Université de Bordeaux
Licence de Sciences, Technologies, Santé
Mentions Mathématiques et Informatique
4TPM201U Algèbre Linéaire 1

# Algèbre Linéaire 1

**Christine Bachoc**

**Année 2019-2020, Série B**

# Table des matières

# Introduction

*Avertissement : ces notes de cours ne forment pas un cours complet d'algèbre linéaire et ne sont pas forcément complètement fidèles au cours qui sera donné ce semestre. En particulier elles ne doivent pas dispenser les étudiants d'assister au cours ! L'auteur souhaite qu'elles constituent une aide utile aux étudiants qui découvriront ce semestre les cours donnés en amphi et devront notamment apprendre à y prendre des notes.*

L'objectif principal de ce cours est l'étude des espaces vectoriels définis sur $\mathbb{R}$ ou $\mathbb{C}$. C'est donc le cadre que nous adopterons et nous utiliserons dans tout le cours la notation commune $\mathbb{K}$ pour désigner l'un de ces deux ensembles de nombres.

Cela étant dit, il se trouve que tout ce qui suit est valable pour des ensemble de 'nombres' plus généraux qu'on appelle *des corps*. Les corps seront étudiés pour eux-mêmes dans les cours d'Algèbre de L2 et L3 du cursus de Mathématiques ; pour le lecteur curieux, en voici la définition. Il s'agit d'un ensemble muni d'une addition et d'une multiplication vérifiant les rêgles de calcul suivantes :

- L'addition est :
  - commutative : $\lambda + \mu = \mu + \lambda$
  - associative : $(\lambda + \mu) + \nu = \lambda + (\mu + \nu)$
  - possède un zéro i.e. un élément noté 0 vérifiant $\lambda + 0 = \lambda$
  - tout élément $\lambda$ possède un opposé noté $-\lambda$ vérifiant $\lambda + (-\lambda) = 0$
- La multiplication est :
  - commutative : $\lambda\mu = \mu\lambda$
  - associative : $(\lambda\mu)\nu = \lambda(\mu\nu)$
  - possède un élément noté 1 vérifiant $\lambda 1 = \lambda$
  - tout élément $\lambda \neq 0$ possède un inverse noté $\lambda^{-1}$ vérifiant $\lambda(\lambda^{-1}) = 1$
- La multiplication est distributive sur l'addition :
  - $\lambda(\mu + \nu) = \lambda\mu + \lambda\nu$

Les ensembles $\mathbb{Q}$ (nombres rationnels), $\mathbb{R}$ (nombres réels) et $\mathbb{C}$ (nombres complexes) sont des corps connus et étudiés au niveau L1. D'autres exemples de corps seront rencontrés au cours de la Licence, notamment l'ensemble $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo $p$ où $p$ est un nombre premier, ou encore le corps des fractions rationnelles.

# Chapitre 1

# Résolution de systèmes linéaires

Ce chapitre est essentiellement un chapitre de révisions puisque les systèmes linéaires ont été étudiés dans l'UE de S1 *Bases de Mathématiques pour les Sciences*.

## 1.1 Systèmes linéaires

Un système linéaire $(S)$ sur $\mathbb{K}$ à $n$ inconnues (appelées aussi variables) $x_1, x_2, \ldots, x_n$ et $k$ équations $(E_1), \ldots, (E_k)$ se présente sous la forme :

$$(S) \quad \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \quad (E_1) \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \quad (E_2) \\ & \vdots \\ a_{k,1}x_1 + a_{k,2}x_2 + \cdots + a_{k,n}x_n &= b_k \quad (E_k) \end{cases}$$

On note $\mathcal{S}$ l'ensemble de ses solutions, c'est-à-dire

$$\mathcal{S} = \big\{(x_1, x_2, \ldots, x_n) \in \mathbb{K}^n \text{ tels que } (x_1, \ldots, x_n) \text{ vérifie } (E_1), \ldots, (E_k)\big\}.$$

Notre but dans ce chapitre est de décrire un *algorithme* permettant de déterminer $\mathcal{S}$ exactement et en toutes circonstances. C'est *l'algorithme du pivot de Gauss*. Tout d'abord introduisons un peu de vocabulaire.

**Définition 1.1.1.**

1. On dit que le système $(S)$ est *homogène* si $b_1 = b_2 = \cdots = b_k = 0$.
2. Deux systèmes linéaires sont dits *équivalents* s'ils ont le même ensemble de solutions. On note alors
$$(S) \iff (S')$$

**Exemple 1.1.2.** Voici un système linéaire à trois inconnues et trois équations ($n = k = 3$). Un système de ce type est dit *triangulaire* pour des raisons évidentes.

$$(S_1) \quad \begin{cases} x + 2y + 3z = 0 \\ -y + 2z = 1 \\ 2z = 5 \end{cases}$$

Il se résout facilement, de bas en haut, en calculant successivement $z$, puis $y$, puis $x$. On trouve

$$\mathcal{S} = \big\{(-31/2, 4, 5/2)\big\}.$$

## 1.2 Système linéaire échelonné

**Définition 1.2.1.** Un système linéaire $(S)$ est dit *échelonné* s'il est de la forme :

$$\left\{\begin{array}{lllllllll} a_{1,j_1}x_{j_1} & +\cdots+ & a_{1,j_2}x_{j_2} & +\cdots+ & a_{1,j_k}x_{j_k} & +\cdots+a_{1,n}x_n & = & b_1 \\ & & a_{2,j_2}x_{j_2} & +\cdots+ & a_{2,j_k}x_{j_k} & +\cdots+a_{2,n}x_n & = & b_2 \\ & & & & \vdots & & \vdots & \\ & & & & a_{k,j_k}x_{j_k} & +\cdots+a_{k,n}x_n & = & b_k \end{array}\right.$$

où on a $1 \leq j_1 < j_2 < \cdots < j_k \leq n$, et où les coefficients $a_{1,j_1}, a_{2,j_2}, \ldots, a_{k,j_k}$ sont non nuls. Remarquons que dans ce cas on a $k \leq n$. Les variables $x_{j_1}, x_{j_2}, \ldots, x_{j_k}$ s'appellent les *variables pivot* et il y en a exactement autant que d'équations. Les autres variables s'appellent les *variables auxiliaires*.

Pour résoudre un tel système linéaire, on se ramène à un système triangulaire en passant dans toutes les équations les variables auxiliaires à droite du signe "=". Ensuite on exprime successivement de bas en haut les variables pivot $x_{j_k}$, puis $x_{j_{k-1}}$, et ainsi de suite, jusqu'à $x_{j_1}$, en fonction des variables auxiliaires, c'est-à-dire des $x_i$ pour $i \notin \{j_1, \ldots, j_k\}$. On obtient un ensemble de solutions paramétrées par les variables auxiliaires $x_i$ pour $i \notin \{j_1, \ldots, j_k\}$. Exemple numérique :

$$(S_2) \quad \left\{\begin{array}{lllllllll} x_1 & + & x_2 & + & x_3 & + & x_4 & = & 0 \\ & & x_2 & + & x_3 & - & 6x_4 & = & 0 \\ & & & & & & 3x_4 & = & 1 \end{array}\right.$$

On a

$$(S_2) \iff \left\{\begin{array}{lllllll} x_1 & + & x_2 & + & x_4 & = & -x_3 \\ & & x_2 & - & 6x_4 & = & -x_3 \\ & & & & 3x_4 & = & 1 \end{array}\right.$$

$$\iff \left\{\begin{array}{lll} x_1 & = & -x_2 - x_3 - x_4 \\ x_2 & = & -x_3 + 6x_4 \\ x_4 & = & 1/3 \end{array}\right. \iff \left\{\begin{array}{lll} x_1 & = & -7/3 \\ x_2 & = & -x_3 + 2 \\ x_4 & = & 1/3 \end{array}\right.$$

À chaque $x_3 \in \mathbb{K}$ correspond une solution du système. On obtient

$$\mathcal{S} = \big\{(-7/3, -x_3 + 2, x_3, 1/3) \mid x_3 \in \mathbb{K}\big\}$$

ou encore

$$\mathcal{S} = \big\{(-7/3, 1, 0, 1/3) + x_3(0, -1, 1, 0) \mid x_3 \in \mathbb{K}\big\}.$$

## 1.3 L'algorithme du pivot de Gauss

On va décrire maintenant les opérations que l'on peut exécuter sur un système sans changer son ensemble de solutions, c'est-à-dire en le transformant en un système équivalent.

**Définition 1.3.1.** On appelle *opérations élémentaires sur le système linéaire* $(S)$ les opérations suivantes :

(1) Échange de deux équations.

(2) Remplacement de l'équation $(E_i)$ par $\lambda(E_i)$ pour $\lambda \in \mathbb{K}$, $\lambda \neq 0$.

(3) Remplacement de l'équation $(E_i)$ par $(E_i) + \mu(E_j)$ pour $j \neq i$ et $\mu \in \mathbb{K}$.

**Remarque 1.3.2.** Il faut bien sûr exécuter ces opérations sur les deux membres des équations, i.e. à gauche comme à droite du signe "=".

**Proposition 1.3.3.** On obtient un système linéaire équivalent en appliquant à $(S)$ une opération élémentaire, ou une succession de telles opérations.

*Démonstration.* Il est clair que les opérations (1) et (2) ne changent pas l'ensemble des solutions $\mathcal{S}$. Vérifions-le pour (3) : soit $j \neq i$. Il est clair que si $(E_i)$ et $(E_j)$ sont vérifiées alors $(E_i)+\mu(E_j)$ l'est aussi. Réciproquement, supposons avoir remplacé $(E_i)$ par $(E_i) + \mu(E_j)$. L'équation $(E_j)$ elle n'a pas changé. On remarque que $(E_i) = ((E_i) + \mu(E_j)) - \mu(E_j)$ donc, si $(E_i) + \mu(E_j)$ et $(E_j)$ sont vérifiées alors $(E_i)$ l'est aussi. □

La *méthode du pivot de Gauss* est un algorithme qui, par une succession d'opérations élémentaires, permet de ramener la résolution d'un système linéaire à celle d'un système échelonné.

**Description informelle de l'algorithme :** On procède variable par variable, en travaillant successivement sur les colonnes du système.

Soit $x_{j_1}$ la première variable qui apparait dans le système. Supposons pour simplifier les notations que $j_1 = 1$. On cherche de haut en bas la première équation qui contienne un terme en $x_1$, et si ce n'est pas la première, on l'échange avec $(E_1)$. Puis, on divise $(E_1)$ par le coefficient de $x_1$. Ensuite, on élimine les termes en $x_1$ dans les équations $(E_2), \ldots, (E_k)$ en remplaçant $(E_i)$ par $(E_i) - a_{i,1}(E_1)$. On ne modifiera plus $(E_1)$.

Ensuite on recommence le procédé avec les équations $(E_2), \ldots (E_k)$ : on passe à la première variable présente dans $(E_2), \ldots (E_k)$, soit $x_{j_2}$. On a $j_2 > j_1$. On cherche parmi $(E_2), \ldots (E_k)$, de haut en bas, la première équation qui contienne un terme en $x_{j_2}$, et on l'échange avec $(E_2)$. On divise $(E_2)$ par $a_{2,j_2}$, puis, comme avec $x_1$, on élimine la variable $x_{j_2}$ des équations $(E_3), \ldots (E_k)$. On procède ainsi jusqu'à la dernière équations.

Au cours de l'algorithme, on a pu transformer une équation en une équation du type "$0 = b$". Si $b \neq 0$, il n'y a pas de solutions, et on peut conclure que $\mathcal{S} = \emptyset$. Si $b = 0$, on enlève cette équation du système.

On a démontré le résultat suivant :

**Proposition 1.3.4.** L'algorithme du pivot de Gauss conduit soit à une équation sans solutions du type "$0 = b$" avec $b \neq 0$ (et dans ce cas on peut conclure que le système initial n'a pas de solutions) soit à un système linéaire équivalent, échelonné, et dont le nombre d'équations est inférieur ou égal à celui du système initial.

*Démonstration.* En effet, la seule chose qui peut arriver c'est que l'on élimine une équation du type "$0 = 0$".

□

**Exemple numérique :**

$$(S_3) \quad \begin{cases} & & & & x_3 & + & x_4 & = & 4 \\ x_1 & - & 3x_2 & + & x_3 & - & x_4 & = & 0 \\ -8x_1 & + & 24x_2 & - & 4x_3 & + & 16x_4 & = & 8 \end{cases}$$

$$
(S_3) \iff \left\{ \begin{array}{rcrcrcrcll} x_1 & - & 3x_2 & + & x_3 & - & x_4 & = & 0 & (E_1) \leftrightarrow (E_2) \\ & & & & x_3 & + & x_4 & = & 4 & \\ -8x_1 & + & 24x_2 & - & 4x_3 & + & 16x_4 & = & 8 & \end{array} \right.
$$

$$
\iff \left\{ \begin{array}{rcrcrcrcll} x_1 & - & 3x_2 & + & x_3 & - & x_4 & = & 0 & \\ & & & & x_3 & + & x_4 & = & 4 & \\ & & & & 4x_3 & + & 8x_4 & = & 8 & (E_3) \leftarrow (E_3) + 8(E_1) \end{array} \right.
$$

$$
\iff \left\{ \begin{array}{rcrcrcrcll} x_1 & - & 3x_2 & + & x_3 & - & x_4 & = & 0 & \\ & & & & x_3 & + & x_4 & = & 4 & \\ & & & & & & 4x_4 & = & -8 & (E_3) \leftarrow (E_3) - 4(E_2) \end{array} \right.
$$

On a obtenu un système linéaire échelonné, que l'on résout suivant la méthode du paragraphe 1.2 :

$$
(S_3) \iff \left\{ \begin{array}{rcl} x_1 & = & 3x_2 - x_3 + x_4 = 3x_2 - 8 \\ x_3 & = & 6 \\ x_4 & = & -2 \end{array} \right.
$$

On obtient

$$
\begin{aligned} \mathcal{S} &= \big\{(3x_2 - 8, x_2, 6, -2) \mid x_2 \in \mathbb{K}\big\} \\ &= \big\{(-8, 0, 6, -2) + x_2(3, 1, 0, 0) \mid x_2 \in \mathbb{K}\big\} \end{aligned}
$$

## 1.4 Conclusions

En plus de l'aspect calculatoire, on retiendra de ce chapitre le résultat théorique suivant, qui nous sera utile par la suite :

**Proposition 1.4.1.** Pour qu'un système d'équations linéaires à $n$ inconnues et $k$ équations possède une solution unique, il est *nécessaire* d'avoir $k \geq n$ i.e. au moins autant d'équations que d'inconnues.

*Démonstration.* Soit $(S)$ un système linéaire ayant une solution unique, à $n$ inconnues et $k$ équations. D'après la proposition 1.3.4, il est équivalent à un système $(S')$ échelonné, à $n$ inconnues et $k' \leq k$ équations. Comme il y a autant de variables pivot que d'équations, si $k' < n$, il y a des variables qui ne sont pas des variables pivot, c'est-à-dire des variables auxiliaires, qui vont paramétrer les solutions. Il y a donc une infinité de solutions. Si $(S)$ a une solution unique, $(S')$ aussi, et donc $k' \geq n$ et à fortiori $k \geq n$. □

**Remarque 1.4.2.** La condition $k \geq n$ (au moins autant d'équations que d'inconnues) est nécessaire mais bien évidemment pas suffisante pour avoir unicité de la solution, comme le montrent les exemples stupides suivants :

$$
\left\{ \begin{array}{rl} x + y & = 0 \\ -x - y & = 0 \end{array} \right. \qquad \text{(infinité de solutions)}
$$

$$
\left\{ \begin{array}{rl} x + y & = 0 \\ x + y & = 1 \end{array} \right. \qquad \text{(aucune solution)}
$$

# Chapitre 2

# L'espace vectoriel $\mathbb{K}^n$

## 2.1 Introduction

On apprend au lycée comment repérer un point $M$ dans le plan par deux coordonnées $(x, y)$ dans un repère $(O, \vec{i}, \vec{j})$. Cela revient à identifier le vecteur $\overrightarrow{OM} = x\vec{i}+y\vec{j}$ avec l'élément $(x, y) \in \mathbb{R}^2$. Dans l'espace, on a besoin de trois coordonnées $(x, y, z) \in \mathbb{R}^3$. Nous allons généraliser cette approche aux éléments de $\mathbb{R}^n$ et de $\mathbb{C}^n$, en se détachant de notre vision intuitive de la géométrie. Dans ce chapitre, un vecteur sera simplement un élément de $\mathbb{K}^n$, pour $n \geq 1$.

## 2.2 Définition de l'espace vectoriel $\mathbb{K}^n$

**Notation.** Un élément de $\mathbb{K}^n$ sera noté $v = (v_1, v_2, \ldots, v_n)$. On dit que $v$ est *un vecteur* et les $v_i \in \mathbb{K}$ sont *ses coordonnées*.

**Définition 2.2.1.** On considère deux opérations dans $\mathbb{K}^n$ :

- L'addition de deux vecteurs $u = (u_1, u_2, \ldots, u_n)$ et $v = (v_1, v_2, \ldots, v_n)$ est

$$u + v = (u_1 + v_1, \ldots, u_n + v_n).$$

- La multiplication d'un vecteur $u = (u_1, u_2, \ldots, u_n)$ par un scalaire $\lambda \in \mathbb{K}$ est

$$\lambda u = (\lambda u_1, \ldots, \lambda u_n).$$

**Notation.** On note $\mathbf{0} = (0, 0, \ldots, 0)$ et on l'appelle le *vecteur nul*. Si $u = (u_1, \ldots, u_n)$, on note $-u = (-u_1, \ldots, -u_n)$ et on l'appelle *l'opposé de* $u$.

**Proposition 2.2.2.** Les opérations d'addition et de multiplication par un scalaire dans $\mathbb{K}^n$ ont les propriétés suivantes : pour tout $u, v, w \in \mathbb{K}^n$ et tout $\lambda, \mu \in \mathbb{K}$,

1. $u + v = v + u$ (commutativité de l'addition)
2. $(u + v) + w = u + (v + w)$ (associativité de l'addition)
3. $u + \mathbf{0} = u$
4. $u + (-u) = \mathbf{0}$
5. $1\,u = u$, $0\,u = \mathbf{0}$.
6. $\lambda(\mu u) = (\lambda\mu)u$

7. $(\lambda + \mu)u = \lambda u + \mu u$
8. $\lambda(u + v) = \lambda u + \lambda v$

**Définition 2.2.3.** On dit que $u \in \mathbb{K}^n$ est une *combinaison linéaire* des vecteurs $v_1, v_2, \ldots, v_k$ s'il existe des scalaires $\lambda_1, \ldots, \lambda_k$ tels que

$$u = \lambda_1 v_1 + \cdots + \lambda_k v_k.$$

Les nombres $\lambda_1, \ldots, \lambda_k$ s'appellent les coefficients de la combinaison linéaire.

**Exemple 2.2.4.** Dans $\mathbb{R}^3$, est-ce que $(1, 1, 0)$ est combinaison linéaire de $(1, 2, 0)$ et de $(0, 1, 0)$ ? On cherche s'il existe $\lambda_1$ et $\lambda_2$ tels que $(1, 1, 0) = \lambda_1(1, 2, 0) + \lambda_2(0, 1, 0)$. On a

$$\begin{aligned}(1,1,0) = \lambda_1(1,2,0) + \lambda_2(0,1,0) &\iff (1,1,0) = (\lambda_1, 2\lambda_1 + \lambda_2, 0)\\ &\iff \begin{cases} 1 &= \lambda_1 \\ 1 &= 2\lambda_1 + \lambda_2 \end{cases}\\ &\iff \begin{cases} \lambda_1 &= 1 \\ \lambda_2 &= -1 \end{cases}\end{aligned}$$

On a trouvé la relation $(1, 1, 0) = (1, 2, 0) - (0, 1, 0)$. On remarque que, pour calculer les coefficients $\lambda_1, \lambda_2$, on a été amenés à résoudre un système linéaire.

## 2.3 Sous-espaces vectoriels de $\mathbb{K}^n$

**Définition 2.3.1.** Soit $F \subset \mathbb{K}^n$. On dit que $F$ est un *sous-espace vectoriel de* $\mathbb{K}^n$ si $F$ vérifie les propriétés suivantes :

1. $F$ est non vide
2. Pour tout $u \in F$, $v \in F$, $u + v \in F$.
3. Pour tout $u \in F$, $\lambda \in \mathbb{K}$, $\lambda u \in F$.

**Exemple 2.3.2.** $\{\mathbf{0}\}$ et $\mathbb{K}^n$ sont des sous-espaces vectoriels de $\mathbb{K}^n$.

**Remarque 2.3.3.** Il est important de remarquer qu'un sous-espace vectoriel contient toujours $\mathbf{0}$. En effet, si $F$ est un sous-espace vectoriel de $\mathbb{K}^n$ alors il contient au moins un élément $u$ ; mais alors il contient aussi $0u = \mathbf{0}$. Par conséquent, si $F$ est un ensemble candidat à être un sous-espace vectoriel, pour démontrer qu'il est non vide le mieux la plupart du temps est de montrer qu'il contient $\mathbf{0}$.

Il y a deux exemples très importants de sous-espaces vectoriels de $\mathbb{K}^n$, que l'on va voir maintenant.

## 2.4 Premier Exemple

Le premier exemple de sous-espace vectoriel de $\mathbb{K}^n$ est l'ensemble des solutions d'un système d'équations linéaires homogène.

**Proposition 2.4.1.** L'ensemble des solutions d'un système d'équations linéaires homogène à $k$ équations et $n$ inconnues est un sous-espace vectoriel de $\mathbb{K}^n$.

*Démonstration.* Soit $\mathcal{S}$ l'ensemble des solutions du système linéaire homogène $(S)$ :

$$(S) \quad \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= 0 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= 0 \\ & \vdots \\ a_{k,1}x_1 + a_{k,2}x_2 + \cdots + a_{k,n}x_n &= 0 \end{cases}$$

On remarque d'abord que $\mathbf{0} \in \mathcal{S}$, donc cet ensemble n'est pas vide. Soit $u \in \mathcal{S}$ et $v \in \mathcal{S}$, on doit vérifier que $u + v \in \mathcal{S}$, soit que, pour tout $1 \leq i \leq k$,

$$a_{i,1}(u+v)_1 + a_{i,2}(u+v)_2 + \cdots + a_{i,n}(u+v)_n = 0.$$

On a, avec $w = u + v$ :

$$\begin{aligned} a_{i,1}w_1 + a_{i,2}w_2 + \cdots + a_{i,n}w_n &= a_{i,1}(u_1+v_1) + a_{i,2}(u_2+v_2) + \cdots + a_{i,n}(u_n+v_n) \\ &= a_{i,1}u_1 + a_{i,1}v_1 + a_{i,2}u_2 + a_{i,2}v_2 + \cdots + a_{i,n}u_n + a_{i,n}v_n \\ &= (a_{i,1}u_1 + a_{i,2}u_2 + \cdots + a_{i,n}u_n) + (a_{i,1}v_1 + a_{i,2}v_2 + \cdots + a_{i,n}v_n) \\ &= \underbrace{(a_{i,1}u_1 + a_{i,2}u_2 + \cdots + a_{i,n}u_n)}_{=0} + \underbrace{(a_{i,1}v_1 + a_{i,2}v_2 + \cdots + a_{i,n}v_n)}_{=0} = 0. \end{aligned}$$

On doit vérifier également que $\lambda u \in \mathcal{S}$ :

$$\begin{aligned} a_{i,1}(\lambda u)_1 + a_{i,2}(\lambda u)_2 + \cdots + a_{i,n}(\lambda u)_n &= a_{i,1}(\lambda u_1) + a_{i,2}(\lambda u_2) + \cdots + a_{i,n}(\lambda u_n) \\ &= \lambda(a_{i,1}u_1 + a_{i,2}u_2 + \cdots + a_{i,n}u_n) \\ &= \lambda \underbrace{(a_{i,1}u_1 + a_{i,2}u_2 + \cdots + a_{i,n}u_n)}_{=0} = 0. \end{aligned}$$

□

**Exercice.** Montrez que, si le système linéaire n'est pas homogène, l'ensemble de ses solutions n'est pas un sous-espace vectoriel.

## 2.5 Deuxième Exemple

Le deuxième exemple de sous-espace vectoriel est construit à partir d'un ensemble fini de vecteurs $v_1, \ldots, v_k$ en prenant toutes leurs combinaisons linéaires.

**Définition et Proposition 2.5.1.** Soit $v_1, v_2, \ldots, v_k$ des vecteurs de $\mathbb{K}^n$. On note $\mathrm{Vect}(v_1, \ldots, v_k)$ l'ensemble des combinaisons linéaires de $v_1, \ldots, v_k$ :

$$\mathrm{Vect}(v_1, \ldots, v_k) = \{u \in \mathbb{K}^n \mid \exists (\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^n \mid u = \lambda_1 v_1 + \cdots + \lambda_k v_k\}$$

Alors $\mathrm{Vect}(v_1, \ldots, v_k)$ est un sous-espace vectoriel de $\mathbb{K}^n$.

*Démonstration.* Posons $F = \text{Vect}(v_1, \ldots, v_k)$. On remarque d'abord que $\mathbf{0} = 0\,v_1 + \cdots + 0\,v_k \in F$ donc $F$ est non vide. Soit $u \in F$, $w \in F$, $\lambda \in \mathbb{K}$. Il existe $(\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^n$ tels que $u = \lambda_1 v_1 + \cdots + \lambda_k v_k$ et il existe $(\mu_1, \ldots, \mu_k) \in \mathbb{K}^n$ tels que $u = \mu_1 v_1 + \cdots + \mu_k v_k$. Alors,

$$\begin{aligned} u + v &= (\lambda_1 v_1 + \cdots + \lambda_k v_k) + (\mu_1 v_1 + \cdots + \mu_k v_k) \\ &= (\lambda_1 + \mu_1) v_1 + \cdots + (\lambda_k + \mu_k) v_k \in F. \end{aligned}$$

On a aussi : $\lambda u = \lambda(\lambda_1 v_1 + \cdots + \lambda_k v_k) = (\lambda\lambda_1) v_1 + \cdots + (\lambda\lambda_k) v_k \in F$. Donc $F$ est bien un sous-espace vectoriel de $\mathbb{K}^n$. □

## 2.6 Somme et intersection de sous-espaces vectoriels

Dans ce paragraphe nous allons décrire deux façons de construire un nouveau sous-espace vectoriel à partir de deux sous-espaces vectoriels.

**Proposition 2.6.1.** Si $F$ et $G$ sont deux sous-espaces vectoriels de $\mathbb{K}^n$, alors leur intersection $F \cap G$ est aussi un sous-espace vectoriel de $\mathbb{K}^n$.

*Démonstration.* Posons $V = F \cap G$. On a vu que $\mathbf{0} \in F$ et $\mathbf{0} \in G$ donc on a $\mathbf{0} \in V$ et celui-ci est non vide. Soit $u$ et $v$ deux éléments de $V$. En particulier, $u$ et $v$ appartiennent à $F$, donc, puisque $F$ est un sous-espace vectoriel de $\mathbb{K}^n$, $u + v \in F$. Par le même raisonnement, on montre que $u + v \in G$. On a donc que $u + v \in F \cap G = V$. De la même façon, on montre que, si $\lambda \in \mathbb{K}$ et $u \in V$, alors $\lambda u \in V$. □

**Remarque 2.6.2.** Attention, la réunion de deux sous-espaces vectoriels n'est pas en général un sous-espace vectoriel. La bonne notion est celle de *somme de deux sous-espaces vectoriels.*

**Définition et Proposition 2.6.3.** Si $F$ et $G$ sont deux sous-espaces vectoriels de $\mathbb{K}^n$, on note $F + G$ et on appelle *somme de $F$ et $G$* l'ensemble

$$F + G = \{u + v \text{ tels que } u \in F \text{ et } v \in G\}.$$

Alors $F + G$ est un sous-espace vectoriel de $\mathbb{K}^n$.

*Démonstration.* Tout d'abord, $F + G$ contient $\mathbf{0} = \mathbf{0} + \mathbf{0}$ donc il est non vide. Ensuite, on vérifie qu'il est stable par addition : en effet, si $u, u' \in F$ et $v, v' \in G$, $(u + v) + (u' + v') = (u + u') + (v + v') \in F + G$. L'ensemble $F + G$ est aussi stable par multiplication par les scalaires car $\lambda(u + v) = \lambda u + \lambda v \in F + G$. □

**Remarque 2.6.4.** Remarquons que $F + G$ contient $F$ et $G$. En effet, si $u \in F$, on peut écrire $u = u + \mathbf{0}$ donc $u \in F + G$. On peut démontrer que $F + G$ est *le plus petit sous-espace vectoriel de $\mathbb{K}^n$ contenant $F$ et $G$.*

# Chapitre 3

# Espaces vectoriels abstraits

Nous commençons par généraliser la notion d'espace vectoriel mise en évidence sur $\mathbb{K}^n$ au chapitre précédent dans un cadre abstrait. Lorsqu'un ensemble d'objets mathématiques entre dans ce cadre, l'idée est d'oublier la 'nature' de ses éléments pour ne retenir que les propriétés des opérations que l'on peut effectuer sur ces éléments.

## 3.1 Définitions

**Définition 3.1.1.** Soit $E$ un ensemble non vide, muni de deux opérations : une opération (ou loi) interne appelée *addition* et notée $+$ :

$$E \times E \to E \qquad (u, v) \mapsto u + v$$

et une opération (ou loi) externe appelée *multiplication* et notée $\cdot$ :

$$\mathbb{K} \times E \to E \qquad (\lambda, u) \mapsto \lambda \cdot u$$

On dit que $(E, +, \cdot)$ est un *espace vectoriel sur* $\mathbb{K}$ ou un $\mathbb{K}$-*espace vectoriel* si les propriétés suivantes sont vérifiées :

- L'addition sur $E$ est :
  (1) commutative : $u + v = v + u$ pour tout $(u, v) \in E^2$
  (2) associative : $(u + v) + w = u + (v + w)$ pour tout $(u, v, w) \in E^3$
  (3) possède un 'zéro' (appelé vecteur nul) : il existe $\mathbf{0} \in E$ tel que $u + \mathbf{0} = u$, pour tout $u \in E$
  (4) tout élément possède un opposé : pour tout $u \in E$, il existe un élément noté $-u$ tel que $u + (-u) = \mathbf{0}$.
- La multiplication externe vérifie :
  (5) $1 \cdot u = u$ pour tout $u \in E$
  (6) $\lambda \cdot (\mu \cdot u) = (\lambda\mu) \cdot u$ pour tout $(\lambda, \mu) \in \mathbb{K}^2$, $u \in E$.
- La multiplication est *distributive sur l'addition* :
  (7) $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$ pour tout $\lambda \in \mathbb{K}$, pour tout $(u, v) \in E^2$
  (8) $(\lambda + \mu) \cdot u = \lambda \cdot u + \mu \cdot v$ pour tout $(\lambda, \mu) \in \mathbb{K}^2$, pour tout $u \in E$.

On appelle les éléments d'un espace vectoriel des *vecteurs* et les éléments de $\mathbb{K}$ des *scalaires*. L'élément $\mathbf{0}$ est appelé le *vecteur nul*.

Les opérations d'espaces vectoriels vérifient quelques propriétés supplémentaires qui se déduisent de celles listées dans la définition (lesquelles sont parfois appelées les *axiomes*) :

**Proposition 3.1.2.** Si $(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel, alors :

1. Son vecteur nul est unique
2. Tout vecteur de $E$ possède un unique opposé
3. $\lambda \cdot \mathbf{0} = \mathbf{0}$ pour tout $\lambda \in \mathbb{K}$
4. $0 \cdot u = \mathbf{0}$ pour tout $u \in E$
5. Si $\lambda \cdot u = \mathbf{0}$ alors $\lambda = 0$ ou $u = \mathbf{0}$.
6. $-u = (-1) \cdot u$ pour tout $u \in E$

*Démonstration.* 1. Si $\mathbf{0}'$ est un autre vecteur nul, alors on a en appliquant la propriété (3) d'espace vectoriel, $\mathbf{0} + \mathbf{0}' = \mathbf{0}'$ mais aussi $\mathbf{0} + \mathbf{0}' = \mathbf{0}$ donc $\mathbf{0} = \mathbf{0}'$.

2. Si $u$ possède deux opposés notés $v$ et $w$, alors $v = v + \mathbf{0} = v + (u + w) = (v + u) + w = \mathbf{0} + w = w$ (en appliquant successivement (3) (4) (2) (4) (3)).

3. On a $\lambda \cdot \mathbf{0} = \lambda \cdot (\mathbf{0} + \mathbf{0}) = \lambda \cdot \mathbf{0} + \lambda \cdot \mathbf{0}$ en appliquant successivement les propriétés d'espaces vectoriels (3) et (7), donc, en ajoutant l'opposé de $\lambda \cdot \mathbf{0}$, on trouve $\mathbf{0} = \lambda \cdot \mathbf{0}$.

4. On écrit $0 \cdot u = (0 + 0) \cdot u = 0 \cdot u + 0 \cdot u$ en appliquant (8) et on conclut de même que $0 \cdot u = \mathbf{0}$.

5. Supposons que $\lambda \cdot u = \mathbf{0}$ avec $\lambda \neq 0$, et montrons qu'alors $u = \mathbf{0}$. On a $u = 1 \cdot u = (\lambda^{-1}\lambda) \cdot u = \lambda^{-1} \cdot (\lambda \cdot u) = \lambda^{-1} \cdot \mathbf{0} = \mathbf{0}$ en appliquant successivement (5), (6), et 4. que l'on vient de montrer.

6. On remarque que $u + (-1) \cdot u = 1 \cdot u + (-1) \cdot u = (1 + (-1)) \cdot u = 0 \cdot u = \mathbf{0}$ et on conclut grâce à l'unicité de l'opposé de $u$ qu'on a démontré en 2.

□

**Notation.** Dorénavant, on va simplifier les notations en posant $u + (-v) = u - v$ et $\lambda \cdot u = \lambda u$.

## 3.2 Exemples

On va maintenant décrire quelques exemples d'espaces vectoriels classiques :

**Exemple 1 :** $\mathbb{K}^n$ est bien sûr un $\mathbb{K}$-espace vectoriel au sens de notre définition abstraite.

**Exemple 2 :** $\{\mathbf{0}\}$ où $\mathbf{0}$ est un 'symbole'. Les lois internes et externes sont définies par $\mathbf{0}+\mathbf{0} = \mathbf{0}$ et $\lambda \cdot \mathbf{0} = \mathbf{0}$ et les propriétés (1) à (8) sont bien vérifiées. On dit que $\{\mathbf{0}\}$ est *l'espace vectoriel nul*.

**Exemple 3 :** On va maintenant décrire une famille vraiment nouvelle d'espaces vectoriels. Soit $I$ un ensemble, et soit $\mathcal{F}(I, \mathbb{K})$ l'ensemble des fonctions $f : I \to \mathbb{K}$. On définit sur $\mathcal{F}(I, \mathbb{K})$ une loi d'addition : si $f \in \mathcal{F}(I, \mathbb{K})$ et $g \in \mathcal{F}(I, \mathbb{K})$, la somme $f + g$ est la fonction de $I$ dans $\mathbb{K}$ définie par $(f + g)(x) = f(x) + g(x)$. Pour définir la loi externe, on doit définir une fonction $\lambda \cdot f$ de $I$ dans $\mathbb{K}$. Pour cela on pose $(\lambda \cdot f)(x) = \lambda f(x)$ pour tout $x \in I$. On a donc bien défini nos deux opérations

$$\begin{array}{ccc} \mathcal{F}(I,\mathbb{K}) \times \mathcal{F}(I,\mathbb{K}) & \to & \mathcal{F}(I,\mathbb{K}) \\ (f,g) & \mapsto & f+g \end{array} \qquad \begin{array}{ccc} \mathbb{K} \times \mathcal{F}(I,\mathbb{K}) & \to & \mathcal{F}(I,\mathbb{K}) \\ (\lambda,f) & \mapsto & \lambda \cdot f \end{array}$$

**Proposition 3.2.1.** L'ensemble $\mathcal{F}(I, \mathbb{K})$ des fonctions définies sur un ensemble $I$ et à valeurs dans $\mathbb{K}$, muni des opérations d'addition et de multiplication scalaire définies ci-dessus est un $\mathbb{K}$-espace vectoriel. Son vecteur nul est la fonction nulle prenant constamment la valeur 0.

*Démonstration.* Les axiomes (1) à (8) sont bien vérifiés, essentiellement parce que les opérations ont lieu dans $\mathbb{K}$. □

Les exemples les plus importants d'espaces vectoriels de ce type sont :
- $I = \{1, 2, \ldots, n\}$. Alors $\mathcal{F}(I, \mathbb{K}) = \mathbb{K}^n$.
- $I = \mathbb{N}$. Alors $\mathcal{F}(\mathbb{N}, \mathbb{K})$ est l'ensemble des suites réelles ou complexes.
- $I = [a, b]$ ; $\mathcal{F}([a, b], \mathbb{R})$ est l'ensemble des fonctions à valeurs réelles définies sur l'intervalle $[a, b]$.

## 3.3 Sous-espaces vectoriels

**Définition 3.3.1.** Soit $(E, +, \cdot)$ un espace vectoriel sur $\mathbb{K}$. Un sous-espace vectoriel de $E$ est un sous-ensemble $F$ de $E$ vérifiant :

1. $F \neq \emptyset$
2. Pour tout $(u, v) \in F^2$, $u + v \in F$
3. Pour tout $\lambda \in \mathbb{K}$, $u \in F$, $\lambda u \in F$.

**Remarque 3.3.2.** On peut condenser les proriétés 2. et 3. ci-dessus en une seule, qui s'énonce : pour tout $(u, v) \in F^2$, pour tout $(\lambda, \mu) \in \mathbb{K}^2$, $\lambda u + \mu v \in F$.

**Théorème 3.3.3.** Si $F$ est un sous-espace vectoriel de $(E, +, \cdot)$ alors $(F, +, \cdot)$ est lui-même un espace vectoriel sur $\mathbb{K}$.

*Démonstration.* Par définition, dire que $F$ est un sous-espace vectoriel de $E$ c'est dire que les opérations d'addition et de multiplication scalaire de $E$ se restreignent en des opérations de $F$. Les axiomes d'espace vectoriel sont automatiquement vérifiés pour $F$ par restriction, à ceci près qu'il faut vérifier que $\mathbf{0} \in F$ et que l'opposé d'un vecteur de $F$ appartient à $F$. Montrons donc ces deux propriétés :

Puisque $F$ est supposé non vide, soit $u \in F$. Alors $0 \cdot u \in F$ par la propriété 3. ; comme $E$ est un espace vectoriel, $0 \cdot u = \mathbf{0}$, donc $\mathbf{0} \in F$.

Soit $u \in F$ ; $u$ possède un opposé $-u$ dans $E$. On a vu que $-u = (-1) \cdot u$ donc par la propriété 3., $-u \in F$. □

**Remarque 3.3.4.** Le théorème 3.3.3 est très important dans la pratique. En effet, pour montrer qu'un certain ensemble est un espace vectoriel, plutôt que de vérifier tous les axiomes ce qui est vite fastidieux, il est préférable de montrer que c'est un sous-espace vectoriel d'un espace vectoriel déjà connu (bien sûr, quand c'est possible). Voici quelques exemples, qui pour certains seront détaillés en TD :

1. L'ensemble des suites de support fini (où le support d'une suite $(u_n)_{n\geq 0}$ est l'ensemble des entiers $k$ tels que $u_k \neq 0$) est un sous-espace vectoriel de $\mathcal{F}(\mathbb{N}, \mathbb{K})$.
2. L'ensemble des suites de limite 0 est un sous-espace vectoriel de $\mathcal{F}(\mathbb{N}, \mathbb{K})$.
3. L'ensemble des fonctions continues (respectivement dérivables) sur l'intervalle $[a, b]$ est un sous-espace vectoriel de $\mathcal{F}([a, b], \mathbb{R})$.

## 3.4 Combinaisons linéaires

Soit $E$ un $\mathbb{K}$-espace vectoriel. Si $\lambda_1, \ldots, \lambda_k$ appartiennent à $\mathbb{K}$, et si $v_1, v_2, \ldots, v_k$ appartiennent à $E$, alors

$$u = \lambda_1 v_1 + \cdots + \lambda_n v_k$$

appartient à $E$. On dit que $u$ est une *combinaison linéaire* des vecteurs $v_1, \ldots, v_k$.

**Proposition 3.4.1.** Si $F$ est un sous-espace vectoriel de $E$ alors toute combinaison linéaire d'éléments de $F$ est dans $F$ (on dit qu'un sous-espace vectoriel est *stable par combinaisons linéaires*).

Réciproquement, un sous-ensemble non vide de $E$ qui est stable par combinaisons linéaires est un sous-espace vectoriel de $E$.

*Démonstration.* Soit $v_1, v_2, \ldots, v_k$ des vecteurs de $F$ et soit $\lambda_1, \ldots, \lambda_k$ des éléments de $\mathbb{K}$. Par la propriété 3. de sous-espace vectoriel, $\lambda_i v_i \in F$ pour tout $i = 1, 2, \ldots, k$. Par la propriété 2., $\lambda_1 v_1 + \lambda_2 v_2 \in F$. Donc aussi $(\lambda_1 v_1 + \lambda_2 v_2) + \lambda_3 v_3 = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3$, et ainsi de suite jusqu'à $\lambda_1 v_1 + \cdots + \lambda_k v_k$.

La réciproque est évidente puisque $u + v$ et $\lambda u$ sont des combinaisons linéaires d'éléments de $F$ particulières. □

Comme dans $\mathbb{K}^n$, on obtient des sous-espaces vectoriels en prenant l'ensemble des combinaisons linéaires d'une famille finie de vecteurs.

**Définition et Proposition 3.4.2.** Soit $v_1, v_2, \ldots, v_k$ des vecteurs de $E$. On note $\mathrm{Vect}(v_1, \ldots, v_k)$ l'ensemble des combinaisons linéaires de $v_1, \ldots, v_k$ :

$$\mathrm{Vect}(v_1, \ldots, v_k) = \{u \in E \mid \exists (\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^n \mid u = \lambda_1 v_1 + \cdots + \lambda_k v_k\}$$

Alors $\mathrm{Vect}(v_1, \ldots, v_k)$ est un sous-espace vectoriel de $E$ appelé *le sous-espace vectoriel engendré par* $v_1, \ldots, v_k$.

## 3.5 Somme et intersection de sous-espaces vectoriels

On a les mêmes notions de somme et d'intersection de deux sous-espaces vectoriels que ce qu'on a vu dans le cas de $\mathbb{K}^n$ au chapitre précédent. On se contente de répéter les définitions et résultats sans répéter les démonstrations qui sont identiques.

**Proposition 3.5.1.** Si $F$ et $G$ sont deux sous-espaces vectoriels de $E$, alors leur intersection $F \cap G$ est aussi un sous-espace vectoriel de $E$.

**Définition et Proposition 3.5.2.** Si $F$ et $G$ sont deux sous-espaces vectoriels de $E$, on note $F + G$ et on appelle *somme de $F$ et $G$* l'ensemble

$$F + G = \{u + v \text{ tels que } u \in F \text{ et } v \in G\}.$$

Alors $F + G$ est un sous-espace vectoriel de $E$.

# Chapitre 4

# Familles génératrices, libres, bases

Dans tout le chapitre, $E$ désigne un $\mathbb{K}$-espace vectoriel. On garde en tête le cas très important de $E = \mathbb{K}^n$, sur lequel on va se baser pour les exemples illustratifs.

On a vu comme exemples d'espaces vectoriels les ensembles de la forme $E = \text{Vect}(e_1, \dots, e_k)$ où $e_1, \dots, e_k$ sont des vecteurs de $\mathbb{K}^n$. On dit dans ce cas que $\{e_1, \dots, e_k\}$ *engendre* ou *est une famille génératrice* de $E$. L'avantage, c'est qu'on peut exprimer tous les vecteurs de $E$ avec seulement $k$ d'entre eux. On va voir dans ce chapitre que, d'une part, il y a des parties génératrices plus intéressantes que d'autres parce que minimales (ce sont les bases de $E$) et, d'autres part, que tous les espaces vectoriels de la forme $E = \text{Vect}(e_1, \dots, e_k)$ possèdent des bases.

## 4.1 Familles génératrices

**Définition 4.1.1.** Soit $e_1, \dots, e_k$ des vecteurs de $E$. On dit que $\{e_1, \dots, e_k\}$ est une *famille génératrice de $E$* si tout vecteur de $E$ est combinaison linéaire de $e_1, \dots, e_k$, ou, de façon équivalente, si on a

$$E = \text{Vect}(e_1, \dots, e_k).$$

Pour illustrer l'intérêt d'une telle présentation, montrons que les familles génératrices facilitent la comparaison des sous-espaces de $E$ :

**Proposition 4.1.2.** Soit $F$ et $G$ deux sous-espaces vectoriels de $E$ tels que $F = \text{Vect}(f_1, \dots, f_k)$ et $G = \text{Vect}(g_1, \dots, g_\ell)$. Alors, $F \subset G$ si et seulement si pour tout $1 \leq i \leq k$, $f_i$ est combinaison linéaire de $g_1, g_2, \dots, g_\ell$.

*Démonstration.* Supposons $F \subset G$. Alors, puisque $f_i \in F$, on a aussi $f_i \in G$, donc, puisque $G = \text{Vect}(g_1, \dots, g_\ell)$, $f_i$ est bien combinaison linéaire de $g_1, g_2, \dots, g_\ell$.

Réciproquement, supposons que pour tout $i$, $f_i$ soit combinaison linéaire de $g_1, g_2, \dots, g_\ell$. Cela montre que $f_i \in G$ (on a vu qu'un sous-espace vectoriel est stable par combinaison linéaire). Soit $v \in F$. Puisque $F = \text{Vect}(f_1, \dots, f_k)$, le vecteur $v$ est combinaison linéaire des $f_i$ qui sont dans $G$, donc $v$ lui-même est dans $G$. On a donc $F \subset G$. □

S'il est avantageux de pouvoir exprimer des vecteurs comme combinaison linéaire d'une famille fixée $\{e_1, \dots, e_k\}$, on remarque qu'une telle écriture n'est pas forcément unique. Par exemple, si on prend dans $\mathbb{R}^2$ les vecteurs $e_1 = (1, 0)$, $e_2 = (0, 1)$, $e_3 = (1, 1)$, on a

$$(2, 1) = 2(1, 0) + (0, 1) = (1, 0) + (1, 1)$$

soit

$$2e_1 + e_2 = e_1 + e_3.$$

En calculant la différence de ces deux expressions on obtient la relation

$$e_1 + e_2 - e_3 = \mathbf{0}.$$

Quand une telle relation existe on dit que les vecteurs sont *liés*. On va voir que c'est l'existence d'une telle relation de liaison qui fait obstacle à l'unicité des coefficients.

## 4.2 Familles libres, liées, bases

**Définition 4.2.1.** Les vecteurs $\{e_1, \ldots, e_k\}$ de $E$ forment une *famille liée* ou *linéairement dépendante* s'il existe des scalaires $\lambda_1, \ldots, \lambda_k$ *non tous nuls* tels que

$$\lambda_1 e_1 + \cdots + \lambda_k e_k = \mathbf{0}.$$

Les vecteurs $\{e_1, \ldots, e_k\}$ de $E$ forment une *famille libre* ou *linéairement indépendante* s'ils ne sont pas liés, c'est-à-dire si l'implication suivante est vraie :

$$\lambda_1 e_1 + \cdots + \lambda_k e_k = \mathbf{0} \implies \lambda_1 = \cdots = \lambda_k = 0$$

**Remarque 4.2.2.** Par définition, la famille vide $\emptyset$ est libre.

**Exemple 4.2.3.** Une famille de vecteurs qui contient le vecteur nul, c'est-à-dire une famille de la forme $\{\mathbf{0}, e_2, \ldots, e_k\}$, est toujours liée. En effet, on a la relation :

$$1.\mathbf{0} + 0.e_2 + \cdots + 0.e_k = \mathbf{0}$$

et les coefficients $1, 0, \ldots, 0$ sont bien non tous nuls.

De façon plus générale, une famille de vecteurs qui contient une sous-famille liée est liée.

**Exemple 4.2.4.** Examinons le cas d'une famille à un élément : $\{\mathbf{0}\}$ n'est pas libre. $\{u\}$ est libre si et seulement si $u \neq \mathbf{0}$. Pour une famille à deux éléments, il est facile de voir que $\{u, v\}$ est libre si et seulement si $u$ et $v$ sont non colinéaires i.e. non nuls et non proportionnels.

**Proposition 4.2.5.** Les vecteurs $\{e_1, \ldots, e_k\}$ sont liés si et seulement si l'un de ces vecteurs est combinaison linéaire des autres.

*Démonstration.* Supposons les vecteurs liés ; alors il existe $\lambda_1, \ldots, \lambda_k$ *non tous nuls* tels que

$$\lambda_1 e_1 + \cdots + \lambda_k e_k = \mathbf{0}.$$

Puisque les scalaires $\lambda_1, \ldots, \lambda_k$ ne sont pas tous nuls, il existe un indice $i$ tel que $\lambda_i \neq 0$. Alors on a $\lambda_i e_i = -\sum_{j \neq i} \lambda_j e_j$ et donc $e_i = -\sum_{j \neq i} (\lambda_j / \lambda_i) e_j$.

Réciproquement, supposons que l'un des vecteurs, par exemple $e_1$, soit combinaison linéaire des autres. Alors, il existe des coefficients $\lambda_2, \ldots, \lambda_k$ tels que $e_1 = \lambda_2 e_2 + \cdots + \lambda_k e_k$. On a alors la relation de dépendance linéaire

$$e_1 - \lambda_2 e_2 - \cdots - \lambda_k e_k = \mathbf{0}$$

et les coefficients sont bien non tous nuls puisque le premier vaut 1. □

**Théorème 4.2.6.** Soit $\{e_1, \dots, e_k\}$ une famille de vecteurs. Les deux propositions suivantes sont équivalentes :

(i) La famille $\{e_1, \dots, e_k\}$ est libre.

(ii) Pour tout $v \in \text{Vect}(e_1, \dots, e_k)$, il existe un *unique* $k$-uplet $(\lambda_1, \dots, \lambda_k)$ tel que $v = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_k e_k$.

*Démonstration.* Supposons d'abord (i). Soit $v \in \text{Vect}(e_1, \dots, e_k)$.

Si $v = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_k e_k = \mu_1 e_1 + \mu_2 e_2 + \cdots + \mu_k e_k$, la différence de ces deux expressions conduit à $\mathbf{0} = (\lambda_1 - \mu_1)e_1 + \cdots + (\lambda_k - \mu_k)e_k$. Puisque $\{e_1, \dots, e_k\}$ est libre, on peut en déduire $\lambda_1 - \mu_1 = \cdots = \lambda_k - \mu_k = 0$ soit $\lambda_1 = \mu_1, \dots, \lambda_k = \mu_k$.

Réciproquement, supposons (ii) vérifiée. Alors, si les vecteurs $\{e_1, \dots, e_k\}$ étaient liés, le vecteur $\mathbf{0}$ aurait deux expressions comme combinaison linéaire des $e_i$ : en effet, il existerait des scalaires *non tous nuls* $\lambda_1, \dots, \lambda_k$ tels que

$$\mathbf{0} = 0\, e_1 + \cdots + 0\, e_k = \lambda_1 e_1 + \cdots + \lambda_k e_k$$

ce qui contredirait (ii). □

**Exemple 4.2.7.** Si $E = \mathbb{K}^n$, décider si des vecteurs $e_1, \dots, e_k$ sont libres ou liés revient à résoudre un système linéaire d'inconnues $\lambda_1, \dots, \lambda_k$. Par exemple, si $e_1 = (1, 0, 0)$, $e_2 = (1, 1, 0)$ et $e_3 = (-1, 0, 1)$ on a

$$\begin{aligned}
\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3 = \mathbf{0} &\iff \lambda_1(1,0,0) + \lambda_2(1,1,0) + \lambda_3(-1,0,1) = (0,0,0) \\
&\iff (\lambda_1 + \lambda_2 - \lambda_3, \lambda_2, \lambda_3) = (0,0,0) \\
&\iff \begin{cases} \lambda_1 + \lambda_2 - \lambda_3 = 0 \\ \lambda_2 = 0 \\ \lambda_3 = 0 \end{cases}
\end{aligned}$$

En général pour des vecteurs de $\mathbb{K}^n$, si on note, pour $1 \leq j \leq k$, $e_j = (e_{1,j}, e_{2,j}, \dots, e_{n,j})$, on a l'équivalence :

$$\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_k e_k = \mathbf{0} \iff \begin{cases} \lambda_1 e_{1,1} + \lambda_2 e_{1,2} + \cdots + \lambda_k e_{1,k} = 0 \\ \lambda_1 e_{2,1} + \lambda_2 e_{2,2} + \cdots + \lambda_k e_{2,k} = 0 \\ \qquad\qquad \vdots \\ \lambda_1 e_{n,1} + \lambda_2 e_{n,2} + \cdots + \lambda_k e_{n,k} = 0 \end{cases}$$

Ainsi, les vecteurs $\{e_1, \dots, e_k\}$ sont libres si et seulement si ce système linéaire homogène, d'inconnues $\lambda_1, \dots, \lambda_k$, admet pour unique solution $(0, 0, \dots, 0)$. On remarque que cela implique $k \leq n$ d'après la Proposition 1.4.1.

**Définition 4.2.8.** Une *base* de $E$ est une famille de vecteurs de $E$ libre et génératrice.

**Exemple 4.2.9.** *La base canonique de* $\mathbb{K}^n$. C'est la famille $\epsilon_1 = (1, 0, \dots, 0)$, $\epsilon_2 = (0, 1, 0, \dots, 0)$, jusqu'à $\epsilon_n = (0, 0, \dots, 1)$.

**Théorème 4.2.10.** Une famille $\{e_1, \dots, e_k\}$ de vecteurs de $E$ est une base de $E$ si et seulement, pour tout $v \in E$, il existe un unique $k$-uplet $(\lambda_1, \dots, \lambda_k) \in \mathbb{K}^k$ tel que $v = \lambda_1 e_1 + \cdots + \lambda_k e_k$.

Dans ce cas, on dit que $\lambda_1, \ldots, \lambda_k$ sont *les coordonnées de $v$ dans la base* $\{e_1, \ldots, e_k\}$. On note en général les coordonnées de $v$ sous la forme d'un vecteur colonne :

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix}$$

*Démonstration.* L'existence des coefficients pour tout vecteur $v$ de $E$ est équivalente au fait que la famille soit génératrice. Le théorème 4.2.6 montre que l'unicité de ces coefficients est équivalente au fait que la famille soit libre. □

**Remarque 4.2.11.** Si $E = \{\mathbf{0}\}$, l'ensemble vide $\emptyset$ est une base de $E$.

Notons que nous n'avons défini les notions de famille génératrice, libre, liée, et de base que pour des familles finies de vecteurs. On peut aisément étendre ces notions à des familles infinies de vecteurs.

Un espace vectoriel qui possède une base finie, c'est-à-dire une base au sens de notre définition, est dit *de dimension finie*. Nous allons voir au paragraphe suivant que les espaces vectoriels engendrés par une famille finie de vecteurs sont de dimension finie.

## 4.3 Bases et dimension des espaces vectoriels finiment engendrés

Dans cette section on fait l'hypothèse qu'il existe des vecteurs $g_1, \ldots, g_m$ dans $E$ tels que $E = \mathrm{Vect}(g_1, \ldots, g_m)$. On dit dans ce cas que $E$ est *finiment engendré* ou encore que $E$ est *de dimension finie* (pour des raisons qui apparaitront un peu plus tard). Notons que c'est bien le cas pour $\mathbb{K}^n$ qui est engendré par $\epsilon_1 = (1, 0, \ldots, 0)$, $\epsilon_2 = (0, 1, 0, \ldots, 0), \ldots \epsilon_n = (0, 0, \ldots, 1)$.

Nous allons tout de suite démontrer qu'un espace vectoriel finiment engendré possède des bases.

**Théorème 4.3.1.** Soit $\{e_1, \ldots, e_k\}$ une famille de vecteurs de $E$. Si $\{e_1, \ldots, e_k\}$ est une famille génératrice de $E$, et si $e_k$ est combinaison linéaire de $e_1, \ldots, e_{k-1}$, alors $\{e_1, \ldots, e_{k-1}\}$ est une famille génératrice de $E$.

*Démonstration.* Par hypothèse, il existe des coefficicients $\mu_1, \ldots, \mu_{k-1}$ tels que $e_k = \sum_{i=1}^{k-1} \mu_i e_i$. Soit $v \in E$ ; comme $\{e_1, \ldots, e_k\}$ est génératrice de $E$, il existe $(\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^n$ tels que $v = \lambda_1 e_1 + \cdots + \lambda_k e_k$. On obtient en remplaçant $e_k$ :

$$\begin{aligned} v &= \lambda_1 e_1 + \cdots + \lambda_{k-1} e_{k-1} + \lambda_k(\mu_1 e_1 + \cdots + \mu_{k-1} e_{k-1}) \\ &= (\lambda_1 + \lambda_k \mu_1) e_1 + \cdots + (\lambda_{k-1} + \lambda_k \mu_{k-1}) e_{k-1} \end{aligned}$$

On voit alors que $v$ est combinaison linéaire de $e_1, \ldots e_{k-1}$. Donc on a montré que $\{e_1, \ldots e_{k-1}\}$ est une famille génératrice de $E$. □

**Corollaire 4.3.2.** (Théorème de la base extraite) Soit $\{e_1, \ldots, e_k\}$ une famille de vecteurs de $E$. Si $\{e_1, \ldots, e_k\}$ est une famille génératrice de $E$, alors il existe un sous-ensemble de cette famille qui est une base de $E$.

*Démonstration.* Si la famille $\{e_1, \dots, e_k\}$ est aussi libre, on a fini. Sinon, c'est qu'elle est liée, mais alors l'un de ses vecteurs est combinaison linéaire des autres. D'après le Théorème 4.3.1, on peut enlever ce vecteur en conservant une famille génératrice de $E$. On itère ce procédé jusqu'à obtenir une famille libre et génératrice, donc une base. Notons qu'on ne peut pas itérer indéfiniment puisque à chaque étape la famille de vecteurs perd un élément. □

**Corollaire 4.3.3.** $E$ possède des bases.

*Démonstration.* En effet, d'après le Théorème 4.3.2, on peut extraire de la famille génératrice $\{g_1, \dots, g_m\}$ une base de $E$. □

**Théorème 4.3.4.** Si $\{e_1, \dots, e_k\}$ est une famille libre de $E$ à $k$ éléments et si $\{h_1, \dots, h_s\}$ est une famille génératrice de $E$ à $s$ éléments alors $k \leq s$.

*Démonstration.* Par le Théorème 4.3.2, on peut extraire de $\{h_1, \dots, h_s\}$ une base de $E$ ; notons-la $\{f_1, \dots f_n\}$, et on a $n \leq s$.

Pour tout $j = 1, \dots, k$, puisque $e_j$ appartient à $E$, $e_j$ est combinaison linéaire des vecteurs $f_1, \dots, f_n$. Il existe donc des coefficients $a_{j,i}$ tels que

$$e_j = a_{1,j} f_1 + a_{2,j} f_2 + \cdots + a_{n,j} f_n.$$

On peut alors transformer une combinaison linéaire $\lambda_1 e_1 + \cdots + \lambda_k e_k$ des vecteurs $e_1, \dots, e_k$ en une combinaison linéaire des vecteurs $f_1, \dots, f_n$ :

$$\begin{aligned} \lambda_1 e_1 + \cdots + \lambda_k e_k &= \lambda_1(a_{1,1} f_1 + \cdots + a_{n,1} f_n) + \cdots + \lambda_k(a_{1,k} f_1 + \cdots + a_{n,k} f_k) \\ &= (\lambda_1 a_{1,1} + \cdots + \lambda_k a_{1,k}) f_1 + \cdots + (\lambda_1 a_{n,1} + \cdots + \lambda_k a_{n,k}) f_k \end{aligned}$$

Comme $\{f_1, \dots, f_n\}$ est une base de $E$, on a

$$\lambda_1 e_1 + \cdots + \lambda_k e_k = \mathbf{0} \iff \begin{cases} \lambda_1 a_{1,1} + \cdots + \lambda_k a_{1,k} &= 0 \\ \lambda_1 a_{2,1} + \cdots + \lambda_k a_{2,k} &= 0 \\ \vdots & \\ \lambda_1 a_{n,1} + \cdots + \lambda_k a_{n,k} &= 0 \end{cases}$$

Dire que $\{e_1, \dots, e_k\}$ est libre, c'est dire que ce système linéaire homogène a pour unique solution $(\lambda_1, \dots, \lambda_k) = (0, \dots, 0)$. Ce système a $k$ inconnues et $n$ équations. On fait maintenant appel à un résultat du chapitre 1 : d'après la Proposition 1.4.1, un système linéaire ayant une solution unique a au moins autant d'équations que d'inconnues ; on a donc $n \geq k$, donc a fortiori $s \geq k$. □

**Théorème 4.3.5.** Soit $\{e_1, \dots, e_k\}$ une famille de vecteurs de $E$. Si $\{e_1, \dots, e_k\}$ est libre, et si $e_{k+1} \notin \text{Vect}(e_1, \dots, e_k)$, alors $\{e_1, \dots, e_k, e_{k+1}\}$ est libre.

*Démonstration.* Soit $(\lambda_1, \dots, \lambda_{k+1}) \in \mathbb{K}^{k+1}$ tels que $\lambda_1 e_1 + \cdots + \lambda_k e_k + \lambda_{k+1} e_{k+1} = \mathbf{0}$.

Si $\lambda_{k+1} = 0$ : alors on a $\lambda_1 e_1 + \cdots + \lambda_k e_k = \mathbf{0}$. Mais $\{e_1, \dots, e_k\}$ est libre donc on peut conclure que $\lambda_1 = \cdots = \lambda_k = 0$.

Si $\lambda_{k+1} \neq 0$ : alors on a $e_{k+1} = -(\lambda_1/\lambda_{k+1})e_1 - \cdots - (\lambda_k/\lambda_{k+1})e_k$ ce qui contredit l'hypothèse $e_{k+1} \notin \text{Vect}(e_1, \dots, e_k)$.

Donc on peut conclure que la famille $\{e_1, \dots, e_{k+1}\}$ est libre. □

**Corollaire 4.3.6.** (Théorème de la base incomplète) Soit $\{e_1, \ldots, e_k\}$ une famille de vecteurs de $E$. Si $\{e_1, \ldots, e_k\}$ est libre, alors il existe un ensemble (éventuellement vide) $\{e_{k+1}, \ldots, e_n\}$ de vecteurs de $E$ tels que $\{e_1, \ldots, e_k, e_{k+1}, \ldots, e_n\}$ soit une base de $E$.

*Démonstration.* Si $\{e_1, \ldots, e_k\}$ est aussi génératrice de $E$ alors on a fini. Sinon, il existe un vecteur $e_{k+1}$ qui est dans $E$ mais pas dans $\mathrm{Vect}(e_1, \ldots, e_k)$. Alors, d'après le Théorème 4.3.5, la famille $\{e_1, \ldots, e_k, e_{k+1}\}$ est aussi libre.

On itère cette procédure, jusqu'à obtenir une famille génératrice de $E$. Cela arrive forcément au bout d'un nombre fini d'étapes parce qu'à chaque étape on augmente le cardinal de la famille, et on sait par le Théorème 4.3.4 qu'une famille libre est de cardinal au plus égal à $m$. □

**Théorème 4.3.7.** Tout sous-espace vectoriel de $E$ possède des bases. En particulier, les sous-espaces vectoriels de $\mathbb{K}^n$ possèdent tous des bases.

*Démonstration.* C'est la même preuve que celle du théorème de la base incomplète. Soit $F$ un sous-espace vectoriel de $E$. On part de $\emptyset \subset F$ et on lui rajoute des vecteurs de $F$, disons $f_1, \ldots, f_k, \ldots$, tant que $\mathrm{Vect}(f_1, \ldots, f_k) \neq F$ et en choisissant $f_{k+1} \in F$, $f_{k+1} \notin \mathrm{Vect}(f_1, \ldots, f_k)$. À chaque étape la famille construite est libre donc son cardinal est au plus $m$. Donc la procédure s'arête au bout d'un nombre fini d'étapes, donc $F$ possède une base finie. □

**Théorème 4.3.8.** Toutes les bases de $E$ ont le même cardinal. Le cardinal d'une base de $E$ s'appelle *la dimension de* $E$ et est notée $\dim(E)$.

*Démonstration.* Soit $\{e_1, \ldots, e_k\}$ et $\{f_1, \ldots, f_\ell\}$ deux bases de $E$. Puisque $\{e_1, \ldots, e_k\}$ est une famille libre et que $\{f_1, \ldots, f_\ell\}$ est une famille génératrice de $E$, d'après le Théorème 4.3.4, on a $k \leq \ell$. Réciproquement, puisque $\{f_1, \ldots, f_\ell\}$ est une famille libre et que $\{e_1, \ldots, e_k\}$ est une famille génératrice de $E$, on a aussi $\ell \leq k$. Donc $k = \ell$. □

**Exemple 4.3.9.** On a $\dim(\mathbb{K}^n) = n$ et $\dim(\{\mathbf{0}\}) = 0$.

**Corollaire 4.3.10.** Soit $n = \dim(E)$.

1. Une famille libre de $E$ a au plus $n$ éléments, et, si elle a $n$ éléments, c'est une base de $E$.
2. Une partie génératrice de $E$ a au moins $n$ éléments, et, si elle a $n$ éléments, c'est une base de $E$.
3. Si $F \subset E$ est un sous-espace vectoriel de $E$, alors $\dim(F) \leq n$, et si $\dim(F) = n$ alors $F = E$.

*Démonstration.* Conséquences immédiates des théorèmes 4.3.2, 4.3.6 et 4.3.8. □

On termine ce paragraphe par la formule qui lie les dimensions de la somme $F + G$ et de l'intersection $F \cap G$ de deux sous-espaces vectoriels. C'est une conséquence du théorème de la base incomplète (théorème 4.3.6).

**Théorème 4.3.11.** Soit $F$ et $G$ deux sous-espaces vectoriels de $E$.

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

*Démonstration.* Soit $d = \dim(F)$, $k = \dim(G)$, $\ell = \dim(F \cap G)$. Soit $\{v_1, \dots v_\ell\}$ une base de $F \cap G$. Par le théorème de la base incomplète (Théorème 4.3.6) il existe $\{e_{\ell+1}, \dots, e_d\}$ tels que $\{v_1, \dots, v_\ell, e_{\ell+1}, \dots, e_d\}$ soit une base de $F$ et $\{f_{\ell+1}, \dots, f_k\}$ tels que $\{e_1, \dots, e_\ell, f_{\ell+1}, \dots, f_k\}$ soit une base de $G$. On montre que $\{v_1, \dots, v_\ell, e_{\ell+1}, \dots, e_d, f_{\ell+1}, \dots, f_k\}$ forme une base de $F + G$. On obtient donc en comptant les éléments de cette base :

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

□

## 4.4 Espaces vectoriels de dimension infinie

Dans ce paragraphe nous voulons insister sur le fait que tous les espaces vectoriels ne sont pas de dimension finie. L'exemple typique d'un espace vectoriel de dimension infinie est l'espace $\mathcal{F}(\mathbb{N}, \mathbb{K})$ des suites à valeurs dans $\mathbb{K}$. Notons $E_n$ le sous-ensemble des suites nulles à partir du rang $n$ :

$$E_n = \{s \in \mathcal{F}(\mathbb{N}, \mathbb{K}) \mid s_n = s_{n+1} = \cdots = 0\}.$$

**Exercice :** Montrez que $E_n$ est un sous-espace vectoriel de $\mathcal{F}(\mathbb{N}, \mathbb{K})$.

Notons $\epsilon_0, \epsilon_1, \dots, \epsilon_k, \dots$ les suites suivantes :

$$\begin{array}{lccccccc}
\epsilon_0 = & 1, & 0, & 0, & \dots & 0, & \dots \\
\epsilon_1 = & 0, & 1, & 0, & \dots & 0, & \dots \\
\vdots & & & & & & \\
\epsilon_k = & 0, & 0, & 0, & \dots & 1, & \dots \\
\vdots & & & & & &
\end{array}$$

Plus précisément la suite $\epsilon_k$ est la suite dont tous les termes sont nuls sauf le terme d'indice $k$ qui vaut 1.

Il est clair que $\epsilon_0, \dots, \epsilon_{n-1}$ appartiennent à $E_n$, et forment une base de $E_n$. En effet, une suite $s \in E_n$ s'écrit de façon unique $s = s_0\epsilon_0 + \cdots + s_{n-1}\epsilon_{n-1}$. Donc $\dim(E_n) = n$.

L'espace vectoriel $\mathcal{F}(\mathbb{N}, \mathbb{K})$ contient donc des sous-espaces vectoriels de dimension arbitrairement grande, donc il ne peut pas lui-même être de dimension finie.

# Chapitre 5

# Matrices

## 5.1 Définitions, exemples

Une matrice est simplement un tableau rectangulaire de nombres. On verra que c'est un outil extrêmement pratique pour représenter certains objets de l'algèbre linéaire comme les familles de vecteurs, les systèmes linéaires ou les applications linéaires (dont on n'a pas encore parlé), et pour effectuer des calculs sur ces objets.

**Définition 5.1.1.** Une matrice $A$ à $\ell$ lignes et $n$ colonnes est notée

$$A = (a_{i,j})_{\substack{1\leq i\leq \ell \\ 1\leq j\leq n}} = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{\ell,1} & a_{\ell,2} & \dots & a_{\ell,n} \end{pmatrix}.$$

On dit que $A$ est *de type* $(\ell, n)$ et que les $a_{i,j}$ sont ses *coefficients*. L'ensemble des matrices à $\ell$ lignes et $n$ colonnes, à coefficients dans $\mathbb{K}$, est noté $\mathcal{M}_{\ell,n}(\mathbb{K})$. Si $\ell = n$, on note $\mathcal{M}_{\ell,n}(\mathbb{K}) = \mathcal{M}_n(\mathbb{K})$.

**Définition 5.1.2.** (et notations)

- La *matrice nulle* notée $\mathbf{0}$, est une matrice dont tous les coefficients sont égaux à 0.
- Une *matrice ligne* est une matrice de type $(1, n)$ ; une *matrice colonne* est une matrice de type $(\ell, 1)$. On identifiera le plus souvent les matrices lignes, les matrices colonnes, et les vecteurs de $\mathbb{K}^n$.
- Une *matrice carrée* est une matrice ayant le même nombre de lignes que de colonnes. La *diagonale* d'une matrice carrée de taille $n$ est le $n$-uplet des coefficients diagonaux $(a_{1,1}, a_{2,2} \dots, a_{n,n})$.
- Parmi les matrices carrées, on distingue les *matrices diagonales*, dont les coefficients en dehors de la diagonale sont nuls, ainsi que les *matrices triangulaires supérieures* (ayant des zéros sous la diagonale), et *triangulaires inférieures* (ayant des zéros au-dessus de la diagonale).
- La *matrice identité* est la matrice diagonale, dont les coefficients diagonaux sont tous égaux à 1. On la note $I$ ou $I_n$ si elle est de taille $n$.
- Si $A = (a_{i,j})_{\substack{1\leq i\leq \ell \\ 1\leq j\leq n}} \in \mathcal{M}_{\ell,n}(\mathbb{K})$, on note $L_1, \dots, L_\ell$ ses lignes. On a donc $L_i = (a_{i,1}, \dots, a_{i,n}) \in \mathbb{K}^n$.

On note $C_1, \dots, C_n$ ses colonnes. On a donc $C_j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{\ell,j} \end{pmatrix} \in \mathbb{K}^\ell$.

— La *matrice transposée* de $A$ est la matrice notée $A^T$, à $n$ lignes et $\ell$ colonnes, obtenue en échangeant dans $A$ les lignes avec les colonnes :

$$A^T = (a_{j,i})_{\substack{1 \le i \le n \\ 1 \le j \le \ell}}.$$

## 5.2 Opérations sur les matrices

On définit d'abord l'addition de deux matrices et la multiplication d'une matrice par un scalaire, de la même manière qu'on l'a déjà fait pour les vecteurs.

**Définition 5.2.1.** On considère deux opérations dans $\mathcal{M}_{\ell,n}(\mathbb{K})$ :

- L'addition de deux matrices $A = (a_{i,j})_{\substack{1 \le i \le \ell \\ 1 \le j \le n}}$ et $B = (b_{i,j})_{\substack{1 \le i \le \ell \\ 1 \le j \le n}}$ est

$$A + B = \big(a_{i,j} + b_{i,j}\big)_{\substack{1 \le i \le \ell \\ 1 \le j \le n}}$$

- La multiplication d'une matrice $A = (a_{i,j})_{\substack{1 \le i \le \ell \\ 1 \le j \le n}}$ par un scalaire $\lambda \in \mathbb{K}$ est

$$\lambda A = (\lambda a_{i,j})_{\substack{1 \le i \le \ell \\ 1 \le j \le n}}$$

**Proposition 5.2.2.** Les opérations d'addition et de multiplication par un scalaire dans $\mathcal{M}_{\ell,n}(\mathbb{K})$ ont les propriétés suivantes : pour tout $A, B, C \in \mathcal{M}_{\ell,n}(\mathbb{K})$ et tout $\lambda, \mu \in \mathbb{K}$,

1. $A + B = B + A$ (commutativité de l'addition)
2. $(A + B) + C = A + (B + C)$ (associativité de l'addition)
3. $A + \mathbf{0} = A$
4. $A + (-A) = \mathbf{0}$
5. $1\,A = A$, $0\,A = \mathbf{0}$.
6. $\lambda(\mu A) = (\lambda\mu)A$
7. $(\lambda + \mu)A = \lambda A + \mu A$
8. $\lambda(A + B) = \lambda A + \lambda B$

Autrement dit, $\mathcal{M}_{\ell,n}(\mathbb{K})$ est un $\mathbb{K}$-espace vectoriel. Sa dimension est $\ell n$.

*Démonstration.* Les propriétés 1. à 8. sont élémentaires et leur vérification est laissée au lecteur.

Définissons la matrice élémentaire $E_{i,j}$ : c'est la matrice dont tous les coefficients sont nuls sauf le coefficient $(i, j)$ qui est égal à 1. Il est clair que

$$A = \sum_{\substack{1 \le i \le \ell \\ 1 \le j \le n}} a_{i,j} E_{i,j}$$

et que cette expression de $A$ comme combinaison linéaire des matrices $E_{i,j}$ est unique. Par conséquent, l'ensemble des matrices élémentaires $E_{i,j}$ est une base de $\mathcal{M}_{\ell,n}(\mathbb{K})$ (appelée la base canonique) et en particulier $\dim(\mathcal{M}_{\ell,n}(\mathbb{K})) = \ell n$. □

Maintenant, on va définir une opération de *multiplication* entre matrices, qui est plus subtile et compliquée.

**Définition 5.2.3.** Soit $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$ et $B \in \mathcal{M}_{n,p}(\mathbb{K})$. Le produit $C = AB$ de $A$ et $B$ est la matrice de $\mathcal{M}_{\ell,p}(\mathbb{K})$ définie par :

$$C = (c_{i,j})_{\substack{1\leq i\leq \ell,\\ 1\leq j\leq p}} \text{ où } c_{i,j} = \sum_{k=1}^{n} a_{i,k}b_{k,j}.$$

**Remarque 5.2.4.** Il faut bien noter que le produit de $A$ par $B$ n'est défini que pour des matrices $A$ et $B$ telles que le nombre de colonnes de $A$ soit égal au nombre de lignes de $B$. Autrement dit, le produit de $A$ et $B$ n'existe que si $A$ est de type $(\ell, n)$ et $B$ est de type $(n, p)$ et dans ce cas le produit est de type $(\ell, p)$.

**Exemple 5.2.5.**

1. Le produit de $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$ par une matrice ligne à gauche (i.e. de type $(1, \ell)$) ; le résultat est la combinaison linéaire des lignes de $A$ par les coefficients de la matrice ligne :

$$(x_1, x_2, \ldots, x_\ell)\begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{\ell,1} & a_{\ell,2} & \ldots & a_{\ell,n} \end{pmatrix} = (\sum_{k=1}^{\ell} x_k a_{k,1}, \sum_{k=1}^{\ell} x_k a_{k,2}, \ldots, \sum_{k=1}^{\ell} x_k a_{k,n})$$
$$= x_1 L_1 + x_2 L_2 + \cdots + x_\ell L_\ell.$$

2. Le produit de $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$ par une matrice colonne à droite (i.e. de type $(n, 1)$) ; le résultat est la combinaison linéaire des colonnes de $A$, par les coefficients de la matrice colonne :

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{\ell,1} & a_{\ell,2} & \ldots & a_{\ell,n} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{k=1}^{n} a_{1,k}x_k \\ \sum_{k=1}^{n} a_{2,k}x_k \\ \vdots \\ \sum_{k=1}^{n} a_{n,k}x_k \end{pmatrix}$$
$$= x_1 C_1 + x_2 C_2 + \cdots + x_n C_n.$$

**Proposition 5.2.6.** La multiplication des matrices vérifie les propriétés suivantes :

1. Pour tout $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$, $\mathbf{0}A = A\mathbf{0} = \mathbf{0}$, $I_\ell A = AI_n = A$.
2. Pour tout $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$, $B \in \mathcal{M}_{n,p}(\mathbb{K})$, $C \in \mathcal{M}_{p,q}(\mathbb{K})$, $(AB)C = A(BC)$ (associativité de la multiplication)).
3. Pour tout $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$, $B \in \mathcal{M}_{n,p}(\mathbb{K})$, $C \in \mathcal{M}_{n,p}(\mathbb{K})$, $A(B + C) = AB + AC$ (distributivité de l'addition sur la multiplication).
4. Pour tout $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$, $B \in \mathcal{M}_{\ell,n}(\mathbb{K})$, $C \in \mathcal{M}_{n,p}(\mathbb{K})$, $(A + B)C = AC + BC$ (distributivité de l'addition sur la multiplication).
5. Pour tout $\lambda \in \mathbb{K}$, $A \in \mathcal{M}_{n,n}(\mathbb{K})$, $(\lambda I_n)A = A(\lambda I_n) = \lambda A$.
6. Pour tout $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$, $B \in \mathcal{M}_{n,p}(\mathbb{K})$, $(AB)^T = B^T A^T$.

**Remarque 5.2.7.** Attention, la multiplication des matrices n'est pas commutative, c'est-à-dire que l'on n'a pas, en général, pour des matrices carrées, $AB = BA$. Par exemple,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$$

alors que

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}.$$

**Notation.** Si $A$ est une matrice carrée de type $(n, n)$, i.e. si $A \in \mathcal{M}_n(\mathbb{K})$, on peut multiplier $A$ par elle-même autant de fois que l'on veut. On note $A^k$ le produit de $A$ par elle-même itéré $k$ fois, avec la convention $A^0 = I_n$.

## 5.3 Le rang d'une matrice

À une matrice $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$, on peut associer deux familles de vecteurs : ses lignes, qui sont des vecteurs de $\mathbb{K}^n$, et ses colonnes, qui sont des vecteurs de $\mathbb{K}^\ell$. Ces deux familles n'ont à priori rien en commun, puisque, en général, elles ne vivent même pas dans le même espace. Pourtant, on va voir un résultat remarquable qui dit qu'elles engendrent des sous-espaces vectoriels *de même dimension*.

**Théorème 5.3.1.** Soit $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$. Les sous-espaces vectoriels respectivement engendrés par les lignes de $A$ dans $\mathbb{K}^n$, et par les colonnes de $A$ dans $\mathbb{K}^\ell$, sont de même dimension. Cette dimension est appelée *le rang de la matrice* $A$ et est noté $\operatorname{rang}(A)$. En particulier, $\operatorname{rang}(A) \leq \min(\ell, n)$.

*Démonstration.* Notons $A = (a_{i,j})_{\substack{1 \leq i \leq \ell \\ 1 \leq j \leq n}}$, $\{L_1, \ldots, L_\ell\}$ ses lignes, $\{C_1, \ldots, C_n\}$ ses colonnes. Notons $E = \operatorname{Vect}(L_1, \ldots, L_\ell) \subset \mathbb{K}^n$, et $F = \operatorname{Vect}(C_1, \ldots, C_n) \subset \mathbb{K}^\ell$. Notre but est de montrer que $\dim(E) = \dim(F)$.

Soit $d = \dim(E)$ et soit $\{b_1, \ldots, b_d\}$ une base de $E$. Chacun des $b_i$ appartient à $\mathbb{K}^n$ ; notons $b_i = (b_{i,1}, \ldots, b_{i,n})$. Chacun des $L_i$ est combinaison linéaire des $b_j$. Notons $L_i = \sum_{j=1}^{d} \lambda_{i,j} b_j$. On a donc

$$A = \Lambda B \quad \text{avec} \quad \Lambda = (\lambda_{i,j}) \in \mathcal{M}_{\ell,d}(\mathbb{K}).$$

Maintenant, on regarde l'équation matricielle $A = \Lambda B$ du point de vue des colonnes. Cette équation signifie que les colonnes de $A$ sont combinaison linéaire des colonnes de $\Lambda$ avec les coefficients de la matrice $B$. En particulier, ces colonnes appartiennent à un sous-espace vectoriel engendré par $d$ vecteurs (les $d$ colonnes de $\Lambda$) donc elles appartiennent à un sous-espace vectoriel de dimension au plus $d$. Donc, $\dim(F) \leq d = \dim(E)$.

En remplaçant $A$ par $A^T$, on obtient l'autre inégalité $\dim(E) \leq \dim(F)$.

□

**Définition 5.3.2.** Le *rang* d'une famille de vecteurs d'un espace vectoriel $E$ est la dimension de l'espace vectoriel engendré par ses vecteurs.

Si $E = \mathbb{K}^n$, c'est donc le rang de la matrice dont les lignes (ou les colonnes) sont constituées de ces vecteurs.

On va décrire maintenant les transformations qu'on peut exécuter sur une famille de vecteurs sans changer son rang.

**Définition 5.3.3.** Soit $\{v_1, \dots, v_k\}$ une famille de vecteurs de $\mathbb{K}^n$. On appelle *opérations élémentaires* les transformations suivantes de la famille :

1. Échange de deux vecteurs
2. Remplacement d'un vecteur $v_i$ par $\lambda v_i$, pour $\lambda \in \mathbb{K}$, $\lambda \neq 0$.
3. Remplacement d'un vecteur $v_i$ par $v_i + \mu v_j$ pour $j \neq i$ et $\mu \in \mathbb{K}$.

Par extension, on définit les opérations élémentaires sur les lignes $L_1, \dots, L_\ell$ et les colonnes $C_1, \dots, C_n$ d'une matrice $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$ :

1. Échange de deux lignes (noté $L_i \leftrightarrow L_j$).
2. Multiplication d'une ligne par un scalaire non nul (noté $L_i \leftarrow \lambda L_i,\ \lambda \neq 0$).
3. Ajout à une ligne d'un multiple d'une autre ligne (noté $L_i \leftarrow L_i + \mu L_j$).

et, de même :

1. Échange de deux colonnes (noté $C_i \leftrightarrow C_j$).
2. Multiplication d'une colonne par un scalaire non nul (noté $C_i \leftarrow \lambda C_i,\ \lambda \neq 0$).
3. Ajout à une colonne d'un multiple d'une autre colonne (noté $C_i \leftarrow C_i + \mu C_j$, $\mu \in \mathbb{K}$).

**Proposition 5.3.4.** On ne change pas le sous-espace vectoriel engendré par une famille de vecteurs si on effectue une opération élémentaire (ou une succession de telles opérations) sur cette famille.

En particulier, on ne change pas le rang d'une matrice si on effectue une opération élémentaire (ou une succession de telles opérations) sur les lignes ou sur les colonnes d'une matrice.

*Démonstration.* Il est bien clair qu'un échange entre deux vecteurs ne va pas changer l'ensemble $\mathrm{Vect}(v_1, \dots, v_k)$ des combinaisons linéaires de $v_1, \dots, v_k$.

Soit $\lambda \neq 0$ ; comme $v_i = \lambda^{-1}(\lambda v_i)$, on a $v_i \in \mathrm{Vect}(v_1, \dots, \lambda v_i, \dots, v_k)$ ; bien sûr, $\lambda v_i \in \mathrm{Vect}(v_1, \dots, v_k)$, donc on a bien $\mathrm{Vect}(v_1, \dots, v_k) = \mathrm{Vect}(v_1, \dots, \lambda v_i, \dots, v_k)$.

Soit $\mu \in \mathbb{K}$ et $i \neq j$ ; soit $v_i' = v_i + \mu v_j$. Il est clair que $v_i' \in \mathrm{Vect}(v_1, \dots, v_k)$ ; on a aussi $v_i = v_i' - \mu v_j$ donc $v_i \in \mathrm{Vect}(v_1, \dots, v_i', \dots, v_k)$. On peut donc conclure que $\mathrm{Vect}(v_1, \dots, v_k) = \mathrm{Vect}(v_1, \dots, v_i', \dots, v_k)$.

□

L'algorithme du pivot de Gauss que nous avons déjà vu sur les systèmes linéaires peut s'effectuer sur les lignes (ou sur les colonnes) d'une matrice et permet, par une succession d'opérations élémentaires, de mettre une matrice sous forme échelonnée, et par conséquent de calculer efficacement le rang d'une famille de vecteurs, ou d'une matrice. Précisons ce que l'on entend par là :

**Définition 5.3.5.** Soit $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$. Pour tout $i = 1, \dots, \ell$, on note $j_i$ la position du premier coefficient non nul de la ligne $L_i$ (s'il y en a un ; si la ligne ne contient que des 0 on note $j_i = \infty$). On dit que $A$ est *ligne échelonnée* si on a : $j_1 < j_2 < \cdots < j_\ell$. Les coefficients $a_{i,j_i} \neq 0$, pour $j_i < \infty$, s'appellent les pivots de $A$.

On dit que $A$ est *ligne échelonnée réduite* si $A$ est ligne échelonnée, et si, de plus, pour tout $i = 1, \dots, \ell$, $a_{i,j_i} = 1$, et $a_{s,j_i} = 0$ pour $1 \leq s < j_i$.

On définit de façon analogue la notion de matrice *colonne échelonnée*, respectivement *colonne échelonnée réduite*.

**Théorème 5.3.6.** Le rang d'une matrice ligne échelonnée est égal au nombre de ses pivots, c'est à dire au nombre de ses lignes non nulles.

*Démonstration.* Supposons pour fixer les idées que la matrice soit ligne échelonnée, et soit $r$ l'indice de la dernière ligne non nulle. Alors, $\text{Vect}(L_1, \ldots, L_\ell) = \text{Vect}(L_1, \ldots, L_r)$. Il suffit donc de montrer que les $r$ lignes $L_1, \ldots, L_r$ sont linéairement indépendantes. Soit $(\lambda_1, \ldots, \lambda_r) \in \mathbb{K}^r$ tels que $\lambda_1 L_1 + \cdots + \lambda_r L_r = \mathbf{0}$. De cette équation vectorielle, on retient les $r$ équations linéaires correspondant aux pivots, c'està-dire aux coordonnées d'indice $j_1, j_2, \ldots, j_r$. Il est clair que le système correspondant est échelonné (après division par le coefficient du pivot qui est non nul) avec $r$ équations et $r$ inconnues donc il a une solution unique $(0, 0, \ldots, 0)$. □

## 5.4 Matrices carrées inversibles

**Définition 5.4.1.** Une matrice carrée $A \in \mathcal{M}_n(\mathbb{K})$ est dite *inversible* s'il existe une matrice $B \in \mathcal{M}_n(\mathbb{K})$ telle que $AB = BA = I_n$.

Afin de motiver cette définition, revenons aux systèmes linéaires. Un système linéaire

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= c_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= c_2 \\ & \vdots \\ a_{k,1}x_1 + a_{k,2}x_2 + \cdots + a_{k,n}x_n &= c_k \end{cases}$$

s'écrit matriciellement :

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{\ell,1} & a_{\ell,2} & \ldots & a_{\ell,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$$

soit, en posant $A = (a_{i,j})$, $x = (x_1, \ldots, x_n)^T$ et $c = (c_1, \ldots, c_n)^T$,

$$Ax = c.$$

Supposons maintenant que la matrice $A$ carrée soit inversible. Alors on voit facilement que

$$Ax = c \Leftrightarrow BAx = Bc \Leftrightarrow x = Bc.$$

Donc, le système linéaire a une unique solution qui est $x = Bc$. On est en train de reproduire la façon usuelle de résoudre une équation du premier degré dans $\mathbb{K}$ : $ax = c \Leftrightarrow x = a^{-1}c$.

On va maintenant donner une caractérisation des matrices inversibles par leur rang.

**Théorème 5.4.2.** Soit $A \in \mathcal{M}_n(\mathbb{K})$. Les propriétés suivantes sont équivalentes :

1. $A$ est inversible.
2. Il existe $B \in \mathcal{M}_n(\mathbb{K})$ telle que $AB = I_n$ *ou* il existe $B \in \mathcal{M}_n(\mathbb{K})$ telle que $BA = I_n$.
3. $\text{rang}(A) = n$.

De plus, si $A$ est inversible, il existe une unique matrice $B$ telle que $AB = BA = I_n$. On dit que $B$ est l'inverse de $A$ et on note $B = A^{-1}$.

**Remarque 5.4.3.** Il faut bien comprendre la différence entre les points 1. et 2. Dans 2., on fait l'hypothèse à priori plus faible que $A$ a un inverse *à droite* ou bien *à gauche*. L'équivalence entre 1. et 2. signifie que si on a $AB = I_n$, alors l'égalité $BA = I_n$ est automatiquement vérifiée.

*Démonstration.* On montre les implications $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$. L'implication $1 \Rightarrow 2$ est triviale.

Pour montrer $2 \Rightarrow 3$, on montre d'abord le résultat général suivant, valable pour des matrices quelconques :

$$\text{rang}(MN) \leq \min(\text{rang}(M), \text{rang}(N))$$

En effet, les lignes de $MN$ sont des combinaisons linéaires des lignes de $N$ donc l'espace vectoriel qu'elles engendrent est contenu dans l'espace vectoriel engendré par les lignes de $N$ donc $\text{rang}(MN) \leq \text{rang}(N)$. En raisonnant avec les colonnes, on obtient que $\text{rang}(MN) \leq \text{rang}(M)$. Notons qu'on utilise ici de façon déterminante le théorème 5.3.1.

Revenons maintenant à la démonstration de $2 \Rightarrow 3$. Si $AB = I_n$, on a $n = \text{rang}(I_n) = \text{rang}(AB) \leq \text{rang}(A)$ donc $n \leq \text{rang}(A)$.

Montrons maintenant que $3 \Rightarrow 1$. Soit $B$ une matrice carrée de taille $n$ et de colonnes $b_1, \ldots, b_n$. Soit $\epsilon_1, \ldots, \epsilon_n$ les colonnes de $I_n$. On a $AB = I_n$ si et seulement si, pour tout $j = 1, \ldots, n$, $Ab_j = \epsilon_j$. Le vecteur $b_j$ s'obtient donc comme solution d'un système linéaire de matrice $A$ ; comme $A$ est de type $(n, n)$ et de rang $n$, ce système est équivalent à un système triangulaire qui a donc une solution unique. Donc il existe bien une matrice $B$ telle que $AB = I_n$. Le même raisonnement appliqué à $A^T$ montre l'existence d'une matrice $C$ telle que $CA = I_n$. En multipliant à gauche par $C$ l'égalité $AB = I_n$ on obtient $C(AB) = C$ soit $(CA)B = C$ soit $B = C$ puisque $CA = I_n$. On a bien montré que $A$ est inversible.

Au passage on a bien montré l'unicité de l'inverse : si $AB = BA = I_n$ et $AC = CA = I_n$ alors $B = C$. □

**Exemple 5.4.4.**

1. Inverse d'une matrice diagonale :

$$A = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$$

est inversible si et seulement si $d_i \neq 0$ pour tout $i$, et

$$A^{-1} = \begin{pmatrix} d_1^{-1} & & \\ & \ddots & \\ & & d_n^{-1} \end{pmatrix}$$

2. Inverse d'une matrice $(2, 2)$ :

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

$A$ est inversible si et seulement si $ad - bc \neq 0$ et

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

**Proposition 5.4.5.** On note $\mathcal{G}\ell_n(\mathbb{K})$ l'ensemble des matrices carrée $(n, n)$ inversibles. On a les propriétés, si $A \in \mathcal{G}\ell_n(\mathbb{K})$, $B \in \mathcal{G}\ell_n(\mathbb{K})$ :

1. $I_n^{-1} = I_n$
2. $(A^{-1})^{-1} = A$
3. $(AB)^{-1} = B^{-1}A^{-1}$

**Calcul effectif de l'inverse d'une matrice :** Il suffit d'effectuer *simultanément* sur $A$ et $I_n$ des opérations élémentaires de lignes jusqu'à ce que $A$ soit transformée $I_n$. Alors $I_n$ est transformée en $A^{-1}$ ! En effet, effectuer une succession d'opérations sur les lignes d'une matrice revient à multiplier cette matrice à gauche par une certaine matrice $P$. Si on a $PA = I_n$ alors $P = A^{-1}$ et $PI_n = P$ est bien l'inverse de $A$. Alternativement on peut travailler sur les colonnes de $A$ et $I_n$ ce qui revient à multiplier à droite.

**Exemple 5.4.6.** On va calculer par cette méthode l'inverse de la matrice

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

$$\begin{array}{cccccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{array}$$

$$\begin{array}{cccccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & -2 & -1 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{array} \quad L_2 \leftarrow L_2 - L_1$$

$$\begin{array}{cccccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \\ 0 & -2 & -1 & -1 & 1 & 0 \end{array} \quad L_2 \leftrightarrow L_3$$

$$\begin{array}{cccccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \\ 0 & 0 & -3 & -1 & 1 & 2 \end{array} \quad L_3 \leftarrow L_3 + 2L_2$$

$$\begin{array}{cccccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1/3 & -1/3 & -2/3 \end{array} \quad L_3 \leftarrow -1/3 * L_3$$

$$\begin{array}{cccccc} 1 & 1 & 0 & 2/3 & 1/3 & 2/3 \\ 0 & 1 & 0 & 1/3 & -1/3 & 1/3 \\ 0 & 0 & 1 & 1/3 & -1/3 & -2/3 \end{array} \quad \begin{array}{l} L_1 \leftarrow L_1 - L_3 \\ L_2 \leftarrow L_2 + L_3 \end{array}$$

$$\begin{array}{cccccc} 1 & 0 & 0 & 1/3 & 2/3 & 1/3 \\ 0 & 1 & 0 & 1/3 & -1/3 & 1/3 \\ 0 & 0 & 1 & 1/3 & -1/3 & -2/3 \end{array} \quad L_1 \leftarrow L_1 - L_2$$

De ce calcul on peut conclure (et vérifier) que l'inverse de $A$ est

$$A^{-1} = \frac{1}{3} \begin{pmatrix} 1 & 2 & 1 \\ 1 & -1 & 1 \\ 1 & -1 & -2 \end{pmatrix}$$

# Chapitre 6

# Applications linéaires

Les applications linéaires sont les applications d'un espace vectoriel vers un autre espace vectoriel qui sont compatibles avec les opérations d'espaces vectoriel.

## 6.1 Définition et premières propriétés

**Définition 6.1.1.** Soit $(E, +, \cdot)$ et $(F, +, \cdot)$ deux $\mathbb{K}$-espaces vectoriels. Une *application linéaire* de $E$ dans $K$ est une application $f : E \to F$ vérifiant :

$$\text{Pour tout } (u, v) \in E^2,\ (\lambda, \mu) \in \mathbb{K}^2,\ f(\lambda u + \mu v) = \lambda f(u) + \mu f(v).$$

Si $f$ est un bijection, on dit que $f$ est un *isomorphisme d'espaces vectoriels.*

**Exemple 6.1.2.** Si $E = \mathbb{K}^n$ et $F = \mathbb{K}^\ell$, et si $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$, l'application

$$\begin{aligned} \mathbb{K}^n &\to \mathbb{K}^\ell \\ x \mapsto Ax = A &\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \end{aligned}$$

est une application linéaire.

**Remarque 6.1.3.** Une application linéaire envoie toujours le vecteur nul de $E$ sur le vecteur nul de $F$. En effet, $f(\mathbf{0}) = f(\mathbf{0} + \mathbf{0}) = f(\mathbf{0}) + f(\mathbf{0})$ donc $\mathbf{0} = f(\mathbf{0})$.

**Théorème 6.1.4.** Soit $(E, +, \cdot)$ un $K$-espace vectoriel de dimension finie $n$, et soit $\{e_1, \ldots, e_n\}$ une base de $E$. Alors, l'application :

$$\begin{aligned} K^n &\to E \\ (x_1, \ldots, x_n) &\mapsto x_1 e_1 + \cdots + x_n e_n \end{aligned}$$

est un isomorphisme d'espaces vectoriels.

*Démonstration.* Montrons que cette application, que l'on appellera $f$, est un application linéaire : soit $x = (x_1, \ldots, x_n) \in K^n$ et $y = (y_1, \ldots, y_n) \in K^n$.

$$\begin{aligned} f(\lambda x + \mu y) &= f((\lambda x_1 + \mu y_1, \ldots, \lambda x_n + \mu y_n)) \\ &= (\lambda x_1 + \mu y_1) e_1 + \cdots + (\lambda x_n + \mu y_n) e_n \\ &= \lambda(x_1 e_1 + \cdots + x_n e_n) + \mu(y_1 e_1 + \cdots + y_n e_n) = \lambda f(x) + \mu f(y). \end{aligned}$$

On a vu que si $\{e_1, \ldots, e_n\}$ est une base de $E$, alors tout vecteur de $E$ possède des coordonnées uniques dans cette base. Cela signifie exactement que l'application $f$ est une bijection. □

**Remarque 6.1.5.** Le théorème précédent est très important dans la pratique. En effet, il permet de ramener tous les problèmes d'algèbre linéaire dans un espace de dimension finie à un problème dans $\mathbb{K}^n$ *par le choix d'une base*, en le transposant aux vecteurs de coordonnées. Par exemple, si on veut savoir si une famille de vecteurs est libre, il suffit de considérer la famille des vecteurs de coordonnées, à laquelle on peut appliquer l'algorithme du pivot de Gauss ; en effet, c'est une conséquence immédiate du théorème qui suit.

**Théorème 6.1.6.** Soit $f : E \to F$ une application linéaire, et soit $\{e_1, \ldots, e_k\}$ une famille de vecteurs de $E$. Alors :

1. Si $\{e_1, \ldots, e_k\}$ est libre et si $f$ est injective, alors $\{f(e_1), \ldots, f(e_k)\}$ est libre.
2. Si $\{e_1, \ldots, e_k\}$ est génératrice de $E$ et si $f$ est surjective, alors $\{f(e_1), \ldots, f(e_k)\}$ est génératrice de $F$.
3. Si $\{e_1, \ldots, e_k\}$ est une base de $E$ et si $f$ est un isomorphisme, alors $\{f(e_1), \ldots, f(e_k)\}$ est une base de $F$.

*Démonstration.* 1. Supposons $\lambda_1 f(e_1) + \cdots + \lambda_k f(e_k) = \mathbf{0}$. On a donc $f(\lambda_1 e_1 + \cdots + \lambda_k e_k) = \mathbf{0} = f(\mathbf{0})$ et comme $f$ est injective on en déduit $\lambda_1 e_1 + \cdots + \lambda_k e_k = \mathbf{0}$. Comme $\{e_1, \ldots, e_k\}$ est libre, on peut conclure que $\lambda_1 = \cdots = \lambda_k = 0$.

2. Soit $y \in F$ ; comme $f$ est surjective, il existe $x \in E$ tel que $y = f(x)$. Comme $\{e_1, \ldots, e_k\}$ est génératrice de $E$, il existe $(x_1, \ldots, x_k) \in \mathbb{K}^k$ tels que $x = x_1 e_1 + \cdots + x_k e_k$. On en déduit que $y = f(x) = f(x_1 e_1 + \cdots + x_k e_k) = x_1 f(e_1) + \cdots + x_k f(e_k)$.

3. On applique les propriétés 1. et 2.

□

**Proposition 6.1.7.** On a les propriétés suivantes :

1. Si $f$ et $g$ sont des applications linéaires de $E$ dans $F$ et si $\lambda \in \mathbb{K}$, $\mu \in \mathbb{K}$, alors $\lambda f + \mu g$ est aussi une application linéaire de $E$ dans $F$. En particulier, l'ensemble $\mathcal{L}(E, F)$ des applications linéaires de $E$ dans $F$ est un $\mathbb{K}$-espace vectoriel.
2. Si $f : E \to F$ et $g : F \to G$ sont des applications linéaires alors $g \circ f : E \to G$ est encore une application linéaire.
3. Si $f : E \to F$ est un isomorphisme d'espaces vectoriels, alors $f^{-1} : F \to E$ est aussi un isomorphisme d'espaces vectoriels.

*Démonstration.* Il suffit de l'écrire. Démontrons en détails le point 3 : soit $(x, y) \in F^2$ et $(\lambda, \mu) \in \mathbb{K}^2$, on doit montrer que $f^{-1}(\lambda x + \mu y) = \lambda f^{-1}(x) + \mu f^{-1}(y)$. Par la surjectivité de $f$, il existe $(u, v) \in E^2$ tels que $x = f(u)$ et $y = f(v)$. Alors

$$f^{-1}(\lambda x + \mu y) = f^{-1}(\lambda f(u) + \mu f(v)) = f^{-1}(f(\lambda u + \mu v)) = \lambda u + \mu v.$$

□

**Exemple 6.1.8.** Si $f = f_A$ comme dans l'Exemple 6.1.2, on a $\lambda f_A + \mu f_B = f_{\lambda A + \mu B}$, $f_A \circ f_B = f_{AB}$, et $f_A$ est un isomorphisme si et seulement si $A$ est une matrice inversible, et dans ce cas, $f_A^{-1} = f_{A^{-1}}$.

## 6.2 Noyau et image d'une application linéaire

**Définition 6.2.1.** Soit $f : E \to F$ une application linéaire. On définit :

$$\mathrm{Ker}(f) = \{x \in E \mid f(x) = \mathbf{0}\}$$

et

$$\mathrm{Im}(f) = \{f(x) \mid x \in E\}.$$

**Théorème 6.2.2.** On a les propriétés suivantes :

1. $\mathrm{Ker}(f)$ est un sous-espace vectoriel de $E$.
2. $\mathrm{Im}(f)$ est un sous-espace vectoriel de $F$.
3. $f$ est injective si et seulement si $\mathrm{Ker}(f) = \{\mathbf{0}\}$.
4. $f$ est surjective si et seulement si $\mathrm{Im}(f) = F$.

*Démonstration.* Le vecteur nul appartient à $\mathrm{Ker}(f)$ car $f(\mathbf{0}) = \mathbf{0}$. Si $u$ et $v$ appartiennent à $\mathrm{Ker}(f)$ et $(\lambda, \mu) \in \mathbb{K}^2$, alors $f(\lambda u + \mu v) = \lambda f(u) + \mu f(v) = \lambda\mathbf{0} + \mu\mathbf{0} = \mathbf{0}$ donc $\lambda u + \mu v \in \mathrm{Ker}(f)$. On a démontré que $\mathrm{Ker}(f)$ est un sous-espace vectoriel de $E$.

Le vecteur nul appartient à $\mathrm{Im}(f)$ car $\mathbf{0} = f(\mathbf{0})$. Si $x$ et $y$ appartiennent à $\mathrm{Im}(f)$ alors il existe $(u, v) \in E^2$ tels que $x = f(u)$ et $y = f(v)$. Alors $\lambda x + \mu y = \lambda f(u) + \mu f(v) = f(\lambda u + \mu v) \in \mathrm{Im}(f)$. Donc $\mathrm{Im}(f)$ est un sous-espace vectoriel de $F$.

$\mathrm{Ker}(f)$ est l'image réciproque de $\{\mathbf{0}\}$ et contient $\mathbf{0}$, donc la condition $\mathrm{Ker}(f) = \{\mathbf{0}\}$ est clairement nécessaire pour que $f$ soit injective. Réciproquement, supposons $\mathrm{Ker}(f) = \{\mathbf{0}\}$ et montrons que $f$ est injective. Si $(u, v) \in E^2$ sont tels que $f(u) = f(v)$, alors $f(u) - f(v) = \mathbf{0}$ donc $f(u - v) = \mathbf{0}$ et $u - v \in \mathrm{Ker}(f)$. Par hypothèse $\mathrm{Ker}(f) = \{\mathbf{0}\}$, on peut donc conclure que $u - v = \mathbf{0}$ soit $u = v$.

Le point 4. n'est rien d'autre que la définition d'une application surjective. □

**Exemple 6.2.3.** Si $f = f_A$ avec $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$ comme dans l'Exemple 6.1.2, on a

$$\mathrm{Ker}(f_A) = \{x \in \mathbb{K}^n \mid Ax = \mathbf{0}\}.$$

Notons que $\mathrm{Ker}(f_A)$ est l'ensemble des solutions du système linéaire homogène de matrice $A$ et qu'on a déjà vu que c'est un sous-espace vectoriel de $\mathbb{K}^n$. On le note aussi $\mathrm{Ker}(A)$ et on dit que c'est *le noyau de $A$*.

On a $\mathrm{Im}(f_A) = \{Ax \mid x \in \mathbb{K}^n\}$ ; c'est donc l'ensemble des combinaisons linéaires des colonnes de la matrice $A$. On le note aussi $\mathrm{Im}(A)$ et on l'appelle *l'image de la matrice $A$*. C'est un sous-espace vectoriel de $\mathbb{K}^\ell$ et sa dimension est par définition le rang de la matrice $A$ :

$$\mathrm{Im}(f_A) = \mathrm{Im}(A) = \mathrm{Vect}(C_1, \ldots, C_n)$$

où $C_1, \ldots, C_n$ sont les colonnes de $A$.

On termine ce paragraphe par un théorème important sur les applications linéaires, il s'agit du *théorème du rang*.

**Théorème 6.2.4.** (Théorème du rang) Soit $E$ et $F$ deux $\mathbb{K}$-espaces vectoriels de dimension finie, et soit $f : E \to F$ une application linéaire. Alors,

$$\dim(\mathrm{Ker}(f)) + \dim(\mathrm{Im}(f)) = \dim(E).$$

*Démonstration.* Soit $n = \dim(E)$ et soit $k = \dim(\mathrm{Ker}(f))$. Soit $\{e_1, \dots, e_k\}$ une base de $\mathrm{Ker}(f)$. On complète cette base en une base $\{e_1, \dots, e_n\}$ de $E$. Alors,$\{f(e_{k+1}), \dots, f(e_n)\}$ forme une base de $\mathrm{Im}(f)$. En effet, c'est une famille génératrice de $\mathrm{Im}(f)$ car $f(e_1) = \cdots = f(e_k) = \mathbf{0}$. Montrons qu'elle est libre : supposons qu'il existe $\lambda_{k+1}, \dots, \lambda_n$ tels que $\lambda_{k+1}f(e_{k+1}) + \cdots + \lambda_n f(e_n) = \mathbf{0}$. Alors, $f(\lambda_{k+1}e_{k+1} + \cdots + \lambda_n e_n) = \mathbf{0}$, et on peut conclure que $\lambda_{k+1}e_{k+1} + \cdots + \lambda_n e_n \in \mathrm{Ker}(f)$. Comme $\{e_1, \dots, e_k\}$ est une base de $\mathrm{Ker}(f)$, il existe donc $\lambda_1, \dots, \lambda_k$ tels que $\lambda_{k+1}e_{k+1} + \cdots + \lambda_n e_n = \lambda_1 e_1 + \cdots + \lambda_k e_k$ ; mais alors, comme la famille $\{e_1, \dots, e_n\}$ est libre, on obtient que tous les $\lambda_i$, $i = 1, \dots, n$ sont nuls, donc que $\{f(e_{k+1}), \dots, f(e_n)\}$ est libre.

Puisque $\{f(e_{k+1}), \dots, f(e_n)\}$ forme une base de $\mathrm{Im}(f)$, la dimension de cet espace est égal au cardinal de cette base, soit $\dim(\mathrm{Im}(f)) = n - k = \dim(E) - \dim(\mathrm{Ker}(f))$. □

**Notation.** On note $\mathrm{rang}(f)$ (rang de $f$) la dimension de $\mathrm{Im}(f)$.

**Corollaire 6.2.5.** (Théorème du rang pour les matrices) Soit $A \in \mathcal{M}_{\ell,n}(\mathbb{K})$.

$$\dim(\mathrm{Ker}(A)) = n - \mathrm{rang}(A).$$

*Démonstration.* On applique le théorème du rang à $f = f_A$. □

## 6.3 Matrices d'une application linéaire

Dans cette section, nous allons faire le lien entre application linéaire et matrices. On ne considère plus que des espaces vectoriels de dimension finie.

Soit $E$ et $F$ deux $\mathbb{K}$-espaces vectoriels de dimensions respectives $n$ et $k$, et soit $\mathcal{B}_E = \{e_1, \dots, e_n\}$ une base de $E$. Si $x = x_1e_1 + \cdots + x_ne_n \in E$, alors par linéarité on a

$$f(x) = x_1 f(e_1) + \cdots + x_n f(e_n).$$

En particulier, cela signifie que *$f$ est uniquement déterminée par les images $f(e_1), \dots, f(e_n)$ de $e_1, \dots, e_n$ dans $F$.*

Si on fixe également une base $\mathcal{B}_F = \{f_1, \dots, f_k\}$ de $F$, les images $f(e_j)$ peuvent être exprimées sur la base $\mathcal{B}_F$. Notons $\begin{pmatrix} a_{1,j} \\ \vdots \\ a_{k,j} \end{pmatrix}$ les coordonnées de $f(e_j)$ dans la base $\mathcal{B}_F$, et $\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix}$ les coordonnées de $f(x)$ dans la base $\mathcal{B}_F$. Alors l'équation

$$f(x) = x_1 f(e_1) + \cdots + x_n f(e_n)$$

devient

$$\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} = x_1 \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{k,1} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{k,n} \end{pmatrix}$$

soit

$$\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{k,1} & \dots & a_{k,n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

La matrice qui apparait ci-dessus s'appelle *la matrice de $f$ dans les bases $\mathcal{B}_E$ et $\mathcal{B}_F$*. Résumons nous maintenant :

**Définition et Proposition 6.3.1.** *La matrice de $f$ dans les bases $\mathcal{B}_E$, $\mathcal{B}_F$*, notée $M_{\mathcal{B}_E,\mathcal{B}_F}(f)$, est la matrice de taille $(k,n)$ dont les colonnes sont les coordonnées dans la base $\mathcal{B}_F$ des images des vecteurs de la base $\mathcal{B}_E$.

Alors, si on note $X$ le vecteur colonne des coordonnées de $x$ dans la base $\mathcal{B}_E$, et $Y$ le vecteur colonne des coordonnées de $f(x)$ dans la base $\mathcal{B}_F$, on a

$$Y = M_{\mathcal{B}_E,\mathcal{B}_F} X.$$

Les opérations sur les applications linéaires se traduisent en des opérations matricielles :

**Théorème 6.3.2.** Soit $E$, $F$, $G$ trois $\mathbb{K}$-espaces vectoriels de dimensions finies. Soit $\mathcal{B}_E$, $\mathcal{B}_F$, $\mathcal{B}_G$ des bases de ces espaces.

1. Si $f$ et $g$ sont des applications linéaires de $E$ dans $F$ et si $\lambda \in \mathbb{K}$, $\mu \in \mathbb{K}$, alors
$$M_{\mathcal{B}_E,\mathcal{B}_F}(\lambda f + \mu g) = \lambda M_{\mathcal{B}_E,\mathcal{B}_F}(f) + \mu M_{\mathcal{B}_E,\mathcal{B}_F}(g).$$
2. Si $f : E \to F$ et $g : F \to G$ sont des applications linéaires, alors
$$M_{\mathcal{B}_E,\mathcal{B}_G}(g \circ f) = M_{\mathcal{B}_F,\mathcal{B}_G}(g) M_{\mathcal{B}_E,\mathcal{B}_F}(f)$$
3. Si $f : E \to F$ est un isomorphisme d'espaces vectoriels, alors $f^{-1} : F \to E$ est aussi un isomorphisme d'espaces vectoriels, et
$$M_{\mathcal{B}_F,\mathcal{B}_E}(f^{-1}) = \big(M_{\mathcal{B}_E,\mathcal{B}_F}(f)\big)^{-1}.$$

*Démonstration.* On démontre le point 2. Soit $x \in E$, $y = f(x) \in F$ et $z = g(y) = g \circ f(x)$. Soit $X$, $Y$, $Z$, les vecteurs colonne des coordonnées respectives de $x$, $y$, $z$ dans les bases $\mathcal{B}_E$, $\mathcal{B}_F$, $\mathcal{B}_G$. Alors :

$$Z = M_{\mathcal{B}_F,\mathcal{B}_G}(g) Y = M_{\mathcal{B}_F,\mathcal{B}_G}(g)\big(M_{\mathcal{B}_E,\mathcal{B}_F}(f) X\big) = \big(M_{\mathcal{B}_F,\mathcal{B}_G}(g) M_{\mathcal{B}_E,\mathcal{B}_F}(f)\big) X$$

donc

$$M_{\mathcal{B}_E,\mathcal{B}_G}(g \circ f) = M_{\mathcal{B}_F,\mathcal{B}_G}(g) M_{\mathcal{B}_E,\mathcal{B}_F}(f).$$

□

**Exemple 6.3.3.** Quelques exemples de matrices d'applications linéaires :

1. $M_{\mathcal{B}_E,\mathcal{B}_F}(\mathbf{0}) = \mathbf{0}$.
2. Si $E = F$ et $\mathcal{B}_E = \mathcal{B}_F$, alors $M(\mathrm{Id}) = I_n$.
3. Avec les notations du paragraphe précédent (exemple 6.1.2), dans les bases canoniques de $\mathbb{K}^n$ et de $\mathbb{K}^\ell$, $M(f_A) = A$.

## 6.4 Changement de base

Dans cette partie, $E$ est un espace vectoriel de dimension finie $n$ sur $\mathbb{K}$. Un vecteur donné de $E$ a plusieurs systèmes de coordonnées, suivant la base choisie. De même, la matrice d'une application linéaire dépend des bases choisies. On va voir comment effectuer calculatoirement ces changements.

Soit donc $\mathcal{B} = \{e_1, \ldots, e_n\}$ et $\mathcal{B}' = \{e'_1, \ldots, e'_n\}$ deux bases de $E$.

**Définition et Proposition 6.4.1.** La *matrice de changement de base de $\mathcal{B}$ à $\mathcal{B}'$*, encore appelée la *matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$* est la matrice $(n, n)$ dont les colonnes sont les coordonnées des vecteurs de $\mathcal{B}'$ (la nouvelle base) dans $\mathcal{B}$ (l'ancienne base).

Soit $x \in E$, soit $X$ et $X'$ les coordonnées de $x$ respectivement dans les bases $\mathcal{B}$ et $\mathcal{B}'$, et soit $P$ la matrice de changement de base de $\mathcal{B}$ à $\mathcal{B}'$, on a

$$X = PX'.$$

*Démonstration.* On obtient la relation annoncée à partir de l'égalité

$$x = x'_1 e'_1 + \cdots + x'_n e'_n,$$

en passant aux coordonnées dans la base $\mathcal{B}$. □

**Remarque 6.4.2.** Il est clair que la matrice $P$ de changement de base de $\mathcal{B}$ à $\mathcal{B}'$ est inversible (car elle est de rang $n$) et que son inverse $P^{-1}$ est la matrice de changement de base de $\mathcal{B}'$ à $\mathcal{B}$.

Soit maintenant $f : E \to F$ une application linéaire, on cherche une relation entre les matrices $M_{\mathcal{B}}(f)$ et $M_{\mathcal{B}'}(f)$.

**Proposition 6.4.3.** Soit $P$ la matrice de changement de base de $\mathcal{B}$ à $\mathcal{B}'$. On a

$$M_{\mathcal{B}'}(f) = P^{-1} M_{\mathcal{B}}(f) P.$$

*Démonstration.* On remarque que $P = M_{\mathcal{B}',\mathcal{B}}(\mathrm{Id})$ et que $P^{-1} = M_{\mathcal{B},\mathcal{B}'}(\mathrm{Id})$. On considère le diagramme :

$$\begin{array}{ccc} {}_{\mathcal{B}}E & \xrightarrow{\quad f \quad} & {}_{\mathcal{B}}E \\ \mathrm{Id}\uparrow & & \downarrow\mathrm{Id} \\ {}_{\mathcal{B}'}E & \xrightarrow[\quad f \quad]{} & {}_{\mathcal{B}'}E \end{array}$$

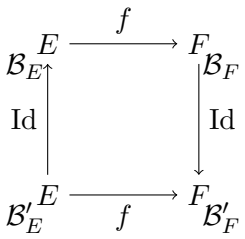
qui se traduit en termes matriciels, en appliquant le 2. du Théorème 6.3.2, par $M_{\mathcal{B}'}(f) = P^{-1} M_{\mathcal{B}}(f) P$.

□

**Remarque 6.4.4.** On peut donner de la même manière une formule pour le changement de bases plus générale, où $f : E \to F$, et où on change les bases à la fois dans $E$ et dans $F$. Plus précisément, si $\mathcal{B}_E$ et $\mathcal{B}'_E$ sont deux bases de $E$, si $P$ est la matrice de passage de $\mathcal{B}_E$ à $\mathcal{B}'_E$, si $\mathcal{B}_F$ et $\mathcal{B}'_F$ sont deux bases de $F$, si $Q$ est la matrice de passage de $\mathcal{B}_F$ à $\mathcal{B}'_F$, alors

$$M_{\mathcal{B}'_E,\mathcal{B}'_F}(f) = Q^{-1} M_{\mathcal{B}_E,\mathcal{B}_F}(f) P.$$

Pour obtenir cette formule, on considère le diagramme analogue


$f$
$E$
$F$
$\mathcal{B}_E$
$\mathcal{B}_F$
Id
Id
$E$
$F$
$\mathcal{B}'_E$
$f$
$\mathcal{B}'_F$

# Chapitre 7

# Compléments

## 7.1 Somme directe de sous-espaces vectoriels

Soit $(E, +, \cdot)$ un espace vectoriel et soit $U$ et $V$ deux sous-espaces vectoriels de $E$. On rappelle la notion de somme $U + V$ : c'est le sous-espace vectoriel de $E$ défini par :

$$U + V = \{u + v \mid u \in U, v \in V\}.$$

On a vu aussi que l'intersection $U \cap V$ est un sous-espace vectoriel de $E$ et on a démontré dans le cas de la dimension finie la formule (Chapitre 4, Théorème 4.3.11) :

$$\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V).$$

**Définition 7.1.1.** On dit que $E$ est *la somme directe de $U$ et $V$*, et on note $E = U \oplus V$, si les conditions suivantes sont réalisées :

1. $E = U + V$
2. $U \cap V = \{\mathbf{0}\}$

**Théorème 7.1.2.** Les conditions suivantes sont équivalentes :

(1) $E = U \oplus V$

(2) Tout vecteur $u \in E$ s'écrit *d'une façon unique* $u = x + y$ avec $x \in U$ et $y \in V$.

Si, en outre, $E$ est de dimension finie, alors on a équivalence de :

(3) $E = U \oplus V$

(4) $E = U + V$ et $\dim(E) = \dim(U) + \dim(V)$

(5) $U \cap V = \{0\}$ et $\dim(E) = \dim(U) + \dim(V)$.

*Démonstration.* Montrons d'abord l'équivalence de (1) et (2). Supposons $E = U \oplus V$, et soit $x \in E$. Comme $E = U + V$, on sait qu'il existe $u \in U$, $v \in V$ tels que $x = u + v$. S'il y avait deux décompositions de $x$, on aurait $x = u + v = u' + v''$ mais alors $u - u' = v' - v \in U \cap V$. L'hypothèse $U \cap V = \{\mathbf{0}\}$ montre que $u - u' = v' - v = \mathbf{0}$ donc $u = u'$ et $v = v'$.

Réciproquement, si (2) est vrai, alors on a bien sûr $E = U + V$. Il reste à montrer que $U \cap V = \{0\}$. Si $x \neq \mathbf{0}$, $x \in U \cap V$, on aurait deux décompositions de $\mathbf{0}$ en la somme d'un vecteur de $U$ et d'un vecteur de $V$ : $\mathbf{0} = \mathbf{0} + \mathbf{0} = x + (-x)$ ce qui contredirait (2).

Les équivalences de (3), (4), (5), se montrent avec la formule $\dim(U + V) = \dim(U) + \dim(V) = \dim(U \cap V)$. □

**Exercice :** Montrez que, si $E = U \oplus F$, la réunion d'une base de $U$ et d'une base de $V$ est une base de $E$.

## 7.2 Projections et symétries

La notion de somme directe de sous-espaces vectoriels nous permet de définir des applications linéaires de grande importance, qui sont les projections et les symétries.

**Définition 7.2.1.** Soit $E$ un $\mathbb{K}$-espace vectoriel, soit $U$ et $V$ deux sous-espaces vectoriels de $E$ tels que $E = U \oplus V$. La *projection sur $U$ parallèlement à $V$* est par définition l'application

$$\begin{aligned} p : E &\to E \\ x = u + v &\mapsto u \end{aligned}$$

Notons que, parce que $E = U \oplus V$, tout vecteur $x \in E$ a une unique décomposition sous la forme $x = u + v$ avec $u \in U$ et $v \in V$, et donc que l'application $p$ est définie sans ambiguité.

**Proposition 7.2.2.** Avec les notations de la définition précédente, $p$ est une application linéaire. Son noyau est $\mathrm{Ker}(p) = V$ et son image est $\mathrm{Im}(p) = U$. De plus $p$ vérifie $p \circ p = p$.

*Démonstration.* Soit $x = u + v$ et $x' = u' + v'$ deux vecteurs de $E$. Alors $\lambda x + \mu x' = (\lambda u + \mu u') + (\lambda v + \mu v')$ et, comme $u'' := \lambda u + \mu u' \in U$ et $v'' := \lambda v + \mu v' \in V$, par définition de $p$, on a $p(\lambda x + \mu x') = \lambda u + \mu u'$. Donc on a bien $p(\lambda x + \mu x') = \lambda p(x) + \mu p(x')$ et $p$ est linéaire.

On a bien $\mathrm{Ker}(p) = \{x = u + v \mid u = 0\} = V$ et $\mathrm{Im}(p) = \{p(x) \mid x \in E\} = U$. Finalement, pour tout $x \in E$, $(p \circ p)(x) = p(p(x)) = p(u) = u = p(x)$ donc $p \circ p = p$. □

**Remarque 7.2.3.** On peut montrer que, réciproquement, si $f$ est une application linéaire de $E$ dans $E$ telle que $f \circ f = f$, alors $f$ est une projection.

**Définition 7.2.4.** Soit $E$ un $\mathbb{K}$-espace vectoriel, soit $U$ et $V$ deux sous-espaces vectoriels de $E$ tels que $E = U \oplus V$. La *symétrie par rapport à $U$ parallèlement à $V$* est par définition l'application

$$\begin{aligned} s : E &\to E \\ x = u + v &\mapsto u - v \end{aligned}$$

**Proposition 7.2.5.** Avec les notations de la définition précédente, $s$ est une application linéaire, qui vérifie $s \circ s = \mathrm{Id}$. En particulier, $s$ est un isomorphisme. De plus, $U = \{x \in E \mid s(x) = x\} = \mathrm{Ker}(s - \mathrm{Id})$ et $V = \{x \in E \mid s(x) = -x\} = \mathrm{Ker}(s + \mathrm{Id})$.

*Démonstration.* On montre que $s$ est linéaire comme précédemment pour $p$. Pour tout $x \in E$, $(s \circ s)(x) = s(s(x)) = s(u - v) = u - (-v) = u + v = x$ donc on a bien $s \circ s = \mathrm{Id}$. Cette identité montre que $s$ est inversible d'inverse elle-même.

On a bien $s(x) = x \Leftrightarrow u - v = u + v \Leftrightarrow v = 0 \Leftrightarrow x \in U$. De la même façon $s(x) = -x \Leftrightarrow x \in V$. □

**Remarque 7.2.6.** On peut montrer que, réciproquement, si $f$ est une application linéaire de $E$ dans $E$ telle que $f \circ f = \mathrm{Id}$, alors $f$ est une symétrie.

## 7.3 Produit direct d'espaces vectoriels

Dans ce paragraphe, on suppose que $U$ et $V$ sont deux espaces vectoriels sur $\mathbb{K}$ quelconques. On va construire un nouvel espace vectoriel noté $U \times V$, tel que $U$ et $V$ soient isomorphes à des sous-espaces vectoriels de $U \times V$, et tel que $U \times V$ soit la somme directe de ces deux sous-espaces vectoriels.

**Définition et Proposition 7.3.1.** Soit $(U, +, \cdot)$ et $(V, +, \cdot)$ deux espaces vectoriels sur $\mathbb{K}$. Le produit cartésien $U \times V$ muni des opérations :

— Pour tout $(u, v) \in U \times V$, $(u', v') \in U \times V$, $(u, v) + (u', v') = (u + u', v + v')$

— Pour tout $\lambda \in \mathbb{K}$, $(u, v) \in U \times V$, $\lambda \cdot (u, v) = (\lambda \cdot u, \lambda \cdot v)$

est un espace vectoriel sur $\mathbb{K}$. On l'appelle *le produit direct de $U$ et $V$*.

*Démonstration.* Il faut vérifier les huit propriétés d'espace vectoriel. Le vecteur nul de $U \times V$ est la paire $(\mathbf{0}_U, \mathbf{0}_V)$ ; l'opposé de $(u, v)$ est $-(u, v) = (-u, -v)$. La vérification ne pose pas de difficultés, elle est laissée au lecteur. □

**Théorème 7.3.2.** Si $U$ et $V$ sont de dimension finie, alors $U \times V$ est aussi de dimension finie et $\dim(U \times V) = \dim(U) + \dim(V)$.

*Démonstration.* On vérifie facilement que, si $\{e_1, \ldots, e_k\}$ est une base de $U$ et $\{f_1, \ldots, f_n\}$ est une base de $V$, alors $\{(e_1, \mathbf{0}), \ldots, (e_k, \mathbf{0}), (\mathbf{0}, f_1), \ldots (\mathbf{0}, f_n)\}$ est une base de $U \times V$. □

**Exemple 7.3.3.** Un exemple facile : si $U = \mathbb{K}^k$ et $V = \mathbb{K}^n$ alors $U \times V = \mathbb{K}^k \times \mathbb{K}^n$ est clairement isomorphe à $\mathbb{K}^{k+n}$.

Les deux notions de somme directe et de produit direct d'espaces vectoriels sont étroitement liées. En effet, on peut démontrer facilement que (les démonstrations sont laissées en exercices) :

1. Si $U$ et $V$ sont des espaces vectoriels et si $E = U \times V$, on définit $U_1 = \{(u, 0) \in E \mid u \in U\}$ et $V_1 = \{(0, v) \in \times E \mid v \in V\}$. Alors $U_1$ est un sous-espace de $E$ isomorphe à $U$, $V_1$ est un sous-espace de $E$ isomorphe à $V$, et $E = U_1 \oplus V_1$.
2. Si $U$ et $V$ sont des sous-espaces vectoriels d'un même espace vectoriel $E$, tels que $E = U \oplus V$, alors l'application linéaire : $U \times V \to E$, $(u, v) \mapsto u + v$ est un isomorphisme.

## 7.4 Dualité

Dans cette section, on suppose que $E$ est un espace vectoriel de dimension finie $n$ et on va s'intéresser à l'espace $E^* := \mathcal{L}(E, \mathbb{K})$ des applications linéaires de $E$ dans $\mathbb{K}$. On a déjà vu que c'est un $\mathbb{K}$-espace vectoriel. On appelle cet espace *l'espace dual de $E$*.

**Exemple 7.4.1.** Supposons que $E = \mathbb{K}^n$. Soit $a_1, \ldots, a_n$ des éléments de $\mathbb{K}$. L'application

$$E \to \mathbb{K}$$
$$x = (x_1, \ldots, x_n) \mapsto a_1 x_1 + \cdots + a_n x_n$$

est un élément de $E^*$. En fait, tout élément $\varphi$ de $E^*$ est de cette forme, il suffit de prendre $a_1 = \varphi(\epsilon_1), \ldots, a_n = \varphi(\epsilon_n)$, et d'appliquer la propriété de linéarité :

$$\varphi(x) = \varphi(x_1\epsilon_1 + \cdots + x_n\epsilon_n) = x_1\varphi(\epsilon_1) + \cdots + x_n\varphi(\epsilon_n) = x_1 a_1 + \cdots + x_n a_n.$$

**Définition 7.4.2.** Soit $E$ un $\mathbb{K}$-espace vectoriel de dimension finie, et soit $\{e_1, \dots, e_n\}$ une base de $E$. On définit $\{e_1^*, \dots, e_n^*\}$ par :

$$\begin{aligned} e_k^* \ : \ E &\to \mathbb{K} \\ x = x_1 e_1 + \cdots + x_n e_n &\mapsto e_k^*(x) = x_k \end{aligned}$$

**Théorème 7.4.3.** La famille $\{e_1^*, \dots, e_n^*\}$ est une base de $E^*$, On l'appelle *la base duale* de la base $\{e_1, \dots, e_n\}$. En particulier, $\dim(E^*) = \dim(E)$.

*Démonstration.* On doit démontrer d'abord que $e_k^* \in E^*$, c'est-à-dire que $e_k^*$ est linéaire. En effet, si $x \in E$ et $y \in E$, on peut décomposer ces éléments sur la base $\{e_1, \dots, e_n\}$ : il existe $(x_1, \dots, x_n) \in \mathbb{K}^n$ tels que $x = x_1 e_1 + \cdots + x_n e_n$ et il existe $(y_1, \dots, y_n) \in \mathbb{K}^n$ tels que $y = y_1 e_1 + \cdots + y_n e_n$. Alors, pour tout $(\lambda, \mu) \in \mathbb{K}^2$, on a

$$\lambda x + \mu y = (\lambda x_1 + \mu y_1) e_1 + \cdots + (\lambda x_n + \mu y_n) e_n$$

et donc par définition $e_k^*(\lambda x + \mu y) = \lambda x_k + \mu y_k = \lambda e_k^*(x) + \mu e_k^*(y)$.

Montrons que $\{e_1^*, \dots e_n^*\}$ est une famille libre de $E^*$ : en effet, si $\lambda_1 e_1^* + \cdots + \lambda_n e_n^* = \mathbf{0}$, alors $(\lambda_1 e_1^* + \cdots + \lambda_n e_n^*)(x) = \mathbf{0}$ pour tout $x \in E$. On prend $x = e_k$ et on obtient $\lambda_k = 0$. Ceci vaut pour tout $k = 1, \dots, n$, donc la famille est bien libre.

Montrons que $\{e_1^*, \dots e_n^*\}$ est une famille génératrice de $E^*$ : Soit $\varphi \in E^*$, et $x = x_1 e_1 + \cdots + x_n e_n \in E$. Alors,

$$\begin{aligned} \varphi(x) &= \varphi(x_1 e_1 + \cdots + x_n e_n) \\ &= x_1 \varphi(e_1) + \cdots + x_n \varphi_n(e_n) \\ &= \varphi(e_1) e_1^*(x) + \cdots + \varphi(e_n) e_n^*(x) \end{aligned}$$

Ceci est valable pour tout $x \in E$, ce qui montre que $\varphi = \varphi(e_1) e_1^* + \cdots + \varphi(e_n) e_n^*$ et donc que $\varphi$ est bien une combinaison linéaire de $e_1^*, \dots, e_n^*$. □

**Remarque 7.4.4.** Si $\varphi \in E^*$, $\varphi \neq \mathbf{0}$, son image est $\mathbb{K}$ tout entier (puisque $\mathbb{K}$ est de dimension 1, $\mathrm{Im}(\varphi)$ ne peut pas être plus petit), donc son noyau est, par le théorème du rang, un sous-espace vectoriel de $E$ de dimension $n-1$ (on dit que c'est un espace *de codimension* 1, ou encore *un hyperplan*).

Réciproquement, tout sous-espace $H$ de $E$ de dimension $n-1$ est le noyau d'une forme linéaire. En effet, pour construire une telle forme, on peut procéder de la façon suivante : on choisit une base $\{h_1, \dots, h_{n-1}\}$ de $H$, que l'on complète par un vecteur $h_n$ pour en faire une base de $E$ ; alors, $H = \mathrm{Ker}(h_n^*)$.

Ainsi, on peut décrire un hyperplan soit en choisissant une base, c'est alors l'ensemble des combinaisons linéaires des éléments de la base choisie, soit comme le noyau d'une forme linéaire, qui est dans le cas $E = \mathbb{K}^n$ l'ensemble des solutions d'une équation linéaire. On va généraliser cela aux sous-espaces de dimension quelconque dans la prochaine proposition.

**Proposition 7.4.5.** Soit $F \subset E$ un sous-espace vectoriel de $E$ de dimension $k$. Alors, $F$ est égal à l'intersection de $n-k$ hyperplans.

Plus précisément, si $\{e_1, \dots, e_k\}$ est une base de $E$, et si on la complète en une base $\{e_1, \dots, e_k, e_{k+1}, \dots, e_n\}$ de $E$, alors

$$F = \mathrm{Ker}(e_{k+1}^*) \cap \cdots \cap \mathrm{Ker}(e_n^*).$$

**Remarque 7.4.6.** Dans le case où $E = \mathbb{K}^n$, on a donc montré que tout sous-espace vectoriel de $\mathbb{K}^n$ peut s'exprimer soit comme l'ensemble des combinaison linéaires d'une famille de vecteurs, soit comme l'ensemble des solutions d'un système linéaire. Ainsi, les deux exemples de sous-espaces vectoriels du chapitre 2 sont en fait les mêmes.

# Chapitre 8

# Arithmétique

## 8.1 L'anneau des entiers $\mathbb{Z}$

On a sur l'ensemble $\mathbb{Z}$ des entiers relatifs deux opérations : l'addition et la multiplication, et ces opérations vérifient les propriétés dites d'*anneau* :

- L'addition est commutative, associative, possède un élément neutre 0, et tout élément a un opposé dans $\mathbb{Z}$.
- La multiplication est commutative, associative, possède un élément neutre 1.
- La multiplication est distributive sur l'addition.

**Définition 8.1.1.** Soient $a$ et $b$ deux éléments de $\mathbb{Z}$. Si $b$ est non nul, on dit que $b$ *divise* $a$ ou que $a$ est un *multiple* de $b$, s'il existe un élément $q$ dans $\mathbb{Z}$ tel que $a = bq$. On utilise la notation $b|a$.

**Proposition 8.1.2.** On a les propriétés suivantes : soient $a$, $b$ et $c$ trois éléments de $\mathbb{Z}$ non nuls,

1. si $c$ divise $a$ et $b$, il divise toute expression de la forme $ua + vb$, où $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$, en particulier il divise $a + b$ et $a - b$ ;
2. si $c|b$ et $b|a$ alors $c|a$ ;
3. si $a|b$ et $b|a$ alors $a = \pm b$ ;
4. $1|a$ ;
5. $a|0$.

**Définition 8.1.3.** On dit qu'un entier naturel $n > 1$ est *premier* si ses seuls diviseurs positifs sont 1 et lui-même.

**Exemple 8.1.4.** Exemples de nombres premiers : 2, 3, 5, 10203986625631.

**Définition 8.1.5.** Division euclidienne dans $\mathbb{Z}$ : Pour tout couple d'entiers $(a, b)$ avec $b \neq 0$, il existe un unique couple d'entiers $(q, r)$ tels que

$$a = bq + r \quad \text{avec } 0 \leq r < |b|.$$

On dit que $q$ est *le quotient* et que $r$ est *le reste* de la division euclidienne de $a$ par $b$.

**Remarque 8.1.6.** Remarquons que $b$ divise $a$ si et seulement si le reste de la division de $a$ par $b$ est égal à 0.

**Définition 8.1.7.** Soit $(a, b) \neq (0, 0)$. On appelle *plus grand diviseur commun* de $a$ et $b$, le plus grand entier positif qui divise à la fois $a$ et $b$. On le note :

$$\text{pgcd}(a, b).$$

On pose $\text{pgcd}(0, 0) = 0$.
On dit que deux entiers $a$ et $b$ sont *premiers entre eux* si leur pgcd est égal à 1.

**Proposition 8.1.8.** Si $d = \text{pgcd}(a, b)$ alors il existe $(a', b') \in \mathbb{Z}^2$ tels que $a = da'$, $b = db'$ et $\text{pgcd}(a', b') = 1$

*Démonstration.* Puisque $d$ est un diviseur commun de $a$ et $b$ alors il existe $a'$, $b'$ tels que $a = da'$ et $b = db'$. Montrons que $a'$ et $b'$ sont premiers entre eux. En effet, sinon ils auraient un diviseur commun $d' > 1$ ; mais alors $dd'$ serait un diviseur de $a$ et $b$ plus grand que $d$ ce qui contredit l'hypothèse $d = \text{pgcd}(a, b)$. □

**Définition 8.1.9.** Soit $(a, b) \neq (0, 0)$. On appelle *plus petit commun multiple*, le plus petit entier positif qui soit multiple de $a$ et $b$. On le note :

$$\text{ppcm}(a, b).$$

**Proposition 8.1.10.** Soient $a$ et $b$ deux entiers non tous les deux nuls et $m$ leur ppcm. Alors, si $n$ est un multiple commun à $a$ et $b$, il est aussi multiple de $m$.

*Démonstration.* On effectue la division euclidienne de $n$ par $m$ : $n = mq + r$, $0 \leq r < m$. Alors $a|n$ et $a|m$ donc $a|r$ ; de même $b|r$. Ainsi, $r$, s'il est non nul, fournit un multiple commun à $a$ et $b$ strictement plus petit que $m$, une contradiction. □

**Définition 8.1.11.** Une *relation de Bézout* entre $a$ et $b$ est une relation de la forme

$$d = au + bv$$

où $d = \text{pgcd}(a, b)$ et $(u, v) \in \mathbb{Z}^2$.

## 8.2 Algorithme d'Euclide étendu et relation de Bézout

Dans ce paragraphe on discute de l'algorithme d'Euclide étendu, qui permet de calculer efficacement le pgcd de deux entiers ainsi qu'une relation de Bezout. En particulier, comme on va le voir, cet algorithme montre de façon constructive *l'existence* d'une relation de Bézout.

Soit donc $(a, b) \in \mathbb{Z}^2$. On suppose que $(a, b) \neq (0, 0)$, et, sans perte de généralité, que $a \geq b \geq 0$.

Soit $r_0, r_1, \ldots, r_k, \ldots$ la suite des restes obtenus par divisions euclidiennes successives à partir de $r_0 = a$, $r_1 = b$, et ce tant que $r_k \neq 0$ ; on a donc pour tout $k \geq 1$

$$r_{k-1} = r_k q_k + r_{k+1} \text{ avec } 0 \leq r_{k+1} < r_k$$

Remarquons d'abord que cette suite est finie, c'est-à-dire qu'au bout d'un nombre fini de divisions on obtient un reste nul. En effet, la suite $r_1, \ldots, r_k, \ldots$ est une suite d'entiers positifs ou nuls strictement décroissante donc elle ne peut qu'atteindre 0.

**Lemme 8.2.1.** Avec les notations précédentes, on a, pour tout $k \geq 1$, $\text{pgcd}(r_{k-1}, r_k) = \text{pgcd}(r_k, r_{k+1})$. En particulier, si $n$ est le plus grand indice tel que $r_n \neq 0$, alors $r_n = \text{pgcd}(a, b)$.

*Démonstration.* Soit $d_k = \text{pgcd}(r_k, r_{k+1})$, alors $d_k$ divise $r_k$ et $r_{k+1}$, donc il divise aussi $r_{k-1} = r_k q_k + r_{k+1}$. Donc on peut conclure que $d_k \leq d_{k-1}$. Mais on peut aussi faire le raisonnement inverse : $d_{k-1} \mid r_{k-1}$ et $d_{k-1} \mid r_k$ donc $d_{k-1}$ divise $r_{k+1} = r_{k-1} - r_k q_k$. Comme $d_{k-1}$ divise $r_k$ et $r_{k+1}$, on peut conclure que $d_{k-1} \leq d_k$.

On a donc démontré que $d_{k-1} = d_k$ pour tout $k = 1, \ldots, n+1$. Donc $d_0 = d_n$, et, comme $d_0 = \text{pgcd}(r_0, r_1) = \text{pgcd}(a, b)$ et $d_n = \text{pgcd}(r_n, 0) = r_n$, on obtient que $r_n = \text{pgcd}(a, b)$. □

Revenons maintenant à la relation $r_{k-1} = r_k q_k + r_{k+1}$. On peut exprimer cette relation par une relation matricielle :

$$\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix}.$$

En itérant cette formule, on obtient :

$$\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{k-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}}_{M_k} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

soit

$$\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = M_k \begin{pmatrix} a \\ b \end{pmatrix}.$$

On a pour les matrices $M_k$ :

$$M_k = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} M_{k-1}$$

ce qui montre que l'on peut poser

$$M_k = \begin{pmatrix} u_k & v_k \\ u_{k+1} & v_{k+1} \end{pmatrix}$$

avec

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{cases} u_{k+1} = u_{k-1} - u_k q_k \\ v_{k+1} = v_{k-1} - v_k q_k \end{cases}.$$

Finalement, on a pour $k = n - 1$,

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} u_{n-1} & v_{n-1} \\ u_n & v_n \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

et donc

$$r_n = a u_n + b v_n$$

qui est une relation de Bézout entre $a$ et $b$.

On résume nos conclusions sous la forme d'un algorithme dans le théorème suivant :

**Théorème 8.2.2.** Soit $(a, b) \in \mathbb{Z}^2$ tels que $a \geq b \geq 0$ et $(a, b) \neq (0, 0)$. Soit $r_k$, $q_k$, $u_k$ et $v_k$ les entiers calculés itérativement à partir des initialisations :

$$\begin{array}{lll} r_0 = a & u_0 = 1 & v_0 = 0 \\ r_1 = b & u_1 = 0 & v_1 = 1 \end{array}$$

par division euclidienne :

$$r_{k-1} = r_k q_k + r_{k+1} \text{ avec } 0 \leq r_{k+1} < r_k$$

et les formules

$$u_{k+1} = u_{k-1} - u_k q_k$$
$$v_{k+1} = v_{k-1} - v_k q_k$$

jusqu'à l'obtention d'un reste nul. Soit $r_n$ le dernier reste non nul. alors, $r_n$ est un pgcd de $a$ et $b$ et $r_n = au_n + bv_n$ est une relation de Bézout.

Dans la pratique, on calcule simultanément les nombres $r_k, q_k, u_k, v_k$ que l'on peut disposer dans un tableau, jusqu'à obtenir un reste nul.

**Exemple :** $a = 366$, $b = 56$.

| $r_k$ | $u_k$ | $v_k$ | $q_k$ | |
|---|---|---|---|---|
| 366 | 1 | 0 | | |
| 56 | 0 | 1 | 6 | $(366 = 6 * 56 + 30)$ |
| 30 | 1 | $-6$ | 1 | $(56 = 1 * 30 + 26)$ |
| 26 | $-1$ | 7 | 1 | $(30 = 1 * 26 + 4)$ |
| 4 | 2 | $-13$ | 6 | $(26 = 6 * 4 + 2)$ |
| 2 | $-13$ | 85 | 2 | $(4 = 2 * 2 + 0)$ |
| 0 | | | | |

On a trouvé : $\text{pgcd}(366, 56) = 2$ et $2 = 366 * -13 + 56 * 85$.

## 8.3 Conséquences du Théorème de Bézout

On a démontré, de façon constructive, au paragraphe précédent le théorème de Bézout :

**Théorème 8.3.1** (Théorème de Bézout)**.** Soit $(a, b) \in \mathbb{Z}^2$ et soit $d = \text{pgcd}(a, b)$. Il existe $(u, v) \in \mathbb{Z}^2$ tels que

$$d = au + bv.$$

*Démonstration.* Si $a = b = 0$ on peut prendre $u = v = 0$ puisqu'on a posé $\text{pgcd}(a, b) = 0$. Si $(a, b) \neq (0, 0)$, on peut toujours supposer $a \geq b \geq 0$ ; en effet, on a toujours $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$ et une relation de Bézout pour $|a|$ et $|b|$ fournit immédiatement une relation de Bézout pour $a$ et $b$ en ajustant les signes de $u$ et $v$.

Si $a \geq b \geq 0$, on applique l'algorithme d'Euclide étendu vu au paragraphe précédent. □

On va maintenant en déduire quelques conséquences importantes.

**Proposition 8.3.2.** Soit $d = \text{pgcd}(a, b)$. alors on a

$$c \mid a \text{ et } c \mid b \Longleftrightarrow c \mid d.$$

*Démonstration.* Seule l'implication $\Rightarrow$ n'est pas triviale. Pour la démontrer, on utilise une relation de Bézout $d = au + bv$. Si $c \mid a$ et $c \mid b$, alors $c \mid (au + bv)$ donc $c \mid d$. □

**Remarque 8.3.3.** La proposition précédente montre que le pgcd de $a$ et $b$ est le plus grand diviseur de $a$ et $b$ *au sens de la relation de divisibilité*. En d'autres termes, le point important est que si un entier $c$ est un diviseur commun de $a$ et $b$, on sait non seulement que (par définition) $c \leq \text{pgcd}(a,b)$, mais on peut conclure que $c$ *divise* $\text{pgcd}(a,b)$.

**Proposition 8.3.4.** Soit $(a,b) \in \mathbb{Z}^2$ ; ils sont premiers entre eux si et seulement s'il existe $(u,v)$ tels que $1 = au + bv$.

*Démonstration.* Si $\text{pgcd}(a,b) = 1$, le théorème de Bézout montre l'existence de $(u,v)$ tels que $1 = au + bv$. Réciproquement, si on a $1 = au + bv$, alors $d = \text{pgcd}(a,b)$ divise $a$ et $b$ donc divise $au + bv = 1$. Donc $d \mid 1$, soit $d = 1$. □

Le *Lemme de Gauss* est une conséquence importante du théorème de Bézout :

**Théorème 8.3.5** (Lemme de Gauss)**.** Soit $(a,b,c) \in \mathbb{Z}^3$. Si $a \mid bc$ et si $\text{pgcd}(a,b) = 1$ alors $a \mid c$.

*Démonstration.* Soit $1 = au + bv$ une relation de Bézout entre $a$ et $b$. On la multiplie par $c$ pour obtenir $c = acu + bcv$. Par hypothèse, $a \mid bc$, donc $a \mid bcv$. Comme $a$ divise aussi $acu$, on peut conclure que $a \mid (acu + bcv)$ et donc que $a \mid c$. □

**Remarque 8.3.6.** Attention, la conclusion du Lemme de Gauss n'est pas toujours vraie si on enlève l'hypothèse $\text{pgcd}(a,b) = 1$. Par exemple, 4 divise $6 * 10 = 60$ alors que 4 ne divise ni 6 ni 10.

**Corollaire 8.3.7.** Si $a \mid c$, si $b \mid c$, et si $\text{pgcd}(a,b) = 1$, alors $ab \mid c$.

*Démonstration.* Puisque $a \mid c$, il existe $q$ tel que $c = aq$. On a $b \mid c = aq$ et $\text{pgcd}(a,b) = 1$ donc par le Lemme de Gauss, $b \mid q$. Il existe donc $q'$ tel que $q = bq'$ ; alors $c = aq = abq'$ ce qui montre que $ab \mid c$. □

Une autre conséquence importante du Lemme de Gauss est la décomposition d'un nombre entier en produit de puissances de nombres premiers :

**Théorème 8.3.8.** Tout entier $a$ non nul s'écrit *de manière unique*

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

où les $p_i$ sont des nombres premiers vérifiant $p_1 < p_2 < \dots < p_k$ et les $\alpha_i$ sont des entiers strictement positifs.

*Démonstration.* Sans perte de généralité on se ramène à $a > 0$. L'existence d'une telle décomposition se démontre aisément par récurrence. En effet, si $a$ est premier on a fini, et sinon il possède un diviseur $d \neq 1, a$ ; alors $a = da'$ et on applique la récurrence à $a'$.

C'est l'unicité de la factorisation qui relève du Lemme de Gauss. En effet, si on a deux décompositions distinctes pour $a$ :

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_s^{\beta_s}$$

Si certains des $p_i$ et des $q_j$ sont égaux, on peut simplifier la deuxième égalité pour se ramener à ce qu'un nombre premier n'apparaisse que d'un côté de cette égalité. Alors, le nombre premier $p_1$ est distinct de chacun des $q_j$ ; mais deux nombres premiers distincts sont nécessairement premiers entre eux (ce qui n'est pas vrai pour des entiers quelconques) ce qui contredit le Lemme de Gauss. □