北航中法工程师学院
Centrale Pékin

Géométrie 2

École Centrale de Pékin

Cours de mathématiques du cycle préparatoire

6 juin 2021

Table des matières

Chapitre 1 Espaces vectoriels

De nombreux problèmes de mathématiques ou de physique vérifient la propriété suivante : si u et v sont deux solutions d'un problème alors $u+v$ est aussi solution de ce problème, ainsi que ku, k étant un nombre réel ou complexe. Ces problèmes sont dit linéaires et sont souvent plus faciles à résoudre que les problèmes plus généraux, dits non linéaires. Ce chapitre est le premier chapitre d'algèbre linéaire.

Dans tout ce chapitre, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$. Tous les résultats présentés demeurent vrais sur un corps quelconque.

1.1 Structure d'espace vectoriel

1.1.1 Premières définitions

Définition 1
On appelle ***espace vectoriel sur*** $\mathbb{K}$ \域𝕂上的线性空间 / 向量空间\, *ou* $\mathbb{K}$***-espace vectoriel****, tout triplet* $(E,+,\cdot)$ *où* E *est un ensemble et*

- $+$ *est une loi de composition interne sur* E *:* $E\times E\longrightarrow E$; $(\vec{x},\vec{y})\longmapsto \vec{x}+\vec{y}$,
- $\cdot$ *est une loi de composition externe de* $\mathbb{K}$ *sur* E *:* $\mathbb{K}\times E\longrightarrow E$; $(\lambda,\vec{x})\longmapsto \lambda\cdot\vec{x}$,

vérifiant les propriétés suivantes :

1. $(E,+)$ *est un groupe abélien,*
2. *pour tout* $(\lambda,\mu)\in\mathbb{K}^2$ *et tout* $(\vec{x},\vec{y})\in E^2$,
   (a) $\lambda\cdot(\vec{x}+\vec{y})=\lambda\cdot\vec{x}+\lambda\cdot\vec{y}$,
   (b) $(\lambda+\mu)\cdot\vec{x}=\lambda\cdot\vec{x}+\mu\cdot\vec{x}$,
   (c) $(\lambda\mu)\cdot\vec{x}=\lambda\cdot(\mu\cdot\vec{x})$,
   (d) $1\cdot\vec{x}=\vec{x}$.

Remarque 2 — *Souvent, on parle du* $\mathbb{K}$*-espace vectoriel* E *à la place du* $\mathbb{K}$*-espace vectoriel* $(E,+,\cdot)$*. S'il n'y a pas d'ambiguïté, on ne précise pas nécessairement le corps* $\mathbb{K}$*.*

Définition 3
Soit $(E,+,\cdot)$ *un* $\mathbb{K}$*-espace vectoriel.*

- *Les éléments de l'espace vectoriel* E *sont appelés les* ***vecteurs*** \向量\.
- *Les éléments de* $\mathbb{K}$ *sont appelés les* ***scalaires*** \标量\.
- *La loi* $+$ *est appelée* ***addition****.*
- *La loi* $\cdot$ *est appelée* ***multiplication par un scalaire****.*
- *L'élément neutre du groupe* $(E,+)$ *est noté* $\vec{0}_E$ *ou* $\vec{0}$ *et est appelé le* ***vecteur nul*** *de* E*.*

 Il ne faut pas confondre le vecteur nul $\vec{0}_E$ de E et le scalaire nul 0 de $\mathbb{K}$.

Remarque 4 — *La notation* $\lambda\cdot\vec{x}$ *est souvent remplacée par* $\lambda\vec{x}$*. Mais on n'écrit pas* $\vec{x}\lambda$*. Les flèches sur les vecteurs de* E *sont également souvent omises : on note* x *à la place de* $\vec{x}$*.*

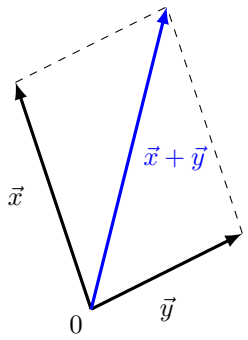
Les règles que nous venons de définir sont celles que l'on connait déjà sur les vecteurs du plan et de l'espace : en considérant deux vecteurs $\vec{x}$ et $\vec{y}$, on peut

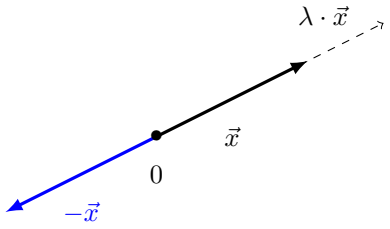
- sommer ces vecteurs : $\vec{x}+\vec{y}$,
- faire la différence de ces vecteurs : $\vec{x}-\vec{y}$,

- multiplier $\vec{x}$ par un scalaire λ : $\lambda \cdot \vec{x}$,
- calculer des expressions de la forme $\sum_{i=1}^{n} \lambda_i \cdot \vec{x}_i$, où pour tout $i \in \{1, \dots, n\}$, $\vec{x}_i \in E$ et $\lambda_i \in \mathbb{K}$.

Par contre, la multiplication de deux vecteurs n'est pas définie.

Nous pourrons nous représenter les espaces vectoriels à l'aide d'un modèle géométrique qui pourra nous aider à visualiser les problèmes. Il faudra alors considérer des vecteurs ayant tous la même origine, ce point jouant le rôle du vecteur nul.





1.1.2 Premiers exemples fondamentaux

Nous donnons des exemples fondamentaux d'espaces vectoriels. Les vérifications sont faciles mais longues.

1.1.2.a. L'ensemble $\mathbb{K}^n$

• Soient $n \in \mathbb{N}^*$ et $E = \mathbb{R}^n$. On munit $\mathbb{R}^n$ des lois suivantes :

Pour tout $\vec{x} = (x_1, \dots, x_n)$ et tout $\vec{y} = (y_1, \dots, y_n)$ éléments de $\mathbb{R}^n$ et pour tout $\lambda \in \mathbb{R}$,

- $\vec{x} + \vec{y} = (x_1 + y_1, \dots, x_n + y_n)$,
- $\lambda \cdot \vec{x} = (\lambda x_1, \dots, \lambda x_n)$.

Alors $(\mathbb{R}^n, +, \cdot)$ est un $\mathbb{R}$-espace vectoriel.

Preuve —

1. $(\mathbb{R}, +)$ est un groupe abélien, donc $(\mathbb{R}^n, +)$ l'est aussi.
2. (a) Soient $\vec{x} = (x_1, \dots, x_n)$ et $\vec{y} = (y_1, \dots, y_n)$ des éléments de $\mathbb{R}^n$, et $\lambda \in \mathbb{R}$. On a
$$\begin{aligned}\lambda \cdot (\vec{x} + \vec{y}) &= \lambda \cdot (x_1 + y_1, \dots, x_n + y_n) \\ &= (\lambda(x_1 + y_1), \dots, \lambda(x_n + y_n)) \\ &= (\lambda x_1 + \lambda y_1, \dots, \lambda x_n + \lambda y_n) \\ &= (\lambda x_1, \dots, \lambda x_n) + (\lambda y_1, \dots, \lambda y_n) \\ &= \lambda \cdot \vec{x} + \lambda \cdot \vec{y}.\end{aligned}$$
(b) Soient $\vec{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$, et $(\lambda, \mu) \in \mathbb{R}^2$. On a
$$\begin{aligned}(\lambda + \mu) \cdot \vec{x} &= ((\lambda + \mu)x_1, \dots, (\lambda + \mu)x_n) \\ &= (\lambda x_1 + \mu x_1, \dots, \lambda x_n + \mu x_n) \\ &= (\lambda x_1, \dots, \lambda x_n) + (\mu x_1, \dots, \mu x_n) \\ &= \lambda \cdot \vec{x} + \mu \cdot \vec{x}.\end{aligned}$$
(c) Soient $\vec{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$, et λ et μ des éléments de $\mathbb{R}$. On a
$(\lambda\mu) \cdot \vec{x} = ((\lambda\mu)x_1, \dots, (\lambda\mu)x_n) = (\lambda(\mu x_1), \dots, \lambda(\mu x_n)) = \lambda \cdot (\mu x_1, \dots, \mu x_n) = \lambda \cdot (\mu \cdot (x_1, \dots, x_n)) = \lambda \cdot (\mu \cdot \vec{x})$,
(d) Soit $\vec{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$. On a $1 \cdot \vec{x} = (1x_1, \dots, 1x_n) = (x_1, \dots, x_n) = \vec{x}$.

□

Notons qu'un vecteur de $\mathbb{R}^n$ est un n-uplet $(x_1, \dots, x_n)$ où pour tout $i \in \{1, \dots, n\}$, $x_i \in \mathbb{R}$.

Le vecteur nul de $\mathbb{R}^n$ est $\vec{0}_{\mathbb{R}^n} = (0, \dots, 0)$.

En particulier, $(\mathbb{R}, +, \cdot)$ est un $\mathbb{R}$-espace vectoriel. Un vecteur est alors un réel et $\lambda \cdot \vec{x} = \lambda \times x$, multiplication entre deux réels.

On retrouve les vecteurs du plan avec $\mathbb{R}^2$ et les vecteurs de l'espace avec $\mathbb{R}^3$.

Exemple 5 — *Dans* $\mathbb{R}^3$, $(1,2,0)+2\cdot(0,1,1)=(1,4,2)$.

• De même, $(\mathbb{C}^n,+,\cdot)$ est un $\mathbb{C}$-espace vectoriel, mais aussi un $\mathbb{R}$-espace vectoriel.

En particulier, $(\mathbb{C},+,\cdot)$ est un $\mathbb{R}$-espace vectoriel. Les vecteurs sont les nombres complexes et les scalaires sont les nombres réels. On a $\lambda\cdot\vec{x}=\lambda\times x$, multiplication entre un réel et un complexe.

Remarque 6 — *Plus généralement, tout espace vectoriel sur* $\mathbb{C}$ *est aussi un espace vectoriel sur* $\mathbb{R}$.

1.1.2.b. L'ensemble des polynômes

• Soient $n\in\mathbb{N}^*$ et $E=\mathbb{R}_n[X]$, l'ensemble des polynômes à coefficients dans $\mathbb{R}$ de degré inférieur ou égal à n. On munit $\mathbb{R}_n[X]$ des lois suivantes :

Pour tout $P=a_0+a_1X+\ldots+a_nX^n$ et $Q=b_0+b_1X+\ldots+b_nX^n$ éléments de $\mathbb{R}_n[X]$ et tout $\lambda\in\mathbb{R}$,

- $P+Q=(a_0+b_0)+(a_1+b_1)X+\ldots+(a_n+b_n)X^n$,
- $\lambda\cdot P=\lambda a_0+\lambda a_1X+\ldots+\lambda a_nX^n$.

Alors $(\mathbb{R}_n[X],+,\cdot)$ est un $\mathbb{R}$-espace vectoriel.

Preuve — Exercice. □

Notons qu'un vecteur de $\mathbb{R}_n[X]$ est un polynôme P qui s'écrit sous la forme $P=a_0+a_1X+\ldots+a_nX^n$, où pour tout $i\in\{1,\ldots,n\}$, $a_i\in\mathbb{R}$.

Le vecteur nul de $\mathbb{R}_n[X]$ est $\vec{0}_{\mathbb{R}^n[X]}=0$, le polynôme nul.

• De même $(\mathbb{C}_n[X],+,\cdot)$ est un $\mathbb{C}$-espace vectoriel, mais aussi un $\mathbb{R}$-espace vectoriel.

• Plus généralement, $(\mathbb{K}[X],+,\cdot)$, l'ensemble des polynômes à coefficients dans $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel, où $+$ et $\cdot$ sont les opérations usuelles sur les polynômes.

Exemple 7 — *Dans* $\mathbb{R}_2[X]$, $1+X+X^2-2(X-X^2)=1-X+3X^2$.

1.1.2.c. L'ensemble des matrices

• Soit $E=\mathcal{M}_2(\mathbb{K})$, l'ensemble des matrices carrées d'ordre 2 à coefficients dans $\mathbb{K}$. On munit $\mathcal{M}_2(\mathbb{K})$ des lois suivantes :

Pour tout $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ et tout $B=\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}$ éléments de $\mathcal{M}_2(\mathbb{K})$ et pour tout $\lambda\in\mathbb{K}$,

- $A+B=\begin{pmatrix}a+a'&b+b'\\c+c'&d+d'\end{pmatrix}$,
- $\lambda\cdot A=\begin{pmatrix}\lambda a&\lambda b\\\lambda c&\lambda d\end{pmatrix}$.

Alors $(\mathcal{M}_2(\mathbb{K}),+,\cdot)$ est un $\mathbb{K}$-espace vectoriel.

Preuve — Exercice. □

Notons qu'un vecteur de $\mathcal{M}_2(\mathbb{K})$ est une matrice $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$.

Le vecteur nul de $\mathcal{M}_2(\mathbb{K})$ est $\vec{0}_{\mathcal{M}_2(\mathbb{K})}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$.

Exemple 8 — *Dans* $\mathcal{M}_2(\mathbb{R})$, $2\cdot\begin{pmatrix}1&1\\-1&1\end{pmatrix}-\begin{pmatrix}2&1\\-1&2\end{pmatrix}=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$.

• Plus généralement, pour tout $(n,m)\in(\mathbb{N}^*)^2$, $(\mathcal{M}_{n,m}(\mathbb{K}),+,\cdot)$ est un $\mathbb{K}$-espace vectoriel (voir cours d'algèbre 2), où $+$ et $\cdot$ sont les opérations usuelles sur les matrices.

1.1.2.d. L'ensemble des suites

Soit $E = \mathbb{K}^{\mathbb{N}}$, l'ensemble des suites à valeurs dans $\mathbb{K}$. On munit $\mathbb{K}^{\mathbb{N}}$ des lois suivantes :

Pour tout $(u_n)_{n\in\mathbb{N}}$ et tout $(v_n)_{n\in\mathbb{N}}$ éléments de $\mathbb{K}^n$ et pour tout $\lambda \in \mathbb{K}$,

* $(u_n)_{n\in\mathbb{N}} + (v_n)_{n\in\mathbb{N}} = (u_n + v_n)_{n\in\mathbb{N}}$,
* $\lambda \cdot (u_n)_{n\in\mathbb{N}} = (\lambda u_n)_{n\in\mathbb{N}}$.

Alors $(\mathbb{K}^{\mathbb{N}}, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

Preuve — Exercice. □

Le vecteur nul de $\mathbb{K}^{\mathbb{N}}$ est la suite nulle $(0)_{n\in\mathbb{N}}$.

1.1.2.e. Le produit d'espaces vectoriels

Soient E_1, ..., E_n des $\mathbb{K}$-espaces vectoriels. Posons $E = E_1 \times \ldots \times E_n$, le produit cartésien de E_1, ..., E_n. On munit E des lois suivantes :

Pour tout $\vec{x} = (\vec{x}_1, \ldots, \vec{x}_n)$ et tout $\vec{y} = (\vec{y}_1, \ldots, \vec{y}_n)$ éléments de E et pour tout $\lambda \in \mathbb{K}$,

* $\vec{x} + \vec{y} = (\vec{x}_1 + \vec{y}_1, \ldots, \vec{x}_n + \vec{y}_n)$,
* $\lambda \cdot \vec{x} = (\lambda \cdot \vec{x}_1, \ldots, \lambda \cdot \vec{x}_n)$.

Alors $(E_1 \times \ldots \times E_n, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel. On l'appelle l'**espace vectoriel produit** \积空间\.

Preuve —La preuve est proche de celle faite pour $\mathbb{R}^n = \mathbb{R} \times \ldots \times \mathbb{R}$. Vérifions seulement deux points de la définition.

• Pour tout $\vec{x} = (\vec{x}_1, \ldots, \vec{x}_n) \in E$, $1 \cdot (\vec{x}_1, \ldots, \vec{x}_n) = (1 \cdot \vec{x}_1, \ldots, 1 \cdot \vec{x}_n) = (\vec{x}_1, \ldots, \vec{x}_n) = \vec{x}$.

• Pour tout $\vec{x} = (\vec{x}_1, \ldots, \vec{x}_n)$ et $\vec{y} = (\vec{y}_1, \ldots, \vec{y}_n)$ éléments de E, et pour tout $\lambda \in \mathbb{K}$,

$$\begin{aligned}
\lambda \cdot (\vec{x} + \vec{y}) &= \lambda \cdot (\vec{x}_1 + \vec{y}_1, \ldots, \vec{x}_n + \vec{y}_n) \\
&= (\lambda \cdot (\vec{x}_1 + \vec{y}_1), \ldots, \lambda \cdot (\vec{x}_n + \vec{y}_n)) \\
&= (\lambda \cdot \vec{x}_1 + \lambda \cdot \vec{y}_1, \ldots, \lambda \cdot \vec{x}_n + \lambda \cdot \vec{y}_n) \\
&= (\lambda \cdot \vec{x}_1, \ldots, \lambda \cdot \vec{x}_n) + (\lambda \cdot \vec{y}_1, \ldots, \lambda \cdot \vec{y}_n) \\
&= \lambda \cdot (\vec{x}_1, \ldots, \vec{x}_n) + \lambda \cdot (\vec{y}_1, \ldots, \vec{y}_n) \\
&= \lambda \cdot \vec{x} + \lambda \cdot \vec{y}.
\end{aligned}$$

□

Le vecteur nul de $E_1 \times \ldots E_n$ est $\vec{0}_{E_1 \times \ldots \times E_n} = (\vec{0}_{E_1}, \ldots, \vec{0}_{E_n})$.

Remarque 9 — *Ainsi, on retrouve que, pour tout $n \in \mathbb{N}^*$, $\mathbb{K}^n = \mathbb{K} \times \ldots \times \mathbb{K}$ est un $\mathbb{K}$-espace vectoriel .*

1.1.2.f. L'ensemble des applications de X dans E

Soient X un ensemble non vide et E un $\mathbb{K}$-espace vectoriel. On munit l'ensemble $\mathcal{F}(X, E)$ des applications de X dans E des lois suivantes :

Pour tout f et tout g éléments de $\mathcal{F}(X, E)$ et pour tout $\lambda \in \mathbb{K}$,

* $f + g$ est l'application de X dans E définie, pour tout $x \in X$, par

$$(f + g)(x) = f(x) + g(x),$$

* $\lambda \cdot f$ est l'application de X dans E définie, pour tout $x \in X$, par

$$(\lambda \cdot f)(x) = \lambda \cdot (f(x)).$$

Alors $(\mathcal{F}(X, E), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

Preuve — Démontrons seulement deux points de la définition.

Soient f et g des éléments de $\mathcal{F}(X, E)$ et $\lambda \in \mathbb{K}$.

• On a $1 \cdot f = f$. En effet, pour tout $x \in X$, $(1 \cdot f)(x) = 1 \cdot (f(x)) = f(x)$.

• On a $\lambda \cdot (f+g) = \lambda \cdot f + \lambda \cdot g$. En effet, pour tout $x \in X$,

$$\begin{aligned}(\lambda \cdot (f+g))(x) &= \lambda \cdot ((f+g)(x)) \\ &= \lambda \cdot (f(x) + g(x)) \\ &= \lambda \cdot (f(x)) + \lambda \cdot (g(x)) \\ &= (\lambda \cdot f)(x) + (\lambda \cdot g)(x) \\ &= (\lambda \cdot f + \lambda \cdot g)(x).\end{aligned}$$

□

Le vecteur nul de $\mathcal{F}(X,E)$, $\vec{0}_{\mathcal{F}(X,E)}$, est l'application nulle : $X \longrightarrow E$; $x \longmapsto \vec{0}_E$.

EXEMPLE 10 — *Pour tout intervalle I de $\mathbb{R}$, l'ensemble $\mathcal{F}(I,\mathbb{R})$ des fonctions de I dans $\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel pour l'addition des fonctions et leur multiplication par un réel. Il s'agit du cas particulier où $X = I$ et $E = \mathbb{R}$.*

EXEMPLE 11 — *Prenons $X = \mathbb{R}$ et $E = \mathbb{R}^2$. Soient f et g éléments de $\mathcal{F}(\mathbb{R},\mathbb{R}^2)$ définies, pour tout $x \in \mathbb{R}$, par*

$$f(x) = (1+x, x^2) \quad \text{et} \quad g(x) = (\exp(x), -x).$$

Alors $f+g$ est l'application définie pour tout $x \in \mathbb{R}$ par

$$(f+g)(x) = (x + 1 + \exp(x), x^2 - x).$$

REMARQUE 12 — *On retrouve que l'ensemble $\mathbb{K}^{\mathbb{N}} = \mathcal{F}(\mathbb{N},\mathbb{K})$ des suites à valeurs dans $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel pour l'addition des suites et leur multiplication par un élément de $\mathbb{K}$.*

1.1.3 Quelques règles de calcul

PROPOSITION 13
Soit E un $\mathbb{K}$-espace vectoriel. Pour tout $\vec{x} \in E$ et tout $\lambda \in \mathbb{K}$,

- $0 \cdot \vec{x} = \vec{0}_E$.
- $\lambda \cdot \vec{0}_E = \vec{0}_E$,
- $\lambda \cdot \vec{x} = \vec{0}_E$ *si et seulement si* $\lambda = 0$ *ou* $\vec{x} = \vec{0}_E$.
- $\overrightarrow{-x} = (-1) \cdot \vec{x}$, *où* $\overrightarrow{-x}$ *est l'opposé de* $\vec{x}$ *dans le groupe* $(E,+)$ *et* -1 *est l'opposé de* 1 *dans le groupe* $(\mathbb{K},+)$.

Preuve — Soient $\vec{x} \in E$ et $\lambda \in \mathbb{K}$.

- On a $0 \cdot \vec{x} = (0+0) \cdot \vec{x} = 0 \cdot \vec{x} + 0 \cdot \vec{x}$.
  Donc, par simplification dans le groupe $(E,+)$, $0 \cdot \vec{x} = \vec{0}_E$.
- On a $\lambda \cdot \vec{0}_E = \lambda \cdot (\vec{0}_E + \vec{0}_E) = \lambda \cdot \vec{0}_E + \lambda \cdot \vec{0}_E$.
  Donc, par simplification dans le groupe $(E,+)$, $\lambda \cdot \vec{0}_E = \vec{0}_E$.
- D'après les points précédents, si $\lambda = 0$ ou $\vec{x} = \vec{0}_E$ alors $\lambda \cdot \vec{x} = \vec{0}_E$.
  Réciproquement, supposons que $\lambda \cdot \vec{x} = \vec{0}_E$.
  1er cas : $\lambda = 0$.
  2nd cas : $\lambda \neq 0$. Alors $\vec{x} = 1 \cdot \vec{x} = \left(\frac{1}{\lambda} \times \lambda\right) \cdot x = \frac{1}{\lambda} \cdot (\lambda \cdot \vec{x}) = \frac{1}{\lambda} \cdot \vec{0}_E = \overrightarrow{0}_E$.
  D'où le résultat.
- On a $\vec{x} + (-1) \cdot \vec{x} = 1 \cdot \vec{x} + (-1) \cdot \vec{x} = (1-1) \cdot \vec{x} = 0 \cdot \vec{x} = \vec{0}_E$.
  Donc $\overrightarrow{-x} = (-1) \cdot \vec{x}$.

□

PROPOSITION 14
Soit E un $\mathbb{K}$-espace vectoriel.

- *Pour tout $\vec{x} \in E$ et tous $\lambda_1, \ldots, \lambda_n$ éléments de $\mathbb{K}$,*

$$\sum_{i=1}^{n} (\lambda_i \cdot \vec{x}) = \left(\sum_{i=1}^{n} \lambda_i\right) \cdot \vec{x}.$$

- *Pour tous $\vec{x}_1, \ldots, \vec{x}_n$ éléments de E, et tout $\lambda \in \mathbb{K}$,*

$$\sum_{i=1}^{n} (\lambda \cdot \vec{x}_i) = \lambda \cdot \left(\sum_{i=1}^{n} \vec{x}_i \right).$$

Preuve — Ces deux propriétés se démontrent par récurrence en utilisant les points suivants de la définition d'un espace vectoriel :

- $\lambda \cdot \vec{x} + \mu \cdot \vec{x} = (\lambda + \mu) \cdot \vec{x}$,
- $\lambda \cdot \vec{x} + \lambda \cdot \vec{y} = \lambda \cdot (\vec{x} + \vec{y})$.

□

1.1.4 Combinaisons linéaires

Définition 15
Soit E un $\mathbb{K}$-espace vectoriel. Soient $\vec{x}_1, \ldots, \vec{x}_n$ des éléments de E. Soit $\vec{x} \in E$.

*On dit que $\vec{x}$ est **combinaison linéaire** \线性组合\ des vecteurs $\vec{x}_1$, …, $\vec{x}_n$ si $\vec{x}$ s'écrit sous la forme*

$$\vec{x} = \sum_{i=1}^{n} \lambda_i \cdot \vec{x}_i = \lambda_1 \cdot \vec{x}_1 + \ldots + \lambda_n \cdot \vec{x}_n,$$

où λ_1, …, λ_n sont des éléments de $\mathbb{K}$.

Remarques 16

- *Une combinaison linéaire d'un seul vecteur $\vec{x}$ est donc un vecteur de la forme $\lambda \cdot \vec{x}$, où $\lambda \in \mathbb{K}$.*
- *Une combinaison linéaire de deux vecteurs $\vec{x}$ et $\vec{y}$ est donc un vecteur de la forme $\lambda \cdot \vec{x} + \mu \cdot \vec{y}$ où $(\lambda, \mu) \in \mathbb{K}^2$.*

Exemples 17

- *Dans $\mathbb{R}_3[X]$, le polynôme $2 + X - 3X^3$ est, par exemple, combinaison linéaire des polynômes 1, X et X^3 avec $\lambda_1 = 2$, $\lambda_2 = 1$ et $\lambda_3 = -3$.*
- *Plus généralement, tout polynôme de $\mathbb{K}_n[X]$ s'écrit comme combinaison linéaire des polynômes 1, X, …, X^n.*
- *Dans $\mathbb{R}^2$, le vecteur $(2, 7)$ est combinaison linéaire des vecteurs $(5, -2)$ et $(1, -3)$:*

$$(2, 7) = (5, -2) - 3(1, -3).$$

Pour trouver cette combinaison linéaire, on cherche des réels λ et μ tels que

$$(2, 7) = \lambda(5, -2) + \mu(1, -3).$$

Cela revient à résoudre le système

$$\begin{cases} 2 = 5\lambda + \mu \\ 7 = -2\lambda - 3\mu \end{cases}.$$

- *Dans $\mathcal{M}_2(\mathbb{K})$, la matrice $M = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ n'est pas combinaison linéaire des matrices $M_1 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, $M_2 = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}$ et $M_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.*

En effet, M est combinaison linéaire de ces matrices si et seulement s'il existe $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$ tel que $M = \lambda_1 M_1 + \lambda_2 M_2 + \lambda_3 M_3$, soit encore si et seulement s'il existe $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$ tel que

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \lambda_1 + \lambda_2 & -\lambda_2 \\ \lambda_1 & \lambda_3 \end{pmatrix},$$

soit finalement, si et seulement si le système suivant admet une solution :

$$\begin{cases} \lambda_1 + \lambda_2 = 2 \\ -\lambda_2 = 1 \\ \lambda_1 = 1 \\ \lambda_3 = 0 \end{cases}.$$

Or ce système n'admet pas de solutions. D'où le résultat.

En général, l'égalité $\sum_{i=1}^{n} \lambda_i \cdot \vec{x}_i = \sum_{i=1}^{n} \mu_i \cdot \vec{x}_i$ n'implique pas que pour tout $i \in \{1, \dots, n\}$, $\lambda_i = \mu_i$.

Exemple 18 — *Dans $\mathbb{R}^2$, le vecteur $(3,3)$ peut s'écrire comme combinaison linéaire des vecteurs $(1,1)$, $(0,1)$ et $(1,0)$ mais il n'y a pas unicité des λ_i :*

$$\begin{aligned}(3,3) &= 1 \cdot (1,1) + 2 \cdot (0,1) + 2 \cdot (1,0) \\ &= 2 \cdot (1,1) + 1 \cdot (0,1) + 1 \cdot (1,0).\end{aligned}$$

Définition 19
*Soit E un $\mathbb{K}$-espace vectoriel. Soit $(\vec{x}_i)_{i \in I}$ une famille d'éléments de E indicée par I. Soit $\vec{x} \in E$. On dit que $\vec{x}$ est **combinaison linéaire** de la famille $(\vec{x}_i)_{i \in I}$ si $\vec{x}$ est combinaison linéaire d'une sous-famille **finie** $(\vec{x}_{i_1}, \dots, \vec{x}_{i_p})$, c'est-à-dire $\vec{x}$ s'écrit sous la forme*

$$\vec{x} = \sum_{i=1}^{p} \lambda_{i_p} \cdot \vec{x}_{i_p},$$

où $\lambda_{i_1}, \dots, \lambda_{i_p} \in \mathbb{K}$.

Exemple 20 — *Tout polynôme de $\mathbb{K}[X]$ est combinaison linéaire finie de la famille $(X^n)_{n \in \mathbb{N}}$.*

1.2 Sous-espace vectoriel

Dans cette partie, $(E, +, \cdot)$ désigne un $\mathbb{K}$-espace vectoriel.

1.2.1 Définition

Définition 21
*Soit F une partie non vide de E. On dit que F est un **sous-espace vectoriel de** E \子空\ si F est stable par les lois $+$ et $\cdot$ (c'est-à-dire, $F + F \subset F$ et $\mathbb{K} \cdot F \subset F$) et si F est un $\mathbb{K}$-espace vectoriel pour les lois $+$ et $\cdot$ induites sur F.*

Remarque 22 — *Si F est un sous-espace vectoriel de E alors F est un sous-groupe de $(E, +)$, donc $\vec{0}_F = \vec{0}_E \in F$. Un sous-espace vectoriel contient donc toujours le vecteur nul.*

Exemple 23 — *Les ensembles $\{\vec{0}_E\}$ et E sont des sous-espaces vectoriels de E, dits **triviaux**.*

Le résultat suivant est celui que l'on utilise majoritairement pour montrer qu'une partie F d'un espace vectoriel E est un sous-espace vectoriel de E. Il évite de vérifier les nombreux points de la définition d'un espace vectoriel.

PROPOSITION 24 (Caractérisation)
Un ensemble F est un sous-espace vectoriel de E si et seulement si

1. $F \subset E$,
2. $\vec{0}_E \in F$,
3. F *est stable par combinaison linéaire* \对线性组合是封闭的\ *: pour tout* $(\vec{x}, \vec{y}) \in F^2$ *et tout* $\lambda \in \mathbb{K}$,

$$\lambda \cdot \vec{x} + \vec{y} \in F.$$

Preuve — ▷ Soit F un sous-espace vectoriel de E.

Alors, par définition $F \subset E$.

D'après la remarque précédente, F étant un sous-groupe de $(E, +)$, $\vec{0}_E \in F$.

Soient $(\vec{x}, \vec{y}) \in F^2$ et $\lambda \in \mathbb{K}$. F étant stable par la loi $\cdot$, $\lambda \cdot \vec{x} \in F$. F étant stable par la loi $+$, $\lambda \cdot \vec{x} + \vec{y} \in F$.

D'où les trois points de la caractérisation.

◁ Réciproquement, supposons les points 1, 2 et 3 vérifiés.

F est une partie non vide de E puisque $F \subset E$ et $\vec{0}_E \in F$. Pour tout $(\vec{x}, \vec{y}) \in F^2$, $\vec{x} - \vec{y} = \vec{x} + (-1) \cdot \vec{y} \in F$ d'après le point 3. Donc F est un sous-groupe de $(E, +)$. $(E, +)$ étant commutatif, $(F, +)$ l'est aussi.

Les autres points de la définition d'un espace vectoriel sont vérifiés car ils le sont pour les éléments de E donc *a fortiori* pour les éléments de F.

D'où le résultat. □

REMARQUE 25 — *Pour montrer qu'un ensemble F muni d'une addition et d'une multiplication par un scalaire est un espace vectoriel, on peut montrer que c'est un sous-espace vectoriel d'un espace vectoriel connu (voir les exemples de la partie 1.1.2). On prendra garde à ne pas oublier de préciser quel est cet espace vectoriel plus grand.*

REMARQUE 26 — *Le point 3 peut être séparé en deux points :*

3.1. Pour tout $(\vec{x}, \vec{y}) \in F^2$, $\vec{x} + \vec{y} \in F$

3.2. Pour tout $\vec{x} \in F$ *et tout* $\lambda \in \mathbb{K}$, $\lambda \cdot \vec{x} \in F$.

Preuve — ▷ Supposons que pour tout $(\vec{x}, \vec{y}) \in F^2$ et tout $\lambda \in \mathbb{K}$, $\lambda \cdot \vec{x} + \vec{y} \in F$.

Soit $(\vec{x}, \vec{y}) \in F^2$. Alors $\vec{x} + \vec{y} = 1 \cdot \vec{x} + \vec{y} \in F$.

Soient $\vec{x} \in F$ et $\lambda \in \mathbb{K}$. Alors $\lambda \cdot \vec{x} = \lambda \cdot \vec{x} + \vec{0}_E \in E$ puisque $\vec{0}_E \in F$.

◁ Réciproquement, supposons les deux points vérifiés. Soient $(\vec{x}, \vec{y}) \in F^2$ et $\lambda \in \mathbb{K}$. Alors $\lambda \cdot \vec{x} \in F$. Puis comme $(\lambda \cdot \vec{x}, \vec{y}) \in F^2$, $\lambda \cdot \vec{x} + \vec{y} \in F$

D'où le résultat. □

EXEMPLES 27

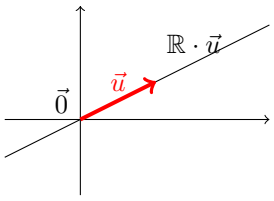
- *Soit* $\vec{u}$ *un vecteur de* $\mathbb{R}^2$. *L'ensemble* $\mathbb{R} \cdot \vec{u} = \{\lambda \cdot \vec{u} \mid \lambda \in \mathbb{R}\}$ *est un sous-espace vectoriel de l'espace vectoriel* $\mathbb{R}^2$, *appelé la* ***droite vectorielle engendrée par*** $\vec{u}$.
  Preuve —
  1. *Pour tout* $\lambda \in \mathbb{R}$, $\lambda \cdot \vec{u} \in \mathbb{R}^2$ *donc* $\mathbb{R} \cdot \vec{u} \subset \mathbb{R}^2$.
  2. $\vec{0}_{\mathbb{R}^2} = (0, 0) = 0 \cdot \vec{u} \in \mathbb{R} \cdot \vec{u}$.
  3. *Soient* $(\vec{x}, \vec{y})$ *des éléments de* $\mathbb{R} \cdot \vec{u}$ *et* $\lambda \in \mathbb{R}$.
     Comme $\vec{x} \in \mathbb{R} \cdot \vec{u}$, *il existe* $\lambda_1 \in \mathbb{R}$ *tel que* $\vec{x} = \lambda_1 \cdot \vec{u}$.
     Comme $\vec{y} \in \mathbb{R} \cdot \vec{u}$, *il existe* $\lambda_2 \in \mathbb{R}$ *tel que* $\vec{y} = \lambda_2 \cdot \vec{u}$.
     Donc

$$\begin{aligned} \lambda \cdot \vec{x} + \vec{y} &= \lambda \cdot (\lambda_1 \cdot \vec{u}) + \lambda_2 \cdot \vec{u} \\ &= (\lambda\lambda_1) \cdot \vec{u} + \lambda_2 \cdot \vec{u} \\ &= (\lambda\lambda_1 + \lambda_2) \cdot \vec{u}. \end{aligned}$$

     Donc $\lambda \cdot \vec{x} + \vec{y} \in \mathbb{R} \cdot \vec{u}$.

  De ces trois points, on en déduit que $\mathbb{R} \cdot \vec{u}$ *est un sous-espace vectoriel de* $\mathbb{R}^2$. □

  En particulier, toute droite de $\mathbb{R}^2$ *passant par* $(0, 0)$ *est un sous-espace vectoriel de* $\mathbb{R}^2$.



- *Soient a, b et c trois réels. Le plan $\mathcal{P}$ de $\mathbb{R}^3$ d'équation $ax+by+cz=0$ est un sous-espace vectoriel de l'espace vectoriel $\mathbb{R}^3$: $\mathcal{P}=\{(x,y,z)\in\mathbb{R}^3 \mid ax+by+cz=0\}$.*

  Preuve —

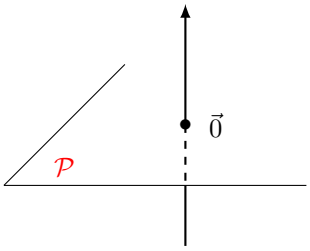
  1. $\mathcal{P}\subset\mathbb{R}^3$.
  2. $\vec{0}_{\mathbb{R}^3}=(0,0,0)\in\mathcal{P}$ *car* $a\times 0+b\times 0+c\times 0=0$.
  3. *Soient* (x_1,y_1,z_1) *et* (x_2,y_2,z_2) *des éléments de* $\mathcal{P}$ *et* $\lambda\in\mathbb{R}$.
     On sait que $ax_1+by_1+cz_1=0$ *et* $ax_2+by_2+cz_2=0$ *car* (x_1,y_1,z_1) *et* (x_2,y_2,z_2) *appartiennent au plan* $\mathcal{P}$.
     Vérifions que $\lambda\cdot(x_1,y_1,z_1)+(x_2,y_2,z_2)=(\lambda x_1+x_2,\lambda x_2+y_2,\lambda x_3+y_3)\in\mathcal{P}$.
     On a

$$\begin{aligned} a(\lambda x_1+x_2)+b(\lambda y_1+y_2)+c(\lambda z_1+z_2) &= a\lambda x_1+ax_2+b\lambda y_1+by_2+c\lambda z_1+cz_2\\ &=\lambda(ax_1+by_1+cz_1)+(ax_2+by_2+cz_2)\\ &=\lambda\times 0+0\\ &=0. \end{aligned}$$

     Donc $\lambda\cdot(x_1,y_1,z_1)+(x_2,y_2,z_2)\in\mathcal{P}$.

  De ces trois points, il vient que $\mathcal{P}$ *est un sous-espace vectoriel de* $\mathbb{R}^3$. □

  En particulier, tout plan de $\mathbb{R}^3$ passant par $(0,0,0)$ est un sous-espace vectoriel de $\mathbb{R}^3$.



- $\mathbb{R}_n[X]$ *est un sous-espace vectoriel de l'espace vectoriel* $\mathbb{R}[X]$.

  Preuve —

  1. $\mathbb{R}_n[X]\subset\mathbb{R}[X]$.
  2. $0\in\mathbb{R}_n[X]$ *car* $\deg(0)=-\infty\leq n$.
  3. *Soient* P *et* Q *des éléments de* $\mathbb{R}_n[X]$ *et* $\lambda\in\mathbb{R}$.
     Alors $\lambda P+Q$ *est un polynôme de degré inférieur ou égal à* n *car* $\deg(\lambda P+Q)\leq\max\{\deg(P),\deg(Q)\}\leq n$ *puisque* $\deg(P\leq n$ *et* $\deg(Q)\leq n$. *Donc* $\lambda P+Q\in\mathbb{R}_n[X]$.

  De ces trois points, il vient que $\mathbb{R}_n[X]$ *est un sous-espace vectoriel de* $\mathbb{R}[X]$. □

- *Soit I un intervalle de $\mathbb{R}$. L'ensemble $\mathcal{C}(I,\mathbb{R})$ des fonctions continues de I dans $\mathbb{R}$ est un sous-espace vectoriel de l'espace vectoriel $\mathcal{F}(I,\mathbb{R})$.*

  Preuve —

  1. $\mathcal{C}(I,\mathbb{R})\subset\mathcal{F}(I,\mathbb{R})$.
  2. *La fonction nulle* $I\longrightarrow\mathbb{R}\ ;\ x\longmapsto 0$ *est continue donc appartient à* $\mathcal{C}(I,\mathbb{R})$.
  3. *Soient* f *et* g *deux éléments de* $\mathcal{C}(I,\mathbb{R})$ *et* $\lambda\in\mathbb{R}$.
     Alors, par somme et produit de fonctions continues, $\lambda f+g$ *est une fonction continue de* I *dans* $\mathbb{R}$, *donc* $\lambda f+g\in\mathcal{C}(I,\mathbb{R})$.

  De ces trois points, il vient que $\mathcal{C}(I,\mathbb{R})$ *est un sous-espace vectoriel de* $\mathcal{F}(I,\mathbb{R})$. □

  De même, les ensembles $\mathcal{D}(I,\mathbb{K})$, $\mathcal{C}^1(I,\mathbb{K})$, $\mathcal{C}^n(I,\mathbb{K})$ sont des sous-espaces vectoriels de $\mathcal{F}(I,\mathbb{K})$.

- *L'ensemble $F=\{(x,y,z)\in\mathbb{R}^3 \mid xy=0\}$ n'est pas un sous-espace vectoriel de $\mathbb{R}^3$.*

  Preuve — *F est un bien un sous-ensemble de $\mathbb{R}^3$ qui contient le vecteur nul puisque $0\times 0=0$. Mais $(1,0,0)\in F$ et $(0,1,0)\in F$ puisque $1\times 0=0$ et $0\times 1=0$, et $(1,0,0)+(0,1,0)=(1,1,0)\notin F$ puisque $1\times 1=1\neq 0$ donc F n'est pas stable par combinaison linéaire. Le point 3. de la caractérisation n'est donc pas vérifié. Donc F n'est pas un sous-espace vectoriel de $\mathbb{R}^3$.* □

PROPOSITION 28

Soit $(E_i)_{i\in I}$ une famille de sous-espaces vectoriels de E. Alors l'intersection $\bigcap_{i\in I}E_i$ est un sous-espace vectoriel de E.

Preuve —

1. Pour tout $i\in I$, $E_i\subset E$ donc $\bigcap_{i\in I}E_i\subset E$.
2. Pour tout $i\in I$, $\vec{0}_E\in E_i$ car E_i est un sous-espace vectoriel de E. Donc $\vec{0}_E\in\bigcap_{i\in I}E_i$.

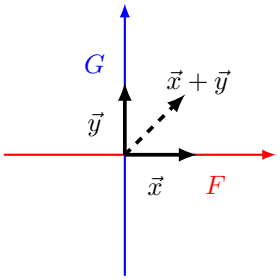
3. Soient $\vec{x}$ et $\vec{y}$ deux éléments de $\bigcap_{i\in I} E_i$ et soit $\lambda \in \mathbb{K}$.
   Soit $i_0 \in I$. Les vecteurs $\vec{x}$ et $\vec{y}$ appartiennent à E_{i_0}. E_{i_0} étant un sous-espace vectoriel de E, d'après la caractérisation, $\lambda \cdot \vec{x} + \vec{y} \in E_{i_0}$.
   i_0 étant quelconque, $\lambda \cdot \vec{x} + \vec{y} \in \bigcap_{i\in I} E_i$.

De ces trois points, on a le résultat. □

La réunion de deux sous-espaces vectoriels n'est pas un sous-espace vectoriel en général car il n'est pas stable par addition. Voyons sur un exemple.

Exemple 29 —

Soit $E = \mathbb{R}^2$. Considérons F la droite vectorielle engendrée par $\vec{x} = (1,0)$ et G la droite vectorielle engendrée par $\vec{y} = (0,1)$.
On a $\vec{x} \in F$ donc $\vec{x} \in F \cup G$.
On a $\vec{y} \in G$ donc $\vec{y} \in F \cup G$.
Mais $\vec{x} + \vec{y} = (1,0) + (0,1) = (1,1) \notin F \cup G$.



Remarque 30 — *Le complémentaire $E \setminus F$ d'un sous-espace vectoriel F n'est pas un sous-espace vectoriel de E : $E \setminus F$ ne contient pas $\vec{0}_E$ puisque $\vec{0}_E \in F$.*

Proposition 31
Soit F un sous-espace vectoriel de E. Toute combinaison linéaire d'éléments $\vec{x}_1$, …, $\vec{x}_n$ de F est élément de F.

Preuve — Ce résultat se démontre par récurrence en utilisant que F est stable par combinaison linéaire. □

1.2.2 Sous-espace vectoriel engendré par une partie

Définition 32
*Soit X une partie de E. Le **sous-espace vectoriel engendré par** X est le plus petit sous-espace vectoriel de E contenant X (au sens de l'inclusion). Il est noté* $\mathrm{Vect}(X)$.

Preuve — Justifions l'existence du plus petit sous-espace vectoriel de E contenant X. E est un sous-espace vectoriel de E contenant X. Considérons alors l'intersection F de tous les sous-espaces vectoriels de E contenant X. F est un sous-espace vectoriel de E comme intersection de sous-espaces vectoriels et F contient X puisque F est l'intersections de parties contenant X. Donc F est un sous-espace vectoriel de E contenant X.

Montrons que F est le plus petit au sens de l'inclusion. Soit H un sous-espace vectoriel de E contenant X. Alors par définition de F, $F \subset H$. Donc F est le plus petit sous-espace vectoriel de E contenant X. □

Remarques 33

- *Dans le cas d'un nombre fini de vecteurs avec $X = \{\vec{x}_1, \ldots, \vec{x}_n\}$, $\mathrm{Vect}(X)$ se note souvent $\mathrm{Vect}(\vec{x}_1, \ldots, \vec{x}_n)$ et on parle du sous-espace vectoriel engendré par la famille $(\vec{x}_1, \ldots, \vec{x}_n)$.*
- *Plus généralement, si $X = \{\vec{x}_i \mid i \in I\}$, $\mathrm{Vect}(X)$ se note souvent $\mathrm{Vect}((\vec{x}_i)_{i\in I})$.*

Proposition 34

- *Soit $(\vec{x}_1, \ldots, \vec{x}_n)$ une famille d'éléments de E. Alors $\mathrm{Vect}(\vec{x}_1, \ldots, \vec{x}_n)$ est l'ensemble des combinaisons linéaires des éléments $\vec{x}_1$, …, $\vec{x}_n$.*
  Autrement dit, $\mathrm{Vect}(\vec{x}_1, \ldots, \vec{x}_n) = \left\{\sum_{i=1}^n \lambda_i \cdot \vec{x}_i \mid (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n\right\}$.
- *Plus généralement, soient $(\vec{x}_i)_{i\in I}$ une famille d'éléments de E indicée par I. Alors $\mathrm{Vect}((\vec{x}_i)_{i\in I})$ est l'ensemble des combinaisons linéaires (finies) de la famille $(\vec{x}_i)_{i\in I}$.*

Preuve — Traitons le premier point, le deuxième se traite de la même manière.

Notons $C = \left\{\sum_{i=1}^{n} \lambda_i \cdot \vec{x}_i \mid (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n\right\}$, l'ensemble des combinaisons linéaires des éléments $\vec{x}_1$, …, $\vec{x}_n$.. Montrons, par double inclusions que $C = \text{Vect}(\vec{x}_1, \ldots, \vec{x}_n)$.

▷ $\text{Vect}(\vec{x}_1, \ldots, \vec{x}_n)$ contient les éléments $\vec{x}_1, \ldots, \vec{x}_n$. Or $\text{Vect}(\vec{x}_1, \ldots, \vec{x}_n)$ est un sous-espace vectoriel de E. Donc $\text{Vect}(\vec{x}_1, \ldots, \vec{x}_n)$ contient les combinaisons linéaires des éléments $\vec{x}_1$, …, $\vec{x}_n$. Donc $C \subset \text{Vect}(\vec{x}_1, \ldots, \vec{x}_n)$.

◁ Réciproquement, montrons que $\text{Vect}(\vec{x}_1, \ldots, \vec{x}_n) \subset C$. Pour cela, montrons que C est un sous-espace vectoriel contenant les éléments $\vec{x}_1$, …, $\vec{x}_n$.

1. On a $C \subset E$ puisque les $\vec{x}_i$ sont éléments de E et E est un espace vectoriel.
2. $\vec{0}_E = \sum_{i=1}^{n} 0 \cdot \vec{x}_i$ donc $\vec{0}_E \in C$.
3. Soient $\vec{u}$ et $\vec{v}$ des éléments de C et $\lambda \in \mathbb{K}$. Montrons que $\lambda \cdot \vec{u} + \vec{v} \in C$.
   Comme $\vec{u} \in C$, il existe $(\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$ tel que $\vec{u} = \sum_{i=1}^{n} \lambda_i \cdot \vec{x}_i$.
   Comme $\vec{v} \in C$, il existe $(\mu_1, \ldots, \mu_n)$ telle que $\vec{v} = \sum_{i=1}^{n} \mu_i \cdot \vec{x}_i$.
   Donc
   $$\lambda \cdot \vec{u} + \vec{v} = \lambda \cdot \sum_{i=1}^{n} \lambda_i \cdot \vec{x}_i + \sum_{i=1}^{n} \mu_i \cdot \vec{x}_i$$
   $$= \sum_{i=1}^{n} (\lambda\lambda_i + \mu_i) \cdot \vec{x}_i.$$
   Donc $\lambda \cdot \vec{u} + \vec{v} \in C$.

De ces trois points, il vient que C est un sous-espace vectoriel de E.

De plus, pour tout $j \in \{1, \ldots, n\}$, $\vec{x}_j = 1 \cdot \vec{x}_j + \sum_{\substack{i=1,\ldots,n \\ i \neq j}} 0 \cdot \vec{x}_i$ donc $\vec{x}_j \in C$. Donc C contient les éléments $\vec{x}_1$, …, $\vec{x}_n$.

Par définition, $\text{Vect}(\vec{x}_1, \ldots, \vec{x}_n)$ étant le plus petit sous-espace vectoriel de E contenant les éléments x_i, on en déduit que $\text{Vect}(\vec{x}_1, \ldots, \vec{x}_n) \subset C$.

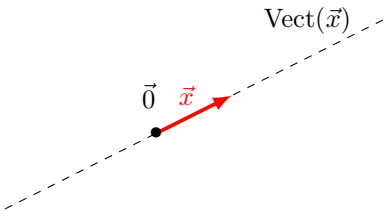
Finalement, $\text{Vect}(\vec{x}_1, \ldots, \vec{x}_n) = C$. □

REMARQUE 35 — *Cela signifie que $\vec{x} \in \text{Vect}(X)$ si et seulement s'il existe $\vec{x}_1$, …, $\vec{x}_n$ éléments de X et λ_1, …, λ_n éléments de $\mathbb{K}$ tels que*

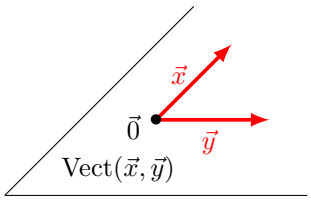
$$\vec{x} = \sum_{i=1}^{n} \lambda_i \cdot \vec{x}_i = \lambda_1 \cdot \vec{x}_1 + \ldots + \lambda_n \cdot \vec{x}_n.$$

EXEMPLES 36

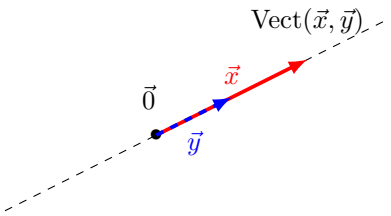
- *Soit $\vec{x}$ un élément de E. Alors*
  $$\text{Vect}(\vec{x}) = \{\lambda \cdot \vec{x} \mid \lambda \in \mathbb{K}\}.$$
  Si $\vec{x} = \vec{0}_E$ alors $\text{Vect}(\vec{x}) = \{\vec{0}_E\}$
  Sinon, $\text{Vect}(\vec{x}) = \mathbb{K} \cdot \vec{x}$ *est la* ***droite vectorielle engendrée par*** $\vec{x}$.



- *Soient $\vec{x}$ et $\vec{y}$ deux éléments de E. Alors*
  $$\text{Vect}(\vec{x}, \vec{y}) = \{\lambda \cdot \vec{x} + \mu \cdot \vec{y} \mid (\lambda, \mu) \in \mathbb{K}^2\}.$$
  Si $\vec{x}$ et $\vec{y}$ ne sont pas colinéaires, $\text{Vect}(\vec{x}, \vec{y})$ *est le* ***plan vectoriel engendré par*** $\vec{x}$ ***et*** $\vec{y}$.



Si $\vec{x}$ et $\vec{y}$ sont ***colinéaires*** *\共线\ (c'est-à-dire qu'il existe $\lambda \in \mathbb{K}$ tel que $\vec{y} = \lambda \cdot \vec{x}$ ou $\vec{x} = \lambda \cdot \vec{y}$) avec $\vec{x} \neq \vec{0}_E$, $\mathrm{Vect}(\vec{x}, \vec{y}) = \mathbb{K} \cdot \vec{x}$ est la droite vectorielle engendrée par $\vec{x}$.*



Exemples 37

- $\mathrm{Vect}(\vec{0}_E) = \vec{0}_E$.
- *Dans $\mathbb{R}^2$, le sous-espace vectoriel* $\mathrm{Vect}((1,1))$ *est la droite vectorielle dirigée par le vecteur $(1,1)$ de $\mathbb{R}^2$ et passant par $(0,0)$:*

$$\mathrm{Vect}((1,1)) = \{\lambda(1,1) \mid \lambda \in \mathbb{K}\} = \{(\lambda, \lambda) \mid \lambda \in \mathbb{R}\}.$$

- *Dans $\mathbb{R}^3$, considérons $\vec{x} = (1,1,0)$ et $\vec{y} = (-1,0,3)$. Le sous-espace vectoriel* $\mathrm{Vect}(\vec{x}, \vec{y})$ *est le plan vectoriel engendré par $\vec{x}$ et $\vec{y}$:*

$$\mathrm{Vect}(\vec{x}, \vec{y}) = \{\lambda(1,1,0) + \mu(-1,0,3) \mid (\lambda, \mu) \in \mathbb{R}^2\} = \{(\lambda - \mu, \lambda, 3\mu) \mid (\lambda, \mu) \in \mathbb{R}^2\}.$$

- *On a* $\mathbb{K}_n[X] = \mathrm{Vect}(1, X, X^2, \ldots, X^n)$ *et* $\mathbb{K}[X] = \mathrm{Vect}((X^n)_{n \in \mathbb{N}})$.
- *Dans le $\mathbb{R}$-espace vectoriel $\mathbb{C}$,*

$$\mathrm{Vect}(1) = \{\lambda \times 1 \mid \lambda \in \mathbb{R}\} = \mathbb{R}$$

et

$$\mathrm{Vect}(1, i) = \{\lambda \times 1 + \mu \times i \mid (\lambda, \mu) \in \mathbb{R}^2\} = \mathbb{C}.$$

- *Dans le $\mathbb{C}$-espace vectoriel $\mathbb{C}$,*

$$\mathrm{Vect}(1) = \{\lambda \times 1 \mid \lambda \in \mathbb{C}\} = \mathbb{C}.$$

Pour démontrer qu'un ensemble est un sous-espace vectoriel de E, on peut montrer qu'il est engendré par une famille de vecteurs de E. C'est parfois pratique, comme sur les exemples suivants.

Exemples 38

- *Soit $F = \{(\lambda + \mu, \lambda - \mu) \mid (\lambda, \mu) \in \mathbb{R}^2\}$. On a*

$$F = \{\lambda(1,1) + \mu(1,-1) \mid (\lambda, \mu) \in \mathbb{R}^2\} = \mathrm{Vect}((1,1),(1,-1)),$$

donc F est un sous-espace vectoriel de $\mathbb{R}^2$, engendré par les vecteurs $(1,1)$ et $(1,-1)$.

- *Soit* $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$. *On a*

$$G = \left\{ a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\} = \mathrm{Vect}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right),$$

donc G est un sous-espace vectoriel de $\mathcal{M}_2(\mathbb{R})$, engendré par le vecteur $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

- *Soit $H = \{(x,y,z) \in \mathbb{R}^3 \mid 2x - y + 3z = 0\}$.*
  Soit $(x,y,z) \in \mathbb{R}^3$. Exprimons y en fonction de x et z. On a $(x,y,z) \in H$ si et seulement si $y = 2x + 3z$. Donc

$$H = \{(x, 2x + 3z, z) \mid (x,z) \in \mathbb{R}^2\} = \{x(1,2,0) + z(0,3,1) \mid (x,z) \in \mathbb{R}^2\} = \mathrm{Vect}((1,2,0),(0,3,1)).$$

Donc H est un sous-espace vectoriel de $\mathbb{R}^3$, engendré par les vecteurs $(1,2,0)$ et $(0,3,1)$.

Proposition 39
Soient $(\vec{x}_1, \dots, \vec{x}_n)$ une famille d'éléments de E. On considère les opérations suivantes :

- *éliminer les vecteurs nuls de la famille.*
- *éliminer un des vecteurs de la famille s'il est égal à un autre,*
- *permuter des vecteurs,*
- *multiplier un vecteur par un scalaire non nul,*
- *ajouter à l'un des vecteurs $\vec{x}_{i_0}$ une combinaison linéaire des autres vecteurs de la famille :*

$$\vec{x}_{i_0} + \sum_{\substack{i=1,\dots,n \\ i \neq i_0}} \lambda_i \cdot \vec{x}_i,$$

L'espace vectoriel engendré par la famille obtenue par ces opérations est encore égal à $\mathrm{Vect}(\vec{x}_1, \dots, \vec{x}_n)$.

Exemple 40 — *(Reprenons l'ensemble F des exemples 38. On a vu que $F = \mathrm{Vect}\big((1,1),(1,-1)\big)$.*

Par opérations sur la famille $\big((1,1),(1,-1)\big)$, on obtient

$$\begin{aligned} F &= \mathrm{Vect}\big((1,1),(1,-1)+(1,1)\big) = \mathrm{Vect}\big((1,1),(2,0)\big) \\ &= \mathrm{Vect}\big((1,1),\frac{1}{2}(2,0)\big) = \mathrm{Vect}\big((1,1),(1,0)\big) \\ &= \mathrm{Vect}\big((1,1)-(1,0),(1,0)\big) = \mathrm{Vect}\big((0,1),(1,0)\big) \\ &= \{(\lambda,\mu) \mid (\lambda,\mu) \in \mathbb{R}^2\} \\ &= \mathbb{R}^2. \end{aligned}$$

1.3 Familles de vecteurs

Dans cette partie, $(E, +, \cdot)$ désigne un $\mathbb{K}$-espace vectoriel.

1.3.1 Familles génératrices

Définition 41
*Soit $(\vec{x}_i)_{i\in I}$ une famille de vecteurs de E. On dit que la famille $(\vec{x}_i)_{i\in I}$ est **génératrice** si tout vecteur de E est combinaison linéaire de la famille $(\vec{x}_i)_{i\in I}$:*

$$E = \mathrm{Vect}((x_i)_{i\in I}).$$

Commençons par donner des exemples classiques de familles génératrices.

Exemples 42

- *Soit $n \in \mathbb{N}^*$. La famille $(1, X, \dots, X^n)$ est une famille génératrice de $\mathbb{K}_n[X]$.*
- *La famille $(X^n)_{n\in\mathbb{N}}$ est une famille génératrice de $\mathbb{K}[X]$.*
- *La famille $((1,0),(0,1))$ est une famille génératrice de $\mathbb{R}^2$:*
  Pour tout $(x,y) \in \mathbb{R}^2$, $(x,y) = x(1,0) + y(0,1)$.
- *La famille $((1,0,0),(0,1,0),(0,0,1))$ est une famille génératrice de $\mathbb{R}^3$:*
  Pour tout $(x,y,z) \in \mathbb{R}^3$, $(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1)$.
- *Plus généralement, soit $n \in \mathbb{N}^*$. Posons $\vec{e}_1 = (1,0,\dots,0)$, $\vec{e}_2 = (0,1,0,\dots,0)$, …, $\vec{e}_n = (0,\dots,0,1)$.*
  La famille $(\vec{e}_1, \dots, \vec{e}_n)$ est une famille génératrice de $\mathbb{K}^n$:
  Pour tout $\vec{x} = (x_1, \dots, x_n) \in \mathbb{K}^n$, $\vec{x} = \sum_{i=1}^n x_i \vec{e}_i$.

- *La famille* $\left(\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\right)$ *est une famille génératrice de* $\mathcal{M}_2(\mathbb{K})$ *: pour tout* $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathcal{M}_2(\mathbb{K})$,
$$\begin{pmatrix}a&b\\c&d\end{pmatrix}=a\begin{pmatrix}1&0\\0&0\end{pmatrix}+b\begin{pmatrix}0&1\\0&0\end{pmatrix}+c\begin{pmatrix}0&0\\1&0\end{pmatrix}+d\begin{pmatrix}0&0\\0&1\end{pmatrix}.$$
- *La famille* $(1,i)$ *est une famille génératrice du* $\mathbb{R}$*-espace vectoriel* $\mathbb{C}$ *:*
Pour tout $z\in\mathbb{C}$, $z=\mathrm{Re}(z)\times 1+\mathrm{Im}(z)\times i$.
- *La famille* (1) *est une famille génératrice du* $\mathbb{K}$*-espace vectoriel* $\mathbb{K}$ *:*
Pour tout $x\in\mathbb{K}$, $x=x\times 1$.

Lorsqu'un ensemble est écrit comme un Vect, on connaît immédiatement une famille génératrice.

Exemple 43 — *Nous avons vu à l'exemple 40, par opérations élémentaires sur les* Vect*, que*
$$\mathrm{Vect}((1,1),(1,-1))=\mathbb{R}^2.$$
La famille $((1,1),(1,-1))$ *est donc une famille génératrice de* $\mathbb{R}^2$.

On peut aussi montrer, par résolution d'un système par exemple, que pour tout $(x,y)\in\mathbb{R}^2$,
$$(x,y)=\frac{x+y}{2}(1,1)+\frac{x-y}{2}(1,-1).$$
On retrouve alors le résultat.

En effet, soit $(x,y)\in\mathbb{R}^2$. *On cherche* $\lambda_1\in\mathbb{R}$ *et* $\lambda_2\in\mathbb{R}$ *tels que* $(x,y)=\lambda_1(1,1)+\lambda_2(1,-1)$, *c'est-à-dire tels que* $(x,y)=(\lambda_1+\lambda_2,\lambda_1-\lambda_2)$. *On doit donc résoudre le système* $\begin{cases}x=\lambda_1+\lambda_2\\y=\lambda_1-\lambda_2\end{cases}$.

On trouve alors $\lambda_1=\dfrac{x+y}{2}$ *et* $\lambda_2=\dfrac{x-y}{2}$.

1.3.2 Familles libres et liées

Définition 44

- *Soient* $\vec{x}_1,\ldots,\vec{x}_n$ *des éléments de* E. *On dit que la famille* $(\vec{x}_1,\ldots,\vec{x}_n)$ *est* ***libre*** *si par définition, pour tout* $(\lambda_1,\ldots,\lambda_n)\in\mathbb{K}^n$, *si* $\sum_{i=1}^n\lambda_i\cdot\vec{x}_i=\vec{0}_E$ *alors, pour tout* $i\in\{1,\ldots,n\}$, $\lambda_i=0$.
On dit aussi que les vecteurs $\vec{x}_1,\ldots,\vec{x}_n$ *sont* ***linéairement indépendants*** \线性无关\.
- *Soit* $(\vec{x})_{i\in I}$ *une famille d'éléments de* E. *On dit que la famille* $(\vec{x}_i)_{i\in I}$ *de vecteurs de* E *est* ***libre*** *si toute sous-famille* ***finie*** *de* $(\vec{x}_i)_{i\in I}$ *est libre.*

Proposition 45
Soit $(\vec{x}_1,\ldots,\vec{x}_n)$ *une famille libre de* E. *Soit* $\vec{x}\in\mathrm{Vect}(\vec{x}_1,\ldots,\vec{x}_n)$. *Alors les coefficients* λ_i *dans la décomposition* $\vec{x}=\sum_{i=1}^n\lambda_i\cdot\vec{x}_i$ *sont uniques :*

Pour tout $(\lambda_1,\ldots,\lambda_n)\in\mathbb{K}^n$ *et tout* $(\mu_1,\ldots,\mu_n)\in\mathbb{K}^n$, *si* $\sum_{i=1}^n\lambda_i\cdot\vec{x}_i=\sum_{i=1}^n\mu_i\cdot\vec{x}_i$ *alors, pour tout* $i\in\{1,\ldots,n\}$, $\lambda_i=\mu_i$.

Preuve — Supposons que $\vec{x}=\sum_{i=1}^n\lambda_i\cdot\vec{x}_i$ et $\vec{x}=\sum_{i=1}^n\mu_i\cdot\vec{x}_i$.

On a donc
$$\sum_{i=1}^n\lambda_i\cdot\vec{x}_i=\sum_{i=1}^n\mu_i\cdot\vec{x}_i,$$
soit
$$\sum_{i=1}^n(\lambda_i-\mu_i)\cdot\vec{x}_i=\vec{0}_E.$$

Donc, la famille $(\vec{x}_1, \ldots, \vec{x}_n)$ étant libre, pour tout $i \in \{1, \ldots, n\}$, $\lambda_i - \mu_i = 0$, soit $\lambda_i = \mu_i$.

D'où le résultat. □

Cela nous autorise donc à identifier les coefficients dans les combinaisons linéaires (uniquement lorsque la famille est libre !).

DÉFINITION 46
Soit $(\vec{x}_i)_{i\in I}$ une famille d'éléments de E. On dit que la famille $(\vec{x}_i)_{i\in I}$ est ***liée*** *si elle n'est pas libre.*

Autrement dit, il existe $\vec{x}_1$, …, $\vec{x}_n$ éléments de la famille $(\vec{x}_i)_{i\in I}$ et $(\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$ tels que

$\sum_{i=1}^n \lambda_i \cdot \vec{x}_i = \vec{0}_E$ *et* $(\lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0)$.

On dit aussi que les vecteurs $\vec{x}_1$, …, $\vec{x}_n$ sont ***linéairement dépendants****.*

PROPOSITION 47
Soient $\vec{x}_1$, …, $\vec{x}_n$ des éléments de E. La famille $(\vec{x}_1, \ldots, \vec{x}_n)$ est liée si et seulement si l'un des vecteurs $\vec{x}_1$, …, $\vec{x}_n$ est combinaison linéaire des autres vecteurs.

Preuve — ▷ Supposons que la $(\vec{x}_1, \ldots, \vec{x}_n)$ soit liée. Alors il existe $(\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$ tel que $\sum_{i=1}^n \lambda_i \cdot \vec{x}_i = \vec{0}_E$ et $(\lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0)$. Il existe donc $i_0 \in \{1, \ldots, n\}$ tel que $\lambda_{i_0} \neq 0$. On a donc

$$\lambda_{i_0} \cdot \vec{x}_{i_0} + \sum_{\substack{i=1,\ldots,n \\ i\neq i_0}} \lambda_i \cdot \vec{x}_i = \vec{0}_E.$$

Donc

$$\vec{x}_{i_0} = -\frac{1}{\lambda_{i_0}} \cdot \sum_{\substack{i=1,\ldots,n \\ i\neq i_0}} \lambda_i \cdot \vec{x}_i = \sum_{\substack{i=1,\ldots,n \\ i\neq i_0}} \frac{-\lambda_i}{\lambda_{i_0}} \cdot \vec{x}_i.$$

Donc $\vec{x}_{i_0}$ est une combinaison linéaire des autres vecteurs.

◁ Réciproquement, supposons que $\vec{x}_{i_0} = \sum_{\substack{i=1\ldots n \\ i\neq i_0}} \lambda_i \cdot \vec{x}_i$. Alors on a $1 \cdot \vec{x}_{i_0} + \sum_{\substack{1\leq i\leq n \\ i\neq i_0}} (-\lambda_i) \cdot \vec{x}_i = \vec{0}_E$ et les λ_i sont non tous nuls puisque $\lambda_{i_0} = 1$. Donc la famille $(\vec{x}_1, \ldots, \vec{x}_n)$ est liée. □

La remarque suivante découle de la définition de deux vecteurs colinéaires.

REMARQUE 48 — *Soient $\vec{x}$ et $\vec{y}$ des éléments de E. La famille $(\vec{x}, \vec{y})$ est liée si et seulement si $\vec{x}$ et $\vec{y}$ sont colinéaires.*

Donnons des exemples classiques de familles libres.

EXEMPLES 49

- *La famille $(1, i)$ est libre dans le $\mathbb{R}$-espace vectoriel $\mathbb{C}$.*
  Preuve *— Soit $(\lambda, \mu) \in \mathbb{R}^2$ tel que $\lambda \cdot 1 + \mu \cdot i = 0$. Alors, par identification des parties réelles et imaginaires, $\lambda = 0$ et $\mu = 0$. D'où la liberté de la famille $(1, i)$ dans le $\mathbb{R}$-espace vectoriel $\mathbb{C}$.* □
- *Soit $n \in \mathbb{N}^*$. Posons $\vec{e}_1 = (1, 0 \ldots, 0)$, $\vec{e}_2 = (0, 1, 0, \ldots, 0)$, …, $\vec{e}_n = (0, \ldots, 0, 1)$. La famille $(\vec{e}_1, \ldots, \vec{e}_n)$ est libre dans $\mathbb{K}^n$.*
  Preuve *— Soit $(\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$ tel que $\sum_{i=1}^n \lambda_i \cdot \vec{e}_i = \vec{0}_{\mathbb{K}^n}$.*
  On a $\sum_{i=1}^n \lambda_i \cdot \vec{e}_i = (\lambda_1, \ldots, \lambda_n)$ et $\vec{0}_{\mathbb{K}^n} = (0, \ldots, 0)$.
  Donc $(\lambda_1, \ldots, \lambda_n) = (0, \ldots, 0)$ et donc, pour tout $i \in \{1, \ldots, n\}$, $\lambda_i = 0$. □
- *La famille $(X^n)_{n\in\mathbb{N}}$ est libre dans $\mathbb{K}[X]$.*
  Preuve *— Soit $(X^{d_1}, \ldots, X^{d_p})$ une sous-famille finie de de $(X^n)_{n\in\mathbb{N}}$ avec $d_1 < d_2 < \ldots < d_p$. Soit $(\lambda_1, \ldots, \lambda_p) \in \mathbb{K}^p$ tel que $\lambda_1 X^{d_1} + \ldots + \lambda_p X^{d_p} = 0$. Alors par unicité des coefficients du polynôme nul, $\lambda_1 = \lambda_1 = \ldots = \lambda_p = 0$. Donc la famille $(X^{d_1}, \ldots, X^{d_p})$ est libre.*
  Toute sous-famille finie de $(X^n)_{n\in\mathbb{N}}$ est donc libre, et donc la famille $(X^n)_{n\in\mathbb{N}}$ est libre. □
- *La famille $(1, X, \ldots, X^n)$ est libre dans $\mathbb{K}_n[X]$.*
  Preuve *— La famille $(1, X, \ldots, X^n)$ est une sous-famille finie de $(X^n)_{n\in\mathbb{N}}$ qui, on vient de le voir, est libre. Par définition de la liberté d'une famille infinie, la famille $(1, X, \ldots, X^n)$ est donc libre.*
  On peut aussi le démontrer en revenant à la définition pour une famille finie. □

- *Une famille de polynômes non nuls de degrés échelonnés est libre.*
  Plus précisément, soit $(P_1, \dots, P_n)$ une famille de polynômes non nuls de $\mathbb{K}[X]$ telle que $\deg(P_1) < \dots < \deg(P_n)$. Alors la famille $(P_1, \dots, P_n)$ est une famille libre de $\mathbb{K}[X]$.
  ***Preuve** —*
  Soit $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$ tel que $\lambda_1 P_1 + \dots + \lambda_n P_n = 0$.
  Supposons par l'absurde que $(\lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$. Soit $i_0 \in \{1, \dots, n\}$ le plus grand indice tel que $\lambda i_0 \neq 0$. Alors $\lambda_1 P_1 + \dots + \lambda_{i_0} P_{i_0}$ est de degré $\deg(P_{i_0}) \neq -\infty$ (car les degrés des polynômes sont échelonnés et $\lambda_{i_0} P_{i_0}$ est non nul) et n'est donc pas le polynôme nul. Or, par hypothèse, $\lambda_1 P_1 + \dots + \lambda_{i_0} P_{i_0} = 0$, ce qui est absurde.
  Donc $(\lambda_1, \dots, \lambda_n) = (0, \dots, 0)$ et la famille $(P_1, \dots, P_n)$ est libre. □
- *La famille $\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right)$ est libre dans $\mathcal{M}_2(\mathbb{R})$.*
  ***Preuve** — Soit $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in \mathbb{R}^4$ tel que*
  $$\lambda_1 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \lambda_4 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \vec{0}_{\mathcal{M}_2(\mathbb{R})}.$$
  Alors $\begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Donc $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (0, 0, 0, 0)$. D'où le résultat. □

Exemples 50

- *La famille $(1, i)$ est liée dans le $\mathbb{C}$-espace vectoriel $\mathbb{C}$.*
  ***Preuve** — En prenant $\lambda = i$ et $\mu = 1$, on a $i \cdot 1 - 1 \times i = 0$ et $(\lambda, \mu) = (i, 1) \neq (0, 0)$. Donc la famille $(1, i)$ est liée dans le $\mathbb{C}$-espace vectoriel $\mathbb{C}$.* □
- *La famille $\big((1, 2, 1), (-1, 3, 1), (-1, 13, 5)\big)$ est liée dans $\mathbb{R}^3$.*
  ***Preuve** — Soit $(\lambda, \mu, \nu) \in \mathbb{R}^3$.*
  $$\lambda(1,2,1) + \mu(-1,3,1) + \nu(-1,13,5) = (0,0,0) \text{ si et seulement si } \begin{cases} \lambda - \mu - \nu = 0 \\ 2\lambda + 3\mu + 13\nu = 0 \\ \lambda + \mu + 5\nu = 0 \end{cases}.$$
  Il existe des solutions non nulles à ce système, par exemple $(\lambda, \mu, \nu) = (2, 3, -1)$.
  On a donc $2(1,2,1) + 3(-1,3,1) - (-1,13,5) = (0,0,0)$ et la famille $\big((1,2,1), (-1,3,1), (-1,13,5)\big)$ est liée. □

Proposition 51

1. *Soit $\vec{x} \in E$. Alors $(\vec{x})$ est une famille libre si et seulement si $\vec{x} \neq \vec{0}_E$.*
2. *Toute sous-famille d'une famille libre est libre.*
3. *Toute famille contenant une famille liée est liée.*
4. *Toute famille $(\vec{x}_1, \dots, \vec{x}_n)$ dont l'un des vecteurs $\vec{x}_i$ est nul, est liée.*
5. *Soit $(\vec{x}_1, \dots, \vec{x}_n)$ une famille libre de E. Soit $\vec{x} \in E$. La famille $(\vec{x}_1, \dots, \vec{x}_n, \vec{x})$ est libre si et seulement si $\vec{x}$ n'est pas combinaison linéaire de la famille $(\vec{x}_1, \dots, \vec{x}_n)$. Autrement dit, $(\vec{x}_1, \dots, \vec{x}_n, \vec{x})$ est libre si et seulement si $\vec{x} \notin \mathrm{Vect}(\vec{x}_1, \dots, \vec{x}_n)$.*

Preuve —

1. ◁ Supposons $\vec{x} \neq \vec{0}_E$. Soit $\lambda \in \mathbb{K}$ tel que $\lambda \cdot \vec{x} = \vec{0}_E$. Alors comme $\vec{x} \neq \vec{0}_E$, $\lambda = 0$. Donc la famille $(\vec{x})$ est libre.
   ▷ Réciproquement, si $\vec{x} = \vec{0}_E$ alors $1 \cdot \vec{x} = \vec{0}_E$, donc la famille $(\vec{x})$ est liée. Donc par contraposée, si $(\vec{x})$ est libre alors $\vec{x} \neq \vec{0}_E$.
2. Soit $(\vec{x}_1, \dots, \vec{x}_n)$ une famille libre de E. Quitte à changer la numérotation, considérons la sous-famille $(\vec{x}_1, \dots, \vec{x}_p)$ avec $p \leq n$. Si $(\vec{x}_1, \dots, \vec{x}_p)$ est une famille liée, alors l'un des vecteurs $\vec{x}_{i_0}$ avec $i_0 \in \{1, \dots, p\}$ est combinaison linéaire des autres et donc $\vec{x}_{i_0}$, vecteur de la famille $(\vec{x}_1, \dots, \vec{x}_n)$ est combinaison linéaire des autres vecteurs $\vec{x}_i$, avec $i \in \{1, \dots, n\}$. Ceci contredit le fait que la famille $(\vec{x}_1, \dots, \vec{x}_n)$ est libre.
3. Soit $(\vec{x}_1, \dots, \vec{x}_n)$ une famille liée de E. Considérons la famille $(\vec{x}_1, \dots, \vec{x}_n, \vec{w}_1, \dots, \vec{w}_p)$. La famille $(\vec{x}_1, \dots, \vec{x}_n)$ étant liée, l'un des vecteurs $\vec{x}_{i_0}$ est combinaison linéaires des autres vecteurs $\vec{x}_i$, donc *a fortiori* des vecteurs de la famille $(\vec{x}_1, \dots, \vec{x}_n, \vec{w}_1, \dots, \vec{w}_p)$. Cette famille est donc liée.
4. Une famille contenant le vecteur $\vec{0}_E$ contient donc la famille $(\vec{0}_E)$ qui est liée, et est donc liée.
5. Soit $(\lambda_1, \dots, \lambda_n, \lambda) \in \mathbb{K}^{n+1}$ tel que
   $$\lambda_1 \cdot \vec{x}_1 + \dots + \lambda_n \cdot \vec{x}_n + \lambda \cdot \vec{x} = \vec{0}_E.$$
   Si $\lambda \neq 0$ alors $\vec{x} = \sum_{i=1}^{n} \frac{-\lambda_i}{\lambda} \cdot \vec{x}_i$, ce qui contredit le fait que $\vec{x}$ n'est pas combinaison linéaire des $\vec{x}_i$. Donc $\lambda = 0$. Donc $\sum_{i=1}^{n} \lambda_i \cdot \vec{x}_i = \vec{0}_E$. La famille $(\vec{x}_1, \dots, \vec{x}_n)$ étant libre, pour tout $i \in \{1, \dots, n\}$, $\lambda_i = 0$. Donc $(\lambda_1, \dots, \lambda_n, \lambda) = (0, \dots, 0, 0)$. Donc la famille $(\vec{x}_1, \dots, \vec{x}_n, \vec{x})$ est libre.

□

1.3.3 Bases

Définition 52
*Soit $(\vec{x}_i)_{i\in I}$ une famille de vecteurs de E. On dit que la famille $(\vec{x}_i)_{i\in I}$ est une **base** de E si c'est une famille libre et génératrice.*

Proposition 53
Soit $(\vec{x}_1,\dots,\vec{x}_n)$ une famille de vecteurs de E. La famille $(\vec{x}_1,\dots,\vec{x}_n)$ est une base si et seulement si tout élément $\vec{x}$ de E s'écrit de façon unique comme combinaison linéaire de la famille $(\vec{x}_1,\dots,\vec{x}_n)$.

Autrement dit, il existe un unique n-uplet $(\lambda_1,\dots,\lambda_n)\in\mathbb{K}^n$ tel que

$$\vec{x}=\sum_{i=1}^{n}\lambda_i\cdot\vec{x}_i.$$

*Les coefficients λ_i de cette combinaison linéaire sont appelés les **coordonnées** de $\vec{x}$ dans la base $(\vec{x}_1,\dots,\vec{x}_n)$.*

Preuve — L'existence provient du caractère générateur et l'unicité du caractère libre. □

Les bases sont des familles et non des ensembles !

Donnons des bases classiques à connaître. Nous avons déjà montré dans les parties précédentes que ces familles sont libres et génératrices, par définition, ce sont donc des bases.

Exemples 54
- *La famille $(1,i)$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$.*
  Les coordonnées d'un élément $z\in\mathbb{C}$ dans la base $(1,i)$ sont $(\mathrm{Re}(z),\mathrm{Im}(z))$.
- *Soit $n\in\mathbb{N}^*$. Posons $\vec{e}_1=(1,0,\dots,0)$, $\vec{e}_2=(0,1,0,\dots,0)$,..., $\vec{e}_n=(0,\dots,0,1)$. La famille $(\vec{e}_1,\dots,\vec{e}_n)$ est une base de $\mathbb{K}^n$, appelée la **base canonique** de $\mathbb{K}^n$.*
  Les coordonnées d'un élément $\vec{x}=(x_1,\dots,x_n)\in\mathbb{K}^n$ dans cette base canonique sont $(x_1,\dots,x_n)$.
- *Soit $n\in\mathbb{N}^*$. La famille $(1,X,\dots,X^n)$ est une base de $\mathbb{K}_n[X]$, appelée la **base canonique** de $\mathbb{K}_n[X]$.*
  Les coordonnées d'un polynôme $P=a_0+a_1X+\dots+a_nX^n\in\mathbb{K}_n[X]$ dans cette base canonique sont $(a_0,a_1,\dots,a_n)$.
- *La famille $(X^n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$, appelée **base canonique** de $\mathbb{K}[X]$.*
- *La famille $\left(\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\right)$ est une base de $\mathcal{M}_2(\mathbb{R})$, appelée la **base canonique** de $\mathcal{M}_2(\mathbb{R})$.*
  Les coordonnées d'une matrice $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathcal{M}_2(\mathbb{R})$ dans cette base canonique sont (a,b,c,d).

Exemple 55 — *Soient $n\in\mathbb{N}$ et $a\in\mathbb{K}$. La famille $\left(1,X-a,\dfrac{(X-a)^2}{2!},\dots,\dfrac{(X-a)^n}{n!}\right)$ est une base de $\mathbb{K}_n[X]$. Les coordonnées d'un polynôme $P\in\mathbb{K}_n[X]$ dans cette base sont $\big(P(a),P'(a),P''(a),\dots,P^{(n)}(a)\big)$.*

***Preuve** — Montrons que la famille $\left(1,X-a,\dfrac{(X-a)^2}{2!},\dots,\dfrac{(X-a)^n}{n!}\right)$ est libre et génératrice.*

• Il s'agit d'une famille de polynômes de degrés échelonnés donc cette famille est libre.

• Soit $P\in\mathbb{K}_n[X]$. D'après la formule de Taylor polynomiale, on a $P=\sum_{k=0}^{n}\dfrac{P^{(k)}(a)}{k!}(X-a)^k=\sum_{k=0}^{n}P^{(k)}(a)\dfrac{(X-a)^k}{k!}$.
La famille de vecteurs $\left(1,X-a,\dfrac{(X-a)^2}{2!},\dots,\dfrac{(X-a)^n}{n!}\right)$ est donc génératrice.

De ces deux points, il vient que la famille est une base et la décomposition précédente nous donne les coordonnées de P dans la base. □

Pour déterminer les coordonnées d'un vecteur dans une base, on doit déterminer la combinaison linéaire de ce vecteur dans la base. C'est souvent ce que l'on fait déjà pour montrer qu'une famille est génératrice.

EXEMPLE 56 — *Nous avons vu à l'exemple 43 que la famille* $\big((1,1),(1,-1)\big)$ *est une famille génératrice de* $\mathbb{R}^2$.

Montrons que c'est une famille libre.

Soit $(\lambda,\mu)\in\mathbb{R}^2$ *tel que* $\lambda(1,1)+\mu(1,-1)=(0,0)$. *Alors* $(\lambda+\mu,\lambda-\mu)=(0,0)$. *Donc*

$$\begin{cases}\lambda+\mu=0\\ \lambda-\mu=0\end{cases}.$$

Donc $\lambda=\mu=0$. *Donc la famille* $\big((1,1),(1,-1)\big)$ *est une famille libre de* $\mathbb{R}^2$.

La famille $\big((1,1),(1,-1)\big)$ *est donc libre et génératrice, c'est donc une base de* $\mathbb{R}^2$.

De plus, on a vu que tout vecteur $(x,y)\in\mathbb{R}^2$ *s'écrit*

$$(x,y)=\frac{x+y}{2}(1,1)+\frac{x-y}{2}(1,-1).$$

Les coordonnées d'un vecteur $(x,y)\in\mathbb{R}^2$ *dans la base* $\big((1,1),(1,-1)\big)$ *sont donc* $\left(\frac{x+y}{2},\frac{x-y}{2}\right)$.

Remarquons que nous avions en fait montré, par résolution d'un système, que pour tout vecteur $(x,y)\in\mathbb{R}^2$, *il existe un unique couple* $(\lambda,\mu)\in\mathbb{R}^2$ *tel que* $(x,y)=\lambda(1,1)+\mu(1,-1)$. *D'après la proposition 53, on obtient alors directement que la famille* $\big((1,1),(1,-1)\big)$ *est une base de* $\mathbb{R}^2$.

Lorsque l'on cherche une base d'un ensemble, on peut commencer par chercher une famille génératrice en écrivant l'ensemble comme un Vect, puis on vérifie qu'il s'agit d'une famille libre.

EXEMPLE 57 — *Reprenons l'ensemble* $H=\{(x,y,z)\in\mathbb{R}^3 \mid 2x-y+3z=0\}$ *des exemples 38 et déterminons une base de* H.

- *Nous avons vu que* $H=\mathrm{Vect}((1,2,0),(0,3,1))$. *La famille* $\big((1,2,0),(0,3,1)\big)$ *est donc une famille génératrice de* H.
- *Vérifions que cette famille est libre. Soit* $(\lambda,\mu)\in\mathbb{R}^2$ *tel que* $\lambda(1,2,0)+\mu(0,3,1)=(0,0,0)$.
  On a donc $\begin{cases}\lambda=0\\ 2\lambda+3\mu=0\\ \mu=0\end{cases}$.
  Donc $\lambda=\mu=0$.
  La famille $\big((1,2,0),(0,3,1)\big)$ *est donc libre.*
- *Conclusion : La famille* $\big((1,2,0),(0,3,1)\big)$ *est donc une base de* H.

1.4 Espaces vectoriels de dimension finie

1.4.1 Définition

DÉFINITION 58
Soit E *un* $\mathbb{K}$*-espace vectoriel. On dit que* E *est de* ***dimension finie*** \有限维\ *si* E *possède une famille génératrice finie. Sinon, on dit que* E *est de* ***dimension infinie*** \无线维\.

EXEMPLES 59

- *Les* $\mathbb{K}$*-espaces vectoriels* $\mathbb{K}^n$, $\mathbb{K}_n[X]$ *et* $\mathcal{M}_2(\mathbb{K})$ *sont de dimension finie. En effet, leur base canonique est une famille génératrice finie.*
- *Le* $\mathbb{K}$*-espace vectoriel* $\mathbb{K}[X]$ *est de dimension infinie. En effet, aucune famille finie n'engendre* $\mathbb{K}[X]$.

1.4.2 Existence de bases finies

Nous allons démontrer dans cette partie que tout espace vectoriel E de dimension finie admet au moins une base, puis dans la partie suivante que deux bases de E ont le même nombre d'éléments. Cela nous permettra de définir la dimension de E comme le nombre d'éléments d'une base quelconque de E.

THÉORÈME 60
Soit E un $\mathbb{K}$-espace vectoriel tel que $E \neq \{\vec{0}_E\}$. Soit $\mathcal{G}$ une famille génératrice finie de E. Soit $\mathcal{L}$ une sous-famille de $\mathcal{G}$ telle que $\mathcal{L}$ est libre[1]*. Alors il existe une base finie $\mathcal{B}$ de E telle que $\mathcal{L} \subset \mathcal{B} \subset \mathcal{G}$.*

Preuve — Soit $\mathcal{G} = (\vec{x}_1, \ldots, \vec{x}_n)$ une famille génératrice de E. Soit $\mathcal{L}$ une famille libre contenue dans $\mathcal{G}$.

Si $\mathcal{L}$ est génératrice alors c'est une base et on a le résultat.

Supposons donc que $\mathcal{L}$ n'est pas génératrice. Quitte à changer la numérotation, supposons que $\mathcal{L} = (\vec{x}_1, \ldots, \vec{x}_p)$ avec $p < n$.

- Alors il existe $\vec{x}_{i_1} \in \{\vec{x}_{p+1}, \ldots, \vec{x}_n\}$ tel que la famille $(\vec{x}_1, \ldots, \vec{x}_p, \vec{x}_{i_1})$ est libre.
  En effet, sinon, chaque vecteur $\vec{x}_i$ avec $i \in \{p+1, \ldots, n\}$ serait combinaison linéaire des vecteurs $\vec{x}_j$ avec $j \in \{1, \ldots, p\}$ et alors chaque vecteur $\vec{x}$ de E pourrait s'écrire comme combinaison linéaire des vecteurs de la famille $\mathcal{L}$. La famille $\mathcal{L}$ serait donc génératrice, ce qui est absurde.
  On peut donc compléter la famille $\mathcal{L}$ par un vecteur $\vec{x}_{i_1} \in \{\vec{x}_{p+1}, \ldots, \vec{x}_n\}$ et la famille $(\vec{x}_1, \ldots, \vec{x}_p, \vec{x}_{i_1})$ est libre.
- Si cette famille est génératrice, c'est une base et on a le résultat. Sinon, on peut à nouveau trouver un vecteur $\vec{x}_{i_2}$ appartenant à $\mathcal{G}$ mais n'étant pas un vecteur de la famille $(\vec{x}_1, \ldots, \vec{x}_p, \vec{x}_{i_1})$ et telle que la famille $(\vec{x}_1, \ldots, \vec{x}_p, \vec{x}_{i_1}, \vec{x}_{i_2})$ soit libre.
- On construit ainsi de proche en proche une suite de familles libres $\mathcal{L}_1$, $\mathcal{L}_2$, …, telles que
  $$\mathcal{L}_1 \subsetneq \mathcal{L}_2 \subsetneq \ldots \subset \mathcal{G}.$$
  Comme $\mathcal{G}$ est une famille finie, il existe $k \in \mathbb{N}$ tel que $\mathcal{L}_k$ est libre et génératrice. C'est donc une base de E telle que $\mathcal{L} \subset \mathcal{L}_k \subset \mathcal{G}$.

□

Nous pouvons en déduire directement les résultats suivants.

THÉORÈME 61
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie tel que $E \neq \{\vec{0}_E\}$.

- *De toute famille génératrice finie, on peut extraire une base finie.*
- Théorème de la base incomplète :
  Toute famille libre peut être complétée en une base finie.
- *E admet au moins une base finie.*

Preuve —

- Soit $\mathcal{G}$ une famille génératrice de E. Comme $E \neq \{\vec{0}_E\}$, la famille $\mathcal{G}$ contient un vecteur non nul $\vec{x}$. La famille $(\vec{x})$ est donc libre. D'après le théorème précédent, il existe donc une base $\mathcal{B}$ telle que $(\vec{x}) \subset \mathcal{B} \subset \mathcal{G}$. La famille $\mathcal{B}$ est donc une base de E, extraite de $\mathcal{G}$.
- Soit $\mathcal{L}$ une famille libre de E. E étant de dimension finie, E admet une famille génératrice finie $\mathcal{G}$. La famille $\mathcal{G} \cup \mathcal{L}$ est génératrice car elle contient une famille génératrice.
  D'après le théorème précédent, il existe donc une base $\mathcal{B}$ telle que $\mathcal{L} \subset \mathcal{B} \subset \mathcal{L} \cup \mathcal{G}$. La famille $\mathcal{L}$ est donc complétée en une famille $\mathcal{B}$, base de E.
- E étant un espace vectoriel de dimension finie, E admet une famille génératrice finie $\mathcal{G}$. D'après le premier point, on peut donc extraire de $\mathcal{G}$ une base finie. E admet donc au moins une base finie.

□

REMARQUE 62 — *Plus précisément, nous avons démontré que toute famille libre peut être complétée en une base en choisissant les vecteurs dans n'importe quelle famille génératrice.*

REMARQUE 63 — *Dans le cas où $E = \{\vec{0}_E\}$, aucune famille de vecteurs de E n'est libre et E ne possède donc pas de base.*

1. Il en existe, il suffit de prendre par exemple la famille constituée d'un vecteur non nul de $\mathcal{G}$, qui est une famille libre. Un tel vecteur existe car on a supposé $E \neq \{\vec{0}_E\}$.

1.4.3 Dimension

PROPOSITION 64
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie engendré par n éléments. Alors toute famille libre de E possède au plus n éléments.

Preuve — Soient $\mathcal{G} = (\vec{x}_1, \dots, \vec{x}_n)$ une famille génératrice finie de E et $\mathcal{F} = (\vec{y}_1, \dots, \vec{y}_m)$ une famille de m vecteurs de E avec $m > n$. Montrons que $\mathcal{F}$ est une famille liée.

- Si $\mathcal{F}$ contient un vecteur nul alors $\mathcal{F}$ est liée et la proposition est démontrée.
- Supposons donc que pour tout $i \in \{1, \dots, m\}$, $\vec{y}_i \neq \vec{0}_E$. La famille $\mathcal{G}$ étant génératrice, il existe $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$ tel que $\vec{y}_1 = \sum_{i=1}^{n} \lambda_i \cdot \vec{x}_i$.
  Comme $\vec{y}_1 \neq \vec{0}_E$, les λ_i sont non tous nuls. Quitte à réindicer, supposons que $\lambda_1 \neq 0$. Alors $\vec{x}_1 = \dfrac{1}{\lambda_1} \cdot \vec{y}_1 + \sum_{i=2}^{n} \dfrac{\lambda_i}{\lambda_1} \cdot \vec{x}_i$.
  On en déduit que tout élément $\vec{x}$ de E s'écrit comme combinaison linéaire de $\vec{y}_1$, $\vec{x}_2$, …, $\vec{x}_n$. La famille $(\vec{y}_1, \vec{x}_2, \dots, \vec{x}_n)$ est donc génératrice.
- Cette famille étant génératrice, il existe $(\mu_1, \dots, \mu_n) \in \mathbb{K}^n$ tel que $\vec{y}_2 = \mu_1 \cdot \vec{y}_1 + \sum_{i=2}^{n} \mu_i \cdot \vec{x}_i$.
  Si, pour tout $i \in \{2, \dots, n\}$, $\mu_i = 0$ alors $\vec{y}_2 = \lambda_1 \cdot \vec{y}_1$ et la famille $(\vec{y}_1, \vec{y}_2, \dots, \vec{y}_m)$ est liée, et la proposition est alors démontrée.
  Sinon, quitte à réindicer, supposons que $\mu_2 \neq 0$. Alors $\vec{x}_2 = \dfrac{1}{\mu_2} \cdot \vec{y_2} + \dfrac{\mu_1}{\mu_2} \cdot \vec{y}_1 + \sum_{i=3}^{n} \dfrac{\mu_i}{\mu_2} \cdot \vec{x}_i$.
  La famille $(\vec{y}_1, \vec{y}_2, \vec{x}_3, \dots, \vec{x}_n)$ est donc génératrice.
  Ainsi, on obtient à chaque étape une famille génératrice sous la forme $(\vec{y}_1, \dots, \vec{y}_p, \vec{x}_{p+1}, \dots, \vec{x}_n)$, où $p \leq n$.
  En particulier, pour $p = n$, la famille $(\vec{y_1}, \dots, \vec{y}_n)$ est génératrice. On en déduit que $\vec{y}_{n+1}$ s'écrit comme combinaison linéaire des $\vec{y}_i$ avec $i \in \{1, \dots, n\}$.
  La famille $(\vec{y}_1, \dots, \vec{y}_n, \vec{y}_{n+1})$ est donc liée. Toute famille contenant une famille liée étant liée, on en déduit que la famille $(\vec{y_1}, \dots, \vec{y}_m)$ est liée.
- Finalement, toute famille contenant strictement plus de n vecteurs est liée. Une famille libre contient donc au maximum n vecteurs.

□

Une famille constituée de n éléments est appelée **famille de cardinal** n.

THÉORÈME 65
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Toutes les bases de E sont finies et de même cardinal.

Preuve — Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E de cardinaux n et n'. Comme $\mathcal{B}$ est génératrice et $\mathcal{B}'$ est libre, d'après la proposition précédente, $n' \leq n$. De même, comme $\mathcal{B}'$ est génératrice et $\mathcal{B}$ est libre, $n \leq n'$. D'où $n = n'$. □

Nous pouvons maintenant définir la notion de dimension.

DÉFINITION 66
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Le cardinal commun à toutes les bases de E est appelé ***dimension*** \维数\ *de E, et est noté* $\dim(E)$ *(ou* $\dim_{\mathbb{K}}(E)$ *s'il y a ambiguïté sur le corps* $\mathbb{K}$*)..*

Par convention, si $E = \{\vec{0}_E\}$, alors $\dim(E) = 0$.

DÉFINITION 67
Soient E un $\mathbb{K}$-espace vectoriel.

- *Si* $\dim(E) = 1$*, on dit que E est une* ***droite vectorielle****.*
- *Si* $\dim(E) = 2$*, on dit que E est un* ***plan vectoriel****.*

Pour déterminer la dimension d'un espace vectoriel E, on trouve donc une base de E puis on compte le nombre d'éléments de cette base.

EXEMPLES 68 *À partir des bases canoniques des espaces vectoriels suivants, on obtient leur dimension :*

- $\dim \mathbb{K}^n = n$,
- $\dim \mathbb{K}_n[X] = n + 1$,
- $\dim \mathcal{M}_{n,p}(\mathbb{K}) = np$.
- $\dim \mathcal{M}_n(\mathbb{K}) = n^2$,
- $\dim_{\mathbb{C}} \mathbb{C} = 1$,
- $\dim_{\mathbb{R}} \mathbb{C} = 2$.

PROPOSITION 69

- *Soient E et F des $\mathbb{K}$-espaces vectoriels de dimension finie. Alors $E \times F$ est de dimension finie et*

$$\dim(E \times F) = \dim E + \dim F.$$

- *Plus généralement, soient E_1, ..., E_p des $\mathbb{K}$-espaces vectoriels de dimension finie. Alors*

$$\dim(E_1 \times \ldots \times E_p) = \dim E_1 + \ldots + \dim E_p.$$

Preuve —

- Soient $(\vec{e}_1, \ldots, \vec{e}_m)$ une base de E et $(\vec{f}_1, \ldots, \vec{f}_n)$ une base de F. Montrons que la famille

$$\mathcal{B} = \big((\vec{e}_1, \vec{0}_F), \ldots, (\vec{e}_m, \vec{0}_F), (\vec{0}_E, \vec{f}_1), \ldots, (\vec{0}_E, \vec{f}_n)\big)$$

  est une base de $E \times F$.

  — Montrons que $\mathcal{B}$ est une famille génératrice de $E \times F$. Soit $(\vec{x}, \vec{y}) \in E \times F$. Comme $\vec{x} \in E$, il existe $(\lambda_1, \ldots, \lambda_m)$ tel que $\vec{x} = \sum_{i=1}^{m} \lambda_i \cdot \vec{e}_i$. Comme $\vec{y} \in F$, il existe $(\mu_1, \ldots, \mu_n)$ tel que $\vec{y} = \sum_{j=1}^{n} \mu_j \cdot \vec{f}_j$. On a donc

$$(\vec{x}, \vec{y}) = \left(\sum_{i=1}^{m} \lambda_i \cdot \vec{e}_i, \sum_{j=1}^{n} \mu_j \cdot \vec{f}_j\right) = \sum_{i=1}^{m} \lambda_i \cdot (\vec{e}_i, \vec{0}_F) + \sum_{j=1}^{n} \mu_j \cdot (\vec{0}_E, \vec{f}_j).$$

  Donc $(\vec{x}, \vec{y})$ s'écrit donc comme combinaison linéaire des éléments de $\mathcal{B}$.

  — Montrons que $\mathcal{B}$ est une famille libre. Soient $(\lambda_1, \ldots, \lambda_m) \in \mathbb{K}^m$ et $(\mu_1, \ldots, \mu_n) \in \mathbb{K}^n$ tels que

$$\sum_{i=1}^{m} \lambda_i \cdot (\vec{e}_i, \vec{0}_F) + \sum_{j=1}^{m} \mu_j \cdot (\vec{0}_E, \vec{f}_j) = (\vec{0}_E, \vec{0}_F).$$

  On a donc

$$(\sum_{i=1}^{m} \lambda_i \cdot \vec{e}_i, \sum_{j=1}^{n} \mu_j \cdot \vec{f}_j) = (\vec{0}_E, \vec{0}_F),$$

  donc $\sum_{i=1}^{m} \lambda_i \cdot \vec{e}_i = \vec{0}_E$ et $\sum_{j=1}^{n} \mu_j \cdot \vec{f}_j = \vec{0}_F$.

  Comme $(\vec{e}_1, \ldots, \vec{e}_m)$ est une base de E, pour tout $i \in \{1, \ldots, m\}$, $\lambda_i = 0$. Comme $(\vec{f}_1, \ldots, \vec{f}_n)$ est une base de F, pour tout $i \in \{1, \ldots, n\}$, $\mu_j = 0$. Donc $\mathcal{B}$ est une famille libre.

  De ces deux points, on en déduit que $\mathcal{B}$ est une base de $E \times F$. Cette base est constituée de $m + n$ éléments avec $m = \dim E$ et $n = \dim F$. Donc $\dim(E \times F) = \dim E + \dim F$.

- On peut le démontrer par récurrence par exemple.

□

1.4.4 Caractérisation des bases en dimension finie

Les résultats de cette partie sont importants et seront beaucoup utilisés en pratique.

PROPOSITION 70

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.

- *Toute famille libre possède au plus n éléments.*
- *Toute famille génératrice possède au moins n éléments.*

Preuve — Soit $\mathcal{B}$ une base de E. Alors, par définition de la dimension, $\mathcal{B}$ est de cardinal n.

- La famille $\mathcal{B}$ étant une famille génératrice à n éléments, d'après la proposition 64, une famille libre possède au plus n éléments.
- Soit $\mathcal{G}$ une famille génératrice à m éléments. La famille $\mathcal{B}$ étant une famille libre à n éléments, d'après la proposition 64, $n \leq m$. Donc $\mathcal{G}$ possède au moins n éléments.

□

THÉORÈME 71

Soit E un $\mathbb{K}$-espace vectoriel de dimension n.

- *Toute famille libre ayant n éléments est une base.*
- *Toute famille génératrice ayant n éléments est une base.*

Preuve —

- Soit $\mathcal{L}$ une famille libre à n éléments. D'après le théorème de la base incomplète, on peut compléter $\mathcal{L}$ en une base. Par définition de la dimension, on obtient alors une famille à n éléments. On n'a donc ajouté aucun élément à $\mathcal{L}$ pour obtenir une base. $\mathcal{L}$ était donc une base.
- Soit $\mathcal{G}$ est une famille génératrice à n éléments. De la même manière, on peut extraire de G une base, composée de n vecteurs. C'est donc que l'on n'a retiré aucun vecteur à $\mathcal{G}$ pour obtenir une base. Donc $\mathcal{G}$ est une base.

□

Corollaire 72
Soit E un $\mathbb{K}$-espace vectoriel de dimension n. Soit $(\vec{x}_1, \dots, \vec{x}_n)$ une famille constituée d'exactement n vecteurs. Alors les propositions suivantes sont équivalentes :

- *$(\vec{x}_1, \dots, \vec{x}_n)$ est une base,*
- *$(\vec{x}_1, \dots, \vec{x}_n)$ est une famille libre,*
- *$(\vec{x}_1, \dots, \vec{x}_n)$ est une famille génératrice.*

 Pour dire qu'une famille libre/génératrice est une base, il faut bien vérifier qu'elle a le même nombre de vecteurs que la dimension de E.

Exemples 73

- *La famille $\big((1,2,0),(0,1,2),(2,0,1)\big)$ est une base de $\mathbb{R}^3$.*
  En effet, on vérifie que c'est une famille libre. Soit $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$ tel que
  $$\lambda_1(1,2,0) + \lambda_2(0,1,2) + \lambda_3(2,0,1) = (0,0,0).$$
  Alors $\begin{cases} \lambda_1 + 2\lambda_3 = 0 \\ 2\lambda_1 + \lambda_2 = 0 \\ 2\lambda_2 + \lambda_3 = 0 \end{cases}$.
  Donc $\lambda_1 = \lambda_2 = \lambda_3 = 0$.
  Donc la famille $\big((1,2,0),(0,1,2),(2,0,1)\big)$ est une famille libre, constituée de trois éléments dans l'espace vectoriel $\mathbb{R}^3$ de dimension 3. La famille $\big((1,2,0),(0,1,2),(2,0,1)\big)$ est donc une base de $\mathbb{R}^3$.
- *Nous avions vu que $\mathrm{Vect}((1,1),(1,-1)) = \mathbb{R}^2$. La famille $((1,1),(1,-1))$ est donc une famille génératrice de $\mathbb{R}^2$, constituée de deux éléments dans l'espace vectoriel $\mathbb{R}^2$ de dimension 2. La famille $((1,1),(1,-1))$ est donc une base de $\mathbb{R}^2$.*
  Il est donc inutile ici de montrer que cette famille est libre (comme nous l'avions fait dans une partie précédente) pour obtenir le fait que c'est une base.
- *La famille $(1, X-2, X^2+X+1, 2X^3-2)$ est une base de $\mathbb{R}_3[X]$.*
  En effet, il s'agit d'une famille de polynômes de degrés échelonnés, c'est donc une famille libre de $\mathbb{R}_3[X]$. Cette famille est constituée de 4 éléments dans l'espace vectoriel $\mathbb{R}_3[X]$ de dimension 4. La famille $(1, X-2, X^2+X+1, 2X^3-2)$ est donc une base de $\mathbb{R}_3[X]$.

Résumons.

Méthode 74 — *Il y a quatre manières de montrer qu'une famille $\mathcal{B}$ de vecteurs est une base d'un espace vectoriel E de dimension finie :*

- *On montre que tout vecteur de E s'écrit de manière unique comme une combinaison linéaire de vecteurs de la famille $\mathcal{B}$.*
- *On montre que la famille $\mathcal{B}$ est une famille libre et génératrice de E.*
- *On montre que la famille $\mathcal{B}$ est une famille libre et on vérifie que $\dim(E) = \mathrm{card}(\mathcal{B})$.*
- *On montre que la famille $\mathcal{B}$ est génératrice de E et on vérifie que $\dim(E) = \mathrm{card}(\mathcal{B})$.*

Si l'on connait la dimension de E, les deux dernières méthodes sont souvent plus rapides.

1.4.5 Dimension d'un sous-espace vectoriel

PROPOSITION 75
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit F un sous-espace vectoriel de E. Alors F est de dimension finie et

- $\dim F \leq \dim E$,
- $\dim F = \dim E$ *si et seulement si* $E = F$.

Preuve —

- Si $F = \{\vec{0}_E\}$, on a le résultat.
  Supposons $F \neq \{\vec{0}_E\}$. Notons n la dimension de E. Soit N l'ensemble des cardinaux des familles libres de F. Toute famille libre de F est une famille libre de E donc contient au plus n éléments. N est donc majoré par n. N étant une partie non vide de $\mathbb{N}$, N admet un maximum p avec $p \leq n$.
  Soit $\mathcal{L} = (\vec{x}_1, \ldots, \vec{x}_p)$ une famille libre de F à p éléments. Montrons que $\mathcal{L}$ est une base de F.
  Soit $\vec{x} \in F$. Comme F n'admet pas de famille libre à plus de p éléments, la famille $(\vec{x}_1, \ldots, \vec{x}_p, \vec{x})$ est liée. Donc $\vec{x}$ est combinaison linéaire des vecteurs $\vec{x}_i$. $\mathcal{L}$ est donc une famille génératrice de F.
  Donc $\mathcal{L}$ est une base de F et F est de dimension finie $p \leq n = \dim E$.
- Supposons que $\dim E = \dim F$. En reprenant la démonstration du point précédent, $\mathcal{L}$ est une famille libre de F donc de E constituée de $n = \dim E$ éléments. C'est donc une base de E. $\mathcal{L}$ étant génératrice, on a $E = \text{Vect}(\mathcal{L}) = F$.

□

DÉFINITION 76
Soit E un $\mathbb{K}$-espace vectoriel de dimension n. Un sous-espace vectoriel de E de dimension $n-1$ est appelé un ***hyperplan****.*

EXEMPLES 77

- *Nous avons vu à l'exemple 38 que l'ensemble* $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$ *est engendré par le vecteur* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. *Ce vecteur étant non nul, la famille* $\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$ *est libre et génératrice, c'est donc une base de G. Donc G est un sous-espace vectoriel de $\mathcal{M}_2(\mathbb{R})$ de dimension 1. C'est une droite vectorielle de $\mathcal{M}_2(\mathbb{R})$.*
- *Nous avons vu à l'exemple 57 qu'une base de l'ensemble* $H = \{(x, y, z) \in \mathbb{R}^3 \mid 2x - y + 3z = 0\}$ *est la famille* $\big((1, 2, 0), (0, 3, 1)\big)$. *Donc H est un sous-espace vectoriel de $\mathbb{R}^3$ de dimension 2. C'est un plan vectoriel de $\mathbb{R}^3$.*
- *Posons* $\vec{u} = (1, 0, 1)$, $\vec{v} = (2, 1, 1)$ *et* $\vec{w} = (1, 1, 0)$. *Déterminons la dimension du sous-espace vectoriel de $\mathbb{R}^3$,* $V = \text{Vect}(\vec{u}, \vec{v}, \vec{w})$.
  Par opérations sur les Vect, *on a*

$$\begin{aligned} V &= \text{Vect}(\vec{u}, \vec{v}, \vec{w}) \\ &= \text{Vect}(\vec{u}, \vec{v} - \vec{u}, \vec{w}) \\ &= \text{Vect}(\vec{u}, \vec{w}, \vec{w}) \\ &= \text{Vect}(\vec{u}, \vec{w}). \end{aligned}$$

  La famille $(\vec{u}, \vec{w})$ est donc une famille génératrice de V.
  Les vecteurs $\vec{u}$ et $\vec{w}$ ne sont pas colinéaires, donc la famille $(\vec{u}, \vec{w})$ est libre.
  Libre et génératrice, $(\vec{u}, \vec{w})$ est donc une base de V et V est de dimension 2.

Le résultat suivant propose une méthode pour montrer l'égalité de deux espaces vectoriels.

PROPOSITION 78
Soit E un $\mathbb{K}$-espace vectoriel. Soient F et G deux sous-espaces vectoriels de dimension finie de E. Si $F \subset G$ et $\dim(F) = \dim(G)$ alors $F = G$.

Preuve — Posons $p = \dim(F)$. Soit $\mathcal{B} = (\vec{x}_1, \ldots, \vec{x}_p)$ une base de F. Alors $\mathcal{B}$ est une famille libre dans F, donc dans G. $\mathcal{B}$ est donc une famille libre constituée de p éléments dans un espace vectoriel G de dimension p. $\mathcal{B}$ est donc une base de G. Donc $G = \text{Vect}(\vec{x}_1, \ldots, \vec{x}_p) = F$. □

1.4.6 Rang d'une famille de vecteurs

Définition 79
Soit E un $\mathbb{K}$-espace vectoriel. Soient $\vec{x}_1, \ldots, \vec{x}_n$ des éléments de E. On appelle ***rang*** *de la famille $(\vec{x}_1, \ldots, \vec{x}_n)$, noté $\mathrm{rg}(\vec{x}_1, \ldots, \vec{x}_n)$, la dimension de l'espace vectoriel engendré par ces vecteurs :*

$$\mathrm{rg}(\vec{x}_1, \ldots, \vec{x}_n) = \dim\left(\mathrm{Vect}(\vec{x}_1, \ldots, \vec{x}_n)\right).$$

Le rang d'une famille de vecteurs est le plus grand nombre de vecteurs linéairement indépendants qu'elle contient.

Exemples 80

- *En reprenant le troisième point de l'exemple 77, on obtient que* $\mathrm{rg}((1,0,1),(2,1,1),(1,1,0)) = 2$.
- $\mathrm{rg}(1, X, X^2, X^3) = 4$
- $\mathrm{rg}(X, 2X, 4X) = 1$.

Proposition 81
Soit E un $\mathbb{K}$-espace vectoriel de dimension quelconque. Soient $\vec{x}_1, \ldots, \vec{x}_p$ des éléments de E. On a

$$\mathrm{rg}(\vec{x}_1, \ldots, \vec{x}_p) \leq p,$$

avec égalité si et seulement si la famille $(\vec{x}_1, \ldots, \vec{x}_p)$ est libre.

Preuve — $\mathrm{Vect}(\vec{x}_1, \ldots, \vec{x}_p)$ est un espace vectoriel engendré par la famille finie $(\vec{x}_1, \ldots, \vec{x}_p)$, il est donc de dimension finie, inférieure à p, nombre d'éléments de cette famille génératrice. Donc

$$\mathrm{rg}(\vec{x}_1, \ldots, \vec{x}_p) = \dim\left(\mathrm{Vect}(\vec{x}_1, \ldots, \vec{x}_p)\right) \leq p.$$

En dimension p, une famille de p vecteurs est libre si et seulement si elle est génératrice. □

Proposition 82
Soit E un $\mathbb{K}$-espace vectoriel de dimension n. Soient $\vec{x}_1, \ldots, \vec{x}_p$ des éléments de E. On a

$$\mathrm{rg}(\vec{x}_1, \ldots, \vec{x}_p) \leq n,$$

avec égalité si et seulement si la famille $(\vec{x}_1, \ldots, \vec{x}_p)$ est génératrice de E.

Preuve — $\mathrm{Vect}(\vec{x}_1, \ldots, \vec{x}_p)$ est un sous-espace vectoriel de E donc $\dim(\mathrm{Vect}(\vec{x}_1, \ldots, \vec{x}_p) \leq \dim(E) = n$, avec égalité si et seulement si $\mathrm{Vect}(\vec{x}_1, \ldots, \vec{x}_p) = E$, c'est-à-dire si et seulement si la famille $(\vec{x}_1, \ldots, \vec{x}_n)$ est génératrice. □

Corollaire 83
Soit E un $\mathbb{K}$-espace vectoriel de dimension n. Soient $\vec{x}_1, \ldots, \vec{x}_n$ des éléments de E. La famille $(\vec{x}_1, \ldots, \vec{x}_n)$ est une base de E si et seulement si

$$\mathrm{rg}(\vec{x}_1, \ldots, \vec{x}_n) = n.$$

1.4.7 Matrice d'une famille de vecteurs

Définition 84
Soit E un $\mathbb{K}$-espace vectoriel de dimension n. Soit $\mathcal{B} = (\vec{e}_1, \ldots, \vec{e}_n)$ une base de E. Soit $\mathcal{F} = (\vec{x}_1, \ldots, \vec{x}_p)$ une famille de vecteurs de E. Pour tout $j \in \{1, \ldots, p\}$, on note $(a_{1,j}, \ldots, a_{n,j})$ les coordonnées de $\vec{x}_j$ dans la base $\mathcal{B}$.

La matrice $A = (a_{i,j})_{\substack{i=1\ldots n \\ j=1\ldots p}}$, notée $\mathrm{mat}_{\mathcal{B}}(\mathcal{F})$ est appelée ***matrice de $\mathcal{F}$ dans la base $\mathcal{B}$.***

Remarque 85 — *Soit $\vec{x} \in E$ et soit $\mathcal{B}$ une base de E. Alors $\mathrm{mat}_{\mathcal{B}}(\vec{x})$ est la colonne des coordonnées de $\vec{x}$ dans la base $\mathcal{B}$.*

Exemples 86

- *Dans la base canonique $\mathcal{B}_c$ de $\mathbb{R}^4$,*

$$\mathrm{mat}_{\mathcal{B}_c}((1,0,-1,2),(2,1,0,1),(-1,0,0,1)) = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \\ 2 & 1 & 1 \end{pmatrix}.$$

- *Dans la base canonique $\mathcal{B}_c$ de $\mathbb{R}_2[X]$,*

$$\mathrm{mat}_{\mathcal{B}_c}(1+X, X+2X^2, -1-X+X^2) = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 1 & -1 \\ 0 & 2 & 1 \end{pmatrix}.$$

1.5 Somme de sous-espaces vectoriels

Dans cette partie, E désigne un $\mathbb{K}$-espace vectoriel.

1.5.1 Somme de deux sous-espaces vectoriels

Définition 87
*Soient F et G deux sous-espaces vectoriels de E. On appelle **somme de F et G** \线性空间F与G的和\ l'ensemble*

$$F+G = \{\vec{x}+\vec{y} \mid \vec{x} \in F \text{ et } \vec{y} \in G\} = \{\vec{u} \in E \mid \exists\, (\vec{x},\vec{y}) \in F \times G,\ \vec{u} = \vec{x}+\vec{y}\}.$$

Proposition 88
Soient F et G deux sous-espaces vectoriels de E. La somme $F+G$ est un sous-espace vectoriel de E. De plus, $F+G$ est le plus petit sous-espace vectoriel de E contenant F et G.

Preuve — Vérifions la caractérisation d'un sous-espace vectoriel.

- E est stable par combinaisons linéaires donc, pour tout $(\vec{x},\vec{y}) \in F \times G$, $\vec{x}+\vec{y} \in E$. Donc $F+G \subset E$.
- Comme F et G sont des sous-espaces vectoriels de E, $\vec{0}_E \in F$ et $\vec{0}_E \in G$. On a donc $\vec{0}_E = \vec{0}_E + \vec{0}_E \in F+G$.
- Soient $(\vec{u},\vec{v}) \in (F+G)^2$ et $(\lambda,\mu) \in \mathbb{K}^2$. Il existe $(\vec{x}_1,\vec{y}_1) \in F \times G$ et $(\vec{x}_2,\vec{y}_2) \in F \times G$ tels que $\vec{u} = \vec{x}_1+\vec{y}_1$ et $\vec{v} = \vec{x}_2+\vec{y}_2$. Alors $\lambda\cdot\vec{u}+\vec{v} = \lambda\cdot\vec{x}_1+\lambda\cdot\vec{y}_1+\vec{x}_2+\vec{y}_2 = (\lambda\cdot\vec{x}_1+\vec{y}_1)+(\lambda\cdot\vec{x}_2+\vec{y}_2) \in F+G$ puisque F et G sont des sous-espaces vectoriels de E.

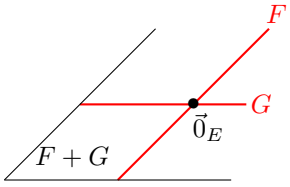
Donc $F+G$ est un sous-espace vectoriel de E ;

On a $F \subset F+G$ car pour tout $\vec{x} \in F$, $\vec{x} = \vec{x}+\vec{0}_E$ et $\vec{0}_E \in G$. De même, $G \subset F+G$. Donc $F+G$ est un sous-espace vectoriel de E contenant F et G.

Soit H un sous-espace vectoriel de E contenant F et G. Alors, pour tout $\vec{x} \in F$ et tout $\vec{y} \in G$, $\vec{x}+\vec{y} \in H$ car $\vec{x} \in H$ et $\vec{y} \in H$ et H est stable par combinaisons linéaires. Donc $F+G \subset H$. □

Ainsi, tout sous-espace vectoriel de E contenant F et G contient aussi $F+G$.

Ne pas confondre la somme avec l'union ! L'union de deux sous-espaces vectoriels n'est pas en général un sous-espace vectoriel.



Exemples 89

- $\mathbb{R} + i\mathbb{R} = \mathbb{C}$. *En effet,* $\mathbb{R} + i\mathbb{R} = \{a + ib \mid (a, b) \in \mathbb{R}^2\}$.
- *Les droites vectorielles* $\text{Vect}((1, 0, 0))$ *et* $\text{Vect}((0, 1, 0))$ *ont pour somme le plan* $z = 0$. *En effet,*

$$\text{Vect}((1, 0, 0)) + \text{Vect}((0, 1, 0)) = \{(x, 0, 0) \mid x \in \mathbb{R}\} + \{(0, y, 0) \mid y \in \mathbb{R}\} = \{(x, y, 0) \mid (x, y) \in \mathbb{R}^2\}.$$

Remarque 90 — *Soient F et G deux sous-espaces vectoriels de E. On vérifie facilement les propriétés suivantes :*

- $F + G = G + F$,
- $F + E = E$,
- $F + \{\vec{0}_E\} = F$,
- $F + F = F$.

Théorème 91 (Formule de Grassmann)
Soient F et G deux sous-espaces vectoriels de dimension finie de E. Alors $F + G$ est de dimension finie et

$$\dim(F + G) = \dim(F) + \dim(G) - \dim(F \cap G).$$

Preuve — Posons $p = \dim(F)$, $q = \dim(G)$ et $r = \dim(F \cap G)$. Puisque $F \cap G$ est un sous-espace vectoriel de F et de G, $r \leq p$ et $r \leq q$. Considérons une base $(\vec{e}_1, \dots, \vec{e}_r)$ de $F \cap G$.

Puisque la famille $(\vec{e}_1, \dots, \vec{e}_r)$ est une famille libre de F, on peut la compléter en une base $(\vec{e}_1, \dots, \vec{e}_r, \vec{x}_{r+1}, \vec{x}_p)$ de F. De même, on peut la compléter en une base $(\vec{e}_1, \dots, \vec{e}_r, \vec{y}_{r+1}, \dots, \vec{y}_q)$ de G.

Or tout vecteur $\vec{u}$ de $F + G$ s'écrit comme somme d'un vecteur de F et d'un vecteur de G, donc est de la forme

$$\begin{aligned}\vec{u} = \lambda_1\vec{e}_1 + \dots + \lambda_r\vec{e}_r + \lambda_{r+1}\vec{x}_{r+1} + \dots + \lambda_p\vec{x}_p \\ + \mu_1\vec{e}_1 + \dots + \mu_r\vec{e}_r + \mu_{r+1}\vec{y}_{r+1} + \dots + \mu_q\vec{y}_q,\end{aligned}$$

où $\lambda_1, \dots, \lambda_p$, $\mu_1, \dots, \mu_q$ sont des éléments de $\mathbb{K}$, soit, en posant, pour tout $i \in \{1, \dots, r\}$, $\nu_i = \lambda_i + \mu_i$,

$$\vec{u} = \nu_1\vec{e}_1 + \dots + \nu_r\vec{e}_r + \lambda_{r+1}\vec{x}_{r+1} + \dots + \lambda_p\vec{x}_p + \mu_{r+1}\vec{y}_{r+1} + \dots + \mu_q\vec{y}_q.$$

La famille $(\vec{e}_1, \dots, \vec{e}_r, \vec{x}_{r+1}, \dots, \vec{x}_p, \vec{y}_{r+1}, \dots, \vec{y}_q)$ est donc une famille génératrice de $F + G$.

Montrons que cette famille est libre.

Soient $\nu_1, \dots, \nu_r, \lambda_{r+1}, \dots, \lambda_p, \mu_{r+1}, \dots, \mu_q$ des éléments de $\mathbb{K}$ tels que

$$\underbrace{\nu_1\vec{e}_1 + \dots + \nu_r\vec{e}_r}_{\vec{u} \in F \cap G} + \underbrace{\lambda_{r+1}\vec{x}_{r+1} + \dots + \lambda_p\vec{x}_p}_{\vec{v} \in F} + \underbrace{\mu_{r+1}\vec{y}_{r+1} + \dots + \mu_q\vec{y}_q}_{\vec{w} \in G} = \vec{0}_E.$$

On a $\vec{u} + \vec{v} + \vec{w} = \vec{0}_E$, donc $\vec{w} = -\vec{u} - \vec{v} \in F$ puisque $\vec{u}$ et $\vec{v}$ sont éléments de F. Donc $\vec{w} \in F \cap G$. Donc $\vec{w}$ s'écrit comme combinaison linéaire des $\vec{e}_i$, ce qui donne :

$$\mu_{r+1}\vec{y}_{r+1} + \dots + \mu_q\vec{y}_q = \rho_1\vec{e}_1 + \dots \rho_r\vec{e}_r,$$

où $(\nu_1, \dots, \nu_r) \in \mathbb{K}^r$.

La famille $(\vec{e}_1, \dots, \vec{e}_r, \vec{y}_{r+1}, \dots, \vec{y}_q)$ étant libre, on en déduit que pour tout $i \in \{r + 1, \dots, q\}$, $\mu_i = 0$.

De même, on obtient que pour tout $i \in \{r + 1, \dots, p\}$, $\lambda_i = 0$.

On en déduit donc que $\nu_1\vec{e}_1 + \dots + \nu_r\vec{e}_r = \vec{0}_E$. La famille $(\vec{e}_1, \dots, \vec{e}_r)$ étant libre, pour tout $i \in \{1, \dots, r\}$, $\nu_i = 0$.

La famille $(\vec{e}_1, \dots, \vec{e}_r, \vec{x}_{r+1}, \dots, \vec{x}_p, \vec{y}_{r+1}, \dots, \vec{y}_q)$ est donc libre. Libre et génératrice, c'est donc une base de $F + G$.

Ainsi,

$$\begin{aligned}\dim(F + G) &= r + (p - r) + (q - r) = p + q - r \\ &= \dim(F) + \dim(G) - \dim(F \cap G).\end{aligned}$$

□

1.5.2 Somme directe

Définition 92
Soient F et G deux sous-espaces vectoriels de E. On dit que la somme $F + G$ est ***directe*** \直和\, *et on note $F \oplus G$, si tout élément $\vec{u}$ de $F + G$ s'écrit de manière unique sous la forme $\vec{u} = \vec{x} + \vec{y}$ avec $\vec{x} \in F$ et $\vec{y} \in G$.*

Autrement dit, pour tout $\vec{u} \in F + G$, si $\vec{u} = \vec{x}_1 + \vec{y}_1$ et $\vec{u} = \vec{x}_2 + \vec{y}_2$ avec $(\vec{x}_1, \vec{y}_1) \in F \times G$ et $(\vec{x}_2, \vec{y}_2) \in F \times G$, alors $\vec{x}_1 = \vec{x}_2$ et $\vec{y}_1 = \vec{y}_2$.

Remarque 93 — *La seule différence entre $F+G$ et $F \oplus G$ est que le symbole $\oplus$ précise l'unicité de la décomposition.*

La proposition suivante est très utilisée pour montrer qu'une somme est directe.

Proposition 94
Soient F et G deux sous-espaces vectoriels de E. La somme $F+G$ est directe si et seulement si

$$F \cap G = \{\vec{0}_E\}.$$

Preuve — $\triangleright$ Supposons que la somme $F+G$ soit directe. Soit $\vec{u} \in F \cap G$. Alors $\vec{u} = \underbrace{\vec{u}}_{\in F} + \underbrace{\vec{0}_E}_{\in G} = \underbrace{\vec{0}_E}_{\in F} + \underbrace{\vec{u}}_{\in G}$. Donc par unicité de la décomposition, $\vec{u} = \vec{0}_E$. Donc $F \cap G \subset \{\vec{0}_E\}$. Comme $\vec{0}_E \in F$ et $\vec{0}_E \in G$, $\{\vec{0}_E\} \subset F \cap G$.

Donc $F \cap G = \{\vec{0}_E\}$.

$\triangleleft$ Réciproquement, supposons que $F \cap G = \{\vec{0}_E\}$. Soit $\vec{u} \in F+G$. Supposons que $\vec{u} = \vec{x}_1 + \vec{y}_1$ et $\vec{u} = \vec{x}_2 + \vec{y}_2$. On a alors $\vec{x}_1 + \vec{y}_1 = \vec{x}_2 + \vec{y}_2$, donc $\vec{x}_1 - \vec{x}_2 = \vec{y}_2 - \vec{y}_1$. Notons $\vec{v}$ cet élément. Comme F et G sont des sous-espaces vectoriels de E, $\vec{v} = \vec{x}_1 - \vec{y}_1 \in F$ et $\vec{v} = \vec{y}_2 - \vec{x}_2 \in G$. Donc $\vec{v} \in F \cap G$. Comme $F \cap G = \{\vec{0}_E\}$, $\vec{v} = \vec{0}_E$, et donc $\vec{x}_1 = \vec{x}_2$ et $\vec{y}_1 = \vec{y}_2$.

Donc F et G sont en somme directe.

D'où le résultat. □

Exemple 95 — *Dans $\mathbb{R}^3$, $F = \{(x,y,z) \in \mathbb{R}^3 \mid x+y+z=0\}$ et $G = \mathrm{Vect}((1,1,1))$ sont des sous-espaces vectoriels en somme directe.*

En effet, F et G sont des sous-espaces vectoriels de $\mathbb{R}^3$ puisque $F = \mathrm{Vect}((1,-1,0),(1,0,-1))$ et $G = \mathrm{Vect}(1,1,1)$.

Montrons qu'ils sont en somme directe. Soit $(x,y,z) \in F \cap G$. Alors $x+y+z=0$ et $x=y=z$. Donc $x=y=z=0$. Donc $(x,y,z)=(0,0,0)$. Donc $F \cap G \subset \{(0,0,0)\}$ et trivialement, $\{(0,0,0)\} \subset F \cap G$. Donc $F \cap G = \{(0,0,0)\}$. De la proposition précédente, on en déduit que F et G sont en somme directe.

Proposition 96
Soient F et G deux sous-espaces vectoriels de dimension finie de E. Alors F et G sont en somme directe si et seulement si

$$\dim(F+G) = \dim(F) + \dim(G).$$

Preuve — D'après la formule de Grassmann,

$$\dim(F+G) = \dim(F) + \dim(G)$$

si et seulement si $\dim(F \cap G) = 0$, soit si et seulement si $F \cap G = \{\vec{0}_E\}$, soit finalement si et seulement si F et G sont en somme directe. □

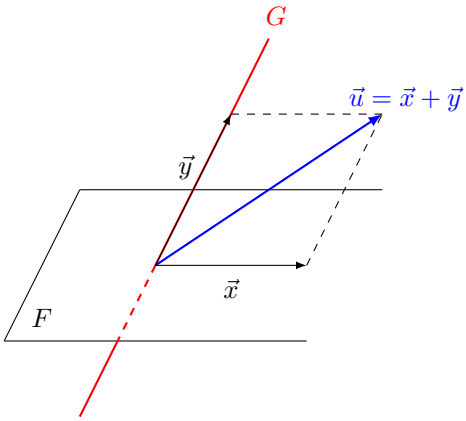
1.5.3 Sous-espaces vectoriels supplémentaires

Définition 97
*Soient F et G deux sous-espaces vectoriels de E. On dit que F et G sont **supplémentaires dans** E \两个子空间F和G互为E的补空间\ (ou que F est un supplémentaire de G dans E) si E est la somme directe de F et G, c'est-à-dire :*

1. *La somme de F et G est directe : $F+G = F \oplus G$,*
2. *La somme de F et G vaut E : $E = F+G$.*

On note alors $E = F \oplus G$.

Il faut bien distinguer les notions de « F et G sont en somme directe » et « E est la somme directe de F et G » (c'est-à-dire que la somme $F+G$ "remplit" E tout entier).



PROPOSITION 98
Soient F et G deux sous-espaces vectoriels de E. Alors F et G sont supplémentaires dans E si et seulement si tout élément $\vec{u}$ de E s'écrit de manière unique sous la forme $\vec{u} = \vec{x} + \vec{y}$ avec $\vec{x} \in F$ et $\vec{y} \in G$.

Preuve — Cela découle de la définition d'une somme directe et du fait que $E = F + G$. □

PROPOSITION 99
Soient F et G deux sous-espaces vectoriels de E. Alors F et G sont supplémentaires dans E si et seulement si

1. *$F \cap G = \{\vec{0}_E\}$,*
2. *$E = F + G$.*

Preuve — Cela découle immédiatement de la proposition 94. □

EXEMPLE 100 — *E et $\{\vec{0}_E\}$ sont des sous-espaces vectoriels supplémentaires de E.*

Ne pas confondre supplémentaire et complémentaire : un supplémentaire est un sous-espace vectoriel et n'est pas nécessairement unique, le complémentaire n'est pas un sous-espace vectoriel et il est unique.

PROPOSITION 101
On suppose ici E de dimension finie. Soient F et G deux sous-espaces vectoriels de E. Soient $\mathcal{B}_1 = (\vec{x}_1, \ldots, \vec{x}_p)$ une base de F et $\mathcal{B}_2 = (\vec{y}_1, \ldots, \vec{y}_q)$ une base de G. Alors $E = F \oplus G$ si et seulement si la famille $\mathcal{B} = (\vec{x}_1, \ldots, \vec{x}_p, \vec{y}_1, \ldots, \vec{y}_q)$, concaténée des bases $\mathcal{B}_1$ et $\mathcal{B}_2$, est une base de E.

Preuve — ▷ Supposons que $E = F \oplus G$. Alors tout élément $\vec{u}$ de E se décompose de manière unique comme somme d'un élément de F et d'un élément de G, et donc comme combinaison linéaire de la famille $\mathcal{B}$. Donc $\mathcal{B}$ est une base.

◁ Réciproquement, supposons que $\mathcal{B}$ est une base de E. Alors tout élément $\vec{u}$ de E s'écrit de manière unique sous la forme

$$\vec{u} = \underbrace{\lambda_1\vec{x}_1 + \ldots + \lambda_p\vec{x}_p}_{\in F} + \underbrace{\mu_1\vec{y}_1 + \ldots + \mu_q\vec{y}_q}_{\in G},$$

et donc de manière unique sous la forme $\vec{u} = \vec{x} + \vec{y}$ avec $\vec{x} \in F$ et $\vec{y} \in G$. Donc $E = F \oplus G$.

D'où le résultat. □

EXEMPLES 102

- *Deux droites non confondues passant par $(0,0)$ sont supplémentaires dans $\mathbb{R}^2$.*
  En effet, en notant $\mathcal{D}_1 = \text{Vect}(\vec{u})$ et $\mathcal{D}_2 = \text{Vect}(\vec{v})$, la famille $(\vec{u}, \vec{v})$ est libre puisque les vecteurs ne sont pas colinéaires. Formée de deux vecteurs, cette famille est donc une base de $\mathbb{R}^2$. Donc $\mathbb{R}^2 = \mathcal{D}_1 \oplus \mathcal{D}_2$.
- *Si $\mathcal{P}$ est un plan passant par $(0,0,0)$ et $\mathcal{D}$ est une droite non contenue dans le plan et passant par $(0,0,0)$ alors $\mathcal{P}$ et $\mathcal{D}$ sont supplémentaires dans $\mathbb{R}^3$.*
  En effet, en notant $\mathcal{P} = \text{Vect}(\vec{u}, \vec{v})$ et $\mathcal{D} = \text{Vect}(\vec{w})$, la famille $(\vec{u}, \vec{v}, \vec{w})$ est une base de $\mathbb{R}^3$.

- *L'ensemble des fonctions paires $\mathcal{P}$ et l'ensemble des fonctions impaires $\mathcal{I}$ sont supplémentaires dans $\mathcal{F}(\mathbb{R},\mathbb{R})$.*
  En effet, $\mathcal{P}$ et $\mathcal{I}$ sont des sous-espaces vectoriels de $\mathcal{F}(\mathbb{R},\mathbb{R})$ (à vérifier).
  1. *Montrons que $\mathcal{P}\cap\mathcal{I}=\{0_{\mathbb{R}\to\mathbb{R}}\}$. Soit $f\in\mathcal{P}\cap\mathcal{I}$. Pour tout $x\in\mathbb{R}$, $f(-x)=f(x)$ car f est paire, et $f(-x)=-f(x)$ car f est impaire. Donc, pour tout $x\in\mathbb{R}$, $f(x)=-f(x)$, donc $f(x)=0$. Donc f est la fonction nulle. Donc $\mathcal{P}\cap\mathcal{I}\subset\{0_{\mathbb{R}\to\mathbb{R}}\}$ et l'inclusion $\{0_{\mathbb{R}\to\mathbb{R}}\}\subset\mathcal{P}\cap\mathcal{I}$ est évidente. Ainsi, $\mathcal{P}\cap\mathcal{I}=\{0_{\mathbb{R}\to\mathbb{R}}\}$ et donc $\mathcal{P}$ et $\mathcal{I}$ sont en somme directe.*
  2. *Montrons que $\mathcal{F}(\mathbb{R},\mathbb{R})=\mathcal{P}+\mathcal{I}$. On a $\mathcal{P}+\mathcal{I}\subset\mathcal{F}(\mathbb{R},\mathbb{R})$. Réciproquement, soit $f\in\mathcal{F}(\mathbb{R},\mathbb{R})$. On a*
  $$f(x)=\frac{f(x)+f(-x)}{2}+\frac{f(x)-f(-x)}{2}$$
  et $x\longmapsto\dfrac{f(x)+f(-x)}{2}$ est une fonction paire et $x\longmapsto\dfrac{f(x)-f(-x)}{2}$ est une fonction impaire. Donc $f\in\mathcal{P}+\mathcal{I}$. Donc $\mathcal{F}(\mathbb{R},\mathbb{R})\subset\mathcal{P}+\mathcal{I}$ et l'inclusion $\mathcal{P}+\mathcal{I}\subset\mathcal{F}(\mathbb{R},\mathbb{R})$. Finalement $\mathcal{F}(\mathbb{R},\mathbb{R})=\mathcal{P}+\mathcal{I}$.

  D'où $\mathcal{F}(\mathbb{R},\mathbb{R})=\mathcal{P}\oplus\mathcal{I}$.
- *Dans $\mathcal{M}_2(\mathbb{R})$, considérons $A=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix}\mid a\in\mathbb{R}\right\}$ et $B=\left\{\begin{pmatrix}0&b\\c&d\end{pmatrix}\mid(b,c,d)\in\mathbb{R}^3\right\}$.*
  Alors $\mathcal{M}_2(\mathbb{R})=A\oplus B$.
  En effet, A et B sont des sous-espaces vectoriels de E puisque $A=\mathrm{Vect}\left(\begin{pmatrix}1&0\\0&0\end{pmatrix}\right)$ et
  $B=\mathrm{Vect}\left(\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\right)$.
  1. *Montrons que $A\cap B=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}\right\}$. Soit $M\in A\cap B$. Alors il existe $a\in\mathbb{R}$ tel que $M=\begin{pmatrix}a&0\\0&0\end{pmatrix}$ et il existe $(b,c,d)\in\mathbb{R}^3$ tel que $M=\begin{pmatrix}0&b\\c&d\end{pmatrix}$. Donc $\begin{pmatrix}a&0\\0&0\end{pmatrix}=\begin{pmatrix}0&b\\c&d\end{pmatrix}$. Par identification des coefficients, on en déduit que $a=0$, $b=0$, $c=0$ et $d=0$. Donc $M=0_2$. Donc $A\cap B\subset\{0_2\}$, puis $A\cap B=\{0_2\}$ (l'autre inclusion est évidente).*
  2. *Pour tout $(a,b,c,d)\in\mathbb{R}^4$, $\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a&0\\0&0\end{pmatrix}+\begin{pmatrix}0&b\\c&d\end{pmatrix}\in A+B$.*
     Donc $\mathcal{M}_2(\mathbb{R})\subset A+B$, puis $\mathcal{M}_2(\mathbb{R})=A+B$ (l'autre inclusion est évidente).

  D'où $\mathcal{M}_2(\mathbb{R})=A\oplus B$.

PROPOSITION 103
Supposons ici que E est de dimension finie. Soit F un sous-espace vectoriel de E. Alors F possède un supplémentaire dans E. De plus, tous les supplémentaires de F dans E ont la même dimension, égale à $\dim(E)-\dim(F)$.

Preuve — Supposons $F\neq\{\vec{0}_E\}$. Considérons une base $(\vec{x}_1,\dots,\vec{x}_p)$ une base de F. D'après le théorème de la base incomplète, cette famille étant libre dans E, on peut la compléter en une base $(\vec{x}_1,\dots,\vec{x}_p,\vec{e}_{p+1},\dots,\vec{e}_n)$ de E.

Posons $G=\mathrm{Vect}(\vec{e}_{p+1},\dots,\vec{e}_n)$.

D'après la proposition 101, on obtient donc que $E=F\oplus G$.

La dimension d'un supplémentaire découle de la formule de Grassmann. □

Ainsi, si E est de dimension n et si F est un sous-espace vectoriel de E de dimension p, alors tout supplémentaire de F est de dimension $n-p$.

EXEMPLE 104 — *Dans $\mathbb{R}^3$, soit $F=\mathrm{Vect}((1,1,1),(0,1,1))$. Déterminons un supplémentaire de F.*

Pour cela, il suffit de compléter la famille libre $((1,1,1),(0,1,1))$ en une base de $\mathbb{R}^3$. Comme $(0,1,0)$ n'est pas combinaison linéaire de $(1,1,1)$ et $(0,1,1)$, la famille $((1,1,1),(0,1,1),(0,1,0))$ est une famille libre de $\mathbb{R}^3$, constituée de trois vecteurs dans un espace vectoriel de dimension 3, c'est donc une base de $\mathbb{R}^3$. Ainsi, $G=\mathrm{Vect}((0,1,0))$ est un sous-espace vectoriel supplémentaire de F dans $\mathbb{R}^3$.

On aurait également pu choisir de compléter la famille $((1,1,1),(0,1,1))$ *avec le vecteur* $(0,0,1)$ *pour obtenir une base et alors, on obtient un sous-espace vectoriel* $H = \text{Vect}((0,0,1))$ *supplémentaire de* F *et différent de* G*.*

REMARQUE 105 — *L'exemple précédent montre ainsi qu'il n'y a pas unicité du supplémentaire.*

Le résultat suivant est très utilisé en pratique.

PROPOSITION 106
Supposons ici E *de dimension finie. Soient* F *et* G *des sous-espaces vectoriels de* E*. Alors* $E = F \oplus G$ *si et seulement si deux des trois propositions ci-dessous sont vérifiées :*

1. $F \cap G = \{\vec{0}_E\}$,
2. $E = F + G$,
3. $\dim(E) = \dim(F) + \dim(G)$.

Preuve — ▷ Si $E = F \oplus G$ alors les trois propositions sont vérifiées.

◁ Réciproquement, supposons que deux des trois propositions soient vérifiées.

On a déjà vu que 1 et 2 impliquent $E = F \oplus G$.

Supposons 1 et 3. Alors $\dim(F+G) = \dim(F) + \dim(G) - \dim(F \cap G) = \dim(F) + \dim(G) = \dim(E)$. Comme $F + G \subset E$, on a donc $E = F + G$. Donc, comme $F \cap G = \{\vec{0}_E\}$, $E = F \oplus G$.

Supposons 2 et 3. Par la formule de Grassmann, on obtient $\dim(F \cap G) = 0$, et donc $F \cap G = \{\vec{0}_E\}$. Donc, comme $E = F + G$, on a $E = F \oplus G$. □

MÉTHODE 107 — *Supposons* E *de dimension finie. Soient* F *et* G *deux sous-espaces vectoriels de* E*. Si l'on connaît la dimension de* F *et* G*, pour démontrer que* $E = F \oplus G$*, on peut vérifier que* $\dim(E) = \dim(F) + \dim(G)$*, puis montrer que* $F \cap G = \{\vec{0}_E\}$ *ou bien que* $E = F + G$*.*

EXEMPLE 108 — *Reprenons l'exemple 95.*

Dans $\mathbb{R}^3$*, les sous-espaces vectoriels* $F = \{(x,y,z) \in \mathbb{R}^3 \mid x + y + z = 0\}$ *et* $G = \text{Vect}((1,1,1))$ *sont supplémentaires.*

En effet, nous avons déjà vu que $F \cap G = \{(0,0,0)\}$*.*

De plus, $F = \text{Vect}((1,-1,0),(0,1,-1))$ *donc* $\dim(F) = 2$ *puisque la famille* $((1,-1,0),(0,1,-1))$ *est libre et génératrice donc est une base, et* $\dim(G) = 1$*.*

Donc $\dim(F) + \dim(G) = 3 = \dim(\mathbb{R}^3)$*.*

De la proposition précédente, on a le résultat.

1.5.4 Somme de plusieurs sous-espaces vectoriels

Dans cette partie, n désigne un entier supérieur ou égal à 2.

Cette partie généralise à n sous-espaces vectoriels ce que nous avons vu pour deux sous-espaces vectoriels. Les démonstrations sont proches de celles faites dans les parties précédentes et sont laissées en exercices. Les résultats présents dans cette partie seront particulièrement utilisés pour l'étude de la réduction des matrices.

DÉFINITION 109
Soient $F_1, \ldots, F_n$ *des sous-espaces vectoriels de* E*. La* ***somme*** *de* $F_1, \ldots, F_n$ *est l'ensemble*

$$\sum_{i=1}^{n} F_i = \{\vec{x}_1 + \ldots + \vec{x}_n \mid (\vec{x}_1, \ldots, \vec{x}_n) \in F_1 \times \ldots \times F_n\}.$$

PROPOSITION 110
Soient $F_1, \ldots, F_n$ *des sous-espaces vectoriels de* E*. La somme* $\sum_{i=1}^{n} F_i$ *est un sous-espace vectoriel de* E*.*

Définition 111

Soit $F_1, \ldots, F_n$ des sous-espaces vectoriels de E. La somme $\sum_{i=1}^n F_i$ est dite ***directe****, et on note $\bigoplus_{i=1}^n F_i$, si tout élément $\vec{u}$ de $\sum_{i=1}^n F_i$ s'écrit de manière unique sous la forme $\vec{u} = \sum_{i=1}^n \vec{x}_i$ où, pour tout $i \in \{1, \ldots, n\}$, $\vec{x}_i \in F_i$.*

Proposition 112

Soient $F_1, \ldots, F_n$ des sous-espaces vectoriels de E. La somme $\sum_{i=1}^n F_i$ est directe si et seulement si, pour tout $j \in \{1, \ldots, n\}$,

$$F_j \cap \sum_{\substack{i=1\ldots n \\ i\neq j}} F_i = \{\vec{0}_E\}.$$

$\$$ On peut pour tout i et j éléments distincts de $\{1, \ldots, n\}$, $F_i \cap F_j = \{\vec{0}_E\}$, ou encore $\bigcap_{i=1}^n F_i = \{\vec{0}_E\}$, sans que les espaces soient en somme directe. Par exemple, pour $n = 3$, plaçons-nous dans $\mathbb{R}^2$ et prenons $F_1 = \text{Vect}((1,0))$, $F_2 = \text{Vect}((0,1))$ et $F_3 = \text{Vect}((1,1))$. On a $F_1 \cap F_2 = F_2 \cap F_3 = F_1 \cap F_3 = \{\vec{0}_E\}$ et $F_1 \cap F_2 \cap F_3 = \{\vec{0}_E\}$. Pourtant la somme de ces trois espaces n'est pas directe puisque, par exemple, le vecteur $(1,1)$ admet deux décompositions :

$$(1,1) = 0(1,0) + 0(0,1) + 1(1,1) \quad \text{et} \quad (1,1) = 1(1,0) + 1(0,1) + 0(1,1).$$

Définition 113

Soient $F_1, \ldots, F_n$ des sous-espaces vectoriels de E. On dit que les espaces $F_1, \ldots, F_n$ sont ***supplémentaires*** *s'ils vérifient les deux points suivants :*

1. *la somme de $F_1, \ldots, F_n$ est directe : $\sum_{i=1}^n F_i = \bigoplus_{i=1}^n F_i$,*
2. *la somme de $F_1, \ldots, F_n$ vaut E : $\sum_{i=1}^n F_i = E$.*

On note alors $E = \bigoplus_{i=1}^n F_i$.

Proposition 114

On suppose E de dimension finie. Soient $F_1, \ldots, F_p$ des sous-espaces vectoriels supplémentaires de E. Pour tout $i \in \{1, \ldots, p\}$, on note n_i la dimension de F_i et $\mathcal{B}_i = (\vec{e}_{i,1}, \ldots, \vec{e}_{i,n_i})$ une base de F_i. Alors la famille $\mathcal{B}$, concaténée des bases $\mathcal{B}_1, \ldots, \mathcal{B}_p$, c'est-à-dire la famille

$$\mathcal{B} = (\vec{e}_{1,1}, \ldots, \vec{e}_{1,n_1}, \vec{e}_{2,1}, \ldots, \vec{e}_{2,n_2}, \ldots, \vec{e}_{n,1}, \ldots, \vec{e}_{p,n_p})$$

est une base de E.

Proposition 115

Supposons E de dimension finie. Soient $F_1, \ldots, F_n$ des sous-espaces vectoriels de E. Alors $E = \bigoplus_{i=1}^n F_i$ si et seulement si

1. $E = \sum_{i=1}^n F_i$,
2. $\dim(E) = \sum_{i=1}^n \dim(F_i)$.

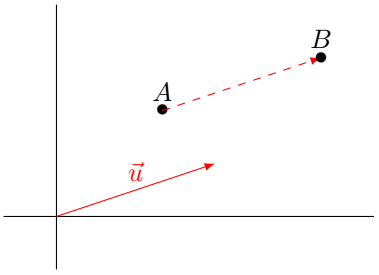
1.6 Sous-espaces affines d'un espace vectoriel

Dans cette partie, E désigne un $\mathbb{K}$-espace vectoriel.

1.6.1 Points et vecteurs

Dans cette partie, les éléments de E peuvent être considérés comme des vecteurs mais aussi comme des points.

Comme on sait additionner des vecteurs de E, on peut additionner un point A et un vecteur $\vec{u}$, ce qui s'écrit $A+\vec{u}$. Le résultat est un point B de E : $B = A+\vec{u}$.
Étant donnés deux points A et B, il existe un unique vecteur $\vec{u} \in E$ tel que $B = A+\vec{u}$. On note alors $\vec{u} = \overrightarrow{AB}$. On écrit parfois $\overrightarrow{AB} = B - A$.



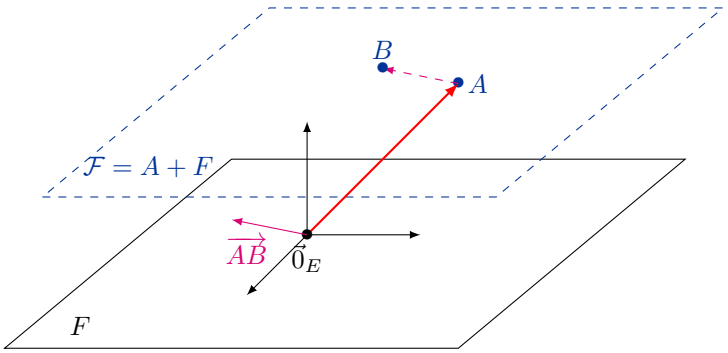
$E = \mathbb{R}^2$.

1.6.2 Définition et premières propriétés

Définition 116
On appelle ***sous-espace affine*** *de E toute partie $\mathcal{F}$ de E de la forme*

$$\mathcal{F} = A + F = \{A + \vec{x} \mid \vec{x} \in F\},$$

où F est un sous-espace vectoriel de E et A est un point de E.



Proposition 117
Soit $\mathcal{F}$ un sous-espace affine de E. Le sous-espace vectoriel F associé au sous-espace affine $\mathcal{F}$ est unique. F est appelé la ***direction*** *de $\mathcal{F}$. Si $\mathcal{F} = A + F$, on dit que F est le sous-espace affine de direction F passant par le point A.*

Preuve — Soit $\mathcal{F}$ un sous-espace affine de E. Supposons qu'il existe deux points A_1 et A_2 de E et F_1 et F_2 deux sous-espaces vectoriels de E tels que

$$\mathcal{F} = A_1 + F_1 = A_2 + F_2.$$

Montrons que $F_1 = F_2$ par double inclusions.

Soit $\vec{x} \in F_1$. On a $A_1 = A_1 + \vec{0}_E \in A_1 + F_1$ puisque $\vec{0}_E \in F_1$. Comme $A_1 + F_1 = A_2 + F_2$, $A_1 \in A_2 + F_2$. Il existe donc $\vec{x}_2 \in F_2$ tel que $A_1 = A_2 + \vec{x}_2$.

Comme $A_1 + \vec{x} \in A_1 + F_1 = A_2 + F_2$, il existe $\vec{y}_2 \in F_2$ tel que $A_1 + \vec{x} = A_2 + \vec{y}_2$.

Donc finalement, $\vec{x} = \vec{y}_2 - \vec{x}_2 \in F_2$. Donc $F_1 \subset F_2$.

Par symétrie des rôles de F_1 et F_2, on a également $F_2 \subset F_1$.

Donc $F_1 = F_2$. D'où l'unicité. □

EXEMPLE 118 — $\mathcal{D} = (1,2) + \text{Vect}((1,1))$ *est un sous-espace affine de* $\mathbb{R}^2$.

REMARQUE 119 — *Tout sous-espace vectoriel* F *de* E *est un sous-espace affine de* E *puisque* $F = \vec{0}_E + F$. *C'est donc le sous-espace affine de direction* F *passant par* $\vec{0}_E$. *La réciproque est fausse car en général,* $\vec{0}_E$ *n'appartient pas à* $\mathcal{F}$.

Géométriquement, les sous-espaces affines se visualisent comme étant des points, des droites ou des plans ne passant pas nécessairement par $\vec{0}_E$.

DÉFINITION 120
Soit $\mathcal{F}$ *un sous-espace affine de* E *de direction* F. *Si* F *est de dimension finie, on dit que* $\mathcal{F}$ *est de* ***dimension finie****, égale à* $\dim(F)$.

DÉFINITION 121

- *Une* ***droite affine*** *est un sous-espace affine dirigée par une droite vectorielle. Elle est de dimension* 1.
- *Un* ***plan affine*** *est un sous-espace affine dirigé par un plan vectoriel. Il est de dimension* 2.
- *Un* ***hyperplan affine*** *est un sous-espace affine dirigé par un hyperplan vectoriel. Il est de dimension* $n-1$ *où* n *est la dimension de* E.

PROPOSITION 122
Soit $\mathcal{F}$ *un sous-espace affine de* E *de direction* F *et* $B \in \mathcal{F}$. *Alors* $\mathcal{F} = B + F$.

Preuve — $\mathcal{F}$ étant un sous-espace affine de E de direction F, il existe un point A de E tel que $\mathcal{F} = A + F$. Comme $B \in \mathcal{F}$, il existe $\vec{x} \in F$ tel que $B = A + \vec{x}$.

Soit $C \in \mathcal{F}$. Alors il existe $\vec{u} \in F$ tel que $C = A + \vec{u}$. Donc $C = B - \vec{x} + \vec{u} = B + (\vec{u} - \vec{x}) \in B + F$ car F est un sous-espace vectoriel. Donc $\mathcal{F} \subset B + F$.

Réciproquement, soit $C \in B + F$. Alors il existe $\vec{v} \in F$ tel que $C = B + \vec{v}$. Donc $C = A + \vec{x} + \vec{v} \in A + F$ car F est un sous-espace vectoriel. Donc $B + F \subset \mathcal{F}$.

Donc $\mathcal{F} = B + F$. □

COROLLAIRE 123
Deux sous-espaces affines sont ***égaux*** *si et seulement s'ils ont la même direction et un point commun.*

PROPOSITION 124
Soit $\mathcal{F}$ *un sous-espace affine de* E *de direction* F. *Soit* $A \in \mathcal{F}$. *Alors, pour tout point* B *de* E, $B \in \mathcal{F}$ *si et seulement si* $\overrightarrow{AB} \in F$.

Preuve — Soit B un point de E. Alors $B \in \mathcal{F} = A + F$ si et seulement s'il existe $\vec{x} \in F$ tel que $B = A + \vec{x}$, soit si et seulement s'il existe $\vec{x} \in F$ tel que $\overrightarrow{AB} = \vec{x}$, soit finalement, si et seulement si $\overrightarrow{AB} \in F$. □

EXEMPLES 125

- *La droite* $\mathcal{D}$ *de* $\mathbb{R}^2$ *d'équation* $\begin{cases} x+y=2 \\ x-y+z=1 \end{cases}$ *est un sous-espace affine de direction la droite vectorielle d'équation* $\begin{cases} x+y=0 \\ x-y+z=0 \end{cases}$.
  Preuve — *On remarque que* $(1,1,1) \in \mathcal{D}$.
  Soit $(x,y,z) \in \mathbb{R}^3$. *Alors* $(x,y,z) \in \mathcal{D}$ *si et seulement si* $\begin{cases} (x-1)+(y-1)=0 \\ (x-1)-(y-1)+(z-1)=0 \end{cases}$, *soit si et seulement si* $(x-1, y-1, z-1) \in D$ *où* $D = \{(x,y,z) \in \mathbb{R}^3 \mid x+y=0 \text{ et } x-y+z=0\}$, *soit finalement si et seulement si* $(x,y,z) \in (1,1,1) + D$.
  On a $D = \text{Vect}(1,-1,-2)$, *donc* D *est une droite vectorielle.*
  Ainsi, $\mathcal{D} = (1,1,1) + D$ *est un sous-espace affine de direction la droite vectorielle* D. □
- *L'ensemble* $\mathcal{P} = \{P \in \mathbb{R}[X] \mid XP' + P = 2X\}$ *est un sous-espace affine de* $\mathbb{R}[X]$ *de direction le sous-espace vectoriel* $F = \{P \in \mathbb{R}[X] \mid XP' + P = 0\}$.

Preuve — *On remarque que $X \in \mathcal{P}$.*
F est un sous-espace vectoriel de $\mathbb{R}[X]$.
Soit $P \in \mathbb{R}[X]$. $P \in \mathcal{P}$ si et seulement si $XP' + P = 2X$, si et seulement si $X(P-X)' + (P-X) = 0$, soit si et seulement si $P - X \in F$, soit finalement, si et seulement si $P \in X + F$.

Ainsi, $\mathcal{P} = X + F$ est un sous-espace affine de direction F. □

- *L'ensemble $\mathcal{S}$ des suites réelles $(u_n)_{n\in\mathbb{N}}$ telles que pour tout $n \in \mathbb{N}$, $u_{n+2} = 4u_{n+1} - 4u_n + n$ est un plan affine de $\mathbb{R}^{\mathbb{N}}$ dirigé par l'ensemble S_h des suites réelles $(u_n)_{n\in\mathbb{N}}$ telles que pour tout $n \in \mathbb{N}$, $u_{n+2} = 4u_{n+1} - 4u_n$.*
  L'ensemble S est facile à expliciter, il reste donc à trouver une suite particulière $(v_n)_{n\in\mathbb{N}}$ de $\mathcal{S}$ pour connaître entièrement $\mathcal{S}$.
  Preuve — • *Cherchons une suite particulière $(v_n)_{n\in\mathbb{N}}$ de $\mathcal{S}$ sous la forme $(v_n)_{n\in\mathbb{N}} = (an+b)_{n\in\mathbb{N}}$.*
  Alors $(v_n)_{n\in\mathbb{N}} \in \mathcal{S}$ si et seulement si, pour tout $n \in \mathbb{N}$,

$$a(n+2) + b = 4a(n+1) + 4b - 4an - 4b + n,$$

soit si et seulement si

$$an + 2a + b = n + 4a,$$

soit si et seulement si $a = 1$ et $b = 2$.
La suite $(v_n)_{n\in\mathbb{N}} = (n+2)_{n\in\mathbb{N}}$ appartient donc à $\mathcal{S}$.
• *Explicitons S_h. L'équation caractéristique associée à $u_{n+2} = 4u_{n+1} + 4u_n$ est $X^2 - 4X + 4 = (X-2)^2$. Donc*

$$S_h = \{((an+b)2^n)_{n\in\mathbb{N}} \mid (a,b) \in \mathbb{R}^2\}.$$

S_h est un espace vectoriel de dimension 2 puisque $S_h = \mathrm{Vect}((n2^n)_{n\in\mathbb{N}}, (2^n)_{n\in\mathbb{N}})$ et la famille $((n2^n)_{n\in\mathbb{N}}, (2^n)_{n\in\mathbb{N}})$ est donc génératrice et libre, et est donc une base de S_h.
• *Toute suite $(u_n)_{n\in\mathbb{N}}$ appartient à $\mathcal{S}$ si et seulement si la suite $(u_n - v_n)_{n\in\mathbb{N}}$ appartient à S_h, soit finalement si et seulement si $(u_n)_{n\in\mathbb{N}} \in (v_n)_{n\in\mathbb{N}} + S_h$.*
Ainsi, $\mathcal{S} = (v_n)_{n\in\mathbb{N}} + S_h$ et $\mathcal{S}$ est un espace affine de dimension 2 dirigé par S_h.

□

Plus généralement, l'ensemble des suites réelles $(u_n)_{n\in\mathbb{N}}$ telles que $u_{n+2} = au_{n+1} + bu_n + c$ où $(a,b,c) \in \mathbb{R}^3$ avec $b \neq 0$, est un plan affine dirigé par l'ensemble des suites réelles vérifiant $u_{n+2} = au_{n+1} + bu_n$.

1.6.3 Intersection de sous-espaces affines

PROPOSITION 126
Soit E un $\mathbb{K}$-espace vectoriel. Soit $(\mathcal{F}_i)_{i\in I}$ une famille de sous-espaces affines de E. Pour tout $i \in I$, on note F_i la direction de $\mathcal{F}_i$.

Si $\bigcap_{i\in I} \mathcal{F}_i \neq \emptyset$ alors $\bigcap_{i\in I} \mathcal{F}_i$ est un sous-espace affine de E de direction $\cap_{i\in I} F_i$.

REMARQUE 127 — *L'intersection de sous-espaces affines peut être vide. Par exemple, si l'on considère dans le plan deux droites parallèles et non confondues, leur intersection est vide.*

Preuve — Posons $\mathcal{F} = \cap_{i\in I}\mathcal{F}_i$ et $F = \cap_{i\in I} F_i$. Supposons $\mathcal{F}$ non vide. Soit alors $A \in \mathcal{F}$. Pour tout $i \in I$, $A \in \mathcal{F}_i$, donc $\mathcal{F}_i = A + F_i$. Montrons que $\mathcal{F} = A + F$.

Soit $M \in \mathcal{F}$. Pour tout $i \in I$, $M \in \mathcal{F}_i = A + F_i$. Pour tout $i \in I$, il existe donc $\vec{x}_i \in F_i$ tel que $M = A + \vec{x}_i$. Donc, pour tout $i \in I$, $\vec{x}_1 = \vec{x}_i$ et $\vec{x}_1 \in \cap_{i\in I} F_i = F$. Donc $M \in A + F$.

Réciproquement, pour tout $i \in I$, $F \subset F_i$, donc $A + F \subset A + F_i = \mathcal{F}_i$. Donc $A + F \subset \mathcal{F}$. □

EXEMPLE 128 — *Soient $\mathcal{P}_1$ et $\mathcal{P}_2$ deux plans affines de $\mathbb{R}^3$ de directions respectives P_1 et P_2.*

L'intersection de $\mathcal{P}_1$ et $\mathcal{P}_2$ est soit l'ensemble vide, soit une droite, soit le plan lui-même, puisque $P_1 \cap P_2$ est soit une droite, soit un plan.

Chapitre 2 Polynômes à une indéterminée

Dans tout ce chapitre, $\mathbb{K}$ désigne le corps $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{Q}$.

2.1 Division de polynômes

2.1.1 Relation de divisibilité

Définition 1
*Soient A, B des éléments de $\mathbb{K}[X]$. On dit que A **divise** \整除\ B s'il existe $P \in \mathbb{K}[X]$ tel que $B = AP$. On note alors $A \mid B$.*

*On dit aussi que A est un **diviseur de** B, ou que B est **divisible par** A, ou que B est un **multiple de** A,*

L'ensemble des multiples d'un polynôme A se note parfois $A\mathbb{K}[X] = \{AP \mid P \in \mathbb{K}[X]\}$.

Exemples 2
- *Le polynôme $X^2 + 3X + 2$ est divisible par $X + 1$ car $X^2 + 3X + 2 = (X + 1)(X + 2)$.*
- *Le polynôme $X + 1$ divise le polynôme $2X + 2$ car $2X + 2 = 2(X + 1)$, et le polynôme $2X + 2$ divise le polynôme $X + 1$ car $X + 1 = \frac{1}{2}(2X + 2)$. Il existe donc des polynômes tels que $A \mid B$ et $B \mid A$ mais $A \neq B$.*

Proposition 3
Pour tous A, $B \in \mathbb{K}[X]$, $A \mid B$ et $B \mid A$ si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.

*On dit que A et B sont **associés**.*

Preuve — Soient A et B deux éléments de $\mathbb{K}[X]$

▷ Supposons qu'il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$. Posons $P = \lambda \in \mathbb{K}[X]$ et $Q = \frac{1}{\lambda} \in \mathbb{K}[X]$. Alors $A = BP$ et $B = AQ$. Donc $A \mid B$ et $B \mid A$.

◁ Supposons que $A \mid B$ et $B \mid A$. Alors, il existe des polynômes P et Q tels que $A = BP$ et $B = AQ$. Donc $A = APQ$.

-1er cas : $A = 0$. Alors $B = AQ = 0$ et donc $A = 1 \times B$.

-2nd cas : $A \neq 0$. Alors $\mathbb{K}[X]$ étant un anneau intègre, $PQ = 1$. Donc P et Q sont nuls et leurs degrés vérifient

$$\deg(P) + \deg(Q) = 0.$$

Donc $\deg(P) = \deg(Q) = 0$. Donc P est une constante non nulle λ. Donc $A = \lambda B$ avec $\lambda \in \mathbb{K}^*$. □

Remarque 4 — *Sur $\mathbb{K}[X]$, la relation de divisibilité est réflexive et transitive mais ce n'est donc pas une relation d'ordre car elle n'est pas antisymétrique.*

Proposition 5
Soient A et B des polynômes de $\mathbb{K}[X]$. Si $A \mid B$ alors $B = 0$ ou $\deg(A) \leq \deg(B)$.

Preuve — Supposons que $A \mid B$ et que $B \neq 0$. Alors, il existe $P \in \mathbb{K}[X]$ tel que $B = AP$. Comme $B \neq 0$, A et P sont aussi non nuls. On a donc $\deg(B) = \deg(P) + \deg(A) \geq \deg(A)$. □

2.1.2 Division euclidienne

THÉORÈME 6 (Division euclidienne)
Soient A et B des éléments de $\mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple de polynômes $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$.

*Q est appelé le **quotient** de la division euclidienne de A par B, et R est appelé le **reste**.*

Preuve —

• *Existence :* Soit $B = \sum_{k=0}^{m} b_k X^k$ un polynôme tel que $b_m \neq 0$. Si B est constant égal à λ alors on prend $Q = \frac{1}{\lambda}A$ et $R = 0$. Supposons maintenant que $\deg(B) \geq 1$.

Démontrons le résultat par récurrence. Notons, pour tout $n \in \mathbb{N}$, (H_n) la propriété : « Pour tout polynôme A de degré strictement inférieur à n, il existe un couple de polynômes (P, Q) tel que $A = BQ + R$ et $\deg(R) < \deg(B)$. »

-(H_0), (H_1), …, (H_m) sont vraies en prenant $R = A$ et $Q = 0$ puisqu'alors $A = B \times 0 + A$ et $\deg(A) < \deg(B)$.

-Soit $n \geq m$. Supposons (H_n), montrons (H_{n+1}).

Soit $A = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré strictement inférieur à $n+1$.

Le polynôme $A - \frac{a_n}{b_m} X^{n-m} B$ est de degré strictement inférieur à n, donc d'après (H_n), il existe un couple (Q_1, R) tel que $A - \frac{a_n}{b_m} X^{n-m} B = BQ_1 + R$ et $\deg(R) < \deg(B)$.

On a alors $A = B(Q_1 + \frac{a_n}{b_m} X^{n-m}) + R$ et $\deg(R) < \deg(B)$.

D'où (H_{n+1}).

On en déduit le résultat par récurrence.

• *Unicité :* Soient (Q_1, R_1) et (Q_2, R_2) deux couples de polynômes vérifiant la relation.

Alors $R_2 - R_1 = B(Q_1 - Q_2)$. Si $Q_1 \neq Q_2$, alors $R_1 \neq R_2$ (car $B \neq 0$ et $\mathbb{K}[X]$ est intègre) et

$$\deg(R_2 - R_1) = \max(\deg(R_1), \deg(R_2)) \geq \deg(B).$$

Ceci n'est pas possible car R_1 et R_2 sont de degrés strictement inférieurs à $\deg(B)$.

Donc $Q_1 = Q_2$, puis $R_1 = R_2$.

D'où l'unicité. □

REMARQUE 7 — *$A \mid B$ si et seulement si le reste de la division euclidienne de B par A est nul.*

EXEMPLE 8 (Algorithme de la division euclidienne \欧几里德算法 / 辗转相除法\) —

Appliquons l'algorithme de division euclidienne du polynôme $A = X^5 + 4X^4 + 2X^3 + X^2 - X - 1$ par le polynôme $B = X^3 - 2X + 3$:

$$\begin{array}{rrrrrr|l}
X^5 & +4X^4 & +2X^3 & +X^2 & -X & -1 & X^3 - 2X + 3 \\
\cline{7-7}
-(X^5 & & -2X^3 & +3X^2) & & & X^2 + 4X + 4 \\
\cline{1-5}
 & 4X^4 & +4\,X^3 & -2X^2 & -X & -1 & \\
 & -(4X^4 & & -8X^2 & +12X) & & \\
\cline{2-5}
 & & 4X^3 & +6X^2 & -13X & -1 & \\
 & & -(4X^3 & & -8X & +12) & \\
\cline{3-5}
 & & & 6X^2 & -5X & -13 &
\end{array}$$

L'algorithme s'arrête lorsque l'on obtient un polynôme de degré strictement inférieur à $X^3 - 2X + 3$.

On trouve finalement $X^5 + 4X^4 + 2X^3 + X^2 - X + 1 = (X^3 - 2X + 3)(X^2 + 4X + 4) + (6X^2 - 5X - 13)$.

On en déduit que le polynôme $X^5 + 4X^4 + 2X^2 + X^2 - X - 1$ n'est pas divisible par $X^3 - 2X + 3$ car le reste $6X^2 - 5X - 13$ est non nul.

2.2 Racines de polynôme

2.2.1 Définition

Définition 9
Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit que α est ***racine*** \根\ *de P (dans $\mathbb{K}$) si $P(\alpha) = 0$.*

Il faut être vigilant sur le corps $\mathbb{K}$ sur lequel on étudie les racines. Par exemple, le polynôme $X^2 + 1$ n'a pas de racine de $\mathbb{R}$ mais a des racines dans $\mathbb{C}$, qui sont i et $-i$. Notons qu'un polynôme de $\mathbb{R}[X]$, à coefficients réels, peut être vu comme un polynôme de $\mathbb{C}[X]$ puisque $\mathbb{R} \subset \mathbb{C}$ et les coefficients réels sont aussi des nombres complexes. Pour un polynôme de $\mathbb{R}[X]$, on peut donc regarder les racines dans $\mathbb{R}$ ou dans $\mathbb{C}$, mais il faut le préciser car les résultats peuvent être très différents !

Remarque 10 — *Un polynôme constant non nul n'a pas de racine et le polynôme nul a tous les éléments de $\mathbb{K}$ comme racines.*

Proposition 11
Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors α est racine de P si et seulement si $X - \alpha$ divise P.

Ainsi, si α est racine de P, on peut écrire $P = (X - \alpha)Q$ où $Q \in \mathbb{K}[X]$.

Preuve — La division euclidienne de P par $X - \alpha$ s'écrit $P = (X - \alpha)Q + R$ avec $Q \in \mathbb{K}[X]$ et $\deg(R) < \deg(X - \alpha) = 1$.

Donc R est constant et peut s'écrire $R = \lambda \in \mathbb{K}$.

En évaluant en α, on obtient alors $P(\alpha) = \lambda$.

Donc α est racine de P si et seulement si $\lambda = 0$, soit si et seulement si $P = (X - \alpha)Q$, soit finalement, si et seulement si $X - \alpha$ divise P. □

Exemple 12 — *Le réel -1 est racine du polynôme $P = X^3 + 2X^2 + 2X + 1$ puisque $P(-1) = 0$ et on a, par division euclidienne, $P = (X + 1)(X^2 + X + 1)$.*

2.2.2 Multiplicité d'une racine

Définition 13
Soient $P \in \mathbb{K}[X]$ un polynôme, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On dit que α est racine de P de ***multiplicité*** \根 α 的重数\ *m si $(X - \alpha)^m$ divise P et $(X - \alpha)^{m+1}$ ne divise pas P.*

On en déduit que si α est racine de P un polynôme de degré n, alors sa multiplicité est comprise entre 1 et n.

Remarque 14 — *Si α est racine de P de multiplicité $m = 1$, on dit que α est* ***racine simple*** \单根\.

Si α est racine de P de multiplicité $m = 2$, on dit que α est ***racine double****.*

Si α est racine de P de multiplicité $m \geq 2$, on dit que α est ***racine multiple*** \重根\.

Parfois, si α n'est pas racine de P, on dit que α est racine de multiplicité 0.

Proposition 15
Soient $P \in \mathbb{K}[X]$ un polynôme, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Alors

- *α est racine de P de multiplicité au moins m si et seulement si $(X - \alpha)^m$ divise P.*
- *α est racine de P de multiplicité m si et seulement s'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)^m Q$ et $Q(\alpha) \neq 0$ (autrement dit, α n'est pas racine de Q).*

Preuve — • ▷ Si α est racine de P de multiplicité $n \geq m$, alors $(X - \alpha)^n = (X - \alpha)^m (X - \alpha)^{n-m}$ divise P par définition, $(X - \alpha)^m$ divise P.

◁ Réciproquement, supposons que $(X-\alpha)^m$ divise P. Comme P est de degré fini, il existe $n \geq m$ tel que $(X-\alpha)^n$ divise P et $(X-\alpha)^{n+1}$ ne divise pas P. Donc α est de multiplicité $n \geq m$.

• ▷ Supposons que α soit racine de P de multiplicité m. Alors par définition, $(X-\alpha)^m$ divise P. Il existe donc $Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha)^m Q$. Comme $(X-\alpha)^{m+1}$ ne divise pas P, $X-\alpha$ ne divise pas Q, et donc $Q(\alpha) \neq 0$.

◁ Réciproquement, supposons qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha)^m Q$ et $Q(\alpha) \neq 0$. Alors $(X-\alpha)^m$ divise P. De plus, comme α n'est pas racine de Q, $X-\alpha$ ne divise pas Q, et donc $(X-\alpha)^{m+1}$ ne divise pas $P = (X-\alpha)^m Q$.

□

EXEMPLE 16 — *Soit $P = (X-1)^2(X^2+1)$. Alors $(X-1)^2$ divise P et 1 n'est pas racine de X^2+1. Donc 1 est une racine double (dans $\mathbb{R}$ et dans $\mathbb{C}$) de P.*

Le polynôme X^2+1 admet i et $-i$ comme racines (dans $\mathbb{C}$) donc $P = (X-1)^2(X-i)(X+i)$. Donc i et $-i$ sont racines simples (dans $\mathbb{C}$) de P.

EXEMPLE 17 — *Le polynôme $P = X(X+1)^2(X-4)^3$ possède trois racines distinctes, 0, -1 et 4. 0 est racine simple, -1 est racine double et 4 est racine de multiplicité 3. On dit que P admet 6 racines* ***comptées avec multiplicité*** \根按重数计算\ *(6 = 1 + 2 + 3).*

Souvent, on cherchera donc à écrire le polynôme sous la forme d'un produit de polynômes. Cela fera l'objet d'une partie ultérieure du cours (factorisation des polynômes).

On déduit de la proposition précédente que si α est racine de P de multiplicité m alors α est racine de P' de multiplicité $m-1$.

On peut calculer la multiplicité d'une racine en évaluant les dérivées successives en ce point.

PROPOSITION 18
Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Alors

• *α est racine de P de multiplicité au moins m si et seulement si pour tout $k \in \{0, \dots, m-1\}$, $P^{(k)}(\alpha) = 0$,*

• *α est racine de P de multiplicité m si et seulement si, pour tout $i \in \{0, \dots, m-1\}$, $P^{(i)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.*

Preuve — Notons n le degré de P. D'après la formule de Taylor polynomiale,

$$\begin{aligned} P &= \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k \\ &= \sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k + \sum_{k=m}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k \\ &= (X-\alpha)^m \sum_{k=m}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^{k-m} + \sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k. \end{aligned}$$

Le polynôme $\sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$ est de degré strictement inférieur à m. On en déduit que α est racine de P de multiplicité au moins m si et seulement si $\sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k = 0$, soit si et seulement si $P^{(k)}(\alpha) = 0$ pour tout $k \in \{0, \dots, m-1\}$.

De même, α est racine de P de multiplicité au moins $m+1$ si et seulement si pour tout $k \in \{0, \dots, m\}$, $P^{(k)}(\alpha) = 0$.

Ainsi, α est racine de P de multiplicité exactement m si et seulement si pour tout $k \in \{0, \dots, m-1\}$, $P^{(k)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$. □

COROLLAIRE 19
Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Alors α est racine simple de P si et seulement si $P(\alpha) = 0$ et $P'(\alpha) \neq 0$.

EXEMPLE 20 — *Soit $n \in \mathbb{N}^*$. Le polynôme $P = X^n - 1$ n'admet que des racines simples puisque 0 n'est pas racine de P et pour tout $\alpha \in \mathbb{C}^*$, $P'(\alpha) = n\alpha^{n-1} \neq 0$.*

PROPOSITION 21
Soient $P \in \mathbb{R}[X]$ un polynôme à coefficients réels et $\alpha \in \mathbb{C}$. Alors α est racine de P si et seulement si $\overline{\alpha}$ est racine de P, et dans ce cas, α et $\overline{\alpha}$ ont la même multiplicité.

Preuve — Notons n le degré de P. P s'écrit sous la forme $P = a_0 + a_1X + \ldots + a_nX^n$ avec $(a_0, \ldots, a_n) \in \mathbb{R}^{n+1}$.

Les coefficients a_i étant réels, on a donc $\overline{P(\alpha)} = \overline{a_0 + a_1\alpha + \ldots + a_n\alpha^n} = a_0 + a_1\overline{\alpha} + \ldots + a_n\overline{\alpha}^n = P(\overline{\alpha})$.

Donc α est racine de P si et seulement $P(\alpha) = 0$, soit si et seulement si $P(\overline{\alpha}) = \overline{P(\alpha)} = \overline{0} = 0$, soit finalement, si $\overline{\alpha}$ est racine de P.

De même, on obtient que pour tout $k \in \mathbb{N}$, $\overline{P^{(k)}(\alpha)} = P^{(k)}(\overline{\alpha})$.

De la proposition 18, on en déduit que α et $\overline{\alpha}$ ont la même multiplicité dans P. □

EXEMPLE 22 — *j est racine de $X^2 + X + 1$, donc $\overline{j}$ l'est aussi et $X^2 + X + 1 = (X - j)(X - \overline{j})$.*

2.2.3 Nombre de racines et degré du polynôme

PROPOSITION 23
Soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré n et $\alpha_1, \ldots, \alpha_r$ des racines distinctes de P de multiplicités respectives $m_1, \ldots, m_r$. Alors $(X - \alpha_1)^{m_1} \ldots (X - \alpha_r)^{m_r}$ divise P. En particulier, $\sum_{i=1}^{r} m_i \leq n$.

Preuve — Se démontre par récurrence, l'initialisation a été faite à la proposition 18. □

COROLLAIRE 24
Un polynôme $P \in \mathbb{K}[X]$ de degré $n \geq 1$ admet au plus n racines comptées avec multiplicité (racines distinctes ou confondues) dans $\mathbb{K}$.

REMARQUE 25 — *Les propriétés suivantes sont des conséquences directes de ce corollaire et sont très utiles en pratique :*

- *Si un polynôme possède une infinité de racines alors c'est le polynôme nul.*
- *Si un polynôme de degré inférieur ou égal à n admet strictement plus de n racines (comptées avec multiplicité) alors c'est le polynôme nul.*
- *Si deux polynômes de degrés inférieurs ou égaux à n coïncident en $n + 1$ points distincts alors ils sont égaux.*

Un polynôme de degré n ne possède pas forcément n racines comptées avec multiplicité. Par exemple, $X^2 + 1$ est de degré 2 et n'admet pas de racine dans $\mathbb{R}$.

Le résultat suivant nous dit que l'on peut identifier polynôme et fonction polynomiale. Ainsi, si deux fonctions polynômiales sont égales alors leurs coefficients sont égaux. Cependant, ce résultat est faux dans un corps fini. Par exemple, dans $\mathbb{Z}/2\mathbb{Z}$, $X^2 + X$ est un polynôme non nul alors que la fonction polynomiale associée est nulle.

COROLLAIRE 26
L'application $P \longmapsto \tilde{P}$, qui associe au polynôme $P \in \mathbb{K}[X]$ la fonction polynomiale $\tilde{P} \in \mathcal{F}(\mathbb{K}, \mathbb{K})$, est injective.

Preuve — Soient P et Q deux polynômes tels que $\tilde{P} = \tilde{Q}$. Alors la fonction polynomiale associée à $P - Q$ est nulle. Le polynôme $P - Q$ admet donc une infinité de racines, et est donc nul. Donc $P = Q$. D'où l'injectivité. □

EXEMPLE 27 — *Montrons que la fonction cosinus n'est pas une fonction polynomiale.*

Supposons par l'absurde qu'il existe $P \in \mathbb{R}[X]$ tel que pour tout $x \in \mathbb{R}$, $\cos(x) = P(x)$.

Alors, pour tout $k \in \mathbb{Z}$, $P\left(\frac{\pi}{2} + k\pi\right) = \cos\left(\frac{\pi}{2} + k\pi\right) = 0$.

Le polynôme P possède donc une infinité de racines. Donc P est le polynôme nul. Ceci est absurde car $\cos(0) = 1 \neq 0$. Donc la fonction cosinus n'est pas une fonction polynomiale.

2.2.4 Polynôme scindé et théorème de d'Alembert-Gauss

DÉFINITION 28
On dit qu'un polynôme $P \in \mathbb{K}[X]$ de degré n est ***scindé*** \可分多项式\ *sur $\mathbb{K}$ s'il n'est pas constant et possède exactement n racines comptées avec multiplicité.*

On dit qu'un polynôme $P \in \mathbb{K}[X]$ de degré n est ***scindé à racines simples*** *si P est scindé et possède n racines distinctes.*

Un polynôme est donc scindé sur $\mathbb{K}$ si on peut l'écrire comme un produit de polynômes de $\mathbb{K}[X]$ de degré 1.

Il est important de préciser « scindé sur $\mathbb{K}$ » car par exemple, X^2+1 est scindé sur $\mathbb{C}$ puisque $X^2+1=(X-i)(X+i)$ mais ne l'est pas sur $\mathbb{R}$ car X^2+1 n'a pas de racine sur $\mathbb{R}$.

REMARQUE 29 — *Un polynôme scindé non constant de degré n et de racines distinctes $\alpha_1, \ldots, \alpha_r$ de multiplicités respectives $m_1, \ldots, m_r$ est de la forme*

$$P = \lambda \prod_{i=1}^{r} (X-\alpha_i)^{m_i}$$

où λ est le coefficient dominant de P et on a vérifie $n = \sum_{i=1}^{r} m_i$.

EXEMPLE 30 — *Pour tout $n \in \mathbb{N}^*$, le polynôme $P = X^n - 1$ est scindé sur $\mathbb{C}$ et*

$$X^n - 1 = \prod_{\omega \in U_n} (X-\omega) = \prod_{k=0}^{n-1} (X - \mathrm{e}^{\frac{2ik\pi}{n}}).$$

En effet, P étant de degré n, il admet au plus n racines et pour tout $k \in \{0, \ldots, n-1\}$, $\mathrm{e}^{\frac{2ik\pi}{n}}$ est racine de P. Donc P possède exactement n racines, et est donc scindé sur $\mathbb{C}$. Ses racines sont les racines n-ième de l'unité.

THÉORÈME 31 (Théorème de d'Alembert-Gauss ou Théorème fondamental de l'algèbre \代数基本定理\)
Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine complexe.

COROLLAIRE 32
Tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Ceci signifie que tout polynôme complexe de degré n admet exactement n racines complexes comptées avec multiplicité.

Ce théorème est faux sur $\mathbb{R}$. Par exemple, le polynôme X^2+1 ne possède pas de racine réelle. Sur $\mathbb{C}$, on a bien sûr $X^2+1=(X-i)(X+i)$.

EXEMPLE 33 — *On retrouve donc que le polynôme X^n-1 est scindé sur $\mathbb{C}$.*

2.2.5 Relations coefficients-racines

Dans cette partie, on considère des polynômes scindés (sur $\mathbb{C}$, c'est toujours le cas comme on vient de le voir). Commençons par étudier le cas des polynômes de degrés 2 et 3.

• Cas des polynômes de degré 2 :

Soit $P = a_0 + a_1X + a_2X^2$ un polynôme scindé de degré 2. P étant scindé, il admet deux racines α_1 et α_2 (distinctes ou non). On a alors $P = a_2(X-\alpha_1)(X-\alpha_2)$.

En développant, on obtient $P = a_2X^2 - a_2(\alpha_1+\alpha_2)X + a_2\alpha_1\alpha_2$.

Par identification, on a donc les relations suivantes entre les coefficients et les racines :

$$\begin{cases} \alpha_1 + \alpha_2 = -\dfrac{a_1}{a_2}, \\ \alpha_1\alpha_2 = \dfrac{a_0}{a_2}. \end{cases} .$$

• **Cas des polynômes de degré 3 :**

Soit $P = a_0 + a_1X + a_2X^2 + a_3X^3$ un polynôme scindé de degré 3. P étant scindé, il admet trois racines α_1, α_2 et α_3 (distinctes ou non). On a alors $P = a_3(X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$.

En développant, on obtient $P = a_3X^3 - a_3(\alpha_1 + \alpha_2 + \alpha_3)X^2 + a_3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)X - a_3\alpha_1\alpha_2\alpha_3$.

Par identification, on a donc les relations suivantes entre les coefficient et les racines :

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = -\dfrac{a_2}{a_3}, \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \dfrac{a_1}{a_3}, \\ \alpha_1\alpha_2\alpha_3 = -\dfrac{a_0}{a_3}. \end{cases}$$

• **Cas général :**

Nous disposons du résultat plus général suivant, valable pour tout polynôme scindé.

PROPOSITION 34
Soit $P = \sum_{k=0}^{n} a_kX^k \in \mathbb{K}[X]$ un polynôme scindé de degré $n \geq 1$. On note α_1, ..., α_n les racines de P distinctes ou non.

Posons, pour tout $k \in \{1, \ldots, n\}$,

$$\sigma_k = \sum_{1 \leq i_1 < \ldots < i_k \leq n} \alpha_{i_1} \ldots \alpha_{i_k}.$$

Alors $\sigma_k = (-1)^k \dfrac{a_{n-k}}{a_n}$.

Autrement dit,

$$P = a_n \prod_{k=1}^{n} (X - \alpha_k) = a_n(X^n - \sigma_1X^{n-1} + \sigma_2X^{n-2} + \ldots + (-1)^n\sigma_n).$$

Preuve — On montre que $P = a_n \prod_{k=1}^{n}(X - \alpha_k) = a_n(X^n - \sigma_1X^{n-1} + \sigma_2X^{n-2} + \ldots + (-1)^n\sigma_n)$, puis on identifie les coefficients sachant que $P = \sum_{k=0}^{n} a_kX^k$. □

On retiendra que σ_1 est la somme des racines et que σ_n est le produit des racines :

$$\sigma_1 = \sum_{k=1}^{n} \alpha_k \quad \text{et} \quad \sigma_n = \prod_{k=1}^{n} \alpha_k.$$

EXEMPLE 35 — *Pour $n = 4$, nous avons par exemple*

$$\begin{cases} \sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4, \\ \sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4, \\ \sigma_3 = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_4 + \alpha_2\alpha_3\alpha_4, \\ \sigma_4 = \alpha_1\alpha_2\alpha_3\alpha_4. \end{cases}$$

EXEMPLES 36

- *Déterminons l'ensemble des solutions du système* $\begin{cases} x + y = -3 \\ xy = 2. \end{cases}$.

  Soit $(x, y) \in \mathbb{R}^2$. Alors (x, y) est solution de ce système si et seulement si x et y sont les racines du polynôme $P = X^2 - (x + y)X + xy = X^2 + 3X + 2$. Or $P = (X - 1)(X - 2)$. On en déduit que l'ensemble des solutions du système est $\{(-1, -2), (-2, 1)\}$.

- *Déterminons l'ensemble des solutions du système* $\begin{cases} x+y+z=1 \\ xy+xz+yz=-1 \\ xyz=-1. \end{cases}$.

  Soit $(x,y,z)\in\mathbb{R}^3$. *Alors* (x,y,z) *est solution de ce système si et seulement si* x, y *et* z *sont les racines du polynôme* $P=X^3-(x+y+z)X^2+(xy+xz+yz)X-xyz=X^3-X^2-X+1$. *Or* $P=(X-1)^2(X+1)$. *On en déduit que l'ensemble des solutions du système est* $\{(1,1,-1),(1,-1,1),(-1,1,1)\}$.

2.3 Polynômes d'interpolation de Lagrange

On considère $n+1$ points distincts x_0, …, x_n de $\mathbb{K}$, puis $n+1$ autres points distincts ou non y_0, …, y_n de $\mathbb{K}$. On cherche un polynôme P de degré au plus n tel que, pour tout $i\in[\![0,n]\!]$, $P(x_i)=y_i$.

On va montrer l'existence et l'unicité d'un tel polynôme, appelé polynôme d'interpolation de Lagrange associé à $(x_0,\dots,x_n)$ et $(y_0,\dots,y_n)$.

Commençons par le cas particulier où tous les y_j sont nuls sauf un.

Proposition 37
Soient x_0, …, x_n $n+1$ *points distincts de* $\mathbb{K}$. *Pour tout* $i\in[\![0,n]\!]$, *il existe un unique polynôme* L_i *de degré inférieur ou égal à* n *tel que*

$$L_i(x_j)=\delta_{i,j}.$$

De plus, $L_i=\prod_{\substack{0\leq k\leq n\\ k\neq i}}\frac{(X-x_k)}{(x_i-x_k)}$. *Les polynômes* L_0, …, L_n *sont appelés les* ***polynômes de Lagrange****.*

Preuve —

On propose ici de retrouver l'expression du polynôme L_i.

Le polynôme L_i doit s'annuler en n points distincts et est de degré n, il est donc de la forme

$$L_i=\lambda\prod_{\substack{0\leq k\leq n\\ k\neq i}}(X-x_k).$$

Comme $L_i(x_i)=1$, on en déduit que

$$1=\lambda\prod_{\substack{0\leq k\leq n\\ k\neq i}}(x_i-x_k),\quad\text{donc}\quad\lambda=\prod_{\substack{0\leq k\leq n\\ k\neq i}}\frac{1}{(x_i-x_k)}.$$

Ainsi, on a nécessairement $L_i=\prod_{\substack{0\leq k\leq n\\ k\neq i}}\frac{(X-x_k)}{(x_i-x_k)}$ et ce polynôme est de degré inférieur ou égal à n et vérifie $L_i(x_j)=\delta_{i,j}$.

□

Proposition 38
Avec les notations de la proposition précédente, la famille de polynômes $(L_0,\dots,L_n)$ *est une base de* $\mathbb{K}_n[X]$. *Les coordonnées d'un polynôme* $P\in\mathbb{K}_n[X]$ *dans cette base sont* $(P(x_0),P(x_1),\dots,P(x_n))$.

Preuve — Montrons que la famille $(L_0,\dots,L_n)$ est libre.

Soit $(\lambda_0,\dots,\lambda_n)\in\mathbb{K}^{n+1}$ tel que $\lambda_0L_0+\ldots+\lambda_nL_n=0$.

Soit $i\in[\![0,n]\!]$. En évaluant en x_i, on obtient $\lambda_0L_0(x_i)+\ldots+\lambda_iL_i(x_i)+\ldots+\lambda_nL_n(x_i)=0$, soit, puisque $L_j(x_i)=\delta_{j,i}$, $\lambda_i=0$.

Comme i est un élément quelconque de $[\![0,n]\!]$, on en déduit que $\lambda_0=\ldots=\lambda_n=0$.

Donc la famille $(L_0,\dots,L_n)$ est libre.

• Composée de $n+1$ éléments dans l'espace vectoriel $\mathbb{K}_n[X]$ de dimension $n+1$, on en déduit que la famille $(L_0,\dots,L_n)$ est une base de $\mathbb{K}_n[X]$.

• La famille $(L_0, \dots, L_n)$ étant une base de $\mathbb{K}_n[X]$, tout polynôme $P \in \mathbb{K}_n[X]$ s'écrit sous la forme $P = \lambda_0 L_0 + \dots + \lambda_n L_n$.

En évaluant en x_i, on obtient $P(x_i) = \lambda_i$. Donc $P = \sum_{i=0}^{n} P(x_i) L_i$. Les coordonnées de P dans la base $(L_0, \dots, L_n)$ sont donc $(P(x_0), \dots, P(x_n))$. □

PROPOSITION 39
Soient x_0, …, x_n $n+1$ points distincts de $\mathbb{K}$, et y_0, …, y_n $n+1$ points de $\mathbb{K}$ distincts ou non. Il existe un unique polynôme L de degré inférieur ou égal à n tel que pour tout $i \in [\![0, n]\!]$,

$$L(x_i) = y_i.$$

De plus,

$$L = \sum_{i=0}^{n} y_i L_i = \sum_{i=0}^{n} y_i \prod_{\substack{j=1\dots n \\ j \neq i}} \frac{X - x_j}{x_i - x_j}.$$

Preuve —

• *Existence :* Pour tout $i \in [\![0, n]\!]$, en évaluant en x_i le polynôme $L = \sum_{i=0}^{n} y_i L_i$, on obtient $L(x_i) = y_i$ puisque $L_j(x_i) = \delta_{j,i}$.

Donc le polynôme L convient.

• *Unicité :* Soient P et Q deux polynômes de degrés inférieurs ou égaux à n tels que pour tout $i \in [\![0, n]\!]$, $P(x_i) = y_i$ et $Q(x_i) = y_i$. Alors le polynôme $P - Q$ admet $n+1$ racines distinctes et est de degré inférieur ou égal à n, c'est donc le polynôme nul. Donc $P = Q$.

□

EXEMPLE 40 — *Déterminons l'expression du polynôme de degré inférieur ou égal à 3 tel que $L(-1) = 1$, $L(0) = 0$, $L(1) = 1$ et $L(2) = -1$.*

On sait que $L = 1 \times L_0 + 0 \times L_1 + 1 \times L_2 - 1 \times L_3 = L_0 + L_2 - L_3$.

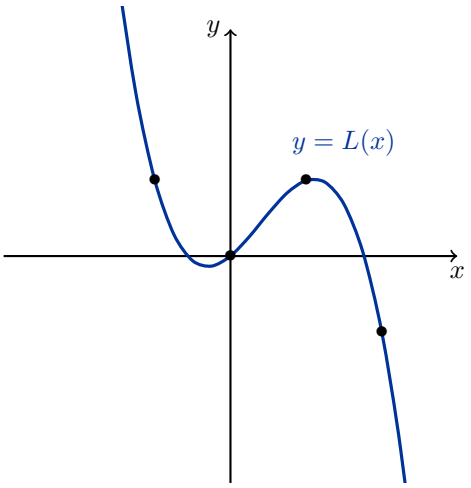
On a $L_0 = \dfrac{(X-0)(X-1)(X-2)}{(-1-0)(-1-1)(-1-2)} = -\dfrac{1}{6} X(X-1)(X-2)$,

$$L_2 = \frac{(X-(-1))(X-0)(X-2)}{(1-(-1))(1-0)(1-2)} = -\frac{1}{2} X(X+1)(X-2),$$

$$L_3 = \frac{(X-(-1))(X-0)(X-1)}{(2-(-1))(2-0)(2-1)} = \frac{1}{6} X(X+1)(X-1).$$

Donc

$$\begin{aligned} L &= -\frac{1}{6} X(X-1)(X-2) - \frac{1}{2} X(X+1)(X-2) - \frac{1}{6} X(X+1)(X-1) \\ &= -\frac{5}{6} X^3 + X^2 + \frac{5}{6} X. \end{aligned}$$



REMARQUE 41 — *Les polynômes d'interpolation de Lagrange permettent d'approcher une fonction réelle f par une fonction polynomiale de degré au plus n coïncidant avec f en $n+1$ points distincts. L'interpolation sert par exemple au calcul approché d'intégrales.*

2.4 POLYNÔMES IRRÉDUCTIBLES

2.4.1 Définition et décomposition en produit de facteurs irréductibles

DÉFINITION 42
*Soit $P \in \mathbb{K}[X]$. On dit que P est **irréductible** \不可约多项式\(sur $\mathbb{K}$) si P n'est pas constant et s'il n'est divisible que par les constantes non nulles ou les polynômes λP avec $\lambda \in \mathbb{K}^*$.*

nous allons voir que le polynôme X^2+1 est irréductible sur $\mathbb{R}$ mais ne l'est pas sur $\mathbb{C}$ puisque $X^2+1=(X-i)(X+i)$.

REMARQUE 43 — *Un polynôme A non constant n'est pas irréductible (on dit qu'il est réductible) s'il admet un diviseur B tel que $1 \leq \deg(B) < \deg(A)$. Ceci signifie que A s'écrit sous la forme $A=BQ$ où B et Q sont des polynômes non constants.*

EXEMPLES 44

- *Un polynôme $P=aX+b$ de degré 1 ($a \neq 0$) est irréductible.*
  ***Preuve** — Soit $P=aX+b$ un polynôme de degré 1. Soit D un diviseur de P. Il existe donc $Q \in \mathbb{K}[X]$ tel que $P=DQ$.*
  Comme P est non nul, D et Q le sont aussi et $1=\deg(P)=\deg(D)+\deg(Q) \geq \deg(D)$. Donc D est de degré 0 ou 1.
  -1er cas : D est de degré 0. Alors D est une constante λ non nulle.
  -2nd cas : D est de degré 1. Alors $\deg(Q)=0$ donc Q est constant égal à $\lambda \in \mathbb{K}^*$. Donc $D=\frac{1}{\lambda}P$.
  D'où le résultat. □
- *Un polynôme de degré 2 est irréductible dans $\mathbb{K}[X]$ si et seulement s'il n'est pas scindé dans $\mathbb{K}$.*
  ***Preuve** — Si P admet deux racines α_1 et α_2 distinctes ou non, on a $P=\lambda(X-\alpha_1)(X-\alpha_2)$ et $X-\alpha_1$ divise P. Donc P est réductible.*
  Si P est réductible alors $P=DQ$ avec D et Q de degré 1. Donc $D=\lambda_1(X-\alpha_1)$ et $Q=\lambda_2(X-\alpha_2)$. Finalement, $P=\lambda_1\lambda_2(X-\alpha_1)(X-\alpha_2)$ et P est scindé sur $\mathbb{K}$. □
- *Un polynôme de degré 2 ou 3 est irréductible dans $\mathbb{K}[X]$ si et seulement s'il n'admet pas de racine dans $\mathbb{K}$.*
  ***Preuve** — Si P admet une racine α dans $\mathbb{K}$ alors $X-\alpha$ divise P et P est réductible.*
  Soit P un polynôme de degré 2 ou 3 que l'on suppose réductible. Alors P s'écrit sous la forme $P=DQ$ avec D et Q non constants. Comme $\deg(P)=\deg(D)+\deg(Q)$, on a nécessairement $\deg(D)=1$ ou $\deg(Q)=1$. Donc D ou Q admet une racine dans $\mathbb{K}$, et donc P également. □

  EXEMPLE 45 — *Le polynôme X^2-2 n'est pas irréductible dans $\mathbb{R}[X]$ puisqu'il admet $\sqrt{2}$ et $-\sqrt{2}$ comme racines, mais X^2-2 est irréductible dans $\mathbb{Q}[X]$ car ce polynôme n'admet pas de racines dans $\mathbb{Q}$.*

- *Un polynôme de degré au moins égal à 2 et irréductible dans $\mathbb{K}[X]$ n'a pas de racines dans $\mathbb{K}$.*
  ***Preuve** — Sinon, il serait divisible par un polynôme de degré 1.* □

Un polynôme qui n'admet pas de racines n'est pas forcément irréductible. Cela n'est valable que pour les degrés 2 et 3. Par exemple, $P=(X^2+1)(X^2+1)$ n'admet pas de racines dans $\mathbb{R}$ et n'est pas irréductible.

Le théorème suivant nous dit que tout polynôme non constant est le produit de polynômes irréductibles.

THÉORÈME 46 (Factorisation en produit d'irréductibles)
Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Alors P s'écrit de manière unique à l'ordre près des termes sous la forme

$$P = \lambda P_1^{m_1} \dots P_r^{m_r},$$

où $\lambda \in \mathbb{K}^*$ est le coefficient dominant de P, les polynômes P_1, ..., P_r sont deux à deux distincts, unitaires et irréductibles et m_1, ..., m_r sont des entiers naturels non nuls.

Preuve — Nous ne démontrons ici que l'existence, l'unicité sera démontrée ultérieurement.

Démontrons l'existence d'une factorisation en produit d'irréductibles par récurrence sur le degré.

• *Initialisation :* Les polynômes constants s'écrivent sous la forme $P = \lambda$ avec $\lambda \in \mathbb{K}^*$.

• *Hérédité :* Soit $n \in \mathbb{N}^*$. Supposons que tout polynôme non nul de degré inférieur ou égal à n admet une factorisation en produit d'irréductibles. Soit P un polynôme de degré $n+1$.

1er cas : P est irréductible. Alors en factorisant par le coefficient dominant, on a le résultat.

2nd cas : P n'est pas irréductible. Alors P s'écrit sous la forme $P = AB$ où A et B sont des polynômes non constants. On en déduit que $\deg(A) < n+1$ et $\deg(B) < n+1$, donc d'après l'hypothèse de récurrence, A et B admettent des factorisations en produit d'irréductibles. Par produit, $P = AB$ admet également une factorisation en produit d'irréductibles. □

EXEMPLES 47

- *La décomposition en produit de facteurs irréductibles de $X^3 - 1$ sur $\mathbb{R}$ est*

  $$X^3 - 1 = (X-1)(X^2 + X + 1)$$

  puisque $X - 1$ et $X^2 + X + 1$ sont irréductibles ($X - 1$ est de degré 1 et $X^2 + X + 1$ est de degré 2 sans racine réelle).
- *La décomposition en produit de facteurs irréductibles de $X^3 - 1$ sur $\mathbb{C}$ est*

  $$X^3 - 1 = (X-1)(X-j)(X-\overline{j})$$

  puisque $X - 1$, $X - j$, $X - \overline{j}$, de degré 1, sont irréductibles.

2.4.2 Polynômes irréductibles complexes et réels

Donnons maintenant les polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

PROPOSITION 48
Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

Preuve — Si $P \in \mathbb{C}[X]$ est de degré 1 alors il est irréductible.

Réciproquement, soit $P \in \mathbb{C}[X]$ un polynôme irréductible. P étant non constant, d'après le théorème de d'Alembert Gauss, P admet une racine $\alpha \in \mathbb{C}$. Donc $X - \alpha$ divise P. Comme P est irréductible, il existe $\lambda \in \mathbb{K}$ tel que $P = \lambda(X - \alpha)$. Donc P est de degré 1. □

Du théorème de factorisation et de la proposition précédente, on déduit immédiatement le résultat suivant.

COROLLAIRE 49
Soit $P \in \mathbb{C}[X]$. Alors P s'écrit de manière unique à l'ordre près des termes sous la forme

$$P = \lambda \prod_{i=1}^{r} (X - \alpha_i)^{m_i},$$

où $\lambda \in \mathbb{K}$ est le coefficient dominant de P et α_1, ..., α_r sont des nombres complexes deux à deux distincts.

Regardons maintenant sur $\mathbb{R}$.

Proposition 50
Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement

- *les polynômes de degré 1, de la forme $aX+b$ avec $(a,b)\in\mathbb{R}^*\times\mathbb{R}$,*
- *les polynômes de degré 2 de discriminant strictement négatif, de la forme aX^2+bX+c avec $(a,b,c)\in\mathbb{R}^*\times\mathbb{R}^2$ et $b^2-4ac<0$.*

Preuve — Nous avons vu que les polynômes de degré 1 et ceux de degré 2 de discriminant strictement négatif (donc n'admettant pas de racines réelles) sont irréductibles.

Réciproquement, soit $P\in\mathbb{R}[X]$ un polynôme irréductible. S'il est de degré 1, on est dans le premier cas. Supposons P de degré supérieur ou égal à 2. P étant irréductible de degré supérieur ou égal à 2, P n'admet pas de racines réelles. De la proposition 21, sa décomposition en facteurs irréductibles dans $\mathbb{C}[X]$ est donc de la forme

$$P=\lambda\prod_{k=1}^{r}(X-\alpha_k)^{m_k}(X-\overline{\alpha_k})^{m_k},$$

où $r\geq 1$ et $\alpha_1,\ldots,\alpha_k$ sont des nombres complexes non réels et $m_1,\ldots,m_r$ sont des entiers naturels non nuls.

On a

$$(X-\alpha_k)^{m_k}(X-\overline{\alpha_k})^{m_k}=(X^2-2\mathrm{Re}(\alpha_k)X+|\alpha_k|^2)^{m_k}\in\mathbb{R}[X].$$

Donc, P étant irréductible, $r=m_1=1$ et $P=\lambda(X^2-2\mathrm{Re}(\alpha_1)X+|\alpha_1|^2)$ et $\Delta=4(\mathrm{Re}(\alpha_1)^2-|\alpha_1|^2)=-4\mathrm{Im}(\alpha_1)^2<0$ puisque α_1 est un nombre complexe non réel.

Donc P est un polynôme de degré 2 de discriminant strictement négatif. □

Rappelons que les polynômes de degré 2 de discriminant strictement négatif sont les polynômes sans racines réelles.

On en déduit que tout polynôme non constant de $\mathbb{R}[X]$ est produit de polynômes de degré 1 ou 2.

Corollaire 51
Soit $P\in\mathbb{R}[X]$. Alors P s'écrit de manière unique à l'ordre près des termes sous la forme

$$P=\lambda\prod_{i=1}^{r}(X-\alpha_i)^{m_i}\prod_{k=1}^{s}(X^2+b_kX+c_k)^{n_k},$$

où $\lambda\in\mathbb{K}$ est le coefficient dominant de P, $\alpha_1,\ldots,\alpha_r$ sont des nombres réels deux à deux distincts et pour tout $j\in\{1,\ldots,s\}$, (b_j,c_j) sont des couples de nombres réels tels que $b_j^2-4c_j<0$.

En pratique, on calcule la décomposition en facteurs irréductibles du polynôme sur $\mathbb{C}$ puis on regroupe les racines complexes conjuguées non réelles. Plus précisément, dans $\mathbb{C}[X]$, on écrit la factorisation en produit d'irréductibles sous la forme

$$P=\lambda\prod_{i=1}^{r}(X-\alpha_i)^{m_i}\prod_{k=1}^{s}(X-\beta_k)^{n_k}(X-\overline{\beta_k})^{n_k},$$

où les α_i sont des nombres réels deux à deux distincts et les β_k et $\overline{\beta}_k$ sont les paires de nombres complexes conjugués non réels (voir proposition ? ? ?).

On obtient alors dans $\mathbb{R}[X]$,

$$P=\lambda\prod_{i=1}^{r}(X-\alpha_i)^{m_i}\prod_{k=1}^{s}(X^2+b_kX+c_k)^{n_j},$$

où $b_k=-2\mathrm{Re}(\beta_k)\in\mathbb{R}$ et $c_k=|\beta_k|^2\in\mathbb{R}$. On a alors, pour tout $k\in\{1,\ldots,s\}$, $b_k^2-4c_k<0$ puisque $X^2+b_kX+c_k$ n'a pas de racine réelle.

Exemple 52 — *Déterminons la factorisation en produit de facteurs irréductibles de X^4+1 sur $\mathbb{C}$ puis sur $\mathbb{R}$.*

• *Les racines 4-èmes de -1 sont $\mathrm{e}^{\frac{i\pi}{4}}$, $\mathrm{e}^{\frac{-i\pi}{4}}$, $\mathrm{e}^{\frac{3i\pi}{4}}$ et $\mathrm{e}^{\frac{-3i\pi}{4}}$.*

Donc $X^4+1=(X-\mathrm{e}^{\frac{i\pi}{4}})(X-\mathrm{e}^{\frac{-i\pi}{4}})(X-\mathrm{e}^{\frac{3i\pi}{4}})(X-\mathrm{e}^{\frac{-3i\pi}{4}})$.

On a décomposé X^4+1 en produit de polynômes complexes de degré 1, c'est donc sa décomposition en produit de facteurs irréductibles sur $\mathbb{C}$.

• *On regroupe les racines complexes conjuguées ensemble pour obtenir la factorisation sur $\mathbb{R}$.*

On a $(X-\mathrm{e}^{\frac{i\pi}{4}})(X-\mathrm{e}^{-i\frac{\pi}{4}}) = X^2-2\cos(\frac{\pi}{4})X+1 = X^2-\sqrt{2}X+1$

et $(X-\mathrm{e}^{3i\frac{\pi}{4}})(X-\mathrm{e}^{\frac{-3i\pi}{4}}) = X^2-2\cos(\frac{3\pi}{4})X+1 = X^2+\sqrt{2}X+1$

Donc $X^4+1=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$.

Il s'agit donc de la décomposition en produit de facteurs irréductibles sur $\mathbb{R}$.

2.5 Arithmétique des polynômes

2.5.1 Idéaux dans les anneaux

2.5.1.a. Définition

Dans tout ce paragraphe, $(A,+,\times)$ désigne un anneau commutatif.

Définition 53
*On appelle **idéal** de l'anneau $(A,+,\times)$ toute partie I de A telle que*

1. *I est un sous-groupe de $(A,+)$,*
2. *Pour tout $x\in I$ et tout $a\in A$, $a\times x\in I$.*

Exemples 54

- *$\{0_A\}$ et A sont des idéaux de A.*
- *Soient $(A,+,\times)$ et $(B,+,\times)$ des anneaux commutatifs. Soit $\varphi: A\longrightarrow B$ un morphisme d'anneaux. Le noyau de φ, $\ker(\varphi)=\varphi^{-1}(\{0_B\})$, est un idéal de $(A,+,\times)$.*
  ***Preuve** —*
  1. *$\ker(\varphi)$ est un sous-groupe comme noyau du morphisme de groupe $\varphi:(A,+)\longrightarrow(B,+)$.*
  2. *Soient $x\in\ker(\varphi)$ et $a\in A$.*
     Alors $\varphi(a\times x)=\varphi(a)\times\varphi(x)=\varphi(a)\times 0_B=0_B$. Donc $a\times x\in\ker(\varphi)$.

  Donc $\ker(\varphi)$ est un idéal de A. □

Proposition 55
Soient I et J des idéaux de $(A,+,\times)$. Alors $I\cap J$ et $I+J$ sont des idéaux de A.

Preuve —

• Montrons que $I\cap J$ est un idéal de A.

1. $I\cap J$ est un sous-groupe comme intersection de sous-groupes.
2. Soit $x\in I\cap J$. Soit $a\in A$. Comme I est un idéal de A et $x\in I$, $ax\in I$. De même, $ax\in J$. Donc $ax\in I\cap J$.

Donc $I\cap J$ est un idéal de A.

• Montrons que $I+J$ est un idéal de A.

1. -$0_A=0_A+0_A\in I+J$ car I et J sont des sous-groupes.
   -Soit $(x,y)\in(I+J)^2$. Alors il existe $(x_I,x_J,y_I,y_J)\in(I\times J)^2$ tel que $x=x_I+x_J$ et $y=y_I+y_J$. Donc $x-y=(x_I-y_I)+(x_J-y_J)\in I+J$ car I et J sont des sous-groupes.
   Donc $I+J$ est un sous-groupe de A.
2. Soit $x\in I+J$. Soit $a\in A$. Il existe $(x_I,x_J)\in I\times J$ tel que $x=x_I+x_J$. Donc $ax=ax_I+ax_J\in I+J$ car I et J sont des idéaux.

D'où le résultat. □

Proposition 56
Soit $a\in A$. On note aA ou (a), l'ensemble $\{a\times k, k\in A\}$. Alors aA est un idéal de A.

Preuve —

1. • $0_A = a \times 0_A$ donc $0_A \in A$.
   • Soit $(x, y) \in aA$. Montrons que $x - y \in aA$. Il existe $(k, k') \in A^2$ tel que $x = a \times k$ et $y = a \times k'$. Donc $x - y = a(k - k') \in aA$.

   Donc aA est un sous-groupe de A.
2. On a $aA \times A = aA$.

D'où le résultat. □

REMARQUE 57 — *L'idéal (a) est le plus petit idéal contenant a. On dit que (a) est l'idéal engendré par a et que a est un générateur de (a).*

PROPOSITION 58
Soit I un idéal de A. On a $I = A$ si et seulement si I contient un élément inversible de A.

Preuve —

▷ Si $I = A$ alors $1 \in I$ et 1 est inversible.

◁ Supposons que I contient un élément inversible $u \in A$.

Soit $a \in A$. Alors $a = u \times (u^{-1}a) \in I$ puisque $u^{-1}a \in A$ et I est un idéal de A. Donc $A \subset I$ et finalement $I = A$. □

REMARQUE 59 — *En particulier, les idéaux d'un corps $\mathbb{K}$ sont exactement $\{0_\mathbb{K}\}$ et $\mathbb{K}$.*

EXEMPLE 60 — *Le seul idéal de l'anneau $(\mathbb{Z}, +, \times)$ qui contient l'entier 1 est $\mathbb{Z}$ lui-même.*

2.5.1.b. Divisibilité dans un anneau intègre

Dans cette partie, on suppose que $(A, +, \times)$ est un anneau commutatif intègre.

DÉFINITION 61
Soient a et b des éléments de A.

- *On dit que a **divise** b s'il existe $k \in A$ tel que $b = k \times a$. On dit aussi que a est un **diviseur** de b ou que b est un **multiple** de a. On note $a \mid b$.*
- *On dit que a et b sont **associés** s'il existe un élément inversible $u \in A$ tel que $b = ua$.*

EXEMPLES 62

- *Les éléments inversibles de $\mathbb{Z}$ sont 1 et -1.*
- *Les éléments inversibles de $\mathbb{K}[X]$ sont les constantes $\lambda \in \mathbb{K}$ non nulles.*

PROPOSITION 63
Soient a et b des éléments de A. Alors $a \mid b$ si et seulement si $(b) \subset (a)$.

Preuve —

▷ Supposons que $a \mid b$. Alors il existe $k \in A$ tel que $b = ak$. Soit $x \in (b)$. Par définition, il existe $k' \in A$ tel que $x = bk'$. Donc $x = akk' \in (a)$. Donc $(b) \subset (a)$.

◁ Réciproquement, supposons que $(b) \subset (a)$. Alors $b \in (a)$ donc il existe $k \in A$ tel que $b = ak$. Donc $a \mid b$. □

PROPOSITION 64
Soient a et b des éléments de A. Les propositions suivantes sont équivalentes :

1. *a et b sont associés*
2. *$b \mid a$ et $a \mid b$*
3. *$(a) = (b)$.*

Preuve —

• Supposons a et b associés. Alors il existe un élément inversible $u \in A$ tel que $b = ua$. Donc $a \mid b$. Comme u est inversible dans A, on a aussi, $a = u^{-1}b$. Donc $b \mid a$.

• Supposons que $b \mid a$ et $a \mid b$. Alors d'après la proposition précédente, $(a) \subset (b)$ et $(b) \subset (a)$, donc $(a) = (b)$.

• Supposons que $(a) = (b)$. Comme $a \in (b)$, il existe $k \in A$ tel que $a = bk$. Comme $b \in (a)$, il existe $k' \in A$ tel que $b = ak'$.

Donc $a = ak'k'$, soit $a(1 - kk') = 0$.

Si $a = 0$ alors $b = 0 = 1 \times a$.

Supposons $a \neq 0$. Par intégrité, on a donc $1 = kk'$ et k est donc inversible dans A. Donc a et b sont associés. □

Exemple 65 — *Si P et P' sont des générateurs d'un même idéal de $\mathbb{K}[X]$ alors ils sont associés, c'est-à-dire qu'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda P'$. Cela découle de la proposition 3.*

2.5.1.c. Anneaux principaux et $\mathbb{K}[X]$

Définition 66

- *Un idéal I de A est dit **principal** s'il est engendré par un élément a de A. Il s'écrit donc sous la forme $(a) = aA$.*
- *L'anneau $(A, +, \times)$ est **principal** s'il est intègre et si tout idéal de A est principal.*

Proposition 67
Les idéaux de l'anneau intègre $(\mathbb{Z}, +, \times)$ sont exactement les ensembles de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}$. Ainsi, l'anneau $(\mathbb{Z}, +, \times)$ est principal.

Preuve — En effet, les idéaux de $\mathbb{Z}$ étant des sous-groupes, ils sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$. Réciproquement, nous venons de voir que les ensembles de la forme $n\mathbb{Z}$ sont des idéaux. □

Proposition 68
Les idéaux de l'anneau intègre $(\mathbb{K}[X], +, \times)$ sont exactement les ensembles de la forme

$$P\mathbb{K}[X] = \{PQ \mid Q \in \mathbb{K}[X]\}.$$

Ainsi, l'anneau $(\mathbb{K}[X], +, \times)$ est principal.

Preuve —

▷ Soit $P \in \mathbb{K}[X]$. D'après ce qui précède, $P\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$.

◁ Soit I un idéal de $\mathbb{K}[X]$. On exclut le cas où $I = \{0\}$ où on a $I = 0\mathbb{K}[X]$.

Soit D l'ensemble des degrés des éléments non nuls de I. Puisque $I \neq \{0\}$, D est une partie non vide de $\mathbb{N}$ qui admet un plus petit élément d_0. Soit alors P_0 un élément de I de degré d_0.

- $P_0\mathbb{K}[X] \subset I$ car $P_0 \in I$ et I est un idéal.

- Soit $T \in I$. Par division euclidienne de T par P_0, il existe $(Q, R) \in \mathbb{K}[X]^2$ tel que $T = P_0Q + R$ et $\deg(R) < \deg(P_0)$.

On a donc $R = T - P_0Q$. Or $T \in I$ et $P_0Q \in I$ car I est un idéal, donc $R = T - P_0Q \in I$ (I est un sous-groupe).

Or $\deg(R) < d_0$ et par définition de d_0, on a donc $R = 0$. Donc $T = P_0Q \in P_0\mathbb{K}[X]$.

Donc $I \subset P_0\mathbb{K}[X]$.

De ces deux points, on obtient $I = P_0\mathbb{K}[X]$. □

Un idéal de $\mathbb{K}[X]$ n'admet pas un unique générateur. Par exemple, $X\mathbb{K}[X] = (2X)\mathbb{K}[X]$. On dispose toutefois du résultat suivant.

Proposition 69
Tout idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$ admet un unique polynôme générateur unitaire.

Preuve — Soit $I = P\mathbb{K}[X]$ un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$. P s'écrit $P = a_{d_0}X^{d_0} + \ldots + a_1X + a_0$ avec $a_{d_0} \neq 0$. Soit $\tilde{P}$ un générateur de I.

P et $\tilde{P}$ sont associés, donc il existe $b \in \mathbb{K}^*$ tel que $P' = bP = ba_{d_0}X^{d_0} + \ldots + ba_1X + ba_0$. Donc $\tilde{P}$ est un générateur unitaire de I si et seulement si $b = \dfrac{1}{a_{d_0}}$.

Donc I admet un unique polynôme générateur unitaire.

□

Rappelons que nous nous sommes placés dans le corps $\mathbb{K} = \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{Q}$. L'anneau $(\mathbb{Z}[X], +, \times)$, lui, n'est pas principal car il admet des idéaux non principaux.

Exemple 70 — *L'idéal $I = (2, X) = 2\mathbb{Z}[X] + X\mathbb{Z}[X]$ de $\mathbb{Z}[X]$ n'est pas principal.*

Preuve — *Supposons par l'absurde qu'il existe $P \in \mathbb{Z}[X]$ tel que $(2, X) = (P)$. Comme $2 \in (2, X) = (P)$, il existe $Q \in \mathbb{Z}[X]$ tel que $2 = PQ$. Donc $\deg(P) = \deg(Q) = 0$ et donc P est constant non nul dans $\mathbb{Z}$ et divise 2. Donc $P = \pm 2$ ou $P = \pm 1$. Comme $P \in (P) = (2, X)$, il existe $(A, B) \in \mathbb{Z}[X]$ tel que $P = 2A + XB$. Donc $P = P(0) = 2A(0)$ est pair. Donc $P = \pm 2$. Comme $X \in (2, X) = (P)$, il existe $C \in \mathbb{Z}[X]$ tel que $X = PC$. Donc $1 = P(1)C(1) = 2C(1)$ avec $C(1) \in \mathbb{Z}$. Ceci est absurde. Donc I n'est pas un idéal principal.* □

2.5.2 PGCD et PPCM dans $\mathbb{K}[X]$

L'étude qui suit est faite dans l'anneau $(\mathbb{K}[X], +, \times)$ mais peut être remplacée par l'anneau $(\mathbb{Z}, +, \times)$, et même à tout anneau principal.

Définition 71
*Soit $(A, B) \in \mathbb{K}[X]^2$. On appelle **plus grand diviseur commun** (pgcd) de A et B l'unique polynôme générateur unitaire D de l'idéal $A\mathbb{K}[X] + B\mathbb{K}[X]$:*

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

Définition 72
*Soit $(A, B) \in \mathbb{K}[X]^2$. On appelle **plus petit multiple commun** (ppcm) de A et B l'unique polynôme générateur unitaire M de l'idéal $A\mathbb{K}[X] \cap B\mathbb{K}[X]$:*

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X].$$

Remarque 73 — *Le pgcd et le ppcm de deux polynômes sont bien définis car la somme et l'intersection de deux idéaux est un idéal et l'anneau $(\mathbb{K}[X], +, \times)$ est principal.*

Proposition 74
Soient A, B et D des éléments de $\mathbb{K}[X]$. Alors $D = pgcd(A, B)$ si et seulement si

1. *$D \mid A$ et $D \mid B$,*
2. *Pour tout élément $D' \in \mathbb{K}[X]$, si $D' \mid A$ et $D' \mid B$ alors $D' \mid D$.*

Proposition 75
Soient A, B et M des éléments de $\mathbb{K}[X]$. Alors $M = pgcd(A, B)$ si et seulement si

1. *$A \mid M$ et $B \mid M$,*
2. *Pour tout élément $M' \in \mathbb{K}[X]$, si $A \mid M'$ et $B \mid M'$ alors $M \mid M'$.*

Lemme 76
Soient A et B deux éléments de $\mathbb{K}[X]$. Notons R le reste de la division euclidienne de A par B. Alors

$$\text{pgcd}(A, B) = \text{pgcd}(B, R).$$

Preuve — On montre que $A\mathbb{K}[X] + B\mathbb{K}[X] = B\mathbb{K}[X] + R\mathbb{K}[X]$. □

On peut calculer le pgcd de deux polynômes avec l'algorithme d'Euclide. Il est basé sur des divisions euclidiennes successives.

PROPOSITION 77 (Algorithme d'Euclide)
Soient A et B deux polynômes non nuls. On pose $R_0 = A$ et $R_1 = B$. Tant que $R_{k+1} \neq 0$, on effectue la division euclidienne de R_k par R_{k+1} :

$$R_k = Q_k R_{k+1} + R_{k+2} \quad et \quad \deg(R_{k+2}) < \deg(R_{k+1}).$$

L'algorithme s'arrête et le pgcd de A et B est le dernier reste non nul, à multiplication par une constante près.

Preuve — On peut supposer $\deg(A) \geq \deg(B)$. On a $\deg(R_0) \geq \deg(R_1) > \deg(R_2) > \ldots$. Or il n'existe qu'un nombre fini d'entiers naturels entre 0 et $\deg(R_0)$. Il existe donc $N \in \mathbb{N}^*$ tel que $\deg(R_N) = -\infty$, soit $R_N = 0$. Donc l'algorithme s'arrête.

Or $\text{pgcd}(A, B) = \text{pgcd}(B, R_2) = \text{pgcd}(R_2, R_3) = \ldots = \text{pgcd}(R_{N-1}, 0) = \lambda R_{N-1}$ où λR_{N-1} est un polynôme unitaire. □

EXEMPLE 78 — *Déterminons le pgcd de $A = X^4 + X^3 + 2X^2 + X + 1$ et $B = X^3 - 3X^2 + X - 3$.*

Par division euclidienne, $A = (X + 4)B + 13X^2 + 13$.

Puis $B = 13(X^2 + 1) \times \dfrac{1}{13}(X - 3) + 0$.

Donc $pgcd(A, B) = X^2 + 1$.

Si l'on connaît la factorisation en produit d'irréductibles des polynômes A et B, on peut déterminer directement leur pgcd, sur le même principe que pour les entiers.

EXEMPLE 79 — *Soient $A = 2X(X + 1)^2(X^2 + X + 1)$ et $B = 3X^2(X + 2)(X^2 + X + 1)^2$. Alors* $\text{pgcd}(A, B) = X(X^2 + X + 1)$.

2.5.3 Polynômes premiers entre eux

DÉFINITION 80
Soient A et B des éléments de $\mathbb{K}[X]$. On dit que A et B sont premiers entre eux si $\text{pgcd}(A, B) = 1$.

EXEMPLE 81 — *Soient a et b deux éléments distincts de $\mathbb{K}$. Les polynômes $X - a$ et $X - b$ sont premiers entre eux.*

THÉORÈME 82 (Théorème de Bezout)
Soient A et B des éléments de $\mathbb{K}[X]$. Alors A et B sont premiers entre eux si et seulement s'il existe des polynômes U et V tels que $AU + BV = 1$.

Preuve — ▷ Supposons A et B premiers entre eux. Alors $A\mathbb{K}[X] + B\mathbb{K}[X] = 1\mathbb{K}[X]$. Donc $1 \in \mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X]$. Il existe donc $(U, V) \in \mathbb{K}[X]^2$ tel que $1 = AU + BV$.

◁ Supposons qu'il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$.

Alors $1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$. Or l'idéal engendré par 1 est $\mathbb{K}[X]$. Donc $1\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X]$ et $\text{pgcd}(A, B) = 1$. □

REMARQUE 83 — *On peut trouver les polynômes U et V à l'aide de l'algorithme d'Euclide étendu, sur le même principe que pour les entiers.*

PROPOSITION 84 (Lemme de Gauss)
Soient A, B et C des éléments de $\mathbb{K}[X]$. Si A divise BC et si A et B sont premiers entre eux alors A divise C.

Preuve — Supposons que $A \mid BC$ et $\text{pgcd}(A, B) = 1$. Alors $A\mathbb{K}[X] + B\mathbb{K}[X] = \mathbb{K}[X]$. Donc $AC\mathbb{K}[X] + BC\mathbb{K}[X] = C\mathbb{K}[X]$.

Or $AC\mathbb{K}[X] \subset A\mathbb{K}[X]$ et $BC\mathbb{K}[X] \subset A\mathbb{K}[X]$ car $A \mid BC$.

Donc $C\mathbb{K}[X] \subset A\mathbb{K}[X] + A\mathbb{K}[X] = A\mathbb{K}[X]$. Donc $A \mid C$. □

PROPOSITION 85
Soient A, B et C des éléments de $\mathbb{K}[X]$. On suppose A et B premiers entre eux. Alors si $A \mid C$ et $B \mid C$ alors $AB \mid C$.

Preuve — Il existe $P \in \mathbb{K}[X]$ tel que $C = AK$. Comme $B \mid C$, $B \mid AK$. Or A et B sont premiers entre eux, donc d'après le lemme de Gauss, $B \mid K$. Il existe donc $K' \in \mathbb{K}[X]$ tel que $K = BK'$. Donc $C = ABK'$. Donc $AB \mid C$. □

PROPOSITION 86
Soient A, B et P des éléments de $\mathbb{K}[X]$. Supposons P irréductible. Alors $P \mid AB$ si et seulement si $P \mid A$ ou $P \mid B$.

Preuve — Supposons que $P \mid AB$ et P ne divise pas A. Montrons que P divise B. Posons $D = \text{pgcd}(P, A)$. Alors D divise P. P étant irréductible, $D = 1$ ou D est un polynôme unitaire associé à P, de la forme $D = \lambda P$ où $\lambda \in \mathbb{K}^*$. Si $D = \lambda P$ alors $P = \frac{1}{\lambda} D$ divise A, ce qui est exclu. Donc $D = 1$. Donc P et A sont premiers entre eux et d'après le lemme de Gauss, $P \mid B$.

La réciproque est évidente. □

De ce théorème, on peut démontrer l'unicité dans la décomposition d'un polynôme en produit de facteurs premiers.

PROPOSITION 87
Soit $P \in \mathbb{K}[X]$. Si P et P' sont premiers entre eux alors P n'a que des racines simples.

Preuve — Soit α une racine de P de multiplicité supérieure ou égale à 2. Alors α est racine de P de multiplicité supérieure ou égale à 1. Donc $X - \alpha$ divise P et divise P'. Donc P et P' ne sont pas premiers entre eux. D'où le résultat par contraposée. □

Chapitre 3 Fractions rationnelles

Dans ce chapitre, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$.

Dans le chapitre précédent, nous avons vu que les seuls polynômes inversibles à coefficients dans $\mathbb{K}$ sont les polynômes constants non nuls. Nous allons donc devoir définir ce qu'est le quotient de deux polynômes puisque *a priori*, cela n'est pas défini lorsque les polynômes ne sont pas inversibles.

3.1 Le corps des fractions rationnelles

Définition 1
L'ensemble $\mathbb{K}(X)$ des fractions rationnelles est un ensemble vérifiant les trois propositions suivantes :

1. *À tout couple $(A,B)\in\mathbb{K}[X]^2$ avec B non nul, on associe un unique élément de $\mathbb{K}(X)$ noté $\dfrac{A}{B}$,*
2. *Tout élément de $\mathbb{K}(X)$ peut s'écrire sous la forme $\dfrac{A}{B}$ avec $(A,B)\in\mathbb{K}[X]^2$ et B non nul,*
3. *Pour tout $(A,B,C,D)\in\mathbb{K}[X]^4$ avec B et D non nuls, $\dfrac{A}{B}=\dfrac{C}{D}$ si et seulement si $AD=BC$.*

*Les éléments de $\mathbb{K}(X)$ sont appelés les **fractions rationnelles** à coefficients dans $\mathbb{K}$.*

Preuve — Expliquons comment construire cet ensemble.

On définit sur $\mathbb{K}[X]\times\mathbb{K}[X]^*$ la relation $(P,Q)\sim(R,S)\Leftrightarrow PS=QR$.

La relation $\sim$ est une relation d'équivalence.

$\mathbb{K}(X)$ est alors l'ensemble quotient de $\mathbb{K}[X]\times\mathbb{K}[X]^*$ par la relation $\sim$ et pour tout $(A,B)\in\mathbb{K}[X]^2$ avec B non nul, $\dfrac{A}{B}$ est la classe d'équivalence de (A,B) associée.

Cet ensemble vérifie bien les trois propriétés. □

Exemple 2 — *Dans $\mathbb{R}(X)$, $\dfrac{1}{X}$ et $\dfrac{X}{X^2}$ sont égales car $1\times X^2=X\times X$.*

Définition 3
On munit $\mathbb{K}(X)$ de deux lois internes $+$ et $\times$ définies, pour tout $(A,B,C,D)\in\mathbb{K}[X]^4$ avec B et D non nul, par

- $\dfrac{A}{B}+\dfrac{C}{D}=\dfrac{AD+BC}{BD}$,
- $\dfrac{A}{B}\times\dfrac{C}{D}=\dfrac{AC}{BD}$.

Alors $(\mathbb{K}(X),+,\times)$ est un corps commutatif.

Preuve —

• Commençons par vérifier que $+$ et $\times$ sont bien définies, c'est-à-dire qu'elles ne dépendent pas du choix des polynômes.

Supposons que $\dfrac{A}{B}=\dfrac{A'}{B'}$ et $\dfrac{C}{D}=\dfrac{C'}{D'}$ avec A,B,C,D,A',B',C',D' des polynômes et B,B',D et D' non nuls.

Montrons que $\dfrac{AD+BC}{BD}=\dfrac{A'D'+B'C'}{B'D'}$ et $\dfrac{AC}{BD}=\dfrac{A'C'}{B'D'}$.

D'une part, $AC\times B'D'=AB'\times CD'=A'B\times C'D=BD\times A'C'$. Donc $\dfrac{AC}{BD}=\dfrac{A'C'}{B'D'}$.

D'autre part, $(AD+BC)\times B'D'=AB'\times DD'+BB'\times CD'=A'B\times D'D+B'B\times D'D=BD\times(A'D'+B'C')$. Donc $\dfrac{AD+BC}{BD}=\dfrac{A'D'+B'C'}{B'D'}$.

• On peut montrer que $(\mathbb{K}(X), +, \times)$ est un corps en vérifiant les différents points de la définition.

Notons que l'élément neutre pour $+$ est $\frac{0}{1}$ puisque $\frac{A}{B} + \frac{0}{1} = \frac{A \times 1 + B \times 0}{B \times 1} = \frac{A}{B}$ et de même, $\frac{0}{1} + \frac{A}{B} = \frac{A}{B}$.

L'opposé de $\frac{A}{B}$ est $\frac{-A}{B}$.

L'élément neutre pour $\times$ est $\frac{1}{1}$.

Toute fraction non nulle $\frac{A}{B}$ admet un inverse qui est $\frac{B}{A}$. □

PROPOSITION 4
Soit $(A, B, C) \in \mathbb{K}[X]^3$ avec B et C non nuls. Alors $\frac{AC}{BC} = \frac{A}{B}$.

Preuve — On a $AC \times B = A \times BC$. D'où le résultat. □

REMARQUE 5 — *Les opérations sur les fractions rationnelles se font finalement comme sur les nombres rationnels.*

EXEMPLES 6

- *Posons $F = \frac{X+1}{X-1}$ et $G = \frac{X^2 - 2X - 1}{X(X+1)}$.*
  Alors
  $$F + G = \frac{2X^3 - X^2 + 2X + 1}{X(X^2 - 1)}$$
  et
  $$FG = \frac{X^2 - 2X - 1}{X(X-1)}.$$
- *Soit $n \in \mathbb{N}$. On a $X^{n+1} - 1 = (X-1)(1 + X + \ldots + X^n)$ dans $\mathbb{K}[X]$. En multipliant par l'inverse de $X - 1$ dans $\mathbb{K}(X)$, on obtient donc*
  $$\frac{X^{n+1} - 1}{X - 1} = 1 + X + \ldots + X^n.$$
  On peut diviser par $X - 1$ car $X - 1$ est non nul. On n'a pas besoin de se préoccuper de ce qui se passe en 1 car X est une indéterminée.

PROPOSITION 7
On identifie tout polynôme $P \in \mathbb{K}[X]$ à la fraction rationnelle $\frac{P}{1} \in \mathbb{K}(X)$. Autrement dit, $\mathbb{K}[X] \subset \mathbb{K}(X)$.

Preuve — L'application $\mathbb{K}[X] \longrightarrow \mathbb{K}(X)$; $P \longmapsto \frac{P}{1}$ est injective car pour tout $(P, Q) \in \mathbb{K}[X]^2$, si $\frac{P}{1} = \frac{Q}{1}$ alors $P \times 1 = Q \times 1$, soit $P = Q$. □

PROPOSITION 8
Soit $R \in \mathbb{K}(X)$. Il existe un couple de polynômes (A, B) avec B non nul tel que $R = \frac{A}{B}$ et A et B sont premiers entre eux. Ce couple est unique à multiplication par une constante près. On dit que $\frac{A}{B}$ est la ***forme irréductible de*** *R.*

EXEMPLE 9 — *Soit $R = \frac{2X(X+1)^2}{(X+1)(X+2)}$. Alors la forme irréductible de R est $R = \frac{2X(X+1)}{X+2}$.*

DÉFINITION 10
Soit $R = \frac{A}{B} \in \mathbb{K}(X)$. La dérivée de R, notée R', est la fraction rationnelle $\frac{A'B - AB'}{B^2}$. Elle ne dépend pas du choix de A et B.

Proposition 11
Soient R et S des éléments de $\mathbb{K}(X)$. Soit $\lambda \in \mathbb{K}$. Alors
- $(R+\lambda S)' = R' + \lambda S'$,
- $(RS)' = R'S + RS'$,
- *Si R est non nul,* $\left(\frac{1}{R}\right)' = -\frac{R'}{R^2}$,
- *Si S est non nul,* $\left(\frac{R}{S}\right)' = \frac{R'S - RS'}{S^2}$,

Exemple 12 — *Pour tout $n \in \mathbb{N}^*$ et tout $a \in \mathbb{K}$,*

$$\left(\frac{1}{(X-a)^n}\right)' = -\frac{n}{(X-a)^{n+1}}.$$

Définition 13
*Soit $R = \frac{A}{B} \in \mathbb{K}(X)$. On appelle **degré de** R, noté $\deg(R)$, la quantité $\deg(A) - \deg(B)$. Il ne dépend pas du choix de A et B.*

Remarque 14 —
- *Le degré d'une fraction rationnelle est soit un entier relatif, soit $-\infty$.*
- *Pour tout $P \in \mathbb{K}[X]$, $\deg(\frac{P}{1}) = \deg(P) - \deg(1) = \deg(P)$. Ainsi, le degré d'un polynôme coïncide avec son degré comme fraction rationnelle.*

Proposition 15
Pour tout $(R,S) \in \mathbb{K}(X)$,
- $\deg(R+S) \leq \max(\deg(R), \deg(S))$,
- $\deg(RS) = \deg(R) + \deg(S)$,
- *Si R est non nul alors* $\deg(R') \leq \deg(R) - 1$,
- *Si R est non nul alors* $\deg(R^{-1}) = -\deg(R)$.

Exemples 16
- *La fraction rationnelle* $\frac{X^5 + 3X^2 + X + 1}{X^2 - 3}$ *est de degré* $5 - 2 = 3$.
- *La fraction rationnelle* $\frac{X^2}{X^2+1}$ *est de degré* 0.
- *La fraction rationnelle* $R = \frac{X+1}{X} = 1 + \frac{1}{X}$ *est de degré* 0 *et R' est de degré* -2.

Définition 17
Soit $R = \frac{A}{B} \in \mathbb{K}(X)$ sous forme irréductible.
- *Soit $\lambda \in \mathbb{K}$. On dit que λ est un **zéro** de R si λ est racine de A. La multiplicité de λ dans A est appelée la **multiplicité** de λ dans R.*
- *Soit $\mu \in \mathbb{K}$. On dit que μ est un **pôle** de R si μ est une racine de B. La multiplicité de μ dans B est appelée la **multiplicité** de μ dans R. Un pôle de multiplicité 1 (resp. 2) est aussi appelé un **pôle simple** (resp. **double**).*

Remarque 18 — *Puisque A et B sont premiers entre eux, un même élément λ ne peut être à la fois zéro et pôle de R.*

EXEMPLE 19 — *Dans* $\mathbb{R}(X)$*, la fraction rationnelle* $\dfrac{(X^2+1)(X-1)^2(X+2)X}{(X-2)^2(X^2+X+1)}$ *a pour zéros* 1*,* -2 *et* 0 *et pour pôle* 2*.*

DÉFINITION 20
Soit $R = \dfrac{A}{B} \in \mathbb{K}(X)$ *sous forme irréductible. La fonction* $x \longmapsto \dfrac{A(x)}{B(x)}$ *définie sur* $\mathbb{K}\setminus\mathcal{P}$ *où* $\mathcal{P}$ *est l'ensemble racines de* B *est appelée* ***fonction rationnelle associée à*** R*.*

EXEMPLE 21 — *On peut donc écrire* $F = \dfrac{X^2+1}{X-1}$ *ou, pour tout* $x \in \mathbb{R}\setminus\{1\}$*,* $F(x) = \dfrac{x^2+1}{x-1}$*.*

PROPOSITION 22
Soit $R = \dfrac{A}{B} \in \mathbb{K}(X)$*. Il existe un unique polynôme* $E \in \mathbb{K}[X]$ *et une unique fraction rationnelle* $S \in \mathbb{K}(X)$ *tels que*

$$R = E + S \quad \text{et} \quad \deg(S) < 0.$$

Le polynôme E *est appelé la* ***partie entière*** *de* R*.*

Preuve — • **Existence :** Par division euclidienne de A par B, on a $A = BQ + F$ où $(Q,F) \in \mathbb{K}[X]^2$ et $\deg(F) < \deg(B)$.

Posons $E = Q$ et $S = \dfrac{F}{B}$.

Alors $R = \dfrac{A}{B} = \dfrac{BE+F}{B} = E + \dfrac{F}{B} = E + S$.

De plus, $\deg(S) = \deg(F) - \deg(B) < 0$.

D'où l'existence.

• **Unicité :** Supposons que $R = E_1 + S_1$ et $R = E_2 + S_2$ avec $\deg(S_1) < 0$ et $\deg(S_2) < 0$.

Alors $\deg(E_1 - E_2) = \deg(S_2 - S_1) \leq \max(\deg(S_1), \deg(S_2)) < 0$. Comme $E_1 - E_2$ est un polynôme, son degré vaut $-\infty$ et c'est donc le polynôme nul. Donc $E_1 = E_2$, puis $S_1 = S_2$.

D'où l'unicité. □

REMARQUE 23 — *La partie entière* E *de* $\dfrac{A}{B}$ *est le quotient de la division euclidienne de* A *par* B*.*

EXEMPLE 24 — *Déterminons la partie entière de* $\dfrac{X^3+2X^2+X+1}{X+1}$*. On calcule la division euclidienne de* X^3+2X^2+X+1 *par* $X+1$ *:*

$$X^3 + 2X^2 + X + 1 = (X^2+X)(X+1) + 1.$$

On en déduit que

$$\frac{X^3+2X^2+X+1}{X+1} = \frac{(X+1)(X^2+X)+1}{X+1} = X^2 + X + \frac{1}{X+1}.$$

La partie entière est donc $X^2 + X$*.*

3.2 Décompositions en éléments simples

Nous savons écrire facilement que

$$X + \frac{1}{X} - \frac{1}{X+1} = \frac{X^3+X^2+1}{X(X+1)}.$$

Dans cette partie, nous allons apprendre à faire l'opération inverse :

passer de $\dfrac{X^3+X^2+1}{X(X+1)}$ à $X+\dfrac{1}{X}-\dfrac{1}{X+1}$.

Cette écriture s'appelle la **décomposition en éléments simples** de $\dfrac{X^3+X^2+1}{X(X+1)}$. Notons que X est sa partie entière.

Elle permet notamment de calculer des intégrales.

Par exemple,

$$\begin{aligned}\int_1^2 \frac{t^3+t^2+1}{t(t+1)}\mathrm{d}t &= \int_1^2 \left(t+\frac{1}{t}-\frac{1}{t+1}\right)\mathrm{d}t\\ &= \left[\frac{t^2}{2}+\ln(t)-\ln(t+1)\right]_1^2\\ &= 2+\ln(2)-\ln(3)-\frac{1}{2}+\ln(2)\\ &= \frac{3}{2}+2\ln(2)-\ln(3).\end{aligned}$$

Proposition 25
Soient P, Q_1, $Q_2 \in \mathbb{K}[X]$ trois polynômes non nuls tels que $\deg P < \deg(Q_1Q_2)$ et Q_1 et Q_2 premiers entre eux. Alors il existe un unique couple de polynômes (P_1,P_2) tel que $\deg P_1 < \deg Q_1$ et $\deg P_2 < \deg Q_2$ et

$$\frac{P}{Q_1Q_2}=\frac{P_1}{Q_1}+\frac{P_2}{Q_2}.$$

Preuve —

• *Existence :* Les polynômes Q_1 et Q_2 étant premiers entre eux, d'après le thérème de Bezout, il existe des polynômes B_1 et B_2 tels que $B_2Q_1+B_1Q_2=1$. On a donc

$$P = PB_2Q_1+PB_1Q_2.$$

En divisant par Q_1Q_2, on obtient

$$\frac{P}{Q_1Q_2}=\frac{PB_2}{Q_2}+\frac{PB_1}{Q_1}.$$

Effectuons la division euclidienne de PB_2 par Q_2. Il existe deux polynômes C et P_2 tels que $PB_2 = CQ_2+P_2$ et $\deg(P_2)<\deg(Q_2)$.

On obtient alors

$$\frac{P}{Q_1Q_2}=C+\frac{P_2}{Q_2}+\frac{PB_1}{Q_1}=\frac{P_2}{Q_2}+\frac{PB_1+Q_1C}{Q_1}.$$

Posons $P_1 = PB_1+Q_1C$. Comme $\dfrac{P_1}{Q_1}=\dfrac{P}{Q_1Q_2}-\dfrac{P_2}{Q_2}$,

$$\deg(\frac{P_1}{Q_1}) \le \max\left(\deg(\frac{P}{Q_1Q_2}),\deg(\frac{P_2}{Q_2})\right) = \max(\deg(P)-\deg(Q_1Q_2),\deg(P_2)-\deg(Q_2)) < 0,$$

donc $\deg(P_1)<\deg(Q_1)$.

D'où l'existence.

• *Unicité :* Supposons qu'il existe deux couples (R_1,R_2) et (S_1,S_2) vérifiant les conditions de l'énoncé. On a alors

$$R=\frac{R_1}{Q_1}+\frac{R_2}{Q_2}=\frac{S_1}{Q_1}+\frac{S_2}{Q_2}.$$

Donc $(R_1-S_1)Q_2=(S_2-R_2)Q_1$. Donc $Q_1 \mid (R_1-S_1)Q_2$. Or Q_1 et Q_2 étant premiers entre eux, d'après le lemme de Gauss, $Q_1 \mid R_1-S_1$. Or $\deg(R_1-S_1)\le\max(\deg(R_1),\deg(S_1))<\deg(Q_1)$. Donc $R_1-S_1=0$, puis $R_1=S_1$.

On en déduit que $\dfrac{R_2}{Q_2}=\dfrac{S_2}{Q_2}$, puis $R_2=S_2$.

D'où l'unicité. □

Exemple 26 — *Soit $F=\dfrac{X}{X^2-3X+2}\in\mathbb{R}(X)$. On a $X^2-3X+2=(X-1)(X-2)$, et $X-1$ et $X-2$ sont premiers entre eux. D'après ce qui précède, on peut donc écrire F sous la forme*

$$\frac{X}{(X-1)(X-2)} = \frac{a}{X-1} + \frac{b}{X-2}$$

où $(a,b) \in \mathbb{R}^2$ *puisque* $\deg(X-1) = \deg(X-2) = 1$.

En multipliant par $X-1$*, on obtient*

$$\frac{X}{X-2} = a + \frac{b(X-1)}{X-2},$$

puis en évaluant en 1*, on trouve* $a = -1$.

De même, en multipliant par $X-2$*, on obtient*

$$\frac{X}{X-1} = \frac{a(X-2)}{X-1} + b,$$

puis en évaluant en 2*, on trouve* $b = 2$.

D'où $F = \dfrac{-1}{X-1} + \dfrac{2}{X-2}$.

Corollaire 27
Soient $B_1, \ldots, B_n$ *des polynômes premiers entre eux deux à deux et* P *un polynôme tel que* $\deg P < \deg(B_1 \cdots B_n)$*. Alors il existe un unique* n*-uplet de polynômes* $(A_1, \ldots, A_n)$ *tel que, pour tout* $i \in [\![1,n]\!]$, $\deg A_i < \deg B_i$ *et*

$$\frac{P}{B_1 \cdots B_n} = \frac{A_1}{B_1} + \ldots + \frac{A_n}{B_n}.$$

Preuve — On procède par récurrence à l'aide de la proposition précédente et en utilisant le fait que pour tout $i \in [\![1,n]\!]$, B_i est premier avec $\prod_{\substack{j=1\ldots n \\ j\neq i}} B_j$. □

Proposition 28
Pour tout $(P,Q) \in \mathbb{K}[X]$ *et tout* $n \in \mathbb{N}^*$ *tels que* $\deg(P) < \deg(Q^n)$*, la fraction rationnelle* $\dfrac{P}{Q^n}$ *s'écrit de manière unique sous la forme*

$$\frac{P}{Q^n} = \frac{A_n}{Q^n} + \cdots + \frac{A_1}{Q}$$

avec, pour tout $i \in [\![1,n]\!]$, $\deg A_i < \deg Q$.

Preuve — Démontrons le résultat par récurrence.

• *Initialisation :* Pour $n = 1$, on a $\dfrac{P}{Q} = \dfrac{A_1}{Q}$ avec $A_1 = P$, uniquement déterminé.

• *Hérédité :* Soit $n \in \mathbb{N}^*$. Supposons le résultat vrai pour n. Soient P et Q des polynômes tels que $\deg(P) < \deg(Q^{n+1})$.
Par division euclidienne de P par Q, il existe $(\tilde{P}, A_{n+1}) \in \mathbb{K}[X]^2$ tel que $P = \tilde{P}Q + A_{n+1}$ et $\deg A_{n+1} < \deg Q$. On a donc

$$\frac{P}{Q^{n+1}} = \frac{A_{n+1}}{Q^{n+1}} + \frac{\tilde{P}}{Q^n}.$$

Par construction, $\deg \tilde{P} < \deg Q^n$ et par hypothèse de récurrence, $\dfrac{\tilde{P}}{Q^n}$ s'écrit sous la forme

$$\frac{\tilde{P}}{Q^n} = \frac{A_n}{Q^n} + \ldots + \frac{A_1}{Q},$$

avec $\deg(A_i) < \deg(Q)$.

On a donc

$$\frac{P}{Q^{n+1}} = \frac{A_{n+1}}{Q^{n+1}} + \frac{A_n}{Q^n} + \ldots + \frac{A_1}{Q},$$

et pour tout $i \in [\![1, n+1]\!]$, $\deg(A_i) < \deg(Q)$.

On vérifie que A_{n+1} est uniquement déterminé comme reste de la division euclidienne de P par Q, puis par récurrence, on obtient l'unicité de A_1, ...,A_n. □

Exemple 29 — *Soit* $F = \dfrac{2X+1}{(X-1)^2}$.

On a

$$\frac{2X+1}{(X-1)^2} = \frac{a}{X-1} + \frac{b}{(X-1)^2},$$

où $(a,b) \in \mathbb{R}^2$ *car* $\deg(X-1) = 1$. *En multipliant par* $(X-1)^2$ *puis en évaluant en* $X = 1$, *on obtient* $b = 3$

Mais, le même raisonnement ne fonctionne pas pour a car multiplier par $X-1$ *puis évaluer en* 1 *revient à diviser par* 0 *! Il faut donc s'y prendre autrement. Proposons plusieurs méthodes :*

1. *On multiplie par* X *pour obtenir*

$$\frac{X(2X+1)}{(X-1)^2} = \frac{aX}{X-1} + \frac{b}{(X-1)^2},$$

   puis on passe à la limite en $+\infty$ *pour obtenir* $2 = a + 0$, *soit* $a = 2$.
2. *On évalue en* 0 *la première relation pour obtenir* $1 = -a + b$, *donc* $a = b - 1 = 3 - 1 = 2$.
3. *On écrit*

$$\frac{a}{X-1} = \frac{2X+1}{(X-1)^2} - \frac{3}{(X-1)^2} = \frac{2X-2}{(X-1)^2} = \frac{2}{X-1}.$$

   Donc $a = 2$.

Dans tous les cas, on trouve $F = \dfrac{2}{X-1} + \dfrac{3}{(X-1)^2}$.

Méthode 30 — *Soit* $R = \dfrac{P}{Q} \in \mathbb{K}(X)$ *une fraction rationnelle sous forme irréductible. Pour déterminer la décomposition en éléments simples de* R *sur* $\mathbb{K}$,

1. *On calcule la partie entière* E *de* R *:* $R = E + \dfrac{\tilde{P}}{Q}$ *avec* $\deg(\tilde{P}) < \deg(Q)$ *en faisant la division euclidienne de* P *par* Q,
2. *On factorise* Q *en produit d'irréductibles sur* $\mathbb{K}$ *:* $Q = Q_1^{\alpha_1} \dots Q_r^{\alpha_r}$,
3. *Les polynômes* $Q_i^{\alpha_i}$ *étant premiers entre eux deux à deux, on obtient*

$$\frac{\tilde{P}}{Q} = \frac{P_1}{Q_1^{\alpha_1}} + \ldots + \frac{P_r}{Q_r^{\alpha_r}} \text{ avec } \deg(P_i) < \deg(Q_i^{\alpha_i}),$$

   et on applique la proposition précédente à chacune des fractions $\dfrac{P_i}{Q_i^{\alpha_i}}$,

4. *Il reste à déterminer les coefficients des polynômes apparaissant aux différents numérateurs.*

La décomposition obtenue est unique et est appelée la ***décomposition en éléments simples****.*

Comme nous l'avons déjà vu sur les premiers exemples, il existe de multiples façons de calculer les coefficients des polynômes des numérateurs :

- Multiplier par $(X-\lambda)^m$ puis évaluer en λ,
- Multiplier par X et passer à la limite en $+\infty$,
- Évaluer en un point,
- Mettre au même dénominateur et identifier,
- Utiliser la parité,
- ...

Traitons d'autres exemples pour illustrer tout cela.

Exemple 31 —

1. *Déterminons la décomposition en éléments simples sur* $\mathbb{R}$ *de* $F = \dfrac{X^2+3X+1}{(X-1)^2(X-2)}$.
   - *On a* $\deg(X^2+3X+1) = 2 < \deg((X-1)^2(X-2)) = 3$ *donc la partie entière est nulle.*
   - *On peut décomposer* F *sous la forme*
   $$\frac{X^2+3X+1}{(X-1)^2(X-2)} = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X-2},$$
   avec $(a,b,c) \in \mathbb{R}^3$.
   - *Déterminons* a *: En multipliant par* $(X-1)^2$ *puis en évaluant en* 1*, on obtient* $a = -5$.
   - *Déterminons* c *: En multipliant par* $X-2$ *puis en évaluant en* 2*, on obtient* $c = 11$.
   - *Déterminons* b *: En multipliant par* X*, on a*
   $$\frac{X(X^2+3X+1)}{(X-1)^2(X-2)} = \frac{aX}{(X-1)^2} + \frac{bX}{X-1} + \frac{cX}{X-2},$$
   puis en passant à la limite en $+\infty$*, on obtient* $1 = 0 + b + c$*, donc* $b = 1 - c = -10$.
   D'autres méthodes sont bien sûr possibles.
   - *D'où* $\dfrac{X^2+3X+1}{(X-1)^2(X-2)} = -\dfrac{5}{(X-1)^2} - \dfrac{10}{X-1} + \dfrac{11}{X-2}$.
2. *Déterminons la décomposition en éléments simples sur* $\mathbb{R}$ *de* $G = \dfrac{4}{(X^2-1)^2}$.
   - *Comme* $\deg(4) = 0 < \deg((X^2-1)^2) = 4$*, la partie entière de* G *est nulle.*
   - *On a* $(X^2-1)^2 = ((X-1)(X+1))^2 = (X-1)^2(X+1)^2$*, donc* G *se décompose sous la forme*
   $$\frac{4}{(X^2-1)^2} = \frac{a}{X+1} + \frac{b}{(X+1)^2} + \frac{c}{X-1} + \frac{d}{(X-1)^2},$$
   avec $(a,b,c,d) \in \mathbb{R}^4$.
   - *On remarque que* $G(-X) = G(X)$*, donc*
   $$\frac{a}{-X+1} + \frac{b}{(-X+1)^2} + \frac{c}{-X-1} + \frac{d}{(-X-1)^2} = \frac{a}{X+1} + \frac{b}{(X+1)^2} + \frac{c}{X-1} + \frac{d}{(X-1)^2},$$
   soit
   $$\frac{-c}{X+1} + \frac{d}{(X+1)^2} - \frac{a}{X-1} + \frac{b}{(X-1)^2} = \frac{a}{X+1} + \frac{b}{(X+1)^2} + \frac{c}{X-1} + \frac{d}{(X-1)^2}.$$
   Donc par unicité de la décomposition en éléments simples, $a = -c$ *et* $b = d$.
   ‘• *Déterminons* d*. En multipliant la première relation par* $(X-1)^2$ *et en évaluant en* $X = 1$*, on obtient* $d = 1$*. Donc* $b = d = 1$.
   • *Déterminons* a*. En évaluant la première relation en* $X = 0$*, on obtient* $4 = a + b - c + d$*, soit* $4 = 2a + 2d$*. Donc* $a = \dfrac{4 - 2 \times 1}{2} = 1$*. Donc* $c = -a = -1$.
   - *D'où* $G = \dfrac{1}{X+1} + \dfrac{1}{(X+1)^2} - \dfrac{1}{X-1} + \dfrac{1}{(X-1)^2}$.

La proposition suivante est utile lorsque Q est sous forme développée.

PROPOSITION 32
Soit $R = \dfrac{A}{B} \in \mathbb{K}(X)$ *sous forme irréductible et* $\lambda \in \mathbb{K}$*. Si* λ *est un pôle simple de* R*, on peut écrire* $R = \dfrac{a}{X-\lambda} + \tilde{R}$ *où* $\tilde{R} \in \mathbb{K}(X)$ *et alors* $a = \dfrac{A(\lambda)}{B'(\lambda)}$.

Preuve — Comme λ est pôle simple de R, on peut écrire $B = (X-\lambda)C$ où $C \in \mathbb{K}[X]$ et $C(\lambda) \neq 0$. La décomposition en éléments simples de R sur $\mathbb{R}$ s'écrit alors $R = \dfrac{a}{X-\lambda} + Q$ où $Q \in \mathbb{C}(X)$ n'admettant pas λ pour pôle. On a alors $\dfrac{A}{C} = (X-\lambda)R = a + (X-\lambda)Q$, donc en évaluant en λ
$$a = \frac{A(\lambda)}{C(\lambda)}.$$

D'autre part, $B' = C + (X-\lambda)C'$, donc $B'(\lambda) = C(\lambda)$. D'où

$$a = \frac{A(\lambda)}{C(\lambda)} = \frac{A(\lambda)}{B'(\lambda)}.$$

□

Exemple 33 —

- *Déterminons la décomposition en éléments simples dans* $\mathbb{C}$ *puis dans* $\mathbb{R}$ *de* $H = \dfrac{\mathrm{X}^4+1}{\mathrm{X}^3-1}$.

  • *On a* $\deg(X^4+1) > \deg(X^3-1)$*, donc pour calculer la partie entière, on effectue la division euclidienne de* X^4+1 *par* X^3-1 *:* $X^4+1 = X(X^3-1)+X+1$.

  Donc $F = X + \dfrac{X+1}{X^3-1}$.

  • *Dans* $\mathbb{C}$, $X^3-1 = (\mathrm{X}-1)(\mathrm{X}-j)\left(\mathrm{X}-j^2\right)$*, donc on a une décomposition sous la forme*

  $$\frac{X+1}{X^3-1} = \frac{a}{\mathrm{X}-1} + \frac{b}{\mathrm{X}-j} + \frac{c}{\mathrm{X}-j^2}$$

  où $(a,b,c) \in \mathbb{C}^3$.

  • *En posant* $P = X+1$ *et* $Q = X^3-1$*, on trouve*

  $$a = \frac{P(1)}{Q'(1)} = \frac{2}{3}$$

  et

  $$b = \frac{P(j)}{Q'(j)} = \frac{j+1}{3j^2} = \frac{-j^2}{3j^2} = -\frac{1}{3}.$$

  On peut calculer de même c, ou remarquer que $H = \overline{H}$*, donc*

  $$\frac{a}{X-1} + \frac{b}{X-j} + \frac{c}{X-j^2} = \frac{\bar{a}}{X-1} + \frac{\bar{c}}{X-j} + \frac{\bar{b}}{X-j^2},$$

  puisque $j^2 = \bar{j}$*. Par unicité de la décomposition en éléments simples, on a* $c = \bar{b} = -\dfrac{1}{3}$.

  • *Donc la décomposition de* H *sur* $\mathbb{C}$ *est* $H = \mathrm{X} + \dfrac{1}{3}\left(\dfrac{2}{\mathrm{X}-1} - \dfrac{1}{\mathrm{X}-j} - \dfrac{1}{\mathrm{X}-j^2}\right)$

- *Pour obtenir la décomposition sur* $\mathbb{C}$*, on peut regrouper les fractions* $\dfrac{1}{X-j}$ *et* $\dfrac{-1}{X-j^2} = \dfrac{-1}{X-\bar{j}}$ *dont les dénominateurs sont conjugués. On obtient*

$$H = X + \frac{2}{3}\frac{1}{X-1} - \frac{1}{3}\frac{X-j^2+X-j}{(X-j)(X-\bar{j})} = X + \frac{1}{3}\left(\frac{2}{X-1} - \frac{2X+1}{X^2+X+1}\right).$$

Passer par la décomposition en élément simples sur $\mathbb{C}$ pour en déduire la décomposition en éléments simples sur $\mathbb{R}$ en regroupant les fractions dont les dénominateurs sont conjugués n'est pas toujours le plus rapide. Voyons sur un dernier exemple.

Exemple 34 — *Déterminons la décomposition en éléments simples sur* $\mathbb{R}$ *de* $J = \dfrac{1}{(X-1)^2(X^2+4)}$.

• *Comme* $\deg(J) < 0$*, la partie entière est nulle.* J *admet donc une décomposition de la forme*

$$\frac{1}{(X-1)^2(X^2+4)} = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{cX+d}{X^2+4},$$

où $(a,b,c) \in \mathbb{R}^3$.

• *Déterminons a. En multipliant par* $(X-1)^2$ *puis en évaluant en* 1*, on obtient :* $a = \dfrac{1}{5}$.

• *Déterminons de c et d. Le polynôme* X^2+4 *admet* 2i *et* -2i *pour racines. En multipliant par* X^2+4 *puis en évaluant en* $2i$*, on obtient*

$$\frac{1}{(2i-1)^2} = 2ic + d.$$

Comme $\dfrac{1}{(2i-1)^2} = \dfrac{-3+4i}{25}$*, on a* $\dfrac{-3}{25} + i\dfrac{4}{25} = d + 2ic$*. Or c et d étant réels, on obtient* $c = \dfrac{2}{25}$ *et* $d = -\dfrac{3}{25}$.

• *Déterminons b. En multipliant par X puis en passant à la limite en* $+\infty$*, on obtient* $0 = b + c$*, donc* $b = -c = -\dfrac{2}{25}$.

• *D'où* $J = \dfrac{1}{5(X-1)^2} - \dfrac{2}{25(X-1)} + \dfrac{2X-3}{25\,(X^2+4)}$.

Chapitre 4 Algèbre

Dans ce chapitre, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$.

La structure d'algèbre est la structure la plus complète et la plus naturelle dans laquelle on puisse calculer. Une algèbre est à la fois un espace vectoriel et un anneau, avec une condition de compatibilité entre la multiplication de l'anneau et l'opération du corps $\mathbb{K}$ sur l'espace vectoriel.

4.1 Définition

Définition 1
On appelle ***algèbre*** *sur le corps $\mathbb{K}$ (en abrégé, $\mathbb{K}$-algèbre), tout quadruplet $(A, +, \times, \cdot)$, où A est un ensemble, $+$ et $\times$ des lois internes sur A, $\cdot$ une opération de l'ensemble $\mathbb{K}$ sur A, tel que :*

1. *$(A, +, \times)$ soit un anneau.*
2. *$(A, +, \cdot)$ soit un espace vectoriel sur $\mathbb{K}$.*
3. *Pour tout $\alpha \in \mathbb{K}$, tout x et tout y éléments de A*

$$(\alpha \cdot x) \times y = x \times (\alpha \cdot y) = \alpha \cdot (x \times y)$$

Si de plus la loi $\times$ est commutative, on dit que l'algèbre est commutative.

Lorsque pour une algèbre $(A, +, \times, \cdot)$, l'espace vectoriel $(A, +, \cdot)$ est de dimension finie n, on dit que l'algèbre est de dimension finie n.

Remarque 2 — *La notation $(\alpha \cdot x) \times y$ est souvent remplacée par αxy. On place en général $\alpha \in \mathbb{K}$ devant les éléments de A.*

Exemples 3

1. *$(\mathbb{K}, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre commutative,*
2. *$(\mathbb{K}[X], +, \times, \cdot)$ est une $\mathbb{K}$-algèbre commutative,*
3. *$(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre non commutative, en général non commutative,*
4. *Pour E un $\mathbb{K}$-espace vectoriel, $(\mathcal{L}(E), +, \circ, \cdot)$ est une $\mathbb{K}$-algèbre, en général non commutative,*
5. *Soit D un ensemble. $(\mathcal{F}(D, \mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.*
6. *Plus généralement, $(\mathcal{F}(D, E), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre, où E est une $\mathbb{K}$-algèbre. En particulier, pour l'ensemble des suites, $(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.*
7. *$(\mathbb{K}(X), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.*

4.2 Sous-algèbre

Comme pour les groupes, anneaux et espaces vectoriels, on définit une notion de sous-algèbre.

Définition 4
Soit $(A, +, \times, \cdot)$ une $\mathbb{K}$-algèbre. Une sous-algèbre B est une partie $B \subset A$ telle que

1. *$(B, +, \times)$ est un sous-anneau de $(A, +, \times)$,*
2. *$(B, +, \cdot)$ est un sous-espace vectoriel de $(A, +, \cdot)$.*

Proposition 5
Si B est une sous-algèbre de $(A, +, \times, \cdot)$, alors $(B, +, \times, \cdot)$ est une algèbre.

Preuve —Puisque B est une sous-algèbre, c'est un sous-anneau et un sous-espace vectoriel, donc un anneau et un espace vectoriel. De plus, le troisième point de la définition est vérifié puisqu'il l'est sur A et donc sur B. □

Donnons une caractérisation des sous-algèbres.

PROPOSITION 6
Soit $(A, +, \times, \cdot)$ une $\mathbb{K}$-algèbre. Alors B est une sous-algèbre de $(A, +, \times, \cdot)$ si et seulement si

1. $1_A \in B$,
2. *B est stable par combinaison linéaire : pour tout $(x, y) \in B^2$ et tout $\lambda \in \mathbb{K}$,*
$$\lambda x + y \in B.$$
3. *B est stable par $\times$: pour tout $(x, y) \in B^2$,*
$$x \times y \in B.$$

Preuve —

• Supposons que B est une sous-algèbre de $(A, +, \times, \cdot)$. Alors B est un sous-anneau donc les points 1 et 3 sont vérifiés, et B est un sous-espace vectoriel donc le point 2 est vérifié.

• Supposons que B vérifie les trois points.

B est un sous-anneau de $(A, +, \times)$ si et seulement si

a. $1_A \in B$,
b. B est stable par addition,
c. B est stable par passage à l'opposé,
d. B est stable par $\times$.

D'après le point 2, les points b et c sont vérifiés, le point 1 correspond à a et le point 3 à d.

Donc B est un sous-anneau de $(A, +, \times)$.

B est un sous-espace vectoriel de $(A, +\cdot)$ si et seulement si

a'. $0_A \in B$,
b'. B est stable par combinaison linéaire.

Le point 2 assure b', et comme $1_A \in B$, $1_A - 1_A = 0_A \in B$ par stabilité par combinaison linéaire.

Donc B est un sous-espace vectoriel de $(A, +, \cdot)$.

Finalement, B est une sous-algèbre de $(A, +, \times, \cdot)$. □

Pour montrer qu'un quadruplet est une algèbre, on montre en général que c'est une sous-algèbre d'une algèbre connue.

EXEMPLES 7

- *$\mathbb{R}$ est une sous-algèbre de la $\mathbb{R}$-algèbre $\mathbb{C}$.*
- *L'ensemble $\mathcal{T}_n(\mathbb{K})$ des matrices triangulaires supérieures d'ordre n à coefficients dans $\mathbb{K}$ est une sous-algèbre de l'algèbre $\mathcal{M}_n(\mathbb{K})$.*
- *L'ensemble $\mathcal{C}(\mathbb{R})$ des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ est une sous-algèbre de l'algèbre $\mathcal{F}(\mathbb{R}, \mathbb{R})$.*

4.3 Morphismes d'algèbres

DÉFINITION 8
Soit $(A, +, \times, .)$ et $(B, +, \times, .)$ deux $\mathbb{K}$-algèbres. Un morphisme d'algèbres $\varphi : A \to B$ est une application vérifiant

1. *$\varphi(1_A) = 1_B$;*
2. *Pour tout $(x, y) \in A^2$, $\varphi(x \times y) = \varphi(x) \times \varphi(y)$*
3. *Pour tout $(x, y) \in A^2$ et tout $(\lambda, \mu) \in \mathbb{K}^2$, $\varphi(\lambda \cdot x + \mu \cdot y) = \lambda \cdot \varphi(x) + \mu \cdot \varphi(y)$.*

Remarque 9 — *Un morphisme d'algèbres $\varphi : A \longrightarrow B$ est donc un morphisme d'anneaux (de l'anneau $(A, +, \times)$ dans $(B, +, \times)$ et une application linéaire de l'espace vectoriel $(A, +, \cdot)$ dans l'espace vectoriel $(B, +, \cdot)$.*

Définition 10
Un morphisme d'algèbres bijectif est appelé un ***isomorphisme d'algèbres*** *et un isomorphisme d'une algèbre sur elle-même est appelée un* ***automorphisme d'algèbre****.*

Exemples 11

- *Dans la $\mathbb{R}$-algèbre $\mathbb{C}$, la conjugaison $z \longmapsto \bar{z}$ est un automorphisme d'algèbres.*
- *Soit E un $\mathbb{K}$-espace vectoriel de dimension n dont $\mathcal{B}$ est une base. L'application*

$$\mathcal{L}(E) \longrightarrow \mathcal{M}_n(\mathbb{K}) \; ; \; u \longmapsto \mathrm{mat}_{\mathcal{B}} u$$

  est un isomorphisme d'algèbres.
- *L'application*

$$\mathbb{K}[X] \longrightarrow \mathcal{F}(\mathbb{K}, \mathbb{K}) \; ; \; P \longmapsto P(x)$$

  qui à un polynôme associe sa fonction polynomiale est un morphisme d'algèbres.

Proposition 12
Soif φ un morphisme de l'algèbre $(A, +, \times, \cdot)$ dans l'algèbre $(B, +, \times, \cdot)$.

- *Si A' est une sous-algèbre de $(A, +, \times, \cdot)$ alors $\varphi(A')$ est une sous-algèbre de $(B, +, \times, \cdot)$.*
- *Si B' est une sous-algèbre de $(B, +, \times, \cdot)$ alors $\varphi^{-1}(B')$ est une sous-algèbre de $(A, +, \times, \cdot)$.*