1$$

Par suite, d'après le théorème de Bezout 3.2.17, $\text{PGCD}(A, BC) = 1$. **(c.q.f.d)**

Corollaire 3.2.26

On considère n éléments a_1, a_2, ..., a_n de $\mathbb{K}$ deux à deux distincts, où $n \in \mathbb{N}^*$. Alors, pour tout $a \in \mathbb{K}\backslash\{a_1, a_2, ..., a_n\}$,

$$\text{PGCD}(\prod_{j=1}^{n}(x - a_j), x - a) = 1.$$

Preuve. Facile à montrer par récurrence sur n en utilisant l'exemple 3.2.18 et le corollaire 3.2.24. **(c.q.f.d)**

Ces trois derniers résultats nous permettent d'établir une relation entre le degré d'un polynôme et le nombre de ces racines. Précisèment, nous avons le résultat suivant :

Proposition 3.2.27

On considère n éléments a_1, a_2, ..., a_n de $\mathbb{K}$ deux à deux distincts, où $n \in \mathbb{N}^*$. Alors, si $a_1, a_2, ..., a_n$ sont des racines d'un polynôme P, alors $\left(\prod_{j=1}^{n}(x - a_j)\right)/P$.

Preuve. On procède par récurrence sur n. Le cas où $n = 1$ est exactement la proposition 3.2.2. Alors, on peut supposer que $n \geq 2$. Supposons que $\left(\prod_{j=1}^{n-1}(x - a_j)\right)/P$. D'après le corollaire 3.2.26, $\text{PGCD}(\prod_{j=1}^{n-1}(x - a_j), x - a_n) = 1$. Par suite, d'après le corollaire 3.2.25, on conclut que $\left(\prod_{j=1}^{n}(x - a_j)\right)/P$.

(c.q.f.d)

Corollaire 3.2.28

Si $P \in \mathbb{K}[x]$ est un polynôme non nul, alors le nombre de racines distinctes de P dans $\mathbb{K}$ est au plus $\deg(P)$.

Preuve. Si $\{a_1, a_2, ..., a_n\}$ est l'ensemble de tous les racines de P (de cardinal $n \in \mathbb{N}^*$), alors $\deg\left(\prod_{j=1}^{n}(x-a_j)\right) = n$ et $\left(\prod_{j=1}^{n}(x-a_j)\right)/P$. D'où, puisque $P \neq 0$, $n \leq \deg(P)$. Cela montre le résultat. **(c.q.f.d)**

Comme conséquence importante du corollaire 3.2.28, on déduit qu'un polynôme qui a plus de racines que son degré est nécessairement nul. En particulier, un polynôme qui a une infinité de racines est nul.

Exemple 3.2.29
Soit $P \in \mathbb{R}[x]$ vérifiant l'équation $(*)$ $P(x^2) = P(x)P(x+1)$. Alors, si P est non nul, alors les seules racines réelles possibles de P sont 0 et 1. En effet, si a est une racince de P, alors en utilisant l'équation, on trouve de même a^2 est une racine de P. Par récurrence on montre que, pour tout $n \in \mathbb{N}$, a^{2^n} est une racine de P. Or la suite $(a^{2^n})_{n\geq 1}$ est croissante et peut montrer facilement qu'elle sera strictement croissante si $a \notin \{-1, 0, 1\}$. Cela montre qu'en particulier, si $a \notin \{-1, 0, 1\}$ alors P admet une infinité de racines ce qui est absurde. Donc, les seules racines réelles possibles de P sont -1, 0 et 1. Supposons que -1 est une racince de P. L'équation $(*)$ peut s'écrire en posant $h = x+1$, $P((h-1)^2) = P(h-1)P(h)$. Ainsi, 4 est aussi une racine de P ce qui est absurde. D'où, 0 et 1 est les seules racines réelles possibles de P lorsqu'il est non nul.
A titre d'exercice, montrer que les seules racines complexes possibles de $P \neq 0$ sont $-j$ et $-j^2$ où $j = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

On termine cette partie par la notion du ppcm de deux polynômes. On peut la définir de la même façon qu'on a définit le pgcd.

Théorème 3.2.30

Soient A et B deux polynômes dans $\mathbb{K}[x]$. On suppose que l'un au moins A ou B est non nul. Alors, pour un multiple commun $M \in \mathbb{K}[x]$ de A et B, les assertions suivantes sont équivalente :

1. $A\mathbb{K}[x] \cap B\mathbb{K}[x] = M\mathbb{K}[x]$.
2. Si Δ est un multiple commun de A et B, alors Δ est un multiple de M.
3. M est de plus petit degré parmi les multiples communs de A et B.

Preuve. Essentiellement duale à celle du théorème 3.2.10. **(c.q.f.d)**

Théorème et Définition 3.2.31

Soient A et B deux polynômes dans $\mathbb{K}[x]$. On suppose que l'un au moins A ou B est non nul. Alors, il existe un unique un diviseur commun unitaire $M \in \mathbb{K}[x]$ de A et B qui vérifie l'une des assertions équivalentes du théorème 3.2.30. Il sera appelé **le plus petit commun multiple** (PPCM, en bref) de A et B et noté $\text{PPCM}(A, B)$.
Si $A = B = 0$, alors nous convenons $\text{PPCM}(0, 0) = 0$.

Proposition 3.2.32

Pour deux polynômes unitaires A et B, on a :

$$AB = \text{PGCD}(A, B)\text{PPCM}(A, B).$$

Preuve. Soit D le pgcd (unitaire) de A et B. On peut alors écrire $A = DA_0$ et $B = DB_0$ avec $\text{PGCD}(A_0, B_0) = 1$. On cherche donc à montrer que $AB_0 = A_0B$ est le ppcm de A et B. Or, c'est bien un multiple commun à A et B et si M est un multiple commun à A et B, alors M est un multiple de D et on peut écrire $M = DM_0$. Alors, M_0 est un multiple commun aux polynômes premiers entre eux A_0 et B_0. Il est donc multiple de A_0 B_0 et finalement M est multiple de DA_0B_0, c'est-à-dire de AB_0. **(c.q.f.d)**

Exercice 3.2.33

Soient $A = x^3 + 2x^2 - x - 2$ et $B = x^3 - 3x - 2$ deux polynômes dans $\mathbb{K}[x]$.

1. Calculer D le pgcd de A et B.
2. Trouver les deux polynômes U_0 et V_0 tels que $D = U_0A + V_0B$ avec $\deg(U_0) < B$ et $\deg(V_0) < A$.
3. Trouver le ppcm de A et B.

3.2.3 Factorisation de polynômes

Le théorème fondamental de l'arithmétique montre que tout entier peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs. Ce résultat est d'une grande utilité théorique et pratique. Dans cette partie nous présentons "le théorème fondamental de l'algèbre", le résultat annalogue du théorème fondamental de l'arithmétique dans le cas des polynômes. Présisèment, nous nous intéressons à la décomposition des polynômes en facteurs de polynômes irréductibles, l'annolgue du nombre premier dans le cas des polynômes.

Définition 3.2.34

Un polynôme P est dit **irréductible** dans $\mathbb{K}[x]$ s'il n'est pas constant et si ses seuls diviseurs sont les polynômes constants et les polynômes associés.

Le théorème fondamental de l'algèbre découle du théorème célèbre, dit **théorème de d'Alembert-Gauss**, qui affirme que tout polynôme non constant de $\mathbb{C}[x]$ possède au moins une racine. La démonstration de ce dernier résultat, qui relève de l'analyse, est hors-programme.
Avant de donner et ainsi démontrer le théorème fondamental de l'algèbre, nous avons besoin de donner quelques résultats. Le résultat suivant découle facilement du théorème de d'Alembert-Gauss.

Proposition 3.2.35

Dans $\mathbb{C}[x]$, les polynômes irréductibles sont les polynômes de degré 1. Autrement dit, un polynôme dans $\mathbb{C}[x]$ est irréductible si et seulement s'il n'admet pas de racines dans $\mathbb{C}$.

Donc la décomposition d'un polynôme dans $\mathbb{C}[x]$ est principalement basée sur l'étude des racines de ce polynôme. Notamment, on aura besoin d'avoir une information sur la multiplicité des racines définie comme suit :

Proposition et Définition 3.2.36

Soit a une racine d'un polynôme non nul $P \in \mathbb{K}[x]$. Alors, il existe un entier $m > 0$ tel que $(x-a)^m / P$ et $(x-a)^{m+1}$ ne divise pas P. Cet entier est appelé l'**ordre de multiplicité** de a ou simplement **la multiplicité** de a. On dit aussi que a est de multiplicité m.
En particulier,
— Si $m = 1$, a est dit une r**acine simple** de P.
— Si $m = 2$, a est dit une **racine double** de P.

Exemple 3.2.37
On considère le polynôme $P = x^3(x+1)(x-\pi)^2(x^2+1)$. Alors, 0 est unr racine de multiplicité 3 de P, -1 est une racine simple de P et π est une racine double de P. Aussi, P admet i et $-i$ comme deux racines complexes simples.

Nous pouvons étendre a proposition 3.2.27 en utlisant le résultat suivant :

Proposition 3.2.38

Pour tout $(a,b) \in \mathbb{K}^2$ et tout $(m,n) \in (\mathbb{N}^*)^2$, si $a \neq b$, alors

$$\text{PGCD}((x-a)^m, (x-b)^n) = 1$$

Autrement dit, $(x-a)^m$ et $(x-b)^n$ sont premiers entre eux.

Proposition 3.2.39

Si $a_1, a_2, ..., a_n \in \mathbb{K}$ sont des racines d'un polynôme P deux à deux distinctes de multiplicité $m_1, m_2, ..., m_n \in \mathbb{N}^*$, respectivement, alors

$$\left(\prod_{j=1}^{n}(x-a_j)^{m_j}\right) / P.$$

Preuve. Similaire à la démonstration de la proposition 3.2.27. **(c.q.f.d)**

Nous verrons que la dérivée nous permettra de déterminer la multiplicité d'une racine d'un polynôme. Pour cela nous avons besoin du théorème suivant :

Lemme 3.2.40 (Formule de Taylor)

On considère un polynôme $P \in \mathbb{K}[x]$ de degré $d \in \mathbb{N}$ et $a \in \mathbb{K}$. Alors, P s'écrit d'une manière unique en fonction des puissances de $(x-a)$ comme suivant :

$$P = \sum_{k=0}^{k=d} \frac{P^{(k)}(a)}{k!}(x-a)^k.$$

De sorte que, si $P = \sum a_k(x-a)^k$, alors $a_k = \dfrac{P^{(k)}(a)}{k!}$ pour tout $k \in \mathbb{N}$.

Proposition 3.2.41

Un élément $a \in \mathbb{K}$ est une racine de multiplicité $m \in \mathbb{N}^*$ d'un polynôme P si et seulement si $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$.

Preuve. $\Rightarrow$. Si $a \in \mathbb{K}$ est une racine de multiplicité m de P. Alors, il existe un polynôme Q tel que $P = Q(x-a)^m$. Alors, d'après la formule de Leibniz de la dérivée d'ordre n d'un produit on trouve :

$$P^n = ((x-a)^m Q)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} \left((x-a)^m\right)^{(k)} Q^{(n-k)}$$

Cela donne le résultat.
$\Leftarrow$. Premièrement, il faut remarquer que $m \leq \deg(P)$ car $P^{(m)}(a) \neq 0$. Maintenant, pour trouver le résultat, il suffit d'écrire la formule de Taylor en a et d'appliquer l'hypothèse. Notamment, on trouve :

$$P = \sum_{k=0}^{k=d} \frac{P^{(k)}(a)}{k!}(x-a)^k = \sum_{k=m}^{k=d} \frac{P^{(k)}(a)}{k!}(x-a)^k = (x-a)^m \sum_{k=0}^{k=d-m} \frac{P^{(k)}(a)}{k!}(x-a)^k.$$

D'où le résultat. **(c.q.f.d)**

Proposition 3.2.42

Si $z \in \mathbb{C}$ est une racine d'un polynôme $P \in \mathbb{R}[x]$ de multiplicité $m \in \mathbb{N}^*$, alors son conjugué $\overline{z}$ est aussi une racine de P de multiplicité m.

Maintenant on peut déterminer les polynômes irréductibles dans $\mathbb{R}[x]$.

Proposition 3.2.43

Dans $\mathbb{R}[x]$, les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Des fois on n'a pas besoin de déterminer exactement le degré de multiplicité d'une racine $a \in \mathbb{K}$ d'un polynôme P mais plutôt juste l'existence d'une certaine puissance de $(x-a)$ qui divise P. Dans ce cas on peut juste utiliser le résultat suivant au lieu de dériver jusqu'à que l'on trouve la condition $P^{(m)}(a) \neq 0$.

Corollaire 3.2.44

Un élément $a \in \mathbb{K}$ est une racine d'un polynôme P de multiplicité au moins $m \in \mathbb{N}^*$ si et seulement si $P(a) = P'(a) = \cdots = P^{(m-1)} = 0$.

Exercice 3.2.45

Déterminer les entiers $n \in \mathbb{N}$ tels que $(x^2+x+1)^2$ divise $(x+1)^n - x^n - 1$.

Remarque 3.2.46
D'après la proposition 3.2.39, si $a_1, a_2, ..., a_n \in \mathbb{K}$ sont des racines d'un polynôme non nul P deux à deux distinctes de multiplicité $m_1, m_2, ..., m_n \in$

$\mathbb{N}^*$, *respectivement, alors il existe un polynôme* Q *tel que*

$$P = Q\left(\prod_{j=1}^{n}(x-a_j)^{m_j}\right).$$

En particulier,

$$\deg(P) = \deg(Q) + m_1 + \cdots + m_n.$$

Alors, si $\deg(P) = m_1 + \cdots + m_n$, *alors* $\deg(Q) = 0$. *Cela veut dire que* $Q = \lambda$ *est un polynôme constant* ($\lambda \in \mathbb{K}$). *D'après le lemme 3.1.6, on déduit que* λ *est le coefficient dominant de* P.

Exercice 3.2.47

Soit $P \in \mathbb{R}[x]$ un polynôme de degré 4 tel que $P(0) = P(1) = 1$, $P(2) = 4$, $P(3) = 9$ et $P(4) = 16$. Calculer $P(-2)$.

Exercice 3.2.48

1. On considère un polynôme $P = x^8 + 2x^6 + 3x^4 + 2x^2 + 1 \in \mathbb{C}[x]$.
   (a) Montrer que j est une racine de P et déterminer son ordre de multiplicité.
   (b) Décomposer P en facteurs irréductibles sur $\mathbb{R}$ et sur $\mathbb{C}$.
2. Décomposer en facteurs irréductibles sur $\mathbb{R}$ et sur $\mathbb{C}$ les polynômes suivants : $P_1 = x^6 + 64$; $P_2 = x^4 - 2x^3 + 27x^2 - 2x + 26$ (noter que $P_2(i) = 0$) ; $P_3 = 2x^4 + 5x^3 + 13x^2 + 7x + 5$ (calculer $P_3(-1+2i)$).

Exercice 3.2.49

Déterminer le polynôme $P \in \mathbb{R}_4[x]$ de racines $\{1; -1; i; -i\}$ et de coefficient dominant 42.

Exercice 3.2.50

Trouver le polynôme $P \in \mathbb{R}_7[x]$ tel que $(x-1)^4$ divise $P+1$ et $(x+1)^4$ divise $P-1$.

Nous sommes maintenant en mesure de présenter le théorème fondamental de l'algèbre.

Théorème 3.2.51 (Le théorème fondamental de l'algèbre)

Tout polynôme non constant $P \in \mathbb{C}[x]$ de coefficient dominant λ s'écrit sous la forme :

$$\lambda(x-a_1)^{m_1}(x-a_2)^{m_2}\cdots(x-a_n)^{m_n}$$

avec $a_1, ..., a_n \in \mathbb{K}$, et $m_1, ..., m_n \in \mathbb{N}^*$.

Comme une conséquence importante, nous obtenons le résultat suivant qui présente la factorisation des polynômes dans $\mathbb{R}[x]$.

Corollaire 3.2.52

Tout polynôme non constant $P \in \mathbb{R}[x]$ de coefficient dominant λ s'écrit sous la forme :

$$\lambda\prod_{k=1}^{r}(x-x_k)^{m_k}\prod_{j=1}^{q}(x^2+s_jx+p_j)^{\mu_j}$$

avec $x_1, ..., x_r \in \mathbb{K}$, $m_1, ..., m_n$, $\mu_1, ..., \mu_q \in \mathbb{N}^*$ et les s_i et p_i sont des éléments de $\mathbb{R}$ vérifiant $s_j^2 - 4p_j < 0$ pour tout $1 \leq j \leq q$.

Exercice 3.2.53

Trouver tous les polynômes $P \in \mathbb{R}[x]$ vérifiant l'équation $(*)$ dans chacun des cas suivants :
$(*)$: $P(x^2) = P(x)P(x+1)$;
$(*)$: $P(x+1) + P(x-1) = 2P(x)$.

3.3 Fractions rationnelles

Dans cette section, nous nous intéressons principalement à la décomposition des fractions rationnelles en une somme de termes particuliers appelés simples. Cette opération est très utile dans de nombreuses situations, y compris le calcul de primitives. Dans cette section, il y a des résultats " théoriques " qui montrent l'existence d'une telle décomposition et il y a des résultats et des méthodes " pratiques " qui aident à la décomposition des fractions rationnelles.

3.3.1 Définitions et premières méthodes de décomposition

Nous commençons par une liste de vocabulaire que nous utilisons tout au long de cette partie.

Définition 3.3.1 (Fractions rationnelles)

Toute fonction de la forme $F = \dfrac{A}{B} \in \mathbb{K}(x)$, où A et B sont deux polynômes de $\mathbb{K}[x]$ avec $B \neq 0$, est appelée une **fraction rationnelle**.

Vocabulaire.

1. Si le numérateur A et le dénominateur B d'une fraction rationnelle $F = \dfrac{A}{B} \in \mathbb{K}(x)$ ne sont pas premiers entre eux, alors on peut réduire F en divisant A et B par le PGCD de A et B, soit D ce PGCD. On pose $A_0 = \dfrac{A}{D}$ et $B_0 = \dfrac{B}{D}$. Alors, A_0 et B_0 sont deux polynômes premiers entre eux et on a : $F = \dfrac{A_0}{B_0}$.
   On dit que $\dfrac{A_0}{B_0}$ est une **forme réduite** (ou **irréductible**) de F.
   Il est facile de voir qu'il existe une forme réduite de F avec un dénominateur unitaire (à faire à titre d'exercie). Ainsi, cette forme sera appelé **la forme réduite** (ou **irréductible**) de F. Elle s'obtient comme suit : Soit B_1 l'associé unitaire de B_0, c'est-à-dire, le polynôme unitaire tel que $B_1 = \beta B_0$, où β est donc l'inverse du coefficient dominant de B_0 qui existe puisque $B_0 \neq 0$ car $B \neq 0$. Alors, $F = \dfrac{\beta A_0}{B_1}$ est la forme réduite de F.
2. Soit $\dfrac{A_0}{B_0}$ une forme irréductible d'une fraction rationnelle F. On appelle **pôle** de F toute racine $\alpha \in \mathbb{K}$ de B_0. La multiplicité de α en tant que racine de B_0 est appelée **l'ordre** (ou la **lmultiplicité**) du pôle α.
   En particulier, un pôle d'ordre 1 est dit **simple**.

3. On appelle **zéro** de F toute racine $\alpha \in \mathbb{K}$ de A_0.
   La multiplicité de α en tant que racine de A_0 est appelée **l'ordre** (ou la **multiplicité**) du zéro α.

Le résultat principal de cette section montre que n'importe quelle fraction rationnelle admet une décomposition en une somme de termes particuliers dits simples définis comme suit :

Définition 3.3.2

— Toute fraction rationnelle F à coefficients dans $\mathbb{C}$ de la forme

$$\frac{a}{(x-z_0)^j}$$

où $a, z_0 \in \mathbb{C}$ et $j \in \mathbb{N}^*$, est dite **simple**.

— Sur $\mathbb{R}$ il y'a deux types de fractions rationnelles simples :

— Toute fraction rationnelle F à coefficients dans $\mathbb{R}$ de la forme

$$\frac{d}{(x-a)^j}$$

où $a, d \in \mathbb{R}$, est dite **simple** de première espèce.

— Toute fraction rationnelle F à coefficients dans $\mathbb{R}$ de la forme

$$\frac{ax+b}{(x^2+\alpha x+\beta)^j}$$

où $a, b, \alpha, \beta \in \mathbb{R}$ et $j \in \mathbb{N}^*$, est dite **simple** de seconde espèce si $x^2+\alpha x+\beta$ est un polynôme irréductible sur $\mathbb{R}$ (i.e., $\alpha^2-4\beta < 0$).

Exemple 3.3.3
Nous considérons les fractions rationnelles suivantes :

— *Les fractions rationnelles suivants sont des exemples des fractions rationnelles simples sur $\mathbb{C}$:*
$\frac{i}{(x-i\sqrt{3})^3}$, $\frac{2}{(x-7)^2}$, $\frac{2i}{x^5}$, $\frac{1}{x-2+3i}$, $\frac{\pi+i}{x-\frac{2}{3}}$.

— *Les fractions rationnelles suivants sont des exemples des fractions rationnelles simples sur $\mathbb{R}$:*
$\frac{3}{x^5}$, $\frac{11}{x-2}$, $\frac{2}{(x-7)^2}$, $\frac{x/4}{x^2+1}$, $\frac{2x-1}{(x^2-x+1)^3}$, $\frac{224}{(x^2+1)^5}$.

— *Noter que les fractions rationnelles simples sur $\mathbb{R}$ de seconde espece ne sont pas des fractions rationnelles simples sur $\mathbb{C}$.*
Par exemple $\frac{x/4}{x^2+1}$ et $\frac{2x-1}{(x^2-x+1)^3}$ ne sont pas des fractions rationnelles simples sur $\mathbb{C}$, car les deux polynômes x^2+1 et x^2-x+1 ne sont pas irréductibles sur sur $\mathbb{C}$.

— *Aussi* $\dfrac{x/4}{x^2-3x+2}$ *n'est pas simple ni sur* $\mathbb{R}$ *ni sur* $\mathbb{C}$*, car le polynôme* x^2-3x+2 *n'est pas irréductibles sur* $\mathbb{C}$ *car* $x^2-3x+2=(x-1)(x-2)$.

Notre objectif dans cette section est d'acquérir des techniques qui nous permettent de décomposer une fraction rationnelle en une somme d'éléments simples. Comme il est indiqué précédemment, nous allons donner deux résultats principaux (théoriques) qui montrent l'existence et l'unicité d'une telle décomposition. Tout d'abord, commençons par quelques méthodes "pratiques" de décomposition des fractions rationnelles particulières. En fait, ces méthodes seront utilisées aussi pour démontrer les résultats principaux.

- Partie entière d'une fraction rationnelle.

Tout d'abord signalons que généralalement, on se ramène à décomposer que des fractions rationnelles de la forme $F=\dfrac{A}{B}$ avec $\deg A<\deg B$. En effet, supposons qu'on a une fraction rationnelle $F=\dfrac{A}{B}$ telle que $\deg A\geq\deg B$. Par la division euclidienne de A par B, il existe $Q,R\in\mathbb{K}[x]$, $A=QB+R$ avec $\deg R<\deg B$. Ainsi, on obtient la décomposition suivante de F :

$$F=Q+\frac{R}{B}$$

On montre facilement que le polynôme Q ainsi trouvé est unique, il sera appelé **la partie entière** de F. Il est claire que si $\deg A<\deg B$, alors la partie entière de F est simplement le polynôme nul.

Cette remarque explique comment trouver la partie entière d'une fraction rationnelle. Elle permet aussi de restreindre l'étude de la décomposition des fractions rationnelles aux cas des fractions rationnelles de type $F=\dfrac{A}{B}$ avec $\deg A<\deg B$.

Passons maintenant aux premières techniques de décomposition.

- Décomposition des fractions rationnelles de la forme $F=\dfrac{A(x)}{(x-a)^k}$ **avec** $\deg A<k$**.**

On considère une fraction rationnelle F de la forme $F(x)=\dfrac{A(x)}{(x-a)^k}$ avec $A\in\mathbb{K}[x]$ et $\deg A<k$.
En utilisant la formule de Taylor de A en a, on trouve :

$$A(x)=A(a)+A'(a)(x-a)+\cdots+\frac{A^{(k-1)}(a)}{(k-1)!}(x-a)^{k-1}$$

On remplace $A(x)$ par son expression obtenue ci-dessus, on trouve donc la décomposition de F en éléments simples :

$$\frac{A(x)}{(x-a)^k} = \sum_{i=1}^{k} \frac{\frac{A^{(k-i)}(a)}{(k-i)!}}{(x-a)^i}$$

Exemple 3.3.4
On considère la fraction rationnelle $F(x) = \dfrac{x^3+2x^2+3x+4}{(x-1)^4}$.
On pose $P = x^3+2x^2+3x+4$.

La formule de Taylor de P *en* 1 *s'écrit :*

$$P(x) = P(1) + P'(1)(x-1) + \frac{P^{(2)}(1)}{2!}(x-1)^2 + \frac{P^{(3)}(1)}{3!}(x-1)^3$$

Après le calcul on trouve :

$$P(x) = 10 + 10(x-1) + 5(x-1)^2 + (x-1)^3$$

D'où, on trouve la décomposition de F *en éléments simples :*

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

- Décomposition des fractions rationnelles de la forme $F = \dfrac{P(x)}{(x^2+ax+b)^k}$ **avec** x^2+ax+b **est irréductible sur** $\mathbb{R}$ **et** $\deg P < 2k$**.**

On considère une fraction rationnelle F de la forme $F(x) = \dfrac{P(x)}{(x^2+ax+b)^k}$ avec $P \in \mathbb{R}[x]$, $\deg P < 2k$ et x^2+ax+b est un polynôme irréductible sur $\mathbb{R}$.

On pose $A = x^2+ax+b$. La décomposition de F peut être obtenue en effectuant des divisions euclidiennes successives comme suit :

$$\begin{array}{ll} (1) & P = Q_1 A + R_1 \\ (2) & Q_1 = Q_2 A + R_2 \\ & \cdots \\ (k-1) & Q_{k-2} = Q_{k-1} A + R_{k-1} \end{array}$$

Puis, on utilise successivement ces égalités comme suit :

$$\begin{aligned} F &= \frac{Q_1 A + R_1}{A^k} \\ &= \frac{Q_1}{A^{k-1}} + \frac{R_1}{A^k} \\ &= \frac{Q_2 A + R_2}{A^{k-1}} + \frac{R_1}{A^k} \\ &= \frac{Q_2}{A^{k-2}} + \frac{R_2}{A^{k-1}} + \frac{R_1}{A^k} \\ &\cdots \\ &= \frac{Q_{k-1}}{A} + \frac{R_{k-1}}{A^2} + \cdots + \frac{R_2}{A^{k-1}} + \frac{R_1}{A^k} \end{aligned}$$

Par un calcul simple, en utilisant les égalités (1), (2), ...,$(k-1)$, on trouve que $\deg(Q_{k-1}) \leq 1$. D'où,

$$F = \frac{Q_{k-1}}{A} + \frac{R_{k-1}}{A^2} + \cdots + \frac{R_2}{A^{k-1}} + \frac{R_1}{A^k}$$

est bien une décomposition de F en éléments simples.

Exemple 3.3.5
On considère la fraction rationnelle suivante :

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

La décomposition peut se faire par divisions euclidienne successives du numérateur $x^5 - 2x^4 + 2x^3 - x^2 + 2x + 2$ par $x^2 + 1$, puis du quotient obtenu par $x^2 + 1$:

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

Quand $k = 2$, on a besoin d'effectuer qu'une seule fois la division euclidienne comme montre l'exemple suivant :

Exemple 3.3.6
On considère la fraction rationnelle suivante : $F(x) = \dfrac{x^3+1}{(x^2+x+1)^2}$.
On effectue la division euclidienne de $x^3 + 1$ par $x^2 + x + 1$:

$$x^3 + 1 = (x-1)(x^2+x+1) + 2$$

Par suite, on trouve la décomposition de F en éléments simples :

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

- Identité de Bézout.

Nous pouvons décomposer certains fractions rationnelles en éléments simples en utilisant l'identité de Bézout. D'abord remarquons la variante suivante du théorème de Bézout.

Lemme 3.3.7

Soient A et B deux polynômes non constants. Si A et B sont premiers entre eux, alors il existe deux polynômes U et V tels que $UA+VB=1$ et $\deg(U)<\deg(B)$ et $\deg(V)<\deg(A)$.

Preuve. D'après le théorème de Bézout, il existe deux polynômes U_0 et V_0 tels que $U_0A+V_0B=1$. On effectue la division euclidienne de U_0 par B, et ainsi on trouve $U_0=QB+R$, avec $Q,R\in\mathbb{R}[x]$, tel que $\deg(R)<\deg(B)$. Alors,

$$1=U_0A+V_0B=(QB+R)A+V_0B=RA+(QA+V_0)B$$

On pose $U=R$ et $V=QA+V_0$. On a bien $UA+VB=1$ et $\deg(U)<\deg(B)$. Et puisque, $VB=1-UA$. Alors,

$$\deg(VB)=\deg(1-UA)=\deg(UA)\text{ (car } A\text{ n'est pas constant).}$$

Donc,

$$\deg(V)+\deg(B)=\deg(U)+\deg(A)<\deg(B)+\deg(A).$$

Par suite, $\deg(V)<\deg(A)$. **(c.q.f.d)**

Ce résultat permet de décomposer une fraction rationnelle F de la forme $F(x)=\dfrac{P}{A^nB^m}$, où $P\in\mathbb{K}[x]$ et $n,m\in\mathbb{N}^*$, avec A et B sont deux polynômes premiers entre eux. En effet, de même, A^n et B^m sont premiers entre eux. Donc, d'après le lemme 3.3.7, il existe deux polynômes U et V tels que $UA^n+VB^m=1$ et $\deg(U)<\deg(B^m)$ et $\deg(V)<\deg(A^n)$. Ainsi,

$$F(x)=\frac{P}{A^nB^m}=\frac{PUA^n+PVB^m}{A^nB^m}=\frac{PU}{B^m}+\frac{PV}{A^n}$$

Nous continuons ainsi la décomposition de chaque terme, $\dfrac{PU}{B^m}$ et $\dfrac{PV}{A^n}$, en utilisant soit lidentité de Bézout une autre fois ou les méthodes indiquées précédemment.
Des fois on obtient directement la décomposition en éléments simple, comme il est le cas dans l'exemple simple suivant :

Exemple 3.3.8
On considère la fraction rationnelle $F(x)=\dfrac{1}{(x-1)(x^2+1)}$.
On remarque que $\dfrac{1}{2}(x^2+1)-\dfrac{1}{2}(x+1)(x-1)=1$. *D'où on trouve la*

décomposition de F en éléments simples :

$$F(x) = \frac{1/2}{x-1} - \frac{1/2(x+1)}{x^2+1}.$$

- La division suivant les puissances croissantes.

Maintenant, pour décomposer une fraction rationnelle du type $F(x) = \dfrac{A(x)}{x^n B(x)}$, on peut utiliser la division suivant les puissances croissantes présentée dans le résultat suivant :

Théorème et Définition 3.3.9

Soient A et B deux polynômes de $\mathbb{K}[x]$ avec $\tilde{B}(0) \neq 0$. Alors, pour tout $p \in \mathbb{N}$, il existe un unique couple $(Q, R) \in \mathbb{K}[x]^2$ tel que

$$A = BQ + x^{p+1}R \quad \text{et} \quad \deg(Q) \leq p.$$

Cette opération s'appelle la **division suivant les puissances croissantes** de A par B à l'ordre p.

La méthode de calcul de la division selon les puissances croissantes est exactement la même que celle de la division euclidienne en rangeant les deux polynômes dans le sens inverse, c'est-à-dire suivant les puissances croissantes.

Exemple 3.3.10
On considère les deux polynômes $A = 1+3x+2x^2-7x^3$ et $B = 1+x-2x^2$. On effectue la division suivant les puissances croissantes de A par B à l'ordre 3.

$$\begin{array}{llllll|l}
1 & +3x & +2x^2 & -7x^3 & & & 1+x-2x^2 \\
 & +2x & +4x^2 & -7x^3 & & & \hline 1+2x+2x^2-5x^3 \\
 & & +2x^2 & -3x^3 & & & \\
 & & & -5x^3 & +4x^4 & & \\
 & & & & +9x^4 & -10x^5 &
\end{array}$$

Ce qui s'écrit :

$$A = B(1+2x+2x^2-5x^3) + x^4(9-10x)$$

Maintenant, on montre comment on peut utiliser la division suivant les puissances croissantes pour aider à la décomposition d'une fraction rationnelle en éléments simples. Soit $F(x) = \dfrac{A(x)}{x^n B(x)}$ une fraction rationnelle, avec A et $B \neq 0$ deux polynômes et $n \geq 1$. Par la division suivant les puissances croissantes de A par B à l'ordre $n-1$, il existe un unique couple $(Q, R) \in \mathbb{K}[x]^2$ tel que

$$A = BQ + x^n R \quad \text{avec} \quad \deg(Q) \leq n-1.$$

Alors, $Q = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$ avec $b_0, ..., b_{n-1} \in \mathbb{K}$. Par suite, on trouve une décomposition de F obtenue comme suit :

$$\begin{aligned} F &= \frac{BQ + x^n R}{x^n B(x)} \\ &= \frac{Q}{x^n} + \frac{x^n R}{x^n B(x)} \\ &= \frac{b_0}{x^n} + \frac{b_1}{x^{n-1}} + \cdots + \frac{b_{n-1}}{x} + \frac{R}{B(x)} \end{aligned}$$

Ainsi, pour obtenir une décomposition de F en éléments simples, il reste à décomposer la fraction rationnelle $\dfrac{R}{B(x)}$.

Exemple 3.3.11
On considère la fraction rationnelle suivante :

$$F(x) = \frac{4x^4 - 10x^3 + 8x^2 - 4x + 1}{x^3(x-1)^2}.$$

Effectuons la division suivant les puissances croissantes à l'ordre 3 (qui est l'exposant du facteur x) du numérateur $1 - 4x + 8x^2 - 10x^3 + 4x^4$ par $(x-1)^2 = 1 - 2x + x^2$:

$$1 - 4x + 8x^2 - 10x^3 + 4x^4 = (1 - 2x + x^2) \times (1 - 2x + 3x^2) + (-2x^3 + x^4).$$

On obtient la décomposition suivante de F :

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

En décomposant aussi la dernière fraction rationnelle comme suit :

$$\frac{x-2}{(x-1)^2} = \frac{(x-1)-1}{(x-1)^2} = \frac{1}{x-1} - \frac{1}{(x-1)^2}$$

obtient la décomposition de F en éléments simples :

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

Remarque 3.3.12

1. *Cette méthode est efficace pour un exposant assez grand (en général plus grand que 3). Pour des petits exposants, on utlise en pratique d'autres méthodes qu'on va présenter dans la prochaine partie.*
2. *En général, cette méthode peut être utilisée aussi pour une fraction rationnelle du type $F = \dfrac{P(x)}{(x-a)^n Q(x)}$. Pour cela, on considère le changement de variable $u = x - a$, puis on exprime F en fonction de*

u. Il aura ainsi la forme $F = \dfrac{P(u+a)}{u^n Q(u+a)}$. *Donc, on peut maintenant appliquer la méthode proposée et à la fin on revient à la variable* $x = u + a$.

Exercice 3.3.13

Décomposer la fraction $F(x) = \dfrac{x^3+x+1}{x^4(x-1)^3}$ en éléments simples.

Réponse.

$$\frac{x^3+x+1}{x^4(x-1)^3} = -\frac{1}{x^4} - \frac{4}{x^3} - \frac{9}{x^2} - \frac{17}{x} + \frac{3}{(x-1)^3} - \frac{8}{(x-1)^2} + \frac{17}{x-1}. \qquad \textbf{(c.q.f.d)}$$

3.3.2 Théorème principal de la décomposition des fractions rationnelles et d'autres méthodes pratiques de décomposition

Les méthodes présentées jusqu'à maintenant aident à la décomposition des fractions rationnelles particulières. En fait, elles sont aussi utiles pour montrer que n'importe quelle fraction rationnelle se décompose en éléments simples d'une manière unique. En utlisant ce dernier résultat, on peut développer d'autres méthodes pour décomposer les fractions rationnelles en éléments simples.

On commence par le cas de la décomposition sur $\mathbb{C}$.

Théorème 3.3.14

Toute fraction rationnelle F à coefficients dans $\mathbb{C}$ admet une décomposition d'une manière unique sous la forme suivante :

$$F = E + \sum_{i=1}^{p} \sum_{k=1}^{m_i} \frac{b_{i,k}}{(x-a_i)^k}$$

où $E \in \mathbb{C}[x]$ et $b_{i,j} \in \mathbb{C}$.

Vocabulaire.

- Cette écriture est appelés la **décomposition en éléments simples** (en bref, DES) de F sur $\mathbb{C}$.
- Le polynôme E s'appelle la **partie entière** de F.
- Pour $i \in \{1, ..., k\}$, les fractions rationnelles $\dfrac{b_{i,j}}{(x-a_i)^j}$ sont les **éléments simples** associés au pôle a_i.

— Pour $i \in \{1, ..., k\}$, la fraction rationnelle $\frac{b_{i,1}}{(x-a_i)} + \frac{b_{i,2}}{(x-a_i)^2} + \cdots + \frac{b_{i,p_i}}{(x-a_i)^{m_i}}$ la **partie polaire** de F associée au pôle a_i.

Comme il existe deux types d'éléments simples sur $\mathbb{R}$, la décomposition $\mathbb{R}$ sera généralement constituée de deux parties : une partie contenant des éléments simples du premier espèce et une autre partie avec des termes des éléments simples de la seconde espèce.

Corollaire 3.3.15

Toute fraction rationnelle F à coefficients dans $\mathbb{R}$ admet une décomposition d'une manière unique sous la forme suivante :

$$F = E + \sum_{i=1}^{p}\sum_{k=1}^{m_i} \frac{b_{i,k}}{(x-a_i)^k} + \sum_{i=1}^{q}\sum_{k=1}^{n_i} \frac{A_{i,k}}{(x^2+b_ix+c_i)^k}$$

où E est un polynôme de $\mathbb{R}[x]$ et les nombres $b_{i,j}$, a_i, b_i et c_i sont des réels, avec $b_i^2 - 4c_i < 0$, et les $A_{i,j} \in \mathbb{R}[x]$ sont des polynômes de degré au plus 1.

Vocabulaire.

— Comme dans le cas des fractions rationnelles à coefficients dans $\mathbb{C}$, la décomposition de F présentée dans le corollaire 3.3.15 est appelée la **décomposition en éléments simples** (en bref, DES) de F sur $\mathbb{R}$ et le polynôme E s'appelle la **partie entière** de F.

— Les fractions rationnelles $\frac{d_{i,j}}{(x-a_i)^j}$ sont les éléments simples de **première espèce** associés au pôle a_i.

— Pour $i \in \{1, ..., k\}$, la fraction rationnelle $\frac{b_{i,1}}{(x-a_i)} + \frac{b_{i,2}}{(x-a_i)^2} + \cdots + \frac{b_{i,p_i}}{(x-a_i)^{m_i}}$ la **partie polaire** de F associée au pôle a_i.

— Les fractions rationnelles $\frac{A_{i,j}}{(x^2+b_ix+c_i)^j}$ sont les **éléments simples de seconde espèce** associés au polynôme (irréductible) $x^2 + b_ix + c_i$.

Maintenant, les informations fournies par les deux résultats fondamentaux de la décomposition ci-dessous peuvent être utilisées pour développer d'autres méthodes pratiques qui aident au calcul du DES des fractions rationnelles. Commençons par la méthode la plus élémentaire :

- Identifications des coefficients.

Cette méthode consiste à réduire au même dénominateur le membre de la DES d'une fraction rationnelle $F = \frac{A}{B}$ avec $\deg A < \deg B$ et à identifier les coefficients dans les numérateurs.

Exemple 3.3.16
On considère la fraction rationnelle suivante : $F(x) = \dfrac{x^2+x+1}{x(x-1)(x+1)}$
La DES de F est de la forme

$$F(x) = \frac{\lambda}{x} + \frac{\mu}{x-1} + \frac{\nu}{x+1}, \quad \text{avec} \quad \lambda, \mu, \nu \in \mathbb{R}$$

On réduit au même dénominateur le membre de la DES, on obtient :

$$\begin{aligned} x^2+x+1 &= \lambda(x-1)(x+1) + \mu x(x+1) + \nu x(x-1) \\ &= (\lambda+\mu+\nu)x^2 + (\mu-\nu)x - \lambda \end{aligned}$$

D'où, par identification, on obtient le système suivant :

$$\begin{cases} \lambda+\mu+\nu &= 1 \\ \mu-\nu &= 1 \\ -\lambda &= 1 \end{cases}$$

Ce système admet pour seule solution $\lambda = -1$, $\mu = 3/2$, $\nu = 1/2$. Par suite, on obtient la DES de F :

$$F(x) = \frac{-1}{x} + \frac{3}{2(x-1)} + \frac{1}{2(x+1)}$$

- Evaluation et Limite.

Si on veut établir des relations entre les coefficients, on peut substituer à x des valeurs α qui ne sont pas des pôles de F ou on peut calculer des limites (par exemple, $\lim\limits_{x\to\infty} xF(x)$) de deux manières. Pour bien comprendre cette méthode, on donne l'exemple suivant :

Exemple 3.3.17
On considère la fraction rationnelle de l'exemple précédent.

$$F(x) = \frac{x^2+x+1}{x(x-1)(x+1)} = \frac{\lambda}{x} + \frac{\mu}{x-1} + \frac{\nu}{x+1}$$

On peut établir des relations entre les coefficients :
— *En utilisant les limites :*
On obtient l'équation $\lambda+\mu+\nu = 1$ en utilisant les limites suivantes :

$$\lim_{x\to\infty} x\frac{x^2+x+1}{x(x-1)(x+1)} = \lim_{x\to\infty} x(\frac{\lambda}{x} + \frac{\mu}{x-1} + \frac{\nu}{x+1})$$

— *En remplaçant x par une valeur :*
Par exemple, on obtient l'équation $\dfrac{7}{6} = \dfrac{\lambda}{2} + \mu + \dfrac{\nu}{3}$ en remplaçant x par 2.

- Multiplication et substitution.

Cette méthode permet de trouver le coefficient du terme de plus haut degré de chaque partie polaire.
On utilise les notations du théorème 3.3.14.
Soit $i \in \{1, ..., k\}$. Pour déterminer le coefficient b_{i,m_i} on multiplie F et sa DES par $(x - a_i)^{m_i}$ et on évalue l'égalité obtenue en remplaçant x par a_i.

Exemple 3.3.18
On considère la fraction rationnelle suivante :

$$F(x) = \frac{2x^4 + x^3 + 3x^2 - 6x + 1}{2x^3 - x^2}$$

Premièrement, en utilisant la division euclidienne on obtient :

$$F(x) = x + 1 + F_1(x)$$

avec $F_1(x) = \dfrac{4x^2 - 6x + 1}{2x^3 - x^2}$.
Puis, en tenant compte de la factorisation du dénominateur de F_1*, la DES de* F_1 *est de la forme :*

$$(*) \quad F_1(x) = \frac{A}{x^2} + \frac{B}{x} + \frac{C}{x - \frac{1}{2}}, \quad \text{avec} \quad A, B, C \in \mathbb{R}$$

On obtient $A = -1$ *en multipliant les deux membres de cette égalité par* x^2 *et en remplaçant* x *par* 0*. Pour cela, on utilise l'écriture suivante :*

$$A = \left.\frac{4x^2 - 6x + 1}{2x - 1}\right|_{x=0} = -1$$

De même, en multipliant par $x - \dfrac{1}{2}$*, on obtient :*

$$C = \left.\frac{4x^2 - 6x + 1}{2x^2}\right|_{x=\frac{1}{2}} = -2$$

Il reste à déterminer B*. Pour cela, on propose deux méthodes :*
- *On remplace* x *par* 1 *dans l'égalité* $(*)$*. Ce qui donne l'équation :* $-1 = A + B - 2C$*. D'où,* $B = 4$*.*
- *On peut aussi obtenir* B *en multipliant les deux membres de l'égalité* $(*)$ *par* x *et en passant à la limite pour* $x \to +\infty$*. Alors, on obtient,* $2 = B + C$*. D'où,* $B = 4$*.*

Par suite,

$$F(x) = x + 1 - \frac{1}{x^2} + \frac{4}{x} - \frac{2}{x - \frac{1}{2}}$$

Exemple 3.3.19
On considère la fraction rationnelle suivante :

$$F(x) = \frac{4x^6 - 2x^5 + 11x^4 - x^3 + 11x^2 + 2x + 3}{x(x^2+1)^3}$$

La DES de F est de la forme

$$F(x) = \frac{a}{x} + \frac{bx+c}{(x^2+1)^3} + \frac{dx+e}{(x^2+1)^2} + \frac{fx+g}{x^2+1}$$

avec $a, b, c, d, e, f, g \in \mathbb{R}$.
Alors, a s'obtient simplement comme suit :

$$a = \left.\frac{4x^6 - 2x^5 + 11x^4 - x^3 + 11x^2 + 2x + 3}{(x^2+1)^3}\right|_{x=0} = 3$$

Maintenant, on effectue la soustraction suivante :

$$F_1(x) = F(x) - \frac{a}{x} = \frac{x^5 - 2x^4 + 2x^3 - x^2 + 2x + 2}{(x^2+1)^3}$$

Ainsi,

$$F_1(x) = \frac{bx+c}{(x^2+1)^3} + \frac{dx+e}{(x^2+1)^2} + \frac{fx+g}{x^2+1}.$$

On peut obtenir b et c en multipliant par $(x^2+1)^3$ puis en replaçant x par i ou par $-i$ (avec séparation des parties réelle et imaginaire). Mais cela est insuffisant pour conclure : il faut encore soustraire $\frac{bx+c}{(x^2+1)^3}$ puis simplifier par $(x^2+1)^2$ et enfin calculer d et e. De même pour calculer f et g. Cela entraîne beaucoup de calculs. Pour cela, on propose la méthode suivante :
La décomposition peut se faire par divisions euclidienne successives du numérateur $x^5 - 2x^4 + 2x^3 - x^2 + 2x + 2$ par x^2+1, puis du quotient obtenu par x^2+1 :

$$\frac{4x^6 - 2x^5 + 11x^4 - x^3 + 11x^2 + 2x + 3}{x(x^2+1)^3} = \frac{3}{x} + \frac{x+1}{(x^2+1)^3} + \frac{3}{(x^2+1)^2} + \frac{x-2}{x^2+1}.$$

- Calcul de la partie polaire relative à un pôle simple.

Si α est un pôle simple d'une fraction rationnelle $F = \frac{A}{B}$, alors le coefficient de la partie polaire relative à α est $\frac{A(\alpha)}{B'(\alpha)}$.

On applique cette méthode sur l'exemple 3.3.16.

Exemple 3.3.20
On considère la fraction rationnelle : $F(x) = \dfrac{x^2+x+1}{x(x-1)(x+1)}$. *Alors,* $F(x) = \dfrac{x^2+x+1}{x^3-x}$.
La DES de F *est de la forme*

$$F(x) = \frac{\lambda}{x} + \frac{\mu}{x-1} + \frac{\nu}{x+1}$$

On a $(x^3-x)' = 3x^2-1$. *Alors, en appliquant la règle ci-dessous, on obtient :* $\lambda = -1$, $\mu = 3/2$, *et* $\nu = 1/2$.

Exercice 3.3.21

On considère un entier $n \in \mathbb{N}^*$. Décomposer $\dfrac{1}{x^n-1}$ en éléments simples sur $\mathbb{C}$.

- Parité.

On suppose que F est une fraction rationnelle paire ou impaire. En comparant les DES de $F(x)$ et de $F(-x) = \pm F(x)$, et en utilisant "l'unicité" de la DES, on obtient des relations simples entre les coefficients.

Exemple 3.3.22

1. *On considère la fraction rationnelle* $F(x) = \dfrac{x^2+1}{(x-1)^2(x+1)^2}$.
   La DES de F *est de la forme :*

$$(*) \quad F(x) = \frac{a}{x-1} + \frac{b}{(x-1)^2} + \frac{c}{x+1} + \frac{d}{(x+1)^2}$$

   où $a, b, c, d \in \mathbb{R}$. *Il est claire que* F *est paire, alors on a :*

$$F(x) = F(-x) = \frac{-a}{x+1} + \frac{b}{(x+1)^2} + \frac{-c}{x-1} + \frac{d}{(x-1)^2}.$$

   Par unicité de la DES, on déduit que : $a = -c$ *et* $b = d$. *Par suite, il reste à déterminer que les deux inconnues* a *et* b. *On les détermine facilement comme suit :*

$$b = \left.\frac{x^2+1}{(x+1)^2}\right|_{x=1} = \frac{1}{2}$$

   Il reste à déterminer a. *Pour cela, on remplace* x *par* 0 *dans l'égalité* $(*)$, *ce qui donne l'équation :* $1 = -a+b+c+d = -2a+2b$. *D'où,*

$a = 0$.
Par suite, $F(x) = \dfrac{1/2}{(x-1)^2} + \dfrac{1/2}{(x+1)^2}$.

2. *On considère la fraction rationnelle* $G(x) = \dfrac{x}{(x-1)^2(x+1)^2}$.
La DES de G *est de la forme :*

$$(**) \quad G(x) = \frac{a}{x-1} + \frac{b}{(x-1)^2} + \frac{c}{x+1} + \frac{d}{(x+1)^2}$$

où $a, b, c, d \in \mathbb{R}$. *Il est claire que* G *est impaire, alors on a :*

$$G(x) = -G(-x) = \frac{a}{x+1} - \frac{b}{(x+1)^2} + \frac{c}{x-1} - \frac{d}{(x-1)^2}.$$

Par unicité de la DES, on déduit que : $a = c$ *et* $b = -d$. *Par suite, il reste à déterminer que les deux inconnues* a *et* b. *On les détermine facilement comme suit :*

$$b = \left.\frac{x}{(x+1)^2}\right|_{x=1} = \frac{1}{4}$$

Il reste à déterminer a. *On remarque que si on remplace* x *par* 0 *dans l'égalité* $(**)$, *on ne peut pas trouver une équation pour déterminer* a. *Alors, on remplace par d'autre nombre par exemple par* 2 *(ou aussi par* i*). On trouve aussi que* $a = c = 0$.
Par suite, $G(x) = \dfrac{1/4}{(x-1)^2} - \dfrac{1/4}{(x+1)^2}$.

Exercice 3.3.23

Décomposer les fractions rationnelles suivantes en éléments simples :
$\dfrac{x}{(x^4-1)^2}$ et $\dfrac{x^8}{x^6-1}$.

Réponse.

$$\frac{x}{(x^4-1)^2} = \frac{1/16}{(x-1)^2} - \frac{1/8}{(x-1)} - \frac{1/16}{(x+1)^2} - \frac{1/8}{(x+1)} + \frac{x/4}{(x^2+1)^2} + \frac{x/4}{x^2+1}$$

$$\frac{x^8}{x^6-1} = x^2 + \frac{1}{6}\left(\frac{1}{x-1} - \frac{1}{x+1} + \frac{2x+1}{x^2+x+1} - \frac{2x-1}{x^2-x+1}\right). \qquad \textbf{(c.q.f.d)}$$

Exercice 3.3.24

Décomposer en éléments simples les fracions rationnelles suivantes :
$F_1 = \dfrac{11x^2 - 5x - 10}{5x^3 - 5x^2}$ (sur $\mathbb{R}$) ; $F_2 = \dfrac{-2x^2 + 20x - 68}{(x+4)(x^2+4)}$ (sur $\mathbb{R}$ et $\mathbb{C}$) ;
$F_3 = \dfrac{5x^4 - 34x^3 + 70x^2 - 33x - 19}{(x-3)^2}$ (sur $\mathbb{R}$) ;
$F_4 = \dfrac{-10x^4 + X^3 - 19x^2 + x - 10}{x^5 + 2x^3 + X}$ (sur $\mathbb{R}$ et $\mathbb{C}$) ;
$F_5 = \dfrac{1}{(x^4-1)^2}$ (sur $\mathbb{R}$) ; $F_6(X) = \dfrac{4x^3}{x^4 - 1}$ (sur $\mathbb{R}$ et $\mathbb{C}$).

Exercice 3.3.25

Décomposer le polynôme $X^4 + 1$ dans $\mathbb{C}$ puis dans $\mathbb{R}$ et en déduire une décomposition de $F = \dfrac{1}{x^4+1}$ en éléments simples sur $\mathbb{R}$.

Exercice 3.3.26

Pour un entier $n > 0$, on considère un polynôme scindé $P = \lambda(x - a_1)^{m_1}(x - a_2)^{m_2} \cdots (x - a_n)^{m_n}$ avec $\lambda \in \mathbb{C}^*$ et $(a_i, m_i) \in \mathbb{C} \times \mathbb{N}^*$ pour $i = 1, ..., n$.
Montrer que $\dfrac{P'}{P} = \dfrac{m_1}{x - a_1} + \cdots + \dfrac{m_n}{x - a_n}$.

Exercice 3.3.27

On considère un entier $n > 0$.

1. Montrer que $\dfrac{n!}{x(x+1)\cdots(x+n)} = \displaystyle\sum_{k=0}^{n} \frac{(-1)^k C_n^k}{x+k}$.
2. Montrer que $\dfrac{1}{x^n - 1} = \dfrac{1}{n} \displaystyle\sum_{k=0}^{n-1} \frac{e^{\frac{2ik\pi}{n}}}{x - e^{\frac{2ik\pi}{n}}}$.