MAT 153: Introduction à l'algèbre linéaire I

Chapitre I: Corps

Les objets d'étude d'algèbre sont des systèmes algébrigues, c'est-à-dire, les ensembles dans lesquels on peut effectuer des opérations arithmétiques. Le premier genre de systèmes algébriques qu'on étudiera sont des corps. On commence par introduire et étudier le corps des nombres complexes. Remarquons que les nombres complexes sont utilisés dans plusieurs domaines des sciences appliquées comme la théorie du contrôle, la mécanique quantique et l'analyse du signal.

1.1. Nombres complexes

D'abord, rappelons un peu l'histoire des nombres. Considérons l'ensemble des nombres naturels

$$\mathbb{N} = \{0, 1, 2, \ldots, n, \ldots, \}.$$

Cet ensemble est stable pour l'addition et la multiplication (c'est-à-dire, $a + b, ab \in \mathbb{N}$ lorsque $a, b \in \mathbb{N}$) mais n'est pas stable pour la soustraction (par exemple, $1 - 2 \notin \mathbb{N}$ car pour tout $n \in \mathbb{N}, 2 + n > 1$). Après l'introduction des nombres négatifs, nous avons l'ensemble des nombres entiers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots, \pm n, \ldots, \}.$$

Ce dernier est stable pour l'addition, la soustraction et la multiplication. Mais encore une fois il n'est pas stable pour la division. Par exemple, $1 \div 2 \notin \mathbb{Z}$ car $2x \neq 1$ pour tout $x \in \mathbb{Z}$. On a donc introduit les fractions. En conséquence, on obtient l'ensemble des nombres rationnels

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0 \right\},$$

qui est stable pour l'addition, la soustraction, la multiplication et la division. De plus, en introduisant les nombres irrationnels, on obtient l'ensemble des nombres réels $\mathbb{R}$. Cet ensemble est encore stable pour ces opérations. Cependant, $\mathbb{R}$ n'est pas stable pour l'extraction de racine. Par exemple, $\sqrt{-1} \notin \mathbb{R}$. En effet, $a^2 \geq 0$, et donc $a^2 \neq -1$, pour tout $a \in \mathbb{R}$. Pour obtenir un ensemble des nombres qui est stable pour toutes les opérations arithmétiques ci-haut mentionées, on introduira les nombres complexes.

1.1.1. Définition. Un *nombre complexe*, ou bien *complexe*, est une expression formelle

$$z = a + bi, \quad a, b \in \mathbb{R},$$

où

(1) le symbol i s'appelle l'*unité imaginaire*;

(2) le nombre réel a s'appelle la *partie réelle* de z, notée $a = \mathrm{Re}(z)$;

(3) le nombre réel b s'appelle la *partie imaginaire* de z, notée $b = \mathrm{Im}(z)$.

En outre, deux nombres complexes $a + bi$ et $c + di$ sont dits *égaux* si $a = c$ et $b = d$.
L'ensemble des nombres complexes sera noté $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$.

Remarque. (1) Si $\mathrm{Re}(z) = 0$, on dit alors que z est *imaginaire pur,* et on note $z = bi$. Par exemple, $0 + 3i = 3i,\ 0 + \sqrt{2}i = \sqrt{2}i$.

(2) Pour brièveté, on écrit $1i = i$, et donc, $0 + 1i = i$.

(3) On identifie $a \in \mathbb{R}$ avec $a + 0i \in \mathbb{C}$. En particulier, $0 = 0 + 0i$. De ce point de vue, un nombre reél est un nombre complexe dont la partie imaginaire est nulle. Par conséquent, $\mathbb{R} \subseteq \mathbb{C}$.

Exercice. Trouver $a, b \in \mathbb{R}$ tels que $(a^2 - a) + (a + b^2)i = i$.

On définira les opérations arithmétiques pour les nombres complexes.

1.1.2. Addition. Pour $z = a + bi, w = c + di \in \mathbb{C}$, on définit la *somme* de z et w par

$$z + w = (a + c) + (b + d)i.$$

Remarque. Le nombre complexe $a + bi$ est la somme du nombre réel a et le nombre imaginaire pur bi. En effet,

$$(a) + (bi) = (a + 0i) + (0 + bi) = (a + 0) + (0 + b)i = a + bi.$$

Le résultat suivant est évident.

1.1.3. Proposition. Soient $z, w, v \in \mathbb{C}$.

(1) (commutativité) $z + w = w + z$.

(2) (associativité) $(z + w) + v = z + (w + v)$.

(3) (neutralité) $z + 0 = z$.

Remarque. (1) $0 + z = z$, pour tout $z \in \mathbb{C}$.

(2) Grâce à l'associativité, on définit la somme de trois complexes z, w et v par

$$z + w + v = (z + w) + v.$$

(3) Plus généralement, pour $z_1, z_2, \cdots, z_n \in \mathbb{C}$ avec $n > 2$, on définit

$$z_1 + z_2 + \cdots + z_n = (\cdots((z_1 + z_2) + z_3) + \cdots + z_{n-1}) + z_n.$$

1.1.4. Proposition. Si $z = a + bi \in \mathbb{C}$, alors

$$-z = (-a) + (-b)i,$$

appelé l'*opposé* de z, est le seul nombre complexe tel que $z + (-z) = 0$.

Démonstration. Il est evident que $z+(-z) = 0$. Si $w = c+di \in \mathbb{C}$ est tel que $z+w = 0$, alors $a + c = 0$ et $b + d = 0$. D'où $c = -a$ et $d = -b$. C'est-à-dire, $w = -z$. Ceci achève la démonstration.

Remarque. (1) Pour tout $z \in \mathbb{C}$, on a $(-z) + z = 0$.

(2) Pour tout $b \in \mathbb{R}$, on a $-(bi) = (-b)i$.

1.1.5. La loi de simplification. Soient $z, w, v \in \mathbb{C}$. Si $z + v = z + w$, alors $v = w$.

Démonstration. Supposons que $z + v = z + w$. Alors $(-z) + (z + v) = (-z) + (z + w)$. Il découle de l'associativité que $((-z) + z) + w = ((-z) + z) + v$. Ainsi $0 + w = 0 + v$, et donc $v = w$. Ceci achève la démonstration.

La soustraction de nombres complexes est définie dans le résultat suivant.

1.1.6. Proposition. Si $z, w \in \mathbb{C}$, alors il existe un unique $v \in \mathbb{C}$ tel que $w + v = z$. Dans ce cas, on écrit $v = z - w$, appelé *différence* entre z et w.

Démonstration. Posant $v = (-w) + z$, on a

$$w + v = w + ((-w)) + z) = (w + (-w)) + z = 0 + z = z.$$

En outre, si v_1 est un autre nombre complexe tel que $w + v_1 = z = w + v$, alors $v_1 = v$ d'après la proposition 1.1.5. Ceci achève la démonstration.

Remarque. (1) Si $z = a + bi, w = c + di \in \mathbb{C}$, alors

$$z - w = z + (-w) = (a - c) + (b - d)i.$$

(2) Si $z, w \in \mathbb{C}$, alors $z - w = 0$ si et seulement si $z = w$.
(3) Si $a, b \in \mathbb{R}$, alors $a + (-b)i = (a) - (bi)$.

1.1.7. Multiplication. Pour $z = a + bi, w = c + di \in \mathbb{C}$, on définit le *produit* de z et w, noté $z \cdot w$, par

$$z \cdot w = (ac - bd) + (ad + bc)i.$$

Remarque. (1) Si $a, b \in \mathbb{R}$, alors $a \cdot b = ab$.
(2) Pour brièveté, on écrit $zw = z \cdot w$.
(3) Si $a, b \in \mathbb{R}$, alors $a + bi = a + b \cdot i$.

Exemple. $i \cdot i = -1$.

On rassemble des propriétés de la multiplication de nombres complexes dans la proposition suivante.

1.1.8. Proposition. Soient $z, w, v \in \mathbb{C}$.
(1) (commutativité) $w \cdot z = z \cdot w$.
(2) (associativité) $(z \cdot w) \cdot v = z \cdot (w \cdot v)$.
(3) (distributivité) $z \cdot (w \pm v) = z \cdot w \pm z \cdot v$.
(4) (neutralité) $1 \cdot z = z$.
(5) $(-1)z = -z$.
(6) $z \cdot w = 0$ si et seulement si $z = 0$ ou $w = 0$.
(7) Si $z \cdot u = z \cdot v$ et $z \neq 0$, alors $u = v$.

Démonstration. Les premiers cinq énoncés découlent facilement des propriétés des nombres réels. On vérifiera seulement les deux derniers énoncés.

(6) Supposons que $z = a + bi$ et $w = c + di$, où $a, b, c, d \in \mathbb{R}$. Si $z \cdot w = 0$, d'après la définition, $ac - bd = 0$ et $ad + bc = 0$. Supposons que $z \neq 0$. Alors $a \neq 0$ ou $b \neq 0$, d'où $a^2 + b^2 \neq 0$ car a, b sont réels. Maintenant, $a^2c - abd = 0$ et $bad + b^2c = 0$. Ceci nous donne $(a^2 + b^2)c = 0$. Comme $a^2 + b^2 \neq 0$, on a $c = 0$. Par conséquent, $ad = 0$ et $bd = 0$. Alors $(a^2 + b^2)d = 0$, et donc, $d = 0$. Ceci montre que $w = 0$.

(7) Supposons que $z \neq 0$ et $zu = zv$. Alors $z(u - v) = zu - zv = 0$. D'après l'énoncé (6), $u - v = 0$, c'est-à-dire, $u = v$. Ceci achève la démonstration.

Remarque. (1) Dans la pratique, on calcule le produit en utilisant la distributivité et la règle $i \cdot i = -1$. En particulier, $r(a + bi) = (ra) + (rb)i$, pour tout $r \in \mathbb{R}$.

(2) Grâce à l'associativité, pour $z_1, z_2, \ldots, z_n \in \mathbb{C}$ avec $n > 2$, on définit

$$z_1 z_2 \cdots z_n = (\cdots((z_1 z_2) z_3) \cdots z_{n-1}) z_n.$$

En particulier, $zwv = z(wv)$.

1.1.9. Définition. Soient $w, z \in \mathbb{C}$ avec $z \neq 0$. Si $q \in \mathbb{C}$ est tel que $z \cdot q = w$, alors q est unique. Dans ce cas, q est appelé *quotient* de w par z et noté $q = \frac{w}{z}$.

On montrera que le quotient $\frac{w}{z}$ existe toujours pour tous $w, z \in \mathbb{C}$ avec z non nul. On commence par le cas spécial où r est réel.

1.1.10. Lemme. Soient $w = a + bi \in \mathbb{C}$ et soit $z \in \mathbb{C}$ non nul.
(1) Si $z = r \in \mathbb{R}$, alors

$$\frac{w}{z} = \frac{a+bi}{r} = \frac{a}{r} + \frac{b}{r}\, i.$$

(2) Si $v \in \mathbb{C}$ est non nul tel que $\frac{wv}{zv}$ existe, alors

$$\frac{w}{z} = \frac{wv}{zv}.$$

Démonstration. (1) Comme

$$r \cdot \left(\frac{a}{r} + \frac{b}{r} i\right) = \left(r \cdot \frac{a}{r}\right) + \left(r \cdot \frac{b}{r}\right) i = a + bi,$$

on a

$$\frac{a+bi}{r} = \frac{a}{r} + \frac{b}{r}\, i.$$

(2) Supposons que $v \neq 0$ tel que $\frac{wv}{zv}$ existe. Alors

$$wv = (zv) \cdot \frac{wv}{zv} = \frac{wv}{zv} \cdot (zv) = (\frac{wv}{zv} \cdot z)v.$$

Comme $v \neq 0$, d'après la proposition 1.1.8(7), on a

$$w = \frac{vw}{vz} \cdot z.$$

Ainsi

$$\frac{vw}{vz} = \frac{w}{z}.$$

Ceci achève la démonstration du lemme.

On étudiera comment calculer le quotient d'un complexe par un autre complexe non nul. Pour ce faire, on a besoin de la notion suivante.

1.1.11. Définition. Pour $z = a + bi \in \mathbb{C}$, on définit le *conjugué* de z, noté $\bar{z}$, par

$$\bar{z} = a - bi.$$

1.1.12. Proposition. Soient $z = a + bi, w = c + di \in \mathbb{C}$.
(1) $\bar{\bar{z}} = z$. (2) $\overline{w + z} = \bar{w} + \bar{z}$.
(3) $\overline{wz} = \bar{w}\bar{z}$. (4) $z\bar{z} = a^2 + b^2 \in \mathbb{R}$.
(5) $z = \bar{z}$ si, et seulement si, $z \in \mathbb{R}$.

Démonstration. On montrera seulement l'énoncé (5), car les autres sont faciles à vérifier. Si $z = a + bi \in \mathbb{R}$, alors $b = 0$. Ainsi $z = a$ et $\bar{z} = a - bi = a - 0i = a = z$. Réciproquement, supposons que $z = \bar{z}$, c'est-à-dire, $a + bi = a - bi$. Alors $b = -b$, et donc $2b = 0$. Par conséquent, $b = 0$, et ainsi, $z = a \in \mathbb{R}$. Ceci achève la démonstration.

1.1.13. Proposition. Soient $z = a + bi, w = c + di \in \mathbb{C}$. Si $z \neq 0$, alors $\dfrac{w}{z}$ existe et

$$\frac{w}{z} = \frac{w\bar{z}}{z\bar{z}} = \frac{ac + bd}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2}i.$$

Démonstration. Comme $w\bar{z} = (ac + bd) + (ad - bc)i$ et $\bar{z}z = a^2 + b^2$, on a

$$\frac{w\bar{z}}{z\bar{z}} = \frac{(ac + bd) + (ad - bc)i}{a^2 + b^2} = \frac{ac + bd}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2}i.$$

Maintenant il découle du lemme 1.1.10(2) que

$$\frac{w}{z} = \frac{w\bar{z}}{z\bar{z}} = \frac{ac + bd}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2}i.$$

Ceci achève la démonstration.

1.1.14. Définition. Si $z \in \mathbb{C}$ est non nul, alors $\dfrac{1}{z}$ est appelé *inverse* de z et noté z^{-1}.

1.1.15. Lemme. Soient $z, w \in \mathbb{C}$ avec $z \neq 0$.
(1) $z \cdot z^{-1} = 1$.
(2) $\frac{w}{z} = w \cdot z^{-1}$.
(3) Si $w \neq 0$, alors $(zw)^{-1} = z^{-1}w^{-1}$.

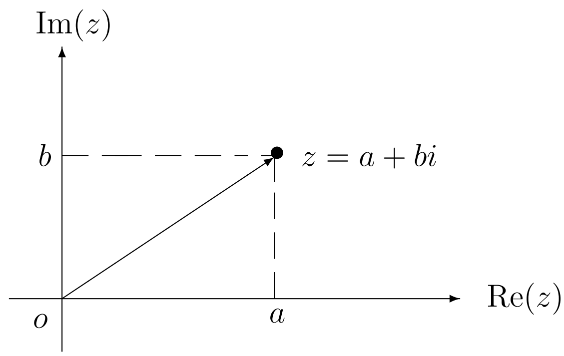
Démonstration. D'abord, dáprès la définition, on a $z \cdot z^{-1} = 1$. Ensuite, on a

$$(w \cdot z^{-1}) \cdot z = w(z^{-1} \cdot z) = w \cdot 1 = w.$$

Ainsi $\frac{w}{z} = w \cdot z^{-1}$. Si $w \neq 0$, alors $(zw)(z^{-1}w^{-1}) = z(ww^{-1})z^{-1} = zz^{-1} = 1$. D'où, $(zw)^{-1} = z^{-1}w^{-1}$. Ceci achève la démonstration.

1.2. Représentation géométrique

Il est bien connu que les nombres réels peuvent être représentés par les points d'un axe. D'une façon analogue, on aura une représentation géométrique des nombres complexes. Comme un nombre complexe dépend de deux invariants indépentants: la partie réelle et la partie imaginaire, on a besoin de deux axes dont l'un est horizontal et l'autre est vertical. L'axe horizontal est appelé *axe réel*, noté $\mathrm{Re}(z)$, et l'axe vertical est appelé *axe imaginaire*, noté $\mathrm{Im}(z)$. Le plan ainsi repéré s'appelle *plan complexe* ou *plan d'Argand*. Dans ce plan, on représente un nombre complexe $z = a + bi$ par le point (a, b), ou bien, par le vecteur de l'origine au point (a, b), et vice versa.



Remarque. Les nombres réels sont ordonnés de sorte que $a < b$ lorsque le point représentant a est à gauche du point représentant b. Cependant, il est impossible d'ordonner les nombres complexes d'une façon évidente. Par exemple, on n'a ni $1 < i$ ni $i < 1$.

1.2.1. Définition. Soit $z = a + bi \in \mathbb{C}$. Remarquant que $a^2 + b^2 \geq 0$, on définit le *module* de z par

$$|z| = \sqrt{a^2 + b^2},$$

la racine réelle non négative de $a^2 + b^2$.

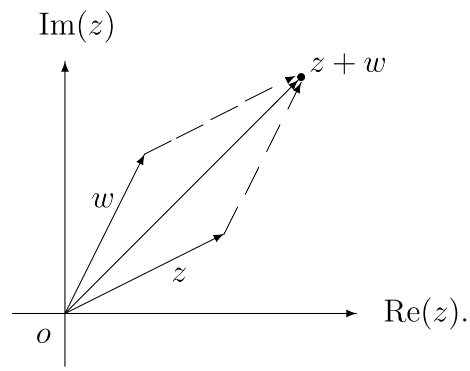
Remarque. (1) $|z|$ est la longueur du vecteur représentant z.
(2) Si $z \in \mathbb{R}$, alors $|z|$ est la valeur absolue de z.

1.2.2. Lemme. Soient $z, w \in \mathbb{C}$.

(1) $|z| = 0$ si et seulement si $z = 0$.

(2) (Inégalité du triangle) $|z + w| \leq |z| + |w|$.

Démonstration. Le premier énoncé est évident. Le deuxième énoncé découle du fait que $z + w$ est représenté par la somme des vecteurs représentant z et w. Ceci achève la démonstration.



La preuve s'achève.

Remarque. Dans le lemme 1.2.2(2), l'égalité peut avoir lieu.

1.2.3. Définition. Soit $z \in \mathbb{C}$ non nul. Un angle θ entre l'axe réel positif et le vecteur représentant z s'appelle *argument* de z, noté $\theta = \mathrm{Arg}(z)$.

Remarque. Si θ est un argument de z, alors $\theta + 2k\pi$ l'est aussi pour tout $k \in \mathbb{Z}$.

Exemple. (1) Comme 0 est un argument de 1, l'angle $2k\pi$ l'est aussi pour tout $k \in \mathbb{Z}$.

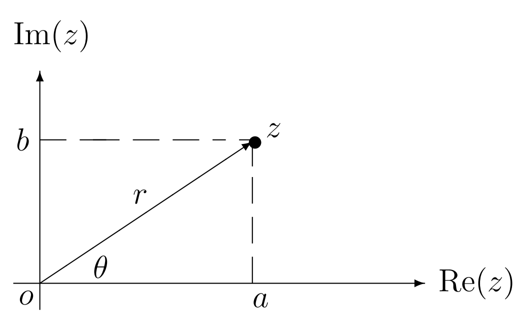
(2) Comme $\frac{\pi}{2}$ est un argument de i, l'angle $2k\pi + \frac{\pi}{2}$ l'est aussi, pour tout $k \in \mathbb{Z}$.

1.2.4. Forme polaire. Soit $z = a + bi \in \mathbb{C}$ non nul. Si θ est un argument et r est le module de z, alors

$$z = r(\cos\theta + i\sin\theta),$$

qui s'appelle une *forme polaire* de z.

Démonstration. L'hypothèse est illustrée par le diagramme suivant:



D'après la trigonométrie, on a $\cos\theta = \frac{a}{r}$ et $\sin\theta = \frac{b}{r}$. Ceci nous donne $a = r\cos\theta$ et $b = r\sin\theta$. Par conséquent, $z = r(\cos\theta + i\sin\theta)$. La preuve s'achève.

Remarque. (1) Ayant une infinité d'arguments, un complexe non nul a une infinité de formes polaires.

(2) Par contre, $z = a + bi$ avec $a, b \in \mathbb{C}$ s'appelle *forme algébrique* de z, ce qui est unique.

Afin de trouver une forme polaire d'un nombre complexe non nul, il sera utile de faire un petit rappel de la trigonométrie.

1.2.5. Proposition. Si θ, ϕ sont des angles, alors

(1) $\cos^2\theta + \sin^2\theta = 1$.

(2) $\cos(\theta + \phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$.

(3) $\sin(\theta + \phi) = \sin\theta\cos\phi + \cos\theta\sin\phi$.

(4) $\cos\theta = \cos\phi$ et $\sin\theta = \sin\phi$ si et seulement si $\theta = \phi + 2k\pi$ pour un certain $k \in \mathbb{Z}$.

On désignera par $\mathbb{R}^+$ l'ensemble des nombres réels strictement positifs.

1.2.6. Corollaire. Si $z = r(\cos\theta + i\sin\theta)$ avec $r \in \mathbb{R}^+$, alors il s'agit d'une forme polaire de z.

Démonstration. Comme $z = a + bi$ avec $a = r\cos\theta$ et $b = r\sin\theta$, on a

$$|z| = \sqrt{(r\cos\theta)^2 + (r\sin\theta)^2} = \sqrt{r^2} = |r| = r.$$

En outre, θ est un angle tel que $\cos\theta = \dfrac{a}{r}$, $\sin\theta = \dfrac{b}{r}$. Donc θ est un argument de z. Ceci achève la démonstration du lemme.

Remarque. Si $r, s \in \mathbb{R}^+$ et θ, ϕ sont des angles, alors $r(\cos\theta + i\sin\theta) = s(\cos\phi + \sin\phi)$ si et seulement si $r = s$ et $\phi - \theta = 2k\pi$ pour un certain entier k.

Voici un tableau du sinus et du cosinus de certains angles spéciaux dans le premier quadrant.

θ	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\cos\theta$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
$\sin\theta$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1

En appliquant la proposition 1.2.5 et le tableau ci-dessus, on obtient le résultat suivant qui nous permet de trouver le sinus et le cosinus des angles spéciaux dans les autres quadrants.

1.2.7. Proposition. Si θ est un angle, alors

(1) $\cos(\pi - \theta) = -\cos\theta$, $\quad \sin(\pi - \theta) = \sin\theta$;

(2) $\cos(\pi + \theta) = -\cos\theta$, $\quad \sin(\pi + \theta) = -\sin\theta$;

(3) $\cos(-\theta) = \cos\theta$, $\quad \sin(-\theta) = -\sin\theta$.

Exercice. Trouver l'angle θ avec $0 \le \theta \le 2\pi$ satisfaisant les conditions suivantes:

(1) $\cos\theta = -\frac{1}{2}$ et $\sin\theta = -\frac{\sqrt{3}}{2}$; (2) $\cos\theta = \frac{\sqrt{2}}{2}$ et $\sin\theta = -\frac{\sqrt{2}}{2}$.

Voici un procédé pour trouver une forme polaire d'un nombre complexe non nul.

1.2.8. Procédé pour trouver une forme polaire. Soit $z = a + bi$ un nombre complexe non nul.

1. Calculer le module $r = \sqrt{a^2 + b^2}$.
2. Trouver un angle ϕ entre 0 et $\frac{\pi}{2}$ tel que

$$\cos\phi = \frac{|\,a|}{\sqrt{a^2+b^2}}, \qquad \sin\phi = \frac{|\,b|}{\sqrt{a^2+b^2}}.$$

3. Trouver un argument θ de z par

$$\theta = \begin{cases} \phi, & \text{si } a \ge 0 \text{ et } b \ge 0. \\ \pi - \phi, & \text{si } a < 0 \text{ et } b \ge 0. \\ \pi + \phi, & \text{si } a < 0 \text{ et } b < 0. \\ 2\pi - \phi, & \text{si } a \ge 0 \text{ et } b < 0. \end{cases}$$

4. Enfin, $z = r(\cos\theta + i\sin\theta)$ est une forme polaire de z.

Exercice. Trouver une forme polaire de

(1) $z = 1 + i$; (2) $z = 1 - \sqrt{3}i$.

La forme polaire facilite les opérations arithmétiques des nombres complexes.

1.2.9. Proposition. Étant donnés deux nombres complexes sous la forme polaire $z = r(\cos\theta + i\sin\theta)$ et $w = s(\cos\phi + i\sin\phi)$.

(1) $zw = (rs)\,[\cos(\theta + \phi) + i\sin(\theta + \phi)]$.

(2) $\frac{z}{w} = \frac{r}{s}\,[\cos(\theta - \phi) + i\sin(\theta - \phi)]$.

Démonstration. (1) On a

$$\begin{aligned} zw &= (rs)(\cos\theta + i\sin\theta)(\cos\phi + i\sin\phi) \\ &= (rs)[(\cos\theta\cos\phi - \sin\theta\sin\phi) + i(\cos\theta\sin\phi + \sin\theta\cos\phi)] \\ &= (rs)[\cos(\theta+\phi) + i\sin(\theta+\phi)], \end{aligned}$$

où la dernière égalité découle de la proposition 1.2.5.

(2) Posons $v = \frac{r}{s}[\cos(\theta-\phi) + i\sin(\theta-\phi)]$. D'après la partie (1), on a

$$w \cdot v = (s \cdot \frac{r}{s})[\cos(\phi+\theta-\phi) + i\sin(\phi+\theta-\phi)] = r(\cos\theta + i\sin\theta) = z.$$

D'après la définition du quotient, on a $v = \frac{z}{w}$. Ceci achève la démonstration de la proposition.

Exercice. (1) Trouver une forme polaire de $\dfrac{1+i}{1-\sqrt{3}i}$ et de $(1+i)(1-\sqrt{3}i)$;

(2) Calculer $\cos\dfrac{\pi}{12}$ et $\sin\dfrac{\pi}{12}$.

L'énoncé suivante est une conséquence immédiate de la proposition précédente.

1.2.10. Corollaire. Soient $z, w \in \mathbb{C}$ non nuls.

(1) $|zw| = |z| \cdot |w|$;

(2) $\mathrm{Arg}(zw) = \mathrm{Arg}(z) + \mathrm{Arg}(w)$;

(3) $\left|\dfrac{z}{w}\right| = \dfrac{|z|}{|w|}$;

(4) $\mathrm{Arg}\dfrac{z}{w} = \mathrm{Arg}(z) - \mathrm{Arg}(w)$.

1.2.11. Puissance. Soit $z \in \mathbb{C}$. Pour $n \geq 1$, on définit

$$z^n = \overbrace{zz\cdots z}^{n \text{ fois}}.$$

Si $z \neq 0$, on définit $z^0 = 1$ par convention; et pour tout $n > 0$, on pose

$$z^{-n} = (z^{-1})^n.$$

Remarque. Pour tous $m, n \geq 1$, on a

$$z^{m+n} = z^m z^n \text{ et } (z^m)^n = z^{mn},$$

qui sont valides pour tous pour tous $m, n \in \mathbb{Z}$, lorsque $z \neq 0$.

Le résultat suivant nous dit comment calculer les puissances d'un nombre complexe en utilisant la forme polaire.

1.2.12. Théorème de de Moivre. Soit $z = r(\cos\theta + i\sin\theta) \in \mathbb{C}$ sous la forme polaire. Pour tout $n \in \mathbb{Z}$, on a

$$z^n = r^n(\cos n\theta + i\sin n\theta).$$

Démonstration. D'abord, on montre par récurrence que le théorème est vrai pour tout $n \geq 0$. C'est évident si $n = 0$. Supposons que $n \geq 0$ et le théorème est vrai pour n. Or

$$z^{n+1} = z^n z = (r^n r)\left(\cos(n\theta + \theta) + i\sin(n\theta + \theta)\right) = r^{n+1}[\cos(n+1)\theta + i\sin(n+1)\theta].$$

Ceci montre que le théorème est vrai pour tous les entiers non négatifs. En outre

$$z^{-1} = \frac{1}{z} = \frac{1(\cos 0 + i\sin 0)}{r(\cos\theta + \sin\theta)} = \frac{1}{r}\left(\cos(0-\theta) + \sin(0-\theta)\right) = r^{-1}\left(\cos(-\theta) + \sin(-\theta)\right).$$

Enfin, pour tout $n \geq 1$,

$$z^{-n} = (z^{-1})^n = \left(r^{-1}\left[\cos(-\theta) + \sin(-\theta)\right]\right)^n = r^{-n}\left(\cos(-n)\theta + i\sin(-n)\theta\right).$$

Ceci achève la démonstration.

Exercice. Calculer $(1+i)^{101}$.

1.2.13. Définition. Soient $z \in \mathbb{C}$ et $n \geq 1$ un entier. Si $w^n = z$, on dit que w est une *racine n-ième* de z. Si $n = 2$ ou 3, on dit que w est une *racine carrée* ou *cubique* de z, respectivement.

Exemple. (1) i et $-i$ sont deux racines carrées de -1 car $i^2 = (-i)^2 = -1$.

(2) Pour tout $n \geq 0$, le complexe nul 0 a la seule racine n-ième de 0.

Afin de montrer que tout nombre complexe admet des racines n-ièmes, on a besoin d'un lemme préparatoire suivant.

1.2.14. Lemme. Soit $n \geq 1$ un entier. Si $r \in \mathbb{R}^+$, alors il existe un unique $s \in \mathbb{R}^+$, noté $s = \sqrt[n]{r}$, tel que $s^n = r$. C'est-à-dire, $\sqrt[n]{r}$ est la seule racine n-ième de r dans $\mathbb{R}^+$.

Démonstration. Considérons la fonction $f(x) = x^n - r$ définie sur $[0, +\infty[$. Alors $f(0) = -r < 0$ et $f(r+1) = (r+1)^n - r \geq (r+1) - r > 0$. Comme f est continue, il existe s avec $0 < s < r+1$ tel que $f(s) = 0$, c'est-à-dire, $s^n = r$.

En outre, comme $f'(x) = nx^{n-1} > 0$ pour tout $x > 0$, $f(x)$ est strictement accroissante sur $[0, +\infty[$. Donc, si $t \in [0, +\infty[$ est tel que $s < t$ ou $t < s$, alors $0 = f(s) < f(t)$ ou $f(t) < f(s) = 0$. Ainsi s est unique tel que $f(s) = 0$. Ceci achève la preuve du lemme.

Exemple. Pour tout $n \geq 1$, on a $\sqrt[n]{1} = 1$.

On a besoin aussi de la propriété suivante des entiers.

1.2.15. Algorithme de division. Si $a, b \in \mathbb{Z}$ avec $b > 0$, alors il existe deux entiers uniques q et r tels que

$$a = bq + r, \ 0 \leq r < b.$$

Démonstration. On montrera premièrement l'existence de q et r. D'abord, supposons que $a \geq 0$. Pour tout entier $k \geq 0$, posons $r_k = a - bk$. Alors $r_{k+1} = r_k - b$. Ainsi on a une suite

$$r_0 > r_1 > \cdots > r_k > r_{k+1} > \cdots .$$

Comme $r_0 = a \geq 0$, il existe un entier $q \geq 0$ tel que $r_q \geq 0$, mais que $r_{q+1} < 0$, c'est-à-dire, $r_q - b < 0$. Posons $r = r_q$. Alors $a = bq + r$ avec $0 \leq r < b$. Supposons maintenant que $a < 0$. Comme $-a > 0$, on a $-a = bq + r$ avec $0 \leq r < b$. Donc $a = b(-q) - r$. Si $r = 0$, alors l'existence est prouvée. Si $r > 0$, alors $a = b(-q-1) + (b - r)$ avec $0 < b - r < b$. Ceci montre l'existence de q et r dans tous les cas.

On montrera maintenant l'unicité de q et r. Supposons que q_1 et r_1 sont deux autres entiers tels que $a = bq_1 + r_1, \ 0 \leq r_1 < b$. On peut supposer que $r_1 \leq r$. Alors $0 \leq r - r_1 = b(q_1 - q) < b$. Comme $b > 0$, on a $q_1 - q \geq 0$. Si $q_1 - q \neq 0$, alors $q_1 - q \geq 1$. Ceci implique que $b > r - r_1 = b(q_1 - q) \geq b$, une contradiction. Ainsi $q_1 - q = 0$ et donc $r_1 - r = 0$, c'est-à-dire, $q = q_1$ et $r = r_1$. Ceci achève la démonstration.

Remarque. (1) Les entiers q et r dans l'algorithme s'appellent le *quotient* et le *reste* de a divisé par b, respectivement. On note $q = q_b(a)$ et $r = r_b(a)$.

(2) Si $r_b(a) = 0$, on dit alors que b est un *diviseur* ou *facteur* de a.

Exercice. Trouver le quotient et le rest de -19 divisé par 5.

Voici la méthode pour trouver les racines n-ième complexes d'un complexe non nul.

1.2.16. Théorème. Soit $z = r(\cos\theta + i\sin\theta) \in \mathbb{C}$ sous la forme polaire. Si $n > 0$ est un entier, alors z admet exactement n racines n-ièmes

$$z_k = \sqrt[n]{r}\left(\cos\frac{\theta + 2k\pi}{n} + i\sin\frac{\theta + 2k\pi}{n}\right), \quad k = 0, 1, \ldots, n-1.$$

Démonstration. D'abord pour tout k avec $0 \leq k \leq n-1$,

$$z_k^n = (\sqrt[n]{r})^n\left(\cos\frac{(\theta + 2k\pi)n}{n} + i\sin\frac{(\theta + 2k\pi)n}{n}\right) = r(\cos\theta + i\sin\theta).$$

Donc $z_0, z_1, \ldots, z_{n-1}$ sont des racines n-ièmes de z.

Ensuite, supposons que $z_k = z_j$ pour certains j, k avec $0 \leq j \leq k < n$. Alors

$$\frac{\theta + 2k\pi}{n} - \frac{\theta + 2j\pi}{n} = \frac{2(k-j)\pi}{n} = 2l\pi, \text{ pour un certain } l \in \mathbb{Z}.$$

Comme $0 \leq \frac{2(k-j)\pi}{n} < 2\pi$, on a $l = 0$. D'où, $k = j$. Ceci montre que $z_0, z_1, \ldots, z_{n-1}$ sont deux à deux distincts.

Enfin, soit $w = s(\cos\phi + i\sin\phi)$ une racine n-ième de z. Alors $w^n = z$, c'est-à-dire, $s^n(\cos n\phi + i\sin n\phi) = r(\cos\theta + i\sin\theta)$. Donc $s^n = r$ et $n\phi = \theta + 2l\pi$ pour certain entier l. Comme $s > 0$, on a $s = \sqrt[n]{r}$. En outre, $\phi = \frac{\theta + 2l\pi}{n}$. D'après l'algorithme de division, $l = nq + k$, où $q, k \in \mathbb{Z}$ avec $0 \leq k \leq n-1$. D'où $\phi = \frac{\theta+2k\pi}{n} + 2q\pi$, et donc

$$w = \sqrt[n]{r}\left(\cos\frac{\theta + 2k\pi}{n} + i\sin\frac{\theta + 2k\pi}{n}\right) = z_k.$$

Ceci achève la démonstration.

Remarque. Dans le théorème 1.2.16, k peut parcourir n'importe quel ensemble de n entiers consécutifs.

Exercice. Trouver les racines carrées de i.

1.2.17. Corollaire. Pour tout $n \geq 1$, il y a exactement n racines n-ièmes de 1:

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad k = 0, 1, \ldots, n-1.$$

Les points du plan d'Argand représentant ces complexes partagent le cercle unité en secteurs égaux d'angle $\frac{2\pi}{n}$.

Remarque. Le complexe

$$\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

s'appelle *racine n-ième primitive de l'unité*, car les autres racines n-ièmes de 1 sont des puissances de ζ_n.

Rappelons que si a est un nombre réel, alors l'exponentielle de a est

$$e^a = \sum_{k=0}^{\infty} \frac{a^k}{k!}.$$

De la même façon, on définit l'*exponentielle* d'un nombre complexe z par

$$e^z = \sum_{k=0}^{\infty} \frac{z^k}{k!} = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{z^k}{k!}.$$

1.2.18. Proposition. (1) Si $z, w \in \mathbb{C}$, alors

$$e^{z+w} = e^z e^w.$$

(2) Si $\theta \in \mathbb{R}$, alors

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Démonstration. (1) D'abord, pour tout $k \geq 0$, d'aprés le théoréme du binôme, on a

$$(z+w)^k = \sum_{p=0}^{k} \binom{k}{p} z^p w^{k-p} = \sum_{p,q\geq 0;\, p+q=k} \frac{k!}{p\,!\,q!} z^p w^q.$$

Pour tous $n, m > 0$, on a

$$\sum_{p=0}^{n} \frac{z^p}{p\,!} \cdot \sum_{q=0}^{m} \frac{w^q}{q!} = \sum_{k=0}^{n+m} \sum_{p+q=k} \frac{z^p w^q}{p\,!\,q!} = \sum_{k=0}^{n+m} \frac{1}{k!} \sum_{p+q=k} \frac{k!}{p\,!\,q!} z^p w^q = \sum_{k=0}^{n+m} \frac{(z+w)^k}{k!}.$$

Lorsque n, m tendent vers l'infini, on obtient $e^{z+w} = e^z e^w$.
(2) Rappelons que

$$\cos\theta = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!}\,\theta^{2n}, \quad \sin\theta = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!}\,\theta^{2n+1}.$$

Or

$$\begin{aligned} e^{i\theta} &= \sum_{k=0}^{\infty} \frac{(i\theta)^k}{k!} = \sum_{n=0}^{\infty} \left(\frac{i^{2n}}{(2n)!}\,\theta^{2n} + \frac{i^{2n+1}}{(2n+1)!}\,\theta^{2n+1} \right) \\ &= \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!}\,\theta^{2n} + i \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!}\,\theta^{2n+1} = \cos\theta + i\sin\theta. \end{aligned}$$

Ceci achève la démonstration de la proposition.

Remarque. (1) Pour tout $\theta \in \mathbb{R}$, on voit que $e^{i\theta}$ se trouve sur le cercle unité.
(2) Si $z = a + bi$ est un complexe sous la forme algébrique, alors $e^{a+bi} = e^a(\cos b + i\sin b)$.

1.2.19. Définition. Soit $z = r(\cos\theta + i\sin\theta) \in \mathbb{C}$ sous la forme polaire. D'après la proposition 1.2.18(2), on a

$$z = re^{i\theta},$$

appelé *formule d'Euler* de z.

Exemple. Les racines n-ièmes de l'unité sont

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = e^{\frac{2k\pi}{n}i},\ k = 0, 1, \ldots, n-1.$$

1.3. Corps

Dans les sections précédentes, on a introduit les nombres complexes et étudié leurs opérations. On a vu que ces opérations satisfont à certains axiomes. Cet exemple nous conduit à la notion abstraire d'un corps.

1.3.1. Définition. Un *corps* est un ensemble non vide K muni d'une addition

$$+ : K \times K \to K : (a, b) \mapsto a + b$$

et d'une multiplication

$$\cdot : K \times K \to K : (a, b) \mapsto a \cdot b$$

telles que, pour tous $a, b, c \in K$,

L'addition satisfait aux axiomes suivants:

(1) (commutativité) $a + b = b + a$.

(2) (associativité) $a + (b + c) = (a + b) + c$.

(3) Il existe $0_K \in K$, appelé *zéro*, tel que $a + 0_K = a$ pour tout $a \in K$.

(4) Tout $a \in K$ a un *opposé* $-a \in K$ tel que $a + (-a) = 0_K$.

La multiplication satisfait aux axiomes suivants:

(5) (commutativité) $a \cdot b = b \cdot a$.

(6) (associativité) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(7) Il existe $1_K \neq 0_K$, appelé *identité*, tel que $1_K \cdot a = a$ pour tout $a \in K$.

(8) Tout $a \in K$ avec $a \neq 0_K$ a un *inverse* $a^{-1} \in K$ tel que $a \cdot a^{-1} = 1_K$.

Les deux opérations sont compatibles:

(9) (distributitvité) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Notation. S'il n'y pas de risque de confusion, on écrit $0 = 0_K,\ 1 = 1_K,\ a \cdot b = ab$.

Remarque. (1) Un corps a au moins deux éléments distincts, c'est-à-dire, 0 et 1.
(2) Un corps K a un seul zéro et un seul identité.
(3) 0_K est un opposé de 0_K, et 1 est un inverse de 1.
(4) On définit $a + b + c = (a + b) + c$.
(5) On définit la *soustraction* par $a - b = a + (-b)$.

Exemple. (1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps pour l'addition et la multiplication habituelles.
(2) $\mathbb{Z}$ n'est pas un corps pour les opérations usuelles.

Le résultat ramasse les propriétés élémentaires d'un corps.

1.3.2. Proposition. Soit K un corps avec $a, b, c \in K$.
(1) Si $a + b = a + c$, alors $b = c$.
(2) Tout élément a un seul opposé.
(3) $ab = 0_K$ si et seulement si $a = 0_K$ ou $b = 0_K$.
(4) $(-1_K)\, a = -a$.
(5) Si $ab = ac$ avec $a \neq 0$, alors $b = c$.
(6) Tout élément non nul a un seul inverse.
(7) $a(b - c) = ab - ac$.
(8) $a - b = c$ si, et seulement si, $a = b + c$.

Démonstration. (1) Si $a + b = a + c$, alors $(-a) + (a + b) = (-a) + (a + c)$. Ceci donne $((-a) + a) + b = ((-a) + a) + c$. Donc $0_K + b = 0_K + c$. Ainsi $b = c$.

(2) Si $a', a'' \in K$ tels que $a + a' = 0$ et $a + a'' = 0$, alors $a + a' = a + a''$. D'après l'énoncé (1), on a $a' = a''$.

(3) On a $0_K a + 0_K a = (0_K + 0_K)a = 0_K a = 0_K a + 0_K$. Donc $0_K a = 0_K$. Supposons $ab = 0_K$. Si $a \neq 0_K$, comme a^{-1} existe, on a $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0_K = 0_K$.

(4) On a $(-1_K)\, a + a = (-1_K) \cdot a + 1 \cdot a = ((-1_K) + 1_K)a = 0_K a = 0_K$. Ainsi $(-1_K)\, a = -a$.

(5) Supposons $ab = ac$ et $a \neq 0_K$. Alors a^{-1} existe et $a^{-1}(ab) = a^{-1}(ac)$. Ceci donne $(a^{-1}a)b = (a^{-1}a)c$. Donc $1_K \cdot b = 1_K \cdot c$. Ainsi $b = c$.

(6) Soit $a \neq 0$. Si $a', a'' \in K$ tels que $aa' = 1_K$ et $aa'' = 1_K$, alors $aa' = aa''$. Comme $a \neq 0$, d'après l'énoncé (5), $a' = a''$.

(7) On a

$$\begin{aligned} a(b - c) &= a(b + (-c)) = ab + a(-c) = ab + a(-1_K)c \\ &= ab + (-1_K)ac = ab + (-ac) = ab - ac. \end{aligned}$$

(8) Si $a - b = c$, alors $a = a + ((-b) + b) = (a + (-b)) + b = c + b = b + c$. Réciproquement, si $a = b + c$, alors $c = c + (b + (-b)) = (c + b) + (-b) = a + (-b) = a - b$. Ceci achève la démonstration de la proposition.

On étudiera maintenant des exemples de corps.

1.3.3. Proposition. Soit $K \subseteq \mathbb{C}$. Alors K est un corps pour l'addition et la multiplication usuelles si et seulement si $1 \in K$, et pour tous $a, b \in K$, on a

$$a+b, a-b, ab, ab^{-1}(\text{lorsque } b \neq 0) \in K.$$

Dans ce cas, on dit que K est un *corps de nombres*.

Démonstration. La necessité est évidente. Supposons maintenant que K satisfait aux conditions énoncées dans la proposition. Si $a, b \in K$, alors $a+b, ab \in K$ par hypothèse. Ainsi K est muni d'une addition

$$K \times K \to K : (a, b) \mapsto a+b$$

et d'une multiplication

$$K \times K \to K : (a, b) \mapsto ab,$$

satisfaisant aux axiomes (1), (2), (5), (6), (7) et (9). Or $0 = 1 - 1 \in K$ par hypothèse. Si $a \in K$, alors $-a = 0 - a \in K$; et si $a \in K$ non nul, alors $a^{-1} = 1 \cdot a^{-1} \in K$. Donc K est un corps. Ceci achève la démonstration de la proposition.

Exemple. Les ensembles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps de nombres.

Exercice. Vérifier que $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ est un corps de nombres.

1.3.4. Proposition. Si K est un corps de nombres, alors $\mathbb{Q} \subseteq K$. En particulier, K est infini.

Démonstration. Par définition, on a $1 \in K$. Comme K est stable pour l'addition, on voit que tout entier positif n appartient à K. Or $0 = 1 - 1 \in K$ et $-n = 0 - n \in K$. Donc $\mathbb{Z} \subseteq K$. Pour tous $m, n \in \mathbb{Z}$ avec $n \neq 0$, par défition, $\frac{m}{n} = mn^{-1} \in K$. D'où, $\mathbb{Q} \subseteq K$. Ceci achève la démonstration.

On donnera des exemples de corps finis. Pour ce faire, on a besoin de la notion d'un nombre premier. Soit $n > 1$ un entier. On sait que 1 et n sont toujours diviseurs positifs de n. Si n n'a pas d'autres diviseurs positifs, on dit alors que n est *premier*. Par exemple, les entiers $2, 3, 5, 7, 11, 13,$ et 17 sont premiers, mais $1, 4, 6,$ et 9 ne le sont pas.

1.3.5. Théorème de Bézout. Soient p, a des entiers avec p premier et $0 < a < p$. Posoant $r_0 = p$ et $r_1 = a$, on obtient une suite de divisions comme suit:

$$\begin{array}{lcllll} r_0 & = & r_1 q_1 & + & r_2, & 0 < r_2 < r_1; \\ r_1 & = & r_2 q_2 & + & r_3, & 0 < r_3 < r_2; \\ & \vdots & & & & \\ r_{i-2} & = & r_{i-1} q_{i-1} & + & r_i, & 0 < r_i < r_{i-1}; \\ & \vdots & & & & \\ r_{t-2} & = & r_{t-1} q_{t-1} & + & r_t, & 0 < r_t < r_{t-1}; \\ r_{t-1} & = & q_t r_t. & & & \end{array}$$

Dans ce cas, $r_t = 1$; et en remontant par substitution à partir de la deuxième dernière équation, on trouve $x, y \in \mathbb{Z}$ tels que

$$p\,x + ay = 1.$$

Démonstration. L'existence de la suite suit de l'algorithme de division. Pour tout i avec $t \geq i \geq 1$, on prétend que r_t est un diviseur commun de r_{i-1} et r_i. En vue de la dernière équation, c'est vrai pour $i = t$. Supposons que i est un indice avec $t \geq i > 1$ et r_t est un diviseur commun de r_{i-1} et r_i. Comme $r_{i-2} = r_{i-1}q_{i-1} + r_i$, on voit que r_t est un diviseur de r_{i-2}, et donc, un diviseur commun de r_{i-2} et r_{i-1}. Ceci montre l'énoncé. En particulier, r_t est un diviseur de $r_0 = p$. Comme p est premier et $0 < r_t < p$, on obtient $r_t = 1$.

Enfin, on montrera que pour tout i avec $2 \leq i \leq t$, il existe des entiers x_i, y_i tels que $r_i = px_i + ay_i$. C'est vrai pour $i = 2$ car $r_2 = p - aq_1$. Supposons que i est un indice avec $2 < i \leq t$ et l'énoncé est vrai pour tout j avec $2 \leq j < i$. Alors

$$r_i = r_{i-2} - r_{i-1}q_{i-1} = p(x_{i-2} + x_{i-1}) + a(y_{i-2} - y_{i-1}q_{i-1}).$$

Ceci achève la démonstration du théorème.

Remarque. Cette méthode pour résoudre l'équation $ax + by = 1$ s'appelle *l'algorithme d'Euclide.*

Exercice. En sachant que 29 est premier, trouver $x, y \in \mathbb{Z}$ tels que $29x + 11y = 1$.

1.3.6. Lemme. Soit $p > 1$ un nombre premier. Si $a, b \in \mathbb{Z}$, alors
(1) $r_p(a + b) = r_p(r_p(a) + r_p(b))$;
(2) $r_p(a \cdot b) = r_p(r_p(a) \cdot r_p(b))$.

Démonstration. Posons $r_p(a) = r$ et $r_p(b) = s$. C'est-à-dire, $a = pc + r$ et $b = pd + s$ avec $c, d \in \mathbb{Z}$.

(1) Posons $r_p(r + s) = t$. Alors $r + s = pm + t$ avec $m \in \mathbb{Z}$. D'où,

$$a + b = p(c + d + m) + t, \ 0 \le t < p.$$

Ainsi $r_p(a + b) = t = r_p(r + s)$.

(2) Posons $r_p(rs) = t'$. C'est-à-dire, $rs = pq + t'$ avec $q \in \mathbb{Z}$. Alors

$$ab = p(pcd + dr + cs + q) + t', \ 0 \le t' < p.$$

D'où, $r_p(ab) = t' = r_p(rs)$. La preuve du lemme s'achève.

1.3.7. Théorème. Si p un nombre premier, alors $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ est un corps pour l'addition $\oplus$ et la multiplication $\odot$ définies ci-dessous:

(1) $a \oplus b = r_p(a + b)$;

(2) $a \odot b = r_p(ab)$.

Démonstration. Soient $a, b, c \in \mathbb{Z}_p$. D'abord, $a \oplus b = r_p(a + b) = r_p(b + a) = b \oplus a$ et $a \odot b = r_p(ab) = r_p(ba) = b \odot a$. De plus, $a \oplus 0 = r_p(a + 0) = a$ et $a \odot 1 = r_p(a \cdot 1) = a$. Maintenant,

$$(a \oplus b) \oplus c = r_p((a \oplus b) + c) = r_p(r_p(a + b) + r_p(c)) = r_p(a + b + c),$$

où la dernière équalité découle du lemme 1.3.7(1). De même,

$$a \oplus (b \oplus c) = r_p(a + (b \oplus c)) = r_p(r_p(a) + r_p(b + c)) = r_p(a + b + c).$$

Ainsi, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

Si $a = 0$, alors $-a = 0 \in \mathbb{Z}_p$. Sinon, on a $0 < a < p$. Or $p - a \in \mathbb{Z}_p$ est tel que $(p - a) \oplus a = r_p(p - a + a) = r_p(p) = 0$. D'où, $-a = p - a \in \mathbb{Z}_p$.

Supposons que $0 \neq a \in \mathbb{Z}_p$. On veut trouver un inverse de a dans $\mathbb{Z}_p$. D'après le théorème de Bézout, il existe $x, y \in \mathbb{Z}$ tels que $px + ay = 1$. En divisant y par p, on a $y = pq + r$, $0 \le r < p$. Or $ar = ay - pq = p(-x - q) + 1$. Donc $r_p(ar) = 1$. Ceci implique que $r \in \mathbb{Z}_p$ est tel que $a \odot r = 1$, c'est-à-dire, $r = a^{-1}$. Ceci achève la démonstration du théorème.

Remarque. Pour tout $a \in \mathbb{Z}_p$, on a

(1) $-a = p - a$.

(2) Si $px + ay = 1$, alors $a^{-1} = r_p(y)$.

On remarque que la théorie des corps finis est appliquée en théorie des codes.

Exemple. (1) $\mathbb{Z}_2 = \{0, 1\}$, dont l'addition et la multiplication sont données par les tableaux suivants:

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

(2) $\mathbb{Z}_3 = \{0, 1, 2\}$, dont l'addition et la multiplication sont données par les tableaux suivants:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Exercice. Considère le corps $\mathbb{Z}_{19}$. Calculer l'inverse de 7 dans $\mathbb{Z}_{19}$.

Pour conclure cette section, on étudie les puissances d'un élément d'un corps.

1.3.8. Définition. Soit K un corps avec $a \in K$. Pour tout entier $n > 0$, on pose

$$a^n = \overbrace{aa \cdots a}^{n \text{ fois}} \in K,$$

et $a^0 = 1_K$ par convention. Si $a \neq 0_K$, pour tout $n > 0$, on pose

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

Remarque. Pour tous $m, n \geq 1$, on a

$$a^{m+n} = a^m a^n \text{ et } (a^m)^n = a^{mn};$$

qui sont valides pour tous $m, n \in \mathbb{Z}$ lorsque $a \neq 0_K$.

1.4. Polynômes

Partout dans cette section, on se fixe un corps K.

1.4.1. Définition. Un *polynôme* sur K est une expression formelle

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \; a_i \in K.$$

Si $a_n \neq 0$, on appelle n *degré* et a_n *coefficient directeur* de $f(x)$.

Si $a_i = 0_K$ pour tout $1 \leq i \leq n$, on dit que $f(x)$ est *nul*.

Remarque. Un polynôme sur $\mathbb{Q}$ (respectivement, $\mathbb{R}$, $\mathbb{C}$) s'appelle un polynôme *rationnel* (*réel, complexe*).

Le produit de deux polynômes est défini ci-dessous.

1.4.2. Définition. Si $f(x) = a_n x^n + \cdots + a_1 x + a_0$ et $g(x) = b_m x^n + \cdots + b_1 x + b_0$ sont deux polynômes sur K, on définit

$$f(x)g(x) = c_{n+m}x^{n+m} + c_{n+m-1}x^{n+m-1} + \cdots + c_1 x + c_0,$$

où

$$c_k = \sum\nolimits_{i+j=k} a_i b_j, \; k = 0, 1, \ldots, n+m.$$

Remarque. Dans la pratique, on utilise la distributivité pour calculer le produit.

1.4.3. Définition. Soient $f(x)$ un polynôme sur K. Pour tout $a \in K$, on pose

$$f(a) = a_n a^n + \cdots + a_1 a + a_0 \in K.$$

Si $f(a) = 0_K$, on dit que a est une *racine* de $f(x)$.

Exercice. Donner les racines du polynôme complexe $g(x) = x^n - 1$.

Solution. Pour tout $\alpha \in \mathbb{C}$, on voit que α est une racine de $g(x)$ si, et seulement si, $g(\alpha) = \alpha^n - 1 = 0$, si et seulement si, $\alpha^n = 1$ si, et seulement si, α est une racine n-ième de 1. Par conséquent, $g(x)$ a exactement n racines suivantes:

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}; \qquad k = 0, 1, \ldots, n-1.$$

Le réultat suivant est évident.

1.4.4. Lemme. Soit un polynôme $f(x) = ax + b$ sur K. Si $a \neq 0$, alors $f(x)$ a une seule racince $c = -(a^{-1}b)$.

Démonstration. Pour tout $c \in K$, on voit que $f(c) = 0$ si seulement si $ca + b = 0$ si et seulement si $ca = -b$ si seulement si $c = -(a^{-1}b)$. La preuve du lemme s'achéve.

Exercice. Trouver la racine du polynôme $f(x) = 7x + 3$ sur $\mathbb{Z}_{19}$.

1.4.5. Lemme. Soit $f(x) = g(x)h(x)$, avce $f(x), g(x), h(x)$ des polynômes sur K. Si $a \in K$, alors a est une racince $f(x)$ si et seulement si a est une racince de $g(x)$ ou de $h(x)$.

Démonstration. Pour tout $a \in K$, on a $f(a) = g(a)h(a)$. D'après la proposition 1.3.2(3), $f(a) = 0$ si et seulement si $g(a)h(a) = 0$, si et seulement si $g(a) = 0$ ou $h(a) = 0$. La preuve du lemme s'achève.

Exercice. Trouver les racines du polynôme $f(x) = (x-5)(x+7)$ sur $\mathbb{Z}_{11}$.

Pour trouver les racinces d'un polynôme, le résultat suivant sera utile pour réduire le degré du polynôme.

1.4.6. Proposition. Soit $f(x)$ un polynôme de degré $n\,(\geq 1)$ sur K.

(1) Si $f(a) = 0$ avec $a \in K$, alors il existe un polynôme de degré $n-1$ tel que

$$f(x) = (x-a)g(x).$$

(2) Le polynôme $f(x)$ admet au plus n racines dans K.

Démonstration. (1) Écrivons $f(x) = a_n x^n + \cdots + a_1 x + a_0$, où $a_n \neq 0$. Si $n = 1$, alors $aa_1 + a_0 = 0$, et donc $f(x) = a_1(x-a) + (a_0 + aa_1) = a_1(x-a)$. Supposons que $n > 0$ et l'énoncé (1) est valide pour les polynômes de degré $< n$. Or

$$f(x) = (x-a)(a_n x^{n-1}) + h(x),$$

où $h(x) = (aa_n + a_{n-1})x^{n-1} + \cdots + a_1 x + a_0$ est de degré $m \leq n-1$. Comme $h(a) = f(a) = 0$, d'après l'hypothèse de récurrence, $h(x) = (x-a)g_1(x)$, où $g_1(x)$ est de degré $m-1$. Ceci nous donne $f(x) = (x-a)g(x)$, où $g(x) = a_n x^{n-1} + g_1(x)$ est de degré $n-1$.

(2) Si $n = 1$, d'après le lemme 1.4.4, $f(x)$ a une seule racince. Supposons que $n > 1$ et l'énoncé (2) est valide pour les polynômes de degré $n-1$. Si $f(x)$ n'a aucune racine dans K, alors l'énoncé (2) est vailde. Si $f(x)$ admet une racince $a \in K$, d'après l'énoncé (1), $f(x) = (x-a)g(x)$, avec $g(x)$ un polynôme de degré $n-1$. Par l'hypothèse de récurrence, $g(x)$ admet au plus $n-1$ racines dans K. D'après le lemme 1.4.5, $f(x)$ admet au plus n racines dans K. La preuve de la proposition s'achève.

Lorsque K est un corps fini, on peut trouver les racines d'un polynôme sur K toujours par *essai et erreur.*

Exercice. Trouver les racines du polynôme $f(x) = x^4 + x^2 + 3$ sur $\mathbb{Z}_5$.

Des maintenant, on se concentre sur les polynômes sur un corps de nombres. Comme on a vu, il y a des polynômes réels qui n'ont aucune racine réelle. Ce phénomène disparaît pour les polynômes complexes, illustré par le résultat célèbre suivant dont la démonstration est trop avancée pour ce cours.

1.4.7. Théorème fondamental d'algèbre. Soit $n \geq 1$. Tout polynôme complexe

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

de degré n admet exactement n racines complexes $x_1, \ldots, x_n$, en comptant les multiplicités. Dans ce cas, $f(x)$ se factorise comme suit :

$$f(x) = a_n(x - x_1) \cdots (x - x_n).$$

Remarque. Grâce à la propriété énoncée dans le théorème 1.4.7, on dit que $\mathbb{C}$ est un corps *algébriquement clos.*

Exercice. Factoriser le polynôme complexe $f(x) = x^n - 1$ avec $n \geq 1$.

Solution. On a vu que $f(x)$ a n racines distinctes ζ_n^k, où ζ_n est la racine n-ième primitive de l'unité, $k = 0, 1, \ldots, n-1$. Comme le coefficient directeur de $f(x)$ est 1, on a

$$x^n - 1 = \prod_{k=0}^{n-1} (x - \zeta_n^k) = (x-1)(x - \zeta_n) \cdots (z - \zeta_n^{n-1}).$$

Considérant le cas où $n = 3$, on a

$$\zeta_3 = \cos \frac{2\pi}{3} + \sin \frac{2\pi}{3} i = -\frac{1}{2} + \frac{\sqrt{3}}{2} i.$$

Ainsi

$$x^3 - 1 = (x - \zeta_3^0)(x - \zeta_3)(x - \zeta_3^2) = (x-1)\left(x + \frac{1}{2} - \frac{\sqrt{3}}{2} i\right)\left(x + \frac{1}{2} + \frac{\sqrt{3}}{2} i\right).$$

Il n'y a aucune méthode générale pour trouver les racines d'un polynôme complexe quelconque. Mais pour les polynômes complexes quadratiques, c'est toujours faisable.

1.4.8. Proposition. Soit un polynôme quadratique complexe

$$f(x) = ax^2 + bx + c.$$

Soit $\Delta = b^2 - 4ac$. Si $\sqrt{\Delta}$ est une racine carrée de Δ, alors les deux racines complexes de $f(x)$ sont données par

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a}, \qquad x_2 = \frac{-b - \sqrt{\Delta}}{2a}.$$

Démonstration.

$$\begin{aligned} ax^2+bx+c &= a\left(x^2+2\frac{b}{2a}x+\frac{b^2}{4a^2}-\frac{b^2}{4a^2}+\frac{c}{a}\right)=a\left[\left(x+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a^2}\right] \\ &= a\left[\left(x+\frac{b}{2a}\right)^2-\left(\frac{\sqrt{\Delta}}{2a}\right)^2\right]=a\left(x+\frac{b}{2a}+\frac{\sqrt{\Delta}}{2a}\right)\left(x+\frac{\beta}{2a}-\frac{\sqrt{\Delta}}{2a}\right). \end{aligned}$$

Ceci achève la démonstration de la proposition.

Exercice. Factoriser le polynôme complexe $3x^2+2x+1$.

Pour conclure cette section, on donne un résultat très pratique concernant les racines rationnelles d'un polynôme sur $\mathbb{Z}$.

1.4.9. Proposition. Soit le polynôme

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, \quad a_i\in\mathbb{Z}.$$

Si $q\in\mathbb{Q}$ est une racine de $f(x)$, alors $q\in\mathbb{Z}$ est un facteur de a_0.

Démonstration. Tout $q\in\mathbb{Q}$ s'écrit $q=\frac{a}{b}$, où $a,b\in\mathbb{Z}$ avec $\mathrm{pgcd}(a,b)=1$. Si

$$f(q)=\frac{a^n}{b^n}+a_{n-1}\frac{a^{n-1}}{b^{n-1}}+\cdots+a_1\frac{a}{b}+a_0=0,$$

alors

$$a^n+a_{n-1}ba^{n-1}+\cdots+a_1b^{n-1}a+a_0b^n=0.$$

D'où, b divise a^n. Comme $\mathrm{pgcd}(a,b)=1$, $\mathrm{pgcd}(a^n,b)=1$. Ainsi $b=\pm1$, c'est-à-dire, $a\in\mathbb{Z}$. Ceci achève la démonstration de la proposition.

Exercice. Factoriser le polynôme rationnel $f(x)=x^3-4x^2+x+6$.

1.5. Exercices

1. Mettre sous la forme algébrique chacun des nombres complexes suivants:

(1) $\dfrac{13-i}{\sqrt{3}+\sqrt{2}i}$; (2) $\dfrac{1}{(1+i)(-1+i)(2+i)}$;

(3) $\dfrac{6-i}{2+i}+\dfrac{6+i}{2-i}$; (4) $\dfrac{(1+2i)(-2+i)}{(7+3i)(1-i)}+\dfrac{(1+i)(-1+i)}{(1+3i)(2i)}$.

2. Déterminer $a, b \in \mathbb{R}$ tels que $a(1+i) + b(2-5i) = -3 + 7i$.

3. Soient $z, w \in \mathbb{C}$. Montrer, pour tout entier $k \geq 0$, que
$$(z+w)^k = \sum_{p=0}^{k} \binom{k}{p} z^p w^{k-p}.$$

4. Représenter chacun des nombres complexes suivants dans le plan d'Argand:
$$(1) \quad (2+i)(2-i); \qquad (2) \quad \frac{2-2i}{1+i}; \qquad (3) \quad -3\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right).$$

5. Trouver tous les nombres complexes z tels que $\bar{z} = z^2$.

6. Si $z \in \mathbb{C}$, montrer que $z^{-1} = \bar{z}$ si, et seulement si, $|z| = 1$.

7. Si $z \in \mathbb{C}$ est tel que $z^8 = 16$, trouver $|z|$. *Indice*: $|z^n| = |z|^n$.

8. Mettre premièrement sous la forme polaire et ensuite sous la formule d'Euler chacun des nombres complexes suivants:
$$(1) \quad \frac{1+\sqrt{3}i}{2}; \qquad (2) \quad \frac{-1+\sqrt{3}i}{3}; \qquad (3) \quad -2\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right).$$

9. Trouver $\cos\frac{7\pi}{12}$ et $\sin\frac{7\pi}{12}$.
Indice: Calculer le produit $(1+i)(1+\sqrt{3}i)$ en utilisant la forme polaire et la forme algébrique.

10. Calculer en utilisant la forme polaire:
$$(1) \quad (1-i)^{100}; \qquad (2) \quad \left(\frac{1+\sqrt{3}i}{1-i}\right)^{20}; \qquad (3) \quad \frac{(-1+\sqrt{3}i)^{15}}{(1-i)^{20}} + \frac{(-1-\sqrt{3}i)^{15}}{(1+i)^{20}}.$$

11. Montrer, pour tout entier $n \geq 1$, les énoncés suivants:
$$(1) \quad (1+i)^n = \sqrt{2}^{\,n}\left(\cos\frac{n\pi}{4} + i\sin\frac{n\pi}{4}\right); \qquad (2) \quad (\sqrt{3}-i)^n = 2^n\left(\cos\frac{n\pi}{6} - i\sin\frac{n\pi}{6}\right).$$

12. Soit $z = r(\cos\theta + i\sin\theta)$ un complexe sous la forme polaire. Trouver une forme polaire de $\bar{z}$.

13. Soit $z \in \mathbb{C}$ tel que $z + z^{-1} = 2\cos\theta$. Montrer que $z^n + z^{-n} = 2\cos n\theta$, pour tout $n \geq 0$.

14. Montrer les égalités trigonométriques suivantes:

    (1) $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$; (2) $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$.

    Indice: Poser $z = \cos\theta + i\sin\theta$ et calculer z^3 à l'aide de la formule du binôme et du théorème de de Moivre.

15. Donner le quotient ainsi que le reste de -576 divisé par 97.

16. (1) Trouver les racines carrées de $1 - \sqrt{3}i$.

    (2) Trouver les racines cubiques de $-1 - \sqrt{3}i$.

    (3) Trouver les racines 6-ième de l'unité.

    (4) Trouver les racines 4-ième de -16.

    (5) Trouver les racines 6-ième de i.

17. Montrer, pour tout $z \in \mathbb{C}$, que $\overline{e^z} = e^{\bar{z}}$. *Indice*: Utiliser la remarque (3) suivant la proposition 1.2.18.

18. Montrer, pour tout angle θ, que

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \qquad \text{et} \qquad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

19. Dans chacun des cas suivants, trouver le polynôme $f(x)$.

    (1) $f(x)$ a pour racines $3, 3, i$, et $-i$, et pour coefficient directeur 2.

    (2) $f(x)$ a pour racines $1, 1, 1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, et $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$, et pour coefficient directeur 3.

20. Trouver les racines des polynômes suivants:

    (1) $(\sqrt{2} - \sqrt{3}i)x + (2 - 3i)$;

    (2) $x^4 + (1 - i)$.

21. Factoriser les polynômes complexes suivants en produit de facteurs linéaires.

    (1) $x^3 + x^2 - 2$; (2) $x^3 - x^2 - x - 2$; (3) $x^2 + (1+i)x + \dfrac{1}{2}$;

    (4) $x^6 + 4x^3 + 3$; (5) $x^4 - 9x^2 - 4x + 12$.

22. Soit a un nombre réel positif. Si ζ est la racine n-ième primitive de l'unité, montrer que les racinces n-ième de a sont $\sqrt[n]{a}\,\zeta^k$, $k = 0, 1, \cdots, n-1$.

23. Trouver les racines du polynôme $x^6 - 4x^3 + 1$.

    Indice: Remarquer premièmement que $x^6 - 4x^3 + 1 = (x^3 - 2)^2 - 3$, et ensuite appliquer le numéro précédent.

24. Soient $f(x)$ un polynôme réel. Montrer, pour $w \in \mathbb{C}$, que w est une racine de $f(x)$ si et seulement si $\bar{w}$ l'est également. En déduire que tout polynôme réel de degré impaire a au moins une racine réelle.

25. Montrer que $K = \{a + bi \mid a, b \in \mathbb{Q}\}$ est un corps de nombres.

26. Donner la table d'addition et la table de multiplication de $\mathbb{Z}_5$.

27. Calculer dans le corps $\mathbb{Z}_{11}$:

    (1) $5 \cdot 6 - 7 \cdot 8 + 4 \cdot 5^{-1}$; (2) $3 \cdot 2^3 - 4 \cdot 2^2 + 1$.

28. Résoudre l'équation $47x + 89 = 0$ sur le corps $\mathbb{Z}_{97}$.

29. Factoriser sur le corps $\mathbb{Z}_5$ le polynôme suivant:

$$f(x) = x^4 + 3x^3 + x^2 + 4x + 3.$$

30. Soit p un nombre premier. Montrer, pour $a, b, c \in \mathbb{Z}_p$, que

    (1) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$; (2) $a \odot (b \oplus c) = a \odot b \oplus a \odot c$.

31. Soit K un corps. Montrer que, pour tous $a, b \in K$,

    (1) $-(-a) = a$; (2) $-(ab) = (-a)b = a(-b)$; (3) $(a^{-1})^{-1} = a$ si $a \neq 0$.

32. Soit $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$ un polynôme sur un corps K. Montrer que les racines de $f(x)$ dans K sont $a_1, a_2, \ldots, a_n$.

33. Soit K un corps. Si $a \in K$ est tel que $a^n = 0_K$ pour certain entier $n \geq 1$, montrer que $a = 0_K$.

Chapitre II: Matrices

Le but de ce chapitre est d'étudier les opérations et les propriétés de matrices. Applications des matrices se trouvent dans la plupart des domaines scientifiques et du génie. Dans chaque branche de la physique, y compris la mécanique classique, optique et mécanique quantique, elles sont utilisées pour étudier des phénomènes physiques, tels que le mouvement des corps rigides. En infographie, elles sont utilisées pour projeter une image en 3 dimensions sur un écran en 2 dimensions.

Partout dans ce chapitre, K désignera un corps.

2.1. Opérations matricielles

2.1.1. Définition. Une *matrice* de type $m \times n$ sur K est un tableau de mn éléments de K rangés sur m lignes et n colonnes comme suit:

$$\begin{array}{cc} \begin{array}{cccc} C_1 & C_2 & \cdots & C_n \end{array} & \\ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} & \begin{array}{c} L_1 \\ L_2 \\ \\ L_m \end{array} \end{array}$$

On appelle a_{ij} le (i, j)-*terme* où i est l'*indice de ligne* et j est l'*indice de colonne*.

La matrice est dite *nulle*, notée $0_{m\times n}$, si $a_{ij} = 0_K$ pour tous $1 \leq i \leq m$ et $1 \leq j \leq n$.

Deux matrices sont dites *égales* si elles sont du même type et les termes en même position sont égaux.

La matrice est dite *carrée d'ordre* n si $m = n$. Dans ce cas, les termes $a_{11}, a_{22}, \ldots, a_{nn}$ sont appelés les *termes diagonaux*.

La matrice s'appelle une *matrice-ligne* si $m = 1$; et une *matrice-colonne* si $n = 1$.

Une matrice (a) de type 1×1 sera identifié avec l'élément a.

Remarque. Une matrice sur $\mathbb{Q}$ (respectivement, $\mathbb{R}, \mathbb{C}$) s'appelle *rationnelle* (respectivelment, *réelle, complexe*).

Notation. On désignera par $M_{m\times n}(K)$ l'ensemble des matrices de type $m \times n$ sur K et par $M_n(K)$ l'ensemble des matrices carrées d'ordre n sur K.

On définira des opérations arithmétiques pour les matrices. Il est à noter que ces opérations seront partiellement définies.

2.1.2. Définition. Soient $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n} \in M_{m\times n}(K)$ et $a \in K$. On définit

(1) (multiplication scalaire) $\quad a \cdot A = (aa_{ij})_{m\times n} = A \cdot a$.

(2) (opposé) $-A = (-a_{ij})_{m\times n}$.

(3) (addition) $A + B = (a_{ij} + b_{ij})_{m\times n}$.

(4) (soustraction) $A - B = (a_{ij} - b_{ij})_{m\times n}$.

Remarque. (1) $-A = (-1_K)A$.

(2) Si A et B ne sont pas du même type, alors ni $A + B$ ni $A - B$ n'est défini.

Le résultat suivant est évident.

2.1.3. Proposition. Soient $A, B \in M_{m\times n}(K)$ et $a, b \in K$.

(1) $(ab)A = a(bA)$.	(2) $aA = 0_{m\times n}$ si $a = 0_K$ ou $A = 0_{m\times n}$.
(3) $A + B = B + A$.	(4) $(A + B) + C = A + (B + C)$.
(5) $A + 0_{m\times n} = A$.	(6) $A + (-A) = 0_{m\times n}$.
(7) $a(A \pm B) = aA \pm aB$.	(8) $(a \pm b)A = aA \pm bA$.

Remarque. Si $A_1, \cdots, A_r \in M_{m\times n}(K)$ avec $r > 2$, on définit alors

$$A_1 + A_2 + \cdots + A_r = (\cdots(A_1 + A_2) + \cdots + A_{r-1}) + A_r.$$

2.1.4. Multiplication. (1) Le produit d'une matrice de type $1 \times n$ et une matrice de type $n \times 1$ est une matrice de type 1×1 définie par

$$(a_1 \ \cdots \ a_n) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{k=1}^{n} a_k b_k.$$

(2) Si $A = (a_{ik}) \in M_{m\times n}(K)$ et $B = (b_{kj}) \in M_{n\times p}(K)$, alors le *produit* de A et B est défini par $AB = (c_{ij})_{m\times p}$, où

$$c_{ij} = (a_{i1} \ \cdots \ a_{in}) \begin{pmatrix} b_{1j} \\ \vdots \\ b_{jn} \end{pmatrix} = \sum_{k=1}^{n} a_{ik} b_{kj}, \quad i = 1, \ldots, m;\ j = 1, \ldots, p.$$

Remarque. (1) Si $A = 0_{m\times n}$ ou $B = 0_{n\times p}$, alors $AB = 0_{m\times p}$.
(2) Si $A, B \in M_n(K)$, alors $AB \in M_n(K)$.

Pour définir une matrice identité, il est commode d'introduire le *symbole de Kronecker* δ_{ij} sur K avec $i, j \in \mathbb{N}$, qui est défini par

$$\delta_{ij} = \begin{cases} 1_K, & \text{si } i = j; \\ 0_K, & \text{si } i \neq j. \end{cases}$$

À l'aide de cette notation, on définit *matrice identité* d'ordre n comme étant la matrice carrée

$$I_n = (\delta_{ij})_{n\times n} = \begin{pmatrix} 1_K & 0 & \cdots & 0 \\ 0 & 1_K & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1_K \end{pmatrix}_{n\times n}.$$

2.1.5. Proposition. (1) Si $A \in M_{m\times n}(K)$, alors $A_{m\times n} = I_m A = A I_n$.
(2) Si $A \in M_{m\times n}(K), B \in M_{n\times p}(K)$ et $C \in M_{p\times q}(K)$, alors $(AB)C = A(BC)$.
(3) Si $A \in M_{m\times n}(K), B \in M_{n\times p}(K)$ et $a, b \in K$, alors $(aA)(bB) = (ab)(AB)$.
(4) Si $A \in M_{m\times n}(K)$ et $B, C \in M_{n\times p}(K)$, alors $A(B + C) = AB + AC$.
(5) Si $A, B \in M_{m\times n}(K)$ et $C \in M_{n\times p}(K)$, alors $(A + B)C = AC + BC$.

Démonstration. (1) Soit $A = (a_{kj})_{m\times n}$. Alors $I_m A = (\delta_{ik})_{m\times m}(a_{kj})_{m\times n} = (d_{ij})_{m\times n}$, où

$$d_{ij} = \sum\nolimits_{k=1}^{m} \delta_{ik} a_{kj} = a_{ij}.$$

Ainsi $I_m A = A$. De même, $AI_n = A$.

(2) Soit $A = (a_{ik})_{p\times m}$, $B = (b_{kl})_{m\times n}$ et $C = (c_{lj})_{n\times q}$. Alors $AB = (d_{il})_{p\times n}$, où $d_{il} = \sum_{k=1}^{m} a_{ik} b_{kl}$, pour tous $1 \le i \le p$ et $1 \le l \le m$. Donc $(AB)C = (h_{ij})_{p\times q}$, où

$$h_{ij} = \sum_{l=1}^{n} d_{il} c_{lj} = \sum_{l=1}^{n} \left(\sum_{k=1}^{m} a_{ik} b_{kl} \right) c_{lj} = \sum_{l=1}^{n} \sum_{k=1}^{m} a_{ik} b_{kl} c_{lj}.$$

D'autre part, $BC = (f_{kj})_{m\times q}$, où $f_{kj} = \sum_{l=1}^{n} b_{kl} c_{lj}$, pour tous $1 \le k \le m$ et $1 \le j \le q$. Donc $A(BC) = (g_{ij})_{p\times q}$, où

$$g_{ij} = \sum_{k=1}^{m} a_{ik} f_{kj} = \sum_{k=1}^{m} a_{ik} \left(\sum_{l=1}^{n} b_{kl} c_{lj} \right) = \sum_{k=1}^{m} \sum_{l=1}^{n} a_{ik} b_{kl} c_{lj} = \sum_{l=1}^{n} \sum_{k=1}^{m} a_{ik} b_{kl} c_{lj} = h_{ij}.$$

Ainsi $(AB)C = A(BC)$. Les preuves des autres énoncés sont laissées comme exercices. Ceci achève la démonstration de la proposition.

Remarque. (1) La multiplication matricielle n'est pas commutative.

(2) Le produit AB peut être nul sans que A ou B soit nulle.

(3) Si $A_1, \cdots, A_r$, où $r > 2$, sont des matrices sur K telles que $A_i A_{i+1}$ est définie, pour $i = 1, \ldots, r-1$, alors on définit

$$A_1 A_2 \cdots A_r = (\cdots (A_1 A_2) \cdots A_{r-1}) A_r.$$

2.1.6. Puissance. Soit A une matrice carrée sur K. Pour tout entier $r \geq 1$, on définit

$$A^r = \overbrace{AA \cdots A}^{r \text{ fois}},.$$

Si $A \neq 0$, on définit par convention $A^0 = I_n$.

Remarque. (1) $A^r A^s = A^{r+s}$ et $(A^r)^s = A^{rs}$, pour tous $r, s \geq 0$.

(2) En général, $(AB)^r \neq A^r B^r$.

2.1.7. Définition. Une matrice carrée A est dite *nilpotente* si $A^r = 0$ pour un certain entier $r \geq 1$.

Exercice. Vérifier que la matrice

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

sur le corps $\mathbb{Z}_5$ n'est pas nilpotente.

2.1.8. Définition. Une matrice carrée $D = (d_{ij})_{n \times n}$ est dite *diagonale* si $d_{ij} = 0$ pour tous $1 \leq i, j \leq n$ avec $i \neq j$. Dans ce cas, on note $D = \text{diag}\,\{d_{11}, \ldots, d_{nn}\}$.

Exemple. La matrice identité I_n est diagonale.

2.1.9. Proposition. Soient $D_1 = \text{diag}\,\{a_1, \ldots, a_n\}$ et $D_2 = \text{diag}\,\{b_1, \ldots, b_n\}$ des matrices diagonales sur K.

(1) $D_1 + D_2 = \text{diag}\,\{a_1 + b_1, \ldots, a_n + b_n\}$.

(2) $D_1 D_2 = \text{diag}\,\{a_1 b_1, a_2 b_2, \ldots, a_n b_n\}$.

Démonstration. L'énoncé est évident. D'après la définition, $D_1D_2 = (c_{ij})_{n\times n}$, où

$$c_{ij} = \begin{cases} 0+\cdots+0+a_ib_i+0+\cdots+0, & \text{si } i=j; \\ 0+\cdots+0+a_i\cdot 0+0\cdots+0, & \text{si } i\neq j. \end{cases} = \begin{cases} a_ib_i, & \text{si } i=j; \\ 0, & \text{si } i\neq j. \end{cases}$$

Ceci achève la démonstration.

2.1.10. Définition. Soit $A = (a_{ij}) \in M_{m\times n}(K)$. On définit la *transposée* de A comme étant la matrice de type $n \times m$ suivante:

$$A^T = (a'_{ij})_{n\times m},$$

où $a'_{ij} = a_{ji}$, $i = 1, \ldots, n$; $j = 1, \ldots, m$.

Remarque. (1) La i-ième ligne de A^T est la transposée de la i-ième colonne de A.
(2) La j-ième colonne de A^T est la transposée de la j-ième ligne de A.

2.1.11. Proposition. Soient A, B des matrices sur K, et $a \in K$.
(1) $(A^T)^T = A$.
(2) $(aA)^T = aA^T$.
(3) Si $A + B$ est définie, alors $(A + B)^T = A^T + B^T$.
(4) Si AB est défini, alors $(AB)^T = B^TA^T$.

Démonstration. On ne montrera que l'énoncé (4), comme les autres énoncés sont faciles à vérifier. Soient $A = (a_{ik})_{m\times n}$ et $B = (b_{kj})_{n\times p}$. Alors $AB = (c_{ij})_{m\times p}$ avec $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$ pour tous $1 \le i \le m$ et $1 \le j \le p$. Donc $(AB)^T = (c'_{ij})_{p\times m}$ avec $c'_{ij} = c_{ji}$ pour tous $1 \le i \le p$ et $1 \le j \le m$.

D'autre part, $A^T = (a'_{ik})_{n\times m}$ avec $a'_{ik} = a_{ki}$ pour tous $1 \le i \le n$ et $1 \le k \le m$ et $B^T = (b'_{kj})_{p\times n}$ avec $b'_{kj} = b_{jk}$ pour tous $1 \le k \le p$ et $1 \le j \le n$. Donc $B^TA^T = (d_{ij})_{p\times m}$, où

$$d_{ij} = \sum_{k=1}^n b'_{ik}a'_{kj} = \sum_{k=1}^n b_{ki}a_{jk} = \sum_{k=1}^n a_{jk}b_{ki} = c_{ji} = c'_{ij},$$

pour tous $1 \le i \le p$ et $1 \le j \le m$. Ainsi $B^TA^T = (AB)^T$. Ceci achève la démonstration.

2.1.12. Définition. Une matrice carrée $A = (a_{ij})_{n\times n}$ sur K est dite
(1) *symétrique* si $A^T = A$, ou bien, si $a_{ij} = a_{ji}$ pour tous $1 \le i, j \le n$;
(2) *antisymétrique* si $A^T = -A$, ou bien, si $a_{ij} = -a_{ji}$ pour tous $1 \le i, j \le n$.

Remarque. (1) Une matrice diagonale est symétrique.

(2) La diagonale d'une matrice complexe anti-symétrique est nulle. Mais c'est pas nécessairement vrai si le corps est fini.

2.1.13. Définition. Soit $A = (a_{ij})_{n\times n} \in M_n(K)$. On définit la *trace* de A comme étant

$$\operatorname{tr}(A) = \sum_{i=1}^{n} a_{ii} \in K.$$

Exemple. $\operatorname{tr}(0_{n\times n}) = 0_K$.

2.1.14. Proposition. (1) Si $A \in M_{m\times n}(K)$ et $B \in M_{n\times m}(K)$, alors

$$\operatorname{tr}(AB) = \operatorname{tr}(BA).$$

(2) Si $A, B \in M_n(K)$ et $a, b \in K$, alors

$$\operatorname{tr}(aA + bB) = a\operatorname{tr}(A) + b\operatorname{tr}(B).$$

Démonstration. Comme l'énoncé (2) est évident, on ne montrera que l'énoncé (1). Écrivons $A = (a_{ij})_{m\times n}$ et $B = (b_{ij})_{n\times n}$. Posons $AB = (c_{ij})_{m\times m}$ avec $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$ et $BA = (d_{kl})_{n\times n}$ avec $d_{kl} = \sum_{i=1}^{m} b_{ki}a_{il}$. Maintenant, on a

$$\operatorname{tr}(AB) = \sum_{i=1}^{m} c_{ii} = \sum_{i=1}^{m}\sum_{k=1}^{n} a_{ik}b_{ki}$$

et

$$\operatorname{tr}(BA) = \sum_{k=1}^{n} d_{kk} = \sum_{k=1}^{n}\sum_{i=1}^{m} b_{ki}a_{ik} = \sum_{i=1}^{m}\sum_{k=1}^{n} a_{ik}b_{ki}.$$

Donc $\operatorname{tr}(AB) = \operatorname{tr}(BA)$. Ceci achève la démonstration de la proposition.

2.2. Multiplication par blocs

En général, le calcul du produit de deux matrices de grandes tailles est ennuyeux. Mais dans certains cas spéciaux, par exemple, les matrices contiennent beaucoup de termes nulls, il facilitera le calcul si l'on partage les matrices en blocs. On commence par le partage des entiers strictement positifs.

2.2.1. Définition. Soit $n > 0$ un entier. Un *partage* de n est une décomposition

$$n = n_1 + n_2 + \cdots + n_r, \text{ où } n_1, \ldots, n_r > 0.$$

Exemple. En partageant l'entier 5, on obtient les partages suivants:

$$5; 4+1; 3+2; 3+1+1; 2+2+1; 2+1+1+1; 1+1+1+1+1.$$

2.2.2. Définition. Soit $A = (a_{ij})_{m\times n} \in M_{m\times n}(K)$. Partageons $m = m_1 + m_2 + \cdots + m_r$ et $n = n_1 + n_2 + \cdots + n_s$, et posons $m_0 = n_0 = 0$. Pour tous $1 \le p \le r$ et $1 \le q \le s$, considérons la sous-matrice de A suivante:

$$A_{pq} = (a_{ij})_{m_{p-1}<i\le m_p;\, n_{q-1}<j\le n_q} \in M_{m_p\times n_q}(K).$$

Maintenant, la matrice A est partagée comme suit:

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1s} \\ A_{21} & A_{22} & \cdots & A_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ A_{r1} & A_{r2} & \cdots & A_{rs} \end{pmatrix} = (A_{ij})_{r\times s},$$

où A_{ij} s'appelle le (i,j)-*bloc* de A.

Remarque. Les blocs dans la même colonne ont le même nombre de colonnes et les blocs dans la même ligne ont le même nombre de lignes.

Exemple. Les matrices suivantes sont partagées en blocs:

$$\left(\begin{array}{c|c|c} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \end{array}\right), \qquad \left(\begin{array}{c|cc} 0 & 1 & 2 \\ \hline 1 & 2 & 3 \\ 2 & 3 & 4 \end{array}\right), \qquad \left(\begin{array}{cc|cc} 0 & 1 & 2 & 0 \\ \hline 1 & 2 & 3 & 1 \\ \hline 2 & 3 & 4 & 2 \end{array}\right).$$

Le partage de matrices est particulièrement utile dans le calcul du produit de matrices.

2.2.3. Théorème. Soient $A = (A_{ik})_{r\times s}$ et $B = (B_{kj})_{s\times t}$ des matrices partagées sur K. Si les colonnes de A sont partagées de la même façon que les lignes de B, alors

(1) $A_{ik}B_{kj}$ est défini pour tous $1 \le i \le r$; $1 \le k \le s$; $1 \le j \le t$;

(2) $AB = (C_{ij})_{r\times t}$, où

$$C_{ij} = \sum\nolimits_{k=1}^{s} A_{ik}B_{kj}, \quad i = 1, \cdots, r;\ j = 1, \cdots, t.$$

Démonstration. Supposons que A_{ik} est de type $m_i \times n_k$. Alors B_{kj} est de type $n_k \times p_j$. Posons $m = m_1 + \cdots + m_r$, $n = n_1 + \cdots n_s$ et $p = p_1 + \cdots + p_t$. Alors $A = (a_{ij})_{m\times n}$ et

$A_{kl} = (a_{ij})$ avec $m_1 + \cdots + m_{k-1} < i \le m_1 + \cdots + m_k$ et $n_1 + \cdots + n_{l-1} < j \le n_1 + \cdots + n_l$. De même, $B = (b_{ij})_{n\times p}$ et $B_{kl} = (b_{ij})$ avec $n_1 + \cdots + n_{k-1} < i \le n_1 + \cdots + n_k$ et $p_1 + \cdots + p_{l-1} < j \le p_1 + \cdots + p_l$. On se fixe deux indices i_0, j_0 avec $1 \le i_0 \le m$ et $1 \le j_0 \le p$. On peut écrire $i_0 = m_1 + \cdots + m_{r_0-1} + l$ avec $1 \le l \le m_{r_0}$ et $j_0 = p_1 + \cdots + p_{t_0-1} + q$ avec $1 \le q \le p_{t_0}$. Alors le (i_0, j_0)-terme de $(C_{ij})_{r\times t}$ est le (l, q)-terme de $C_{r_0,t_0} = \sum_{k=1}^{s} A_{r_0,k} B_{k,t_0}$, qui est

$$\sum_{k=1}^{n_1} a_{i_0,k} b_{k,j_0} + \sum_{k=n_1+1}^{n_1+n_2} a_{i_0,k} b_{k,j_0} + \cdots + \sum_{k=n_1+\cdots+n_{s-1}+1}^{n} a_{i_0,k} b_{k,j_0} = \sum_{k=1}^{n} a_{i_0,k} b_{k,j_0}.$$

Ce dernier est le (i_0, j_0)-terme de AB. Donc $AB = (C_{ij})_{r\times t}$. Ceci achève la démonstration du théorème.

Remarque. Le mode de multiplication de matrices donné dans le théorème 2.2.3 s'appelle *multiplication par blocs.*

Le résultat suivant nous dit comment multiplier une matrice à gauche par une matrice-ligne ou à droite par une matrice-colonne.

2.2.4. Lemme. Soit A une matrice sur K.
(1) Si $L_1, \ldots, L_m$ sont les lignes de A, alors

$$(b_1 \cdots b_m)A = b_1 L_1 + \cdots + b_m L_m.$$

(2) Si $C_1, \ldots, C_n$ sont les colonnes de A, alors

$$A \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_1 C_1 + \cdots + a_n C_n;$$

Démonstration. Pour la première égalité, on partage la matrice-ligne en colonnes et partage A en lignes. Pour la deuxième égalité, on partage A en colonnes et partage la matrice-colonne en lignes. Maintenant, le résultat suit immédiatement du théorème 2.2.3. Ceci achève la démonstration du lemme.

Le résultat suivant nous dit que le calcul du produit de deux matrices quelconques se ramène au cas où le facteur à gauche est une matrice-ligne ou le facteur à droite est une matrice-colonne.

2.2.5. Lemme. Soient A, B des matrices sur K telles que AB est défini.

(1) Si $B_1, \ldots, B_p$ sont les colonnes de B, alors $AB = (AB_1, \ldots, AB_p)$.

(2) Si $A_1, \ldots, A_m$ sont les lignes de A, alors

$$AB = \begin{pmatrix} A_1 B \\ \vdots \\ A_m B \end{pmatrix}.$$

Démonstration. Pour la première égalité, on partage A en un seul bloc et partage B en colonnes $(B_1 \cdots B_p)$. Pour la deuxième égalité, on partage A en lignes et partage B un seul bloc. Maintenant, le résultat suit immédiatement du théorème 2.2.3. Ceci achève la démonstration.

2.2.6. Corollaire. Soit $A \in M_{m\times n}(K)$. Si e_i est la i-ième ligne de I_m et e'_j est la j-ième colonne de I_n, alors

(1) e_iA est la i-ième ligne de A;

(2) Ae'_j est la j-ième colonne de A;

(3) $e_iAe'_j$ est le (i,j)-terme de A.

Démonstration. Soient $L_1, \ldots, L_m$ les lignes et $C_1, \ldots, C_n$ les colonnes de A. D'abord,

$$\begin{pmatrix} L_1 \\ \vdots \\ L_m \end{pmatrix} = A = I_m A = \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} A = \begin{pmatrix} e_1 A \\ \vdots \\ e_m A \end{pmatrix}.$$

D'où $e_iA = L_i$, $i = 1, \ldots, m$. En outre, on a

$$(C_1 \cdots C_n) = A = AI_n = A(e'_1, \cdots e'_n) = (Ae'_1, \cdots Ae'_n).$$

D'où $Ae'_j = C_j$, $j = 1, \ldots, n$. Enfin, d'après l'énoncés (1), $e_iAe'_j = L_ie'_j$. Et d'après l'énoncés (2), $L_ie'_j$ est la j-ième colonne de L_i, c'est-à-dire, le (i,j)-terme de A. Ceci achève la démonstration du corollaire.

Le résultat suivant nous dit comment multiplier une matrice par une matrice diagonale.

2.2.7. Corollaire. Soit A une matrice sur K.

(1) Si $C_1, \ldots, C_n$ sont les colonnes de A, alors

$$A \begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix} = (a_1C_1, \cdots, a_nC_n).$$

(2) Si $L_1, \ldots, L_m$ sont les lignes de A, alors

$$\begin{pmatrix} b_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & b_m \end{pmatrix} A = \begin{pmatrix} b_1 L_1 \\ \vdots \\ b_m L_m \end{pmatrix}.$$

Démonstration. On voit aisément que $\text{diag}\{a_1, \ldots, a_n\} = (a_1 e'_1 \ \cdots \ a_n e'_n)$. Donc

$$A(a_1 e'_1 \ \cdots \ a_n e'_n) = (A(a_1 e'_1) \ \cdots \ A(a_n e'_n)) = (a_1(Ae'_1) \ \cdots \ a_n(Ae'_n)) = (a_1 C_1, \ \cdots, \ a_n C_n),$$

où la dernière égalité suit du corollaire 2.2.6(2). Ceci montre l'énoncé (1). De la même façon, on vérifie l'énoncé (2). Ceci achève la démonstration du corollaire.

2.2.8. Définition. Soit $A = (a_{ij})_{n \times n} \in M_n(K)$. On dit que A est
(1) *triangulaire supérieure* si $a_{ij} = 0$ pour tous $n \geq i > j \geq 1$;
(2) *triangulaire inférieure* si $a_{ij} = 0$ pour tous $1 \leq i < j \leq n$;
(3) *triangulaire* si A est triangulaire supérieure ou triangulaire inférieure.

Remarque. Une matrice diagonale est triangulaire.

2.2.9. Proposition. Si $A \in M_n(K)$ est triangulaire dont la diagonale est nulle, alors $A^n = 0$. En particulier, A est nilpotente.

Démonstration. On ne considère que le cas où A est triangulaire supérieure. Dans ce cas, A s'écrit comme suit:

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1,n-1} & a_{1n} \\ 0 & 0 & a_{23} & \cdots & a_{2,n-1} & a_{2n} \\ 0 & 0 & 0 & \cdots & a_{3,n-1} & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a_{n-1,n} \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

On procède par récurrence sur n. Si $n = 1$, alors $A = (0)$, et donc $A^1 = 0$. Supposons que $n > 1$ et la proposition est vraie pour $n - 1$. Posons

$$B = \begin{pmatrix} 0 & a_{12} & \cdots & a_{1,n-2} & a_{1,n-1} \\ 0 & 0 & \cdots & a_{2,n-2} & a_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{n-2,n-1} \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{n-1,n} \end{pmatrix}.$$

Alors
$$A = \begin{pmatrix} B & C \\ 0 & 0 \end{pmatrix}.$$
Remarquons que B est triangulaire supérieure d'ordre $n-1$ dont la diagonale est nulle. Ainsi $B^{n-1} = 0$ par hypothèse de récurrence. En particulier, $B^n = 0$. Or
$$A^2 = \begin{pmatrix} B^2 & BC \\ 0 & 0 \end{pmatrix}, \quad A^3 = \begin{pmatrix} B^3 & B^2C \\ 0 & 0 \end{pmatrix}, \quad \cdots, \quad A^i = \begin{pmatrix} B^i & B^{i-1}C \\ 0 & 0 \end{pmatrix}.$$
En particulier, on a
$$A^n = \begin{pmatrix} B^n & B^{n-1}C \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$
Ceci achève la démonstration de la proposition.

2.3. Rang

Soit $A = (a_{ij})_{m\times n}$ une matrice sur K. Un terme a_{i_1,j_1} est dit *plus à gauche* que a_{i_2,j_2} si $j_1 < j_2$. Par exemple, le $(3,2)$-terme d'une matrice est plus à gauche que le $(1,5)$-terme.

2.3.1. Définition. Une matrice A de m lignes est dite *échelonnée* si, pour tout i avec $1 < i \leq m$, la condition suivante est vérifiée:

Si la i-ième ligne de A est non nulle, alors la $(i-1)$-ième ligne est non nulle et son premier terme non nul est plus à gauche que le premier terme non nul de la i-ième ligne.

En outre, si A est échelonnée, alors le premier terme non nul d'une ligne non nulle s'appelle le *pivot* de cette ligne.

Remarque. Chaque ligne, ainsi que chaque colonne, d'une matrice échelonnée contient au plus un pivot.

Exemple. (1) Une matrice ayant une seule ligne est échelonnée.

(2) Une matrice nulle est échelonnée sans pivots.

(3) La matrice identité d'ordre n est échelonnée ayant n pivots.

2.3.2. Définition. Les opérations suivantes s'appellent *opérations élémentaires* sur les lignes d'une matrice sur K:

Type 1: Échanger deux lignes, notée $L_i \leftrightarrow L_j$ avec $i \neq j$.

Type 2: Additionner à une ligne un multiple d'une autre ligne, notée $L_i + aL_j$ avec $i \neq j$.

Type 3: Multiplier une ligne par un élément non nul de K, notée aL_i avec $a \neq 0$.

En outre, on dit qu'une matrice A *se réduit* à une matrice B si B est obtenue à partir de A par une suite finie d'opérations élémentaires sur les lignes.

Remarque. Les opérations élémentaires ne changent pas le type d'une matrice.

On rassemble des propriétés des opérations élémentaires dans les deux résultats suivants.

2.3.3. Lemme. Toute opération élémentaire T sur les lignes d'une matrice est inversible. Plus précisément,

(1) si T est $L_i \leftrightarrow L_j$, alors T^{-1} est $L_i \leftrightarrow L_j$;

(2) si T est $L_i + aL_j$ avec $i \neq j$, alors T^{-1} est $L_i - aL_j$;

(3) si T est aL_i avec $a \neq 0$, alors T^{-1} est $a^{-1}L_i$.

2.3.4. Proposition. Soient A, B, et C des matrices sur K.

(1) A se réduit à A.

(2) Si A se réduit à B et B se réduit à C, alors A se réduit à C.

(3) Si A se réduit à B, alors B se réduit à A.

(4) Si A se réduit à B, alors $A = 0$ si et seulement si $B = 0$.

Démonsatrion. Les deux premiers énnoncés sont évidents. Et l'énoncé (3) est une conséquence immédiate du lemme 2.3.3. Enfin, supposons que A se réduisant à B. Si $A = 0$, alors il est évident que $B = 0$. Supposons que $B = 0$. Comme B se réduit à A, on voit que $A = 0$. Ceci achève la démonstration.

On a maintenant le résultat fondamental suivant.

2.3.5. Théorème. Toute matrice A sur K se réduit à une matrice échelonnée, appelée une *forme échelonnée* de A.

Démonstration. Posons $A = (a_{ij})_{m \times n}$. On procède par récurrence sur m, le nombre de lignes de A. Si $m = 1$, alors A est échelonnée. Supposons que $m > 1$ et le théorème est vrai pour les matrices de $m-1$ lignes. Si $A = 0$, alors A est échelonnée. Sinon, supposons que s est l'indice de colonne de la première colonne non nulle. En échangeant deux lignes si nécessaire, on peut supposer que $a_{1s} \neq 0$. En effectuant les opérations $L_2 - a_{1s}^{-1}a_{2s}L_1, \ldots, L_m - a_{1s}^{-1}a_{ms}L_1$ à partir de A, on obtient une matrice de la forme

$$B = \begin{pmatrix} 0 & \cdots & 0 & a_{1s} & a_{1,s+1} & \cdots & a_{1n} \\ 0 & \cdots & 0 & 0 & b_{2,s+1} & \cdots & b_{2n} \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & b_{m,s+1} & \cdots & b_{mn} \end{pmatrix} := \begin{pmatrix} B_1 \\ C \end{pmatrix},$$

où B_1 est la première ligne de Bk, et C est la sous-matrice de B formée des $m-1$ dernières lignes de B. Par l'hypothèse de récurrence, on peut réduire C à une matrice échelonnée E_1. Maintenant, en effectuant les mêmes opérations élémentaires sur les $m-1$ dernières lignes de B, on obtient la matrice

$$\begin{pmatrix} B_1 \\ E_1 \end{pmatrix}.$$

Cette dernière est échelonnée, car $a_{1s} \neq 0$ et les pivots de E_1 se trouvent dans les $n-s$ dernières colonnes. Ceci achève la démonstration du théorème.

Remarque. Si A est échelonnée, alors A est une forme échelonnée d'elle-même.

Comme on a vu, une matrice A peut posséder plusieurs formes échelonnées. Mais le résultat suivant, dont la démonstration se trouve dans le chapitre IV, nous dit que le nombre de pivots de ces formes échelonnées est un invariant de A.

2.3.6. Proposition. Soit A une matrice sur K. Les formes échelonnées de A ont le même nombre de pivots. Ce nombre commun s'appelle le *rang* de A, noté $\mathrm{rg}(A)$.

Remarque. Le rang d'une matrice échelonnée est le nombre de pivots, c'est-à-dire, le nombre de lignes non nulles.

Exemple. $\mathrm{rg}(0_{m\times n}) = 0$ et $\mathrm{rg}(I_n) = n$.

2.3.7. Lemme. Soit A une matrice de type $m \times n$.
(1) $\mathrm{rg}(A) \leq \min\{m, n\}$.
(2) $\mathrm{rg}(A) = 0$ si et seulement si $A = 0_{m\times n}$.
(3) Si A se réduit à B, alors $\mathrm{rg}(A) = \mathrm{rg}(B)$.
(4) Si B est obtenue à partir de A en supprimant des lignes nulles, alors $\mathrm{rg}(A) = \mathrm{rg}(B)$.
Démonstration. Soit E une forme échelonnée de A.

(1) Comme une ligne ainsi qu'une colonne de E contient au plus un pivot, le nombre de pivots de E est inférieur ou égal à m et à n. Par conséquent, $\mathrm{rg}(A) \leq \min\{m, n\}$.

(2) Supposons que $\mathrm{rg}(A) = 0$. Alors E n'a aucun pivot, c'est-à-dire, E est nulle. D'après la proposition 2.3.4(4), A l'est aussi.

(3) Supposons que A se réduit à B. D'après la proposition 2.3.4(3), B se réduit à A. D'après la proposition 2.3.4(2), B se réduit à E. Cela veut dire que E est aussi une forme échelonnée de B. Donc $\mathrm{rg}(B) = \mathrm{rg}(A)$.

(4) En échangeant des lignes si nécessaire, A se réduit à une matrice de la forme $\binom{B}{0}$. Supposons que B se réduit à une matrice échelonnée E'. Alors $\binom{B}{0}$ se réduit à la matrice $\binom{E'}{0}$ par les même opérations élémentaires. Remarquons que $\binom{E'}{0}$ est échelonnée de même rang que E'. Ainsi

$$\mathrm{rg}(A) = \mathrm{rg}\begin{pmatrix} E' \\ 0 \end{pmatrix} = \mathrm{rg}(E') = \mathrm{rg}(B).$$

Ceci achève la démonstration du lemme.

2.3.8. Définition. On appelle *matrice élémentaire* une matrice obtenue à partir d'une matrice identité par une seule opération élémentaire. Plus précisément, il existe trois types de matrices élémentaires comme suit:

$$\text{Type 1 :} \qquad E_{i,j} = \begin{pmatrix} e_1 \\ \vdots \\ e_j \\ \vdots \\ e_i \\ \vdots \\ e_n \end{pmatrix} = \begin{array}{c} \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \end{array} \begin{array}{l} \\ \\ \leftarrow i\text{-ième} \\ \\ \leftarrow j\text{-ième} \\ \\ \\ \end{array} , \qquad i < j.$$

$$\text{Type 2 :} \quad E_{ij}(a) = \begin{pmatrix} e_1 \\ \vdots \\ e_i + ae_j \\ \vdots \\ e_j \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & a & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{array}{l} \\ \\ \leftarrow i\text{-ième} \\ \\ \leftarrow j\text{-ième} \\ \\ \\ \end{array} \qquad i < j.$$

$$
E_{ij}(a) = \begin{pmatrix} e_1 \\ \vdots \\ e_j \\ \vdots \\ e_i + ae_j \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & a & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{array}{l} \\ \\ \leftarrow j\text{-ième} \\ \\ \leftarrow i\text{-ième} \\ \\ \\ \end{array} \qquad i > j.
$$

$$
\text{Type 3 :} \qquad E_i(a) = \begin{pmatrix} e_1 \\ \vdots \\ e_{i-1} \\ ae_i \\ e_{i+1} \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & a & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{array}{l} \\ \\ \\ \leftarrow\ i\text{-ième}\ a \neq 0. \\ \\ \\ \\ \end{array}
$$

Le résultat suivant donne une interprétation algébrique de la réduction de matrices par des opérations élémentaires sur les lignes.

2.3.9. Proposition. Soit A une matrice sur K de m lignes. Effectuer une opération élémentaire sur les lignes de A est équivalent à multiplier A à gauche par la matrice élémentaire correspondante de type $m \times m$.

Démonstration. Soit A une matrice ayant pour lignes $L_1, L_2, \ldots, L_m$. Soit e_i la i-ième ligne de I_m. Alors

$$
E_{i,j}A = \begin{pmatrix} e_1 \\ \vdots \\ e_j \\ \vdots \\ e_i \\ \vdots \\ e_m \end{pmatrix} A = \begin{pmatrix} e_1A \\ \vdots \\ e_jA \\ \vdots \\ e_iA \\ \vdots \\ e_mA \end{pmatrix} = \begin{pmatrix} L_1 \\ \vdots \\ L_j \\ \vdots \\ L_i \\ \vdots \\ L_m \end{pmatrix} \begin{array}{l} \\ \\ \leftarrow\ i\text{-ième} \\ \\ \leftarrow\ j\text{-ième} \\ \\ \\ \end{array}.
$$

De même façon, on trouve que

$$E_{ij}(a)A = \begin{pmatrix} e_1 \\ \vdots \\ e_i + ae_j \\ \vdots \\ e_m \end{pmatrix} A = \begin{pmatrix} e_1A \\ \vdots \\ e_iA + ae_jA \\ \vdots \\ e_mA \end{pmatrix} = \begin{pmatrix} L_1 \\ \vdots \\ L_i + aL_j \\ \vdots \\ L_m \end{pmatrix} \begin{array}{l} \\ \\ \leftarrow i\text{-ième} \\ \\ \\ \end{array}.$$

$$E_i(a)A = \begin{pmatrix} e_1 \\ \vdots \\ ae_i \\ \vdots \\ e_m \end{pmatrix} A = \begin{pmatrix} e_1A \\ \vdots \\ ae_iA \\ \vdots \\ e_mA \end{pmatrix} = \begin{pmatrix} L_1 \\ \vdots \\ aL_i \\ \vdots \\ L_m \end{pmatrix}.$$

Ceci achève la démonstration de la proposition.

2.3.10. Corollaire. Si $A, B \in M_{m\times n}(K)$, alors A se réduit à B si, et seulement si, il existe des matrices élémentaires $E_r, \ldots, E_2, E_1$ telles que

$$B = E_r \cdots E_2 E_1 A.$$

2.4 Inverse

Tout élément non nul a de K admet un inverse b de sorte que $ab = ba = 1$. Ce n'est pas vrai en général pour les matrices. Tout d'abord, pour que AB et BA soient définis, A et B devraient être carrées de même ordre. Même si A est carrée d'ordre n, il n'existe pas nécessairement une matrice B telle que $AB = BA = I_n$.

2.4.1. Lemme. Soit $A \in M_n(K)$. S'il existe $B \in M_n(K)$ telle que $AB = BA = I_n$, alors B est unique. Dans ce cas, on dit que A est *inversible* et B est l'*inverse* de A, notée $B = A^{-1}$.

Démonstration. Soient $B, C \in M_n(K)$ telles que $AB = BA = I_n$ et $AC = CA = I_n$. Alors

$$B = BI_n = B(AC) = (BA)C = I_nC = C.$$

Ceci achève la démonstration du lemme.

Exemple. I_n est inversible et $0_{n\times n}$ ne l'est pas.

On vérife que $AB = I_2$, mais que A est non inversible.

2.4.2. Lemme. (1) Si A est inversible, alors A n'a ni ligne nulle ni colonne nulle.
(2) Si A est inversible, alors $(A^{-1})^{-1} = A$ et $(A^T)^{-1} = (A^{-1})^T$.
(3) Si $A_1, \ldots, A_r \in M_n(K)$ sont toutes inversibles, alors

$$(A_1 \cdots A_r)^{-1} = A_r^{-1} \cdots A_1^{-1}.$$

Démonstration. (1) Supposons que la i-ième ligne A_i de A est nulle. Pour toute $B \in M_n(K)$, la i-ième ligne de AB est $A_iB = 0$. Ainsi $AB \neq I_n$. C'est-à-dire, A est non inversible.

(2) D'après la définition, $A^{-1} \cdot A = A \cdot A^{-1} = I$. Ainsi A^{-1} est inversible et $(A^{-1})^{-1} = A$. En outre, $I = I^T = (A^{-1} \cdot A)^T = A^T(A^{-1})^T$. De même, $(A^{-1})^T A^T = I$. Ainsi A^T est inversible et $(A^T)^{-1} = (A^{-1})^T$.

(3) Si $r = 2$, alors $(A_2^{-1}A_1^{-1})(A_1A_2) = A_2^{-1}(A_1^{-1}A_1)A_2 = A_2^{-1}IA_2 = A^{-1}A_2 = I$. De même, $(A_1A_2)(A_2^{-1}A_1^{-1}) = I$. Ainsi A_1A_2 est inversible et $(A_1A_2)^{-1} = A_2^{-1}A_1^{-1}$. Supposons que $r > 2$ et $(A_1 \cdots A_{r-1})^{-1} = A_{r-1}^{-1} \cdots A_1^{-1}$. Alors $A_1 \cdots A_r = (A_1 \cdots A_{r-1})A_r$ est inversible et

$$(A_1 \cdots A_r)^{-1} = [(A_1 \cdots A_{r-1})A_r]^{-1} = A_r^{-1}(A_1 \cdots A_{r-1})^{-1} = A_r^{-1}A_{r-1}^{-1} \cdots A_1^{-1}.$$

Ceci achève la démonstration.

2.4.3. Lemme. Soient A, B, C des matrices sur K avec A inversible.
(1) Si $AB = C$, alors $B = A^{-1}C$.
(2) Si $BA = C$, alors $B = CA^{-1}$.
(3) Si $AB = 0$, alors $B = 0$.
(4) Si $AB = AC$, alors $B = C$.

Démonstration. (1) Si $AB = C$, alors $A^{-1}(AB) = A^{-1}C$. Donc $(A^{-1}A)B = A^{-1}C$. Ainsi $B = A^{-1}C$. De même, si $BA = C$, alors $B = CA^{-1}$. Si $AB = 0$, d'après (1), $B = A^{-1}0 = 0$. Si $AB = AC$, alors $A(B - C) = 0$. D'après (3), $B - C = 0$, c'est-à-dire, $B = C$. Ceci achève la démonstration.

Le problème se pose de savoir quand une matrice carrée est inversible et comment trouver son inverse s'il existe.

2.4.4. Lemme. Une matrice élémentaire E est inversible avec E^{-1} une matrice élémentaire de même type. Plus précisément, les énoncés suivants sont valides.

(1) Si $i \neq j$, alors $E_{i,j}^{-1} = E_{i,j}$.

(2) Si $i \neq j$ et $a \in K$, alors $E_{ij}(a)^{-1} = E_{ij}(-a)$.

(3) Si $a \in K$ est non nul, alors $E_i(a)^{-1} = E_i(a^{-1})$.

Démonstration. (1) Comme $E_{i,j}$ se réduit à I_n par l'opération $L_i \leftrightarrow L_j$, on a $E_{i,j}E_{i,j} = I_n$. Donc $E_{i,j}^{-1} = E_{i,j}$.

(2) Comme $E_{ij}(a)$ se réduit à I_n par l'opération $L_i - aL_j$, on a $E_{ij}(-a)E_{ij}(a) = I_n$. Remplaçant a par $-a$, on obtient $E_{ij}(-(-a))E_{ij}(-a) = I_n$, c'est-à-dire, $E_{ij}(a)E_{ij}(-a) = I_n$. Ceci implique $(E_{ij}(a))^{-1} = E_{ij}(-a)$.

(3) Comme $E_i(a)$ se réduit à I_n par l'opération $a^{-1}L_i$, on a $E_i(a^{-1})E_i(a) = I_n$. Remplaçant a par a^{-1}, on a $E_i((a^{-1})^{-1})E_i(a^{-1}) = I_n$, c'est-à-dire, $E_i(a)E_i(a^{-1}) = I_n$. Ceci montre $(E_i(a))^{-1} = E_i(a^{-1})$. Ceci achève la démonstration.

Remarque. Un produit de matrices élémentaires est inversible.

2.4.5. Corollaire. Soit A une matrice carrée sur K. Si A se réduit à une matrice B, alors A est inversible si et seulement si B l'est.

Démonstration. Supposons que A se réduit à une matrice B. Supposons que A est inversible. D'après le corollaire 2.3.10, il existe des matrices élémentaires $E_r, \ldots, E_1$ telles que $(E_r \cdots E_1)A = B$ Comme $E_r \cdots E_1$ est inversible, B l'est aussi.

Supposons réciproquement que B est inversible. D'après la proposition 2.3.4(3). B se réduit à A. Comme on a vu, A l'est également. Ceci achève la démonstration.

2.4.6. Lemme. Soit A une matrice échelonnée de type $m \times n$. Si A a n pivots, alors $m \geq n$ et les pivots sont $a_{11}, a_{22}, \cdots, a_{nn}$.

Démonstration. Supposons que $\operatorname{rg}(A) = n$. Alors $n \leq \min\{m, n\} \leq m$. Soient $a_{1j_1}, a_{2j_2}, \ldots, a_{nj_n}$ les pivots. Comme $1 \leq j_1 < j_2 < \cdots < j_n \leq n$, on a $j_1 = 1$, $j_2 = 2$, $\cdots$, $j_n = n$. C'est-à-dire, $a_{11}, a_{22}, \cdots, a_{nn}$ sont les pivots. Ceci achève la démonstration.

2.4.7. Lemme. Si $A \in M_n(K)$ est échelonnée de rang n, alors on peut réduire A à I_n en éliminant les termes au-dessus de pivots à partir du dernier pivot.

Démonstration. D'après le lemme 2.4.6, A est de la forme

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n-1} & a_{1n} \\ 0 & a_{22} & \cdots & a_{2,n-1} & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & 0 & \cdots & 0 & a_{nn} \end{pmatrix}, \quad a_{ii} \neq 0.$$

En effectuant les opérations $a_{ii}^{-1}L_i, i = 1, \ldots, n$, on obtient une matrice comme suit:

$$B = \begin{pmatrix} 1 & b_{12} & \cdots & b_{1,n-1} & b_{1n} \\ 0 & 1 & \cdots & b_{2,n-1} & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & b_{n-1,n} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

En effectuant les opérations $L_i - b_{in}L_n,\ i = 1, \ldots, n-1$, on obtient la matrice suivante:

$$C = \begin{pmatrix} 1 & b_{12} & \cdots & b_{1,n-1} & 0 \\ 0 & 1 & \cdots & b_{2,n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

On peut continuer ce procédé jusqu'à ce que l'on obtient la matrice identité I_n. Donc A se réduit à I_n. Ceci achève la démonstration du lemme.

2.4.8. Théorème. Soit $A \in M_n(K)$. Les conditions suivantes sont équivalentes:
(1) A est inversible.
(2) $\mathrm{rg}(A) = n$.
(3) A se réduit à I_n.
(4) A se factorise en produit de matrices élémentaires.

Démonstration. Soit E une forme échelonnée de A.

Supposons que A est inversible. D'après le corollaire 2.4.5, E est inversible. D'après le lemme 2.4.2(1), E ne contient aucune ligne nulle. Ainsi, E admet n pivots, c'est-à-dire, $\mathrm{rg}(A) = n$.

Supposons que $\mathrm{rg}(A) = n$. C'est-à-dire, E admet n pivots. D'après le lemme 2.4.7, E se réduit à I_n. Ainsi A se réduit à I_n.

Supposons que A se réduit à I_n. D'après la proposition 2.3.4(3), I_n se réduit à A. D'après le corollaire 2.3.10, il existe des matrices élémentaires $E_r, \ldots, E_1$ telles que

$$A = (E_r \cdots E_1)I_n = E_r \cdots E_1.$$

Enfin, supposons que $A = E_1 \cdots E_r$, où les E_i sont élémentaires. D'après le lemme 2.4.4, les E_i sont toutes inversible, et d'après le lemme 2.4.2(3), A est inversible. Ceci achève la démonstration du théorème.

Exercice. Fractoriser, si possible, la matrice suivante en produit de matrices élémentaires:

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

Exercice. Considérons la matrice réelle suivante:

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

Trouver les valeurs réelles de α pour que A soit inversible.

2.4.9. Théorème. Soit A, B des matrices de n lignes sur K. Si A est inversible, alors
(1) $(A|B)$ s'échelonne à $(I_n|\, C)$, où $C = A^{-1}B$;
(2) $(A|I_n)$ s'échelonne à $(I_n|\, D)$, où $D = A^{-1}$.

Démonstration. Supposons que A est inversible. D'après le théorème 2.4.8(3), A s'échelonne à I_n. D'après le corollaire 2.3.10, il existe des matrices élémentaires $E_r, \ldots, E_1$ telles que $(E_r \cdots E_1)A = I_n$. Multipliant par blocs, on obtient

$$(E_r \cdots E_1)(A|B) = ((E_r \cdots E_1)A|(E_r \cdots E_1)B) = (I_n|C).$$

C'est-à-dire, $(A|B)$ s'échelonne à $(I_n|\, C)$. Maintenant, $(E_r \cdots E_1)A = I_n$ et $C = (E_r \cdots E_1)B$. Donc, $E_r \cdots E_1 = A^{-1}$ et $C = A^{-1}B$. Ceci montre l'énoncé (1).

Posant $B = I_n$ dans l'énoncé (1), on obtient l'énoncé (2). La preuve du théorème s'achève.

Exercice. Calculer $A^{-1}B$ et A^{-1} où

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 3 & 4 \\ 1 & 2 & 0 \end{pmatrix}.$$

2.5. Exercices

1. Calculer les produits suivants de matrices complexes:

(1) $\begin{pmatrix} 1-i & \sqrt{2}-3i & \sqrt{3}i \\ \pi+i & \sqrt{11}+\sqrt{5}i & 4\pi \end{pmatrix} \begin{pmatrix} i & 0 & 0 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & 0 \end{pmatrix}$;

(2) $\begin{pmatrix} 3 & 0 & 1 & 2 \\ 0 & 9 & 0 & 7 \\ 0 & 8 & 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \\ i & -1 & 1+i \end{pmatrix}$.

2. Sur le corps $\mathbb{Z}_{29} = \{0, 1, 2, \ldots, 28\}$, calculer

$$17^{-1} \times \begin{pmatrix} 7 & 8 & 9 \\ 1 & 3 & 7 \end{pmatrix} - 15 \times \begin{pmatrix} 3 & 7 & 9 \\ 5 & 0 & 16 \end{pmatrix}.$$

3. Considérer les matrices rationnelles suivantes:

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & -8 \\ 2 & 3 \end{pmatrix} \quad \text{et} \quad C = \begin{pmatrix} 5 & 2 \\ 1 & -2 \end{pmatrix}.$$

Vérifier que $AB = AC$ mais que $B \neq C$.

4. Considérer les matrices rationnelles suivantes:

$$A = \begin{pmatrix} 7 & 4 \\ 5 & x \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 3 & -4 \\ -5 & 1 \end{pmatrix}.$$

Pour quelle valeur de x, a-t-on que $AB = BA$?

5. (1) Soient $A, B \in M_n(K)$. Si $AB = BA$, montrer la formule du binôme suivante:

$$(A+B)^r = \sum\nolimits_{s=0}^{r} \binom{r}{s} A^s B^{r-s}.$$

(2) Vérifier si l'équalité $(A+B)^2 = A^2 + 2AB + B^2$ est vraie ou non dans le cas suivant :

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

6. (1) Soit $A \in M_n(K)$. À l'aide du numéro précédent montrer, pour tout $r > 0$, que

$$(A + I_n)^r = \sum\nolimits_{s=0}^{r} \binom{r}{s} A^s.$$

(2) À l'aide de la partie (1), pour tout entier positif r, calculer

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}^r.$$

7. Montrer, pour tout $n \geq 1$, que

$$\begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}^n = \begin{pmatrix} a_n & b_n & b_n \\ b_n & a_n & b_n \\ b_n & b_n & a_n \end{pmatrix},$$

où

$$a_n = \frac{1}{3}(2^{n+1} + (-1)^n), \ b_n = -\frac{1}{3}(2^n + (-1)^{n-1}).$$

8. (1) Considérer deux matrices symétriques suivantes:

$$A = \begin{pmatrix} a & c \\ c & b \end{pmatrix}, \ B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Trouver la condition nécesaire et suffisante pour que AB soit symétrique.

(2) Est-ce que le produit de deux matrices symétriques de même type est toujours symétrique?

9. Soient A et B deux matrices symétriques de même type.

(1) Montrer que $A + B$ et $A - B$ sont symétriques.

(2) Si $AB = BA$, montrer que AB est symétrique.

10. Soit A une matrice carrée complexe. Montrer que $A = B + C$ avec B symétrique et C antisymétrique. *Indice*: Vérifier que $A + A^T$ est symétrique et $A - A^T$ est antisymétrique.

11. Montrer, pour toute matrice A, que les matrices AA^T et $A^T A$ sont symétriques.

12. Montrer, pour toutes $A, B \in M_n(\mathbb{C})$, que $AB - BA \neq I_n$.

Indice: Comparer la trace de $AB - BA$ avec celle de I_n.

13. À l'aide du lemme 2.2.5, donner la deuxième ligne, ainsi que la troisième colonne, du produit de matrices complexes suivant :

$$\begin{pmatrix} 3 & 0 & 1 & 2 \\ 0 & 9 & 0 & 7 \\ 0 & 8 & 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \\ i & -1 & 1+i \end{pmatrix}.$$

14. Calculer, à l'aide du lemme 2.2.5 et du corollaire 2.2.6, les produits de matrices suivants.

(1) $$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1+i & 0 & \sqrt{2}-\sqrt{3}i & 4+5i & 6-7i & 3-2i \\ 3-5i & 7-6i & 0 & \sqrt{11} & 3-i & 1+5i \\ 0 & 4-2i & \sqrt{5}+4i & 5-2i & 0 & 3i \\ \sqrt{7} & 0 & 0 & 7+2i & 0 & 7-8i \end{pmatrix}.$$

(2) $$\begin{pmatrix} 1+i & \sqrt{7} & 4+5i & 6-7i & 3-2i \\ 3-5i & 7-6i & \sqrt{11} & 3-i & 1+5i \\ 0 & 4-2i & 5-2i & 0 & 3i \\ \sqrt{5} & 0 & 7+2i & 0 & 7-8i \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

15. Calculer, à l'aide du corollaire 2.2.7, les produits suivants de matrices sur $\mathbb{Z}_{11}$:

(1) $$\begin{pmatrix} 7 & 0 & 0 & 0 \\ 0 & 9 & 0 & 0 \\ 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} 7 & 8 & 0 & 9 & 2 \\ 2 & 9 & 3 & 8 & 0 \\ 5 & 4 & 8 & 7 & 9 \\ 3 & 5 & 7 & 9 & 8 \end{pmatrix};$$ (2) $$\begin{pmatrix} 7 & 8 & 0 & 9 & 2 \\ 2 & 9 & 3 & 8 & 0 \\ 5 & 4 & 8 & 7 & 9 \\ 3 & 5 & 7 & 9 & 8 \end{pmatrix} \begin{pmatrix} 3 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{pmatrix}.$$

16. Soit $A \in M_n(K)$. Montrer que $AB = BA$ pour toute $B \in M_n(K)$ si et seulement si $A = \lambda I_n$ avec $\lambda \in K$. *Indice*: Considérer l'équation $Ae_{ji} = e_{ji}A$ pour tous $1 \leq i, j \leq n$ avec $i \neq j$.

17. Soit $A = (a_{ij})_{n\times n}$ une matrice carrée d'ordre n sur K. Montrer, pour tous $x_1, \ldots, x_n$; $y_1, \ldots, y_n \in K$, que
$$(x_1, \ldots, x_n)A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \sum_{1\leq i,j\leq n}^{n} a_{ij}\, x_i y_j.$$

18. À l'aide du numéro précédent,

 (1) calculer
$$(x_1, x_2, x_3) \begin{pmatrix} 2 & -1 & 0 \\ 0 & -1 & 2 \\ 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix};$$

(2) trouver la matrice A telle que

$$(x_1, x_2, x_3)A \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = x_1y_1 - 4x_1y_2 + 3x_2y_1 + 7x_2y_2 - 5x_3y_2 + 7x_3y_3.$$

19. Soit A une matrice carrée qui est partagée comme suit:

$$A = \begin{pmatrix} B & C \\ 0 & 0 \end{pmatrix},$$

où B est une matrice carrée. Montrer par récurrence que

$$A^n = \begin{pmatrix} B^n & B^{n-1}C \\ 0 & 0 \end{pmatrix},$$

pour tout $n \geq 1$. En déduire que A est nilpotente si et seulement si B est nilpotente.

20. Considérer la matrice carrée d'ordre n suivante:

$$A_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \quad (n \geq 2).$$

Montrer que $A^{n-1} \neq 0$ et $A^n = 0$. *Indice*: Procéder par récurrence en utilisant la multiplication par blocs et le numéro précedent.

21. Trouver le rang de chacune des matrices sur $\mathbb{Z}_5$ suivantes:

$$(1) \quad \begin{pmatrix} 2 & 1 & 2 \\ 3 & 1 & 4 \\ 4 & 4 & 0 \end{pmatrix}; \qquad (2) \quad \begin{pmatrix} 1 & -1 & 3 & 0 \\ 3 & -1 & 2 & 0 \\ 2 & -1 & 4 & 0 \\ 2 & 1 & 1 & 3 \end{pmatrix}; \qquad (3) \quad \begin{pmatrix} 0 & -1 & 2 & 4 \\ 0 & 1 & 3 & 2 \\ 0 & 1 & 3 & 2 \\ 0 & 1 & -1 & 2 \end{pmatrix}.$$

22. Considérer la matrice complexe suivante :

$$\begin{pmatrix} -1 & x & 0 & 0 \\ 0 & -1 & x & 0 \\ 0 & 0 & -1 & x \\ 1 & -1 & -1 & -2 \end{pmatrix}.$$

Vérifier que $\mathrm{rg}(A) \geq 3$, et trouver les valeurs complexes de x pour que A soit de rang 4.

23. Considérer la matrice carrée suivante sur un corps :

$$A_n = \begin{pmatrix} -1 & x & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & x & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & x & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 & x \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 & a_0 \end{pmatrix} \quad (n \geq 1).$$

Vérifier que $\operatorname{rg}(A) \geq n$, et trouver la condition sur x pour que A soit de rang $n+1$.

24. Selon la valeur de a, déterminer le rang de la matrice suivante:

$$A = \begin{pmatrix} 1 & 1 & 1-2a & 2(1+a) \\ 1+a & -(1+a) & 2+a & 0 \\ 2 & -2a & 3 & 2(1+a) \end{pmatrix}.$$

25. Dans chacun des cas suivants, trouver des matrices élémentaires $E_r, \cdots, E_2, E_1$ telles que $E_r \cdots E_2 E_1 A$ est échelonnée, et en déduire le rang de A.

(1) $A = \begin{pmatrix} 1+i & 2 \\ 2+2i & 5 \end{pmatrix}$; (2) $A = \begin{pmatrix} 0 & 0 & 4 \\ 0 & 5 & 0 \\ \sqrt{2} & 0 & 0 \end{pmatrix}$;

(3) $A = \begin{pmatrix} 1 & 1 & 2 & -3 \\ 2 & 3 & 6 & -5 \\ 3 & -1 & 2 & -7 \\ 1 & 2 & 3 & -1 \end{pmatrix}$; (4) $A = \begin{pmatrix} 1 & -1 & 2 & -1 \\ 3 & 1 & 4 & 3 \\ -5 & -3 & -6 & -7 \\ -2 & 2 & -4 & 2 \\ -1 & 1 & 1 & 1 \end{pmatrix}$.

26. Montrer qu'une matrice diagonale est inversible si et seulement si les termes diagonaux sont tous non nuls, et trouver l'inverse dans ce cas.

27. Soit $A \in M_n(K)$ inversible. Si $a \in K$ est non nul, montrer que aA est inversible avec $(aA)^{-1} = a^{-1}A^{-1}$.

28. Pour quelle valeur rationnelle de x, la matrice suivante, est-elle inversible?

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 5-x & 1 \\ 2 & 4 & x+3 \end{pmatrix}.$$

29. Déterminer si la matrice rationnelle

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

est inversible ou non. Si oui, factoriser A en produit de matrices élémentaires.

30. Considérer les matrices sur $\mathbb{Z}_7$ suivantes.

$$(1) \quad \begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix}; \qquad\qquad (2) \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 0 \\ 2 & 3 & 1 \end{pmatrix}.$$

Dans chacun des cas, factoriser la matrice en produit de matrices élémentaires.

31. Soient A et B deux matrices sur K de même type. Montrer que A se réduit à B si, et seulement si, il existe une matrice inversible P telle que $B = PA$.

32. Soient $A = (A_1 \cdots A_n)$ et $B = (B_1 \cdots B_n)$ deux matrices de même type partagées en colonnes. Soient $A' = (A_{j_1} \cdots A_{j_r})$ et $B' = (B_{j_1} \cdots B_{j_r})$ avec $j_1, \ldots, j_r \in \{1, \cdots n\}$. Si A se réduit à B, montrer que A' se réduit à B'. *Indice*: Utiliser le numéro précédent et appliquer la multiplication par blocs.

33. Soient A, B des matrices sur un corps telles que AB soit défini. Si A se réduit à C par des opérations élémentaires sur les lignes, alors AB se réduit à CB par les mêmes opérations élémentaires.

34. Si possible, trouver l'inverse de la matrice suivante sur $\mathbb{Z}_7$:

$$\begin{pmatrix} 3 & 4 & 5 & 1 \\ 3 & 5 & 5 & 2 \\ 6 & 0 & 1 & 6 \\ 3 & 5 & 5 & 3 \end{pmatrix}.$$

35. Trouver l'inverse de chacune des matrices complexes suivantes s'il existe.

$$(1) \quad \begin{pmatrix} 1+i & 2-i \\ 2+i & 1-i \end{pmatrix}; \qquad\qquad (2) \quad \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix};$$

(3) $\begin{pmatrix} 1 & 1 & 2 & -3 \\ 2 & 3 & 6 & -5 \\ 3 & -1 & 2 & -7 \\ 6 & 3 & 10 & -15 \end{pmatrix}$; (4) $\begin{pmatrix} 1 & 1 & 2 & 3 \\ 2 & 3 & 6 & 5 \\ 3 & 3 & 2 & 1 \\ 1 & 1 & 3 & 1 \end{pmatrix}$.

36. Trouver une matrice X telle que

$$\begin{pmatrix} 1 & 1 & 2 & 3 \\ 2 & 3 & 6 & 5 \\ 3 & 3 & 2 & 1 \\ 1 & 1 & 3 & 1 \end{pmatrix} X = \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix}.$$

37. Considérer la matrice sur $\mathbb{Z}_2$ suivante:

$$A_n = \begin{pmatrix} 0 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{pmatrix}_{n\times n}.$$

Montrer que A_n est inversible si et seulement si n est pair; et dans ce cas, trouver l'inverse de A_n.

38. Trouver, pour tout $n \geq 2$, l'inverse de la matrice suivante:

$$A_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ \rho & 1 & 0 & \cdots & 0 & 0 \\ \rho^2 & \rho & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \rho^{n-1} & \rho^{n-2} & \rho^{n-3} & \cdots & \rho & 1 \end{pmatrix}.$$

Indice: Essayer premièrement pour $n = 2, 3$ pour avoir une conjecture, ensuite montrer par récurrence la conjecture en utilisant la multiplication par blocs.

39. Soit A une matrice carrée d'ordre n. Si une matrice partagée $(A|B_1|\cdots|B_r)$ se réduit à la matrice partagée $(I_n|C_1|\cdots|C_r)$, montrer que $C_i = A^{-1}B_i$, $i = 1, \ldots, r$.

40. À l'aide du problème précédent, calculer $A^{-1}B, A^{-1}C$, et $A^{-1}D$, où

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \ B = \begin{pmatrix} 2 & 3 \\ 3 & 2 \\ 4 & 5 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ -1 & 7 \end{pmatrix}, D = \begin{pmatrix} 1+i \\ 2-i \\ 1-i \end{pmatrix}.$$

41. Soit $A \in M_n(K)$ nilpotente.

    (1) Montrer que A n'est pas inversible.

    (2) Si $A^r = 0$ avec $r > 0$, montrer que $(I - A)^{-1} = I + A + \cdots + A^{r-1}$.

    (3) En appliquant la partie (2), calculer l'inverse de la matrice suivante:

$$B = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & a & b \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

42. Soient A, B des matrices inversibles sur K. Montrer que

$$\begin{pmatrix} C & A \\ B & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & B^{-1} \\ A^{-1} & -A^{-1}CB^{-1} \end{pmatrix}$$

    et

$$\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & -A^{-1}CB^{-1} \\ 0 & B^{-1} \end{pmatrix}.$$

43. À l'aide du numéro précédent, calculer l'inverse de la matrice rationnelle suivante:

$$\begin{pmatrix} -1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 \\ -1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

44. Considérer une matrice carrée sur un corps K suivante:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} & a_{1,n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2,n-1} & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & 0 & \cdots & 0 & 0 \\ a_{n,1} & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

    Si $a_{i,n-i+1} \neq 0$ pour $i = 1, \cdots, n$, montrer que A est inversible. *Indice*: Procéder par récurrence en utilisant le numéro 41.

45. Une matrice de Vandermonde est une matrice carrée de la forme suivante:

$$V_n = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{pmatrix},$$

où $n \geq 2$ et les a_i sont deux à deux distincts. Montrer que V_n est inversible. *Indice*: À l'aide du numéro précédent, appliquer la récurrence sur V_n^T.

46. Soit $A \in M_n(K)$. S'il existe $B \in M_n(K)$ telle que $AB = I_n$, montrer que A est inversible.

Chapitre III: Systèmes d'équations linéaires

Beaucoup de problèmes dans les domaines de sciences et du génie se réduisent au problème de la résolution de systèmes d'équations linéaires. Dans ce chapitre, on étudiera les propriétés et la solution de systèmes d'équations linéaires.

Partout dans ce chapitre, K désignera un corps.

3.1. Définition. Un système d'équations linéaires sur K est un ensemble fini d'équations linéaires comme suit:

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m, \end{array}$$

où $a_{ij}, b_i \in K$. Les x_i s'appellent les *inconnues*; les a_{ij}, les *coefficients*; et les b_i, les *termes constants*. Une solution est un n-uplet $(s_1, s_2, \ldots, s_n)$ d'éléments de K tel que

$$a_{i1}s_1 + a_{i2}s_2 + \cdots + a_{in}s_n = b_i, \quad i = 1, 2, \ldots, m.$$

Le système est dit *compatible* s'il admet au moins une solution, et *incompatible* sinon.

Deux systèmes sont dits *équivalents* s'ils ont le même ensemble de solutions.

Remarque. Si l'on enlève une équation de la forme $0 = 0$ d'un système d'au moins deux équations linéaires, on obtient un système équivalent.

Exemple. Considérons un système de deux équations linéaires à deux inconnues x et y sur $\mathbb{R}$ suivant:

$$\begin{array}{ccccc} x & + & y & = & 2 \\ & & y & = & 0. \end{array}$$

Un couple $(a, b) \in \mathbb{R}^2$ est une solution de ce système si et seulement si le point (a, b) de l'espace $\mathbb{R}^2$ est le point d'intersection de la droite l passant par les points $(0, 2)$ et $(2, 0)$ et l'axe des x. Donc le système admet une seule solution $(2, 0)$. En particulier, le système est compatible.

On utilisera la théorie des matrices pour étudier les systèmes d'équations linéaires. Pour ce faire, on introduira la notion suivante.

3.2. Définition. Soit

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array} \qquad (*)$$

un système d'équations linéaires sur K. Les matrices

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad \text{et} \quad \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$

s'appellent respectivement la *matrice de coefficients* et la *matrice augmentée* du système.

Remarque. Un système d'équations linéaires est uniquement déterminé par sa matrice augmentée. De l'autre côté, toute matrice partagée $(A|B)$ avec B une matrice-colonne est la matrice augmentée d'un système d'équations linéaires.

3.3. Lemme. Un système d'équations linéaires

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array} \qquad (*)$$

est équivalent à l'équation matricielle

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \qquad (**)$$

de sorte que $(s_1, s_2, \ldots, s_n)$ est une solution du système $(*)$ si et seulement si la matrice-colonne

$$\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}$$

est une solution de l'équation matricielle $(**)$.

Démonstration. Pour tout n-uplet $(s_1, s_2, \cdots, s_n)$, on a

$$\begin{array}{ccccccccc} a_{11}s_1 & + & a_{12}s_2 & + & \cdots & + & a_{1n}s_n & = & b_1 \\ a_{21}s_1 & + & a_{22}s_2 & + & \cdots & + & a_{2n}s_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}s_1 & + & a_{m2}s_2 & + & \cdots & + & a_{mn}s_n & = & b_m \end{array}$$

si et seulement si

$$\begin{pmatrix} a_{11}s_1 + a_{12}s_2 + \cdots + a_{1n}s_n \\ a_{21}s_1 + a_{22}s_2 + \cdots + a_{2n}s_n \\ \vdots \\ a_{m1}s_1 + a_{m2}s_2 + \cdots + a_{mn}s_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

si et seulement si

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} s_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} s_2 + \cdots + \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} s_n = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

si et seulement si

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Ceci achève la démonstration.

Dès maintenant, un système de m équations linéaires à n inconnues sera noté comme une équation matricielle

$$AX = B,$$

où A est une matrice de type $m \times n$ et B est une matrice de type $m \times 1$.

Notre but est d'étudier la résolution d'un système d'équations linéaires. Ceci signifie que:
(1) déterminer si le système est compatible ou incompatible; et
(2) trouver toutes les solutions s'il est compatible.

On commence par un cas spécial où la matrice de coefficients du système est inversible.

3.4. Proposition. Soit $AX = B$ un système d'équations linéaires sur K. Si A est inversible, alors le système admet une seule solution donnée par

$$X = A^{-1}B.$$

Démonstration. Soit S une matrice-colonne de type $n \times 1$. Comme A est inversible, $AS = B$ si et seulement si $A^{-1}(AS) = A^{-1}B$ si et seulement si $S = A^{-1}B$. Ceci achève la démoncstration.

Exercice. Résoudre le système sur $\mathbb{Q}$ suivant:

$$\begin{array}{rcrcrcr} x & - & y & + & z & = & 6 \\ 3x & - & y & + & z & = & 0 \\ x & + & 4y & - & z & = & -6. \end{array}$$

Ensuite, on étudie la résolution de certains systèmes asset simples, c'est-à-dire, les systèmes échelonnés tels que définis ci-dessous.

3.5. Définition. Un système d'équations linéaires est dit *échelonné* si sa matrice augmentée est échelonnée. Dans ce cas, une inconnue est dite *libre* si aucun de ses coefficients n'est un pivot.

Le résultat suivant est évident.

3.6. Lemme. Soit $AX = B$ un système échelonné d'équations linéiares à n inconnues.
(1) A est échelonnée avec $\mathrm{rg}(A) \le \mathrm{rg}(A \,|\, B)$.
(2) $\mathrm{rg}(A) < \mathrm{rg}(A \,|\, B)$ si et seulement si la colonne B contient un pivot de $(A \,|\, B)$.
(3) Le nombre d'inconnues libres est égal à $n - \mathrm{rg}(A)$.

Démonstration. Posons $A = (a_{ij})_{m\times n}$ et $B = (b_i)_{m\times 1}$. Désignant par $A_1, \ldots, A_m$ les lignes de A, les lignes de $(A \mid B)$ sont $(A_i \mid b_i), i = 1, \ldots, m$.

(1) Supposons que $A_i \neq 0$, dont le pivot est a_{i,j_i} avec $j_i \le n$. Alors $(A_i \mid b_i) \neq 0$, dont le pivot est aussi a_{i,j_i}. Comme $(A \mid B)$ est échelonnée, $(A_{i-1} \mid b_{i-1}) \neq 0$, dont le pivot se trouve dans la colonne j_{i-1} avec $j_{i-1} < j_i$. Comme $j_{i-1} < n$, ce pivot est $a_{i-1,j_{i-1}}$. Ainsi $A_{i-1} \neq 0$, dont le pivot est $a_{i-1,j_{i-1}}$. Ceci montre que A est échelonnée. En outre, comme tout pivot de A est un pivot de $(A \mid B)$, on a $\mathrm{rg}(A) \le \mathrm{rg}(A \,|\, B)$.

(2) Supposons que B contient un pivot b_s de $(A \mid B)$. Alors b_s n'est pas un pivot de A. D'où, $\mathrm{rg}(A) < \mathrm{rg}(A \mid B)$. Suuposons réciproquement que $\mathrm{rg}(A) < \mathrm{rg}(A \mid B)$. Alors une

ligne, disons $(A_s \mid b_s)$, de $(A \mid B)$ contien un pivot qui n'est pas un pivot de A. Ainsi ce pivot est b_s.

(3) On a $n = s + t$, où s est le nombre d'inconnues libres et t est le nombre d'inconnues non libres. Par définition, une inconnue x_j est non libre si et seulement si la j-iìeme colonne de A contient un pivot de A. Ainsi $t = \text{rg}(A)$, D'où, $s = n - \text{rg}(A)$. La preuve du lemme s'achève.

Le résultat suivant donne la condition pour qu'un système échelonné n'ait pas de solution.

3.7. Lemme. Soit $AX = B$ un système échelonné. Si $\text{rg}(A) < \text{rg}(A \,|\, B)$, alors le système est incompatible.

Démonstration. Supposons que $\text{rg}(A) < \text{rg}(A \,|\, B)$. D'après le lemme 3.6(2), B contient un pivot, disons, b_s. Ceci signifie que la s-ième équation du système est de la forme $0 = b_s$. Comme $b_s \neq 0$, la s-ième équation n'a aucune solution; et donc, le système n'a aucune solution. Ceci achève la démonstration.

Le résultat suivant donne la condition pour qu'un système échelonné ait une seule solution.

3.8. Lemme. Soit $AX = B$ un système échelonné avec $\text{rg}(A) = \text{rg}(A|B)$. S'il n'y a pas d'inconnues libres, alors le système admet une seule solution, qui peut être trouvée par substitution à partir de la dernière équation non nulle.

Démonstration. Supposons que le système a n inconnues dont aucun n'est libre. Alors A est échelonnée de n pivots. D'après le lemme 2.4.6, les pivots de A sont $a_{11}, a_{22}, \cdots, a_{nn}$. Comme B ne contient aucun pivot de $(A \,|\, B)$, le système est de la forme

$$\begin{array}{ccccccccc}
a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\
 & & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\
 & & & & \ddots & & & \vdots & \\
 & & & & & & a_{nn}x_n & = & b_n \\
 & & & & & & 0 & = & 0 \\
 & & & & & & & \vdots & \\
 & & & & & & 0 & = & 0,
\end{array}$$

où les a_{ii} sont tous non nuls. Il est évidemment équivalent au système échelonné suivant:

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ & & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & \ddots & & & \vdots & \\ & & & & & & a_{nn}x_n & = & b_n. \end{array}$$

Ayant une matrice de coefficients inversible, d'après la proposition 3.4, ce dernier système admet une seule solution, qui peut être trouvé par substitution à partir de la dernière équation. Ceci achève la démonstration.

Exercice. Résoudre le système sur $\mathbb{Z}_5$ suivant:

$$\begin{array}{ccccccc} 2x & - & y & + & z & = & 1 \\ & & y & - & z & = & 3 \\ & & & & 3z & = & 2 \\ & & & & 0 & = & 0. \end{array}$$

On discutera comment résoudre les systèmes échelonnés ayant plusieurs solutions. Pour ce but, on note $K^s = \{(\lambda_1, \ldots, \lambda_s) \mid \lambda_j \in K\}$, le produit cartésien de s copies de K. Si K est fini, on désigne par $|K|$ le nombre d'éléments de K. Dans ce cas, K^s est également fini et $|K^s| = |K|^s$.

3.9. Lemme. Soit $AX = B$ un système échelonné sur K avec $\mathrm{rg}(A) = \mathrm{rg}(A|B)$ ayant s inconnues libres $x_{j_1}, \ldots, x_{j_s}$. Alors le système est compatible et ses solutions sont en bijection avec les éléments de K^s de la façon suivante :

Étant donné $(\lambda_1, \ldots, \lambda_s) \in K^s$, on pose $x_{j_l} = \lambda_l$, $l = 1, \ldots, s$, et déplace les $a_{i,j_l}\lambda_j$ à droite. Ceci donne un système échelonné sans inconnues libres. En résolvant ce dernier par substitution, on trouve les valeurs pour les inconnues non libres, et ceci donne la solution du système original correspondante à $(\lambda_1, \ldots, \lambda_s)$.

Démonstration. On suppose qu'il n'y a pas d'équations de la forme $0 = 0$. Soient $\{x_{i_1}, \ldots, x_{i_r}\}$ les inconnues non libres avec $1 \leq i_1 < \cdots < i_r \leq n$. Donc A contient r pivots $a_{1,i_1}, \ldots, a_{r,i_r}$. On se fixe un s-uplet quelconque $(\lambda_1, \ldots, \lambda_s) \in K^s$. Posons $x_{j_k} = \lambda_l$ dans le système original, $l = 1, \ldots, s$. En déplaçant les termes $a_{i,j_l}\lambda_j$ à droite, on obtient un système échelonné sans inconnues libres comme suit:

$$\begin{array}{ccccccccc} a_{1,i_1}x_{i_1} & + & a_{1,i_2}x_{i_2} & + & \cdots & + & a_{1,i_r}x_{i_r} & = & c_1 \\ & & a_{2,i_2}x_{i_2} & + & \cdots & + & a_{2,i_r}x_{i_r} & = & c_2 \\ & & & & \ddots & & & \vdots & \\ & & & & & & a_{r,i_r}x_{i_r} & = & c_r \end{array}$$

D'après le lemme 3.8, ce dernier admet une seule solution $x_{i_k} = \mu_k, k = 1, \ldots, r$. Or

$$\{x_{j_1} = \lambda_1, \ \ldots, x_{j_s} = \lambda_s; x_{i_1} = \mu_1, \ldots, x_{i_r} = \mu_r\}$$

est une solution du système original correspondante au r-uplet $(\lambda_1, \ldots, \lambda_s)$. D'autre part, une solution $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ du système original correspond au s-uplet $(\alpha_{j_1}, \ldots, \alpha_{j_s})$. Donc les solutions du système original corréspondent biuniquement aux éléments de K^s. Ceci achève la démonstration.

Exercice. Résoudre le système rationnel suivant:

$$\begin{array}{rcrcrcrcl} 0x_1 & + & 2x_2 & - & x_3 & + & x_4 & = & 1 \\ & & & & x_3 & - & 2x_4 & = & 1. \end{array}$$

La stratégie de résoudre un système général consiste à réduire le système à un système échelonné sans changer l'ensemble des solutions.

3.10. Définition. Les opérations suivantes sur les équations d'un système d'équations linéaires sur K sont dites *élémentaires.*

Type 1: Échanger deux équations, notée $E_i \leftrightarrow E_j$ où $i \neq j$.

Type 2: Additionner à une équation un multiple d'une autre équation, notée $E_i + aE_j$ où $a \in K$ et $i \neq j$.

Type 3: Multiplier une équation par un élément non nul de K, notée aE_i où $a \neq 0_K$.

Remarque. (1) Effectuer une opération élémentaire sur les équations est équivalent à effectuer une opération élémentaire de même type sur les lignes de la matrice augmentée.

(2) Comme toute matrice se réduit à une matrice échelonnée, tout système d'équations linéaires se réduit à un système échelonné.

On voit que la nouvelle matrice augmentée est la matrice augmentée du nouveau système.

3.11. Théorème. Les opérations élémentaires ne changent pas l'ensemble des solutions d'un système d'équations linéaires.

Démonstration. Soit $AX = B$ un système à n inconnues. Supposons qu'il se réduit à un autre système $A'X = B'$. Alors $(A|B)$ se réduit à $(A'|B')$. Donc il existe une matrice inversible P telle que $(A'|B') = P(A|B) = (PA|PB)$. Ceci donne $A' = PA$ et $B' = PB$. Pour toute matrice S de type $n \times 1$, comme P est inversible, on a $AS = B$ si et seulement si $P(AS) = PB$ si et seulement si $A'S = B'$. Ceci achève la démonstration du théorème.

Remarque. Pour résoudre un système d'équations linéaires général, on le réduit à un système échelonné, et résout ce dernier par substitution. Cette méthode s'appelle l'*élimination de Gauss.*

Exercice. Résoudre, par l'élimination de Gauss, le système sur $\mathbb{C}$ suivant:

$$\begin{array}{rcrcrcl} 2x & & & - & z & = & 1-i \\ x & - & 2y & & & = & 0 \\ 2x & + & (1-i)y & - & 2z & = & 0. \end{array}$$

Exercice. Résoudre, par l'élimination de Gauss, le système suivant sur $\mathbb{Z}_5$:

$$\begin{array}{rcrcrcrcl} & & x_2 & - & x_3 & + & x_4 & = & 0 \\ 2x_1 & - & x_2 & + & 3x_3 & - & x_4 & = & 1 \\ x_1 & + & x_2 & & & + & x_4 & = & 3 \\ 3x_1 & - & 3x_2 & + & x_3 & - & 3x_4 & = & 4. \end{array}$$

3.12. Théorème. Soit un système d'équations linéaires sur K à n inconnues

$$AX = B.$$

Le système est compatible si et seulement si $\mathrm{rg}(A) = \mathrm{rg}(A|B)$; et dans ce cas,

(1) si $\mathrm{rg}(A) = \mathrm{rg}(A|B) = n$, alors le système admet une seule solution;

(2) si $\mathrm{rg}(A) = \mathrm{rg}(A|B) < n$, alors les solutions du système sont en bijection avec les éléments de K^s, où $s = n - \mathrm{rg}(A)$. Par conséquent, le système admet au moins deux solutions distinctes. Plus précisément, le nombre de solutions est égal à $|K|^s$ lorsque K est fini; et l'infinité sinon.

Démonstration. Soit $(C|D)$ une forme échelonnée de $(A|B)$. D'après le théorème 3.11, le système original est équivalent au système échelonné $CX = D$; et d'après le lemme 2.3.7(3), $\mathrm{rg}(A|B) = \mathrm{rg}(C|D)$ et $\mathrm{rg}(A) = \mathrm{rg}(C)$. Or, le résultat suit des lemmes 3.7, 3.8 et 3.9. Ceci achève la démonstration du théorème.

Exercice. Selon les valeurs de a, discuter le système sur $\mathbb{Z}_7$ suivant:

$$\begin{array}{rcrcrcl} x & + & y & - & z & = & 1 \\ x & + & 2y & + & az & = & 2 \\ 2x & + & ay & + & 2z & = & 3. \end{array}$$

3.13. Définition. Un système d'équations linéaires

$$AX = B$$

est dit *homogène* si $B = 0$. Dans ce cas, $X = 0$ est toujours une solution du système, appelée la *solution nulle.*

Il s'agit d'un problème très important de savoir quand un système homogène a des solutions non nulles.

3.14. Théorème. Soit $AX = 0$ un système homogène de m équations linéaires à n inconnues.

(1) Le système n'a que la solution nulle si et seulement si $\text{rg}(A) = n$.

(2) Le système a des solutions non nulles si et seulement si $\text{rg}(A) < n$.

(3) Si $m < n$, alors le sysème admet des solutions non nulles.

Démonstration. On a $\text{rg}(A) = \text{rg}(A \mid 0)$. Si $\text{rg}(A) = n$, alors le système a une seule solution, ce qui doit être la solution nulle. Si $\text{rg}(A) < n$, alors le système a au moins deux solutions distinctes dont au moins une est non nulle. Enfin, si $m < n$, alors $\text{rg}(A) \leq m < n$. D'après l'énoncé (1), le système a des solutions non nulles. Ceci achève la dḿonstration.

Exercice. Pour quelle valeur de a, le système homogène

$$\begin{array}{rcrcrcl} x & + & 2y & + & z & = & 0 \\ x & + & y & + & 3z & = & 0 \\ 2x & + & 4y & + & az & = & 0, \end{array}$$

a-t-il des solutions non nulles?

3.15. Corollaire. Si $A \in M_n(K)$, alors le système homogène

$$AX = 0$$

n'a que la solution nulle si et seulement si A est inversible.

Démonstration. D'après la proposition 3.14, le système homogène $AX = 0$ n'a que la solution nulle si et seulement si $\text{rg}(A) = n$ si et seulement si A est inversible d'après le théorème 2.4.8. Ceci achève la démonstration.

3.16. Exercices

1. Résoudre, en trouvant l'inverse de la matrice de coefficients, le système d'équations linéaires sur $\mathbb{C}$ suivant:

$$\begin{array}{rcrcrcl} x & - & y & & & = & 1+i \\ x & + & y & + & 3z & = & i \\ & & y & + & z & = & 2-i. \end{array}$$

2. Résoudre, par l'élimination de Gauss, les systèmes sur $\mathbb{C}$ suivants:

(1)
$$\begin{array}{rcrcrcl} x_1 & - & x_2 & + & x_3 & = & 6 \\ x_1 & + & x_2 & + & 2x_3 & = & 8 \\ 2x_1 & - & 3x_2 & - & x_3 & = & 1; \end{array}$$

(2)
$$\begin{array}{rcrcrcl} x_1 & - & 3x_2 & + & x_3 & = & 6 \\ 2x_1 & + & x_2 & - & 3x_3 & = & 2i \\ x_1 & + & (1+i)x_2 & - & 4x_3 & = & 0. \end{array}$$

3. Résoudre, par l'élimination de Gauss, le système sur $\mathbb{Z}_5$ suivant:

$$\begin{array}{rcrcrcrcl} x_1 & + & 2x_2 & - & x_3 & + & 2x_4 & = & 0 \\ 2x_1 & + & 4x_2 & - & x_3 & + & 3x_4 & = & 1 \\ x_1 & + & 2x_2 & - & 2x_3 & + & 3x_4 & = & 4 \\ x_1 & + & 2x_2 & & & + & x_4 & = & 1. \end{array}$$

4. Résoudre, par l'élimination de Gauss, le système sur $\mathbb{Z}_3$ suivant:

$$\begin{array}{rcrcrcrcl} x_1 & + & 2x_2 & & & + & x_4 & = & 0 \\ 2x_1 & + & 2x_2 & + & x_3 & & & = & 1 \\ x_1 & & & + & x_3 & + & 2x_4 & = & 1. \end{array}$$

5. Soient P_1, P_2, et P_3 les plans affines définis par les équations catésiennes $x+2y+z=1$, et $2x+5y+az=1$, et $x+ay+2z=2$, respectivement. Trouver les valeurs réelles de a pour que les trois plans se coupent, c'est-à-dire, leur intersection est non vide.

6. Dans chacun des cas suivants, trouver la condition pour que le système rationnelle soit compatible.

(1)
$$\begin{array}{rcrcrcl} x & - & 2y & + & z & = & 6 \\ 3x & + & y & - & z & = & 7 \\ -x & + & y & + & az & = & 6; \end{array}$$

(2)
$$\begin{array}{rcrcrcl} x & + & 2y & - & 3z & = & a \\ 2x & + & 6y & - & 11z & = & b \\ x & - & 2y & + & 7z & = & c. \end{array}$$

7. Discuter, selon les valeurs de a, le système réel suivant:

$$\begin{array}{rcrcrcl} x & + & y & + & (1-2a)z & = & 2(1+a) \\ (1+a)x & - & (1+a)y & + & (2+a)z & = & 0 \\ 2x & - & 2ay & + & 3z & = & 2(1+a). \end{array}$$

8. Discuter, selon les valeurs de a, b, le système rationnel suivant:

$$\begin{array}{rcrcl} x & + & y & = & 2 \\ x & + & ay & = & 2b+1. \end{array}$$

9. Considérer le système sur $\mathbb{Q}$ suivant:

$$\begin{array}{rcrcrcl} x & + & y & - & z & = & 1 \\ x & + & 2y & + & az & = & 2 \\ 2x & + & ay & + & 2z & = & 3. \end{array}$$

Déterminer les valeurs de a pour lesquelles le système
(1) n'ait pas de solution;
(2) ait une infinité de solutions;
(3) ait une solution unique.

10. Déterminer si le système homogène suivant admet ou non des solutions non nulles.

$$\begin{array}{rcrcrcrcl} x_1 & - & 3x_2 & + & 6x_3 & - & 3x_4 & = & 0 \\ & & x_2 & - & x_3 & + & x_4 & = & 0 \\ 2x_1 & - & x_2 & + & 3x_3 & - & x_4 & = & 0 \\ 4x_1 & + & 4x_2 & & & + & x_4 & = & 0. \end{array}$$

11. Pour quelle valeur complexe de a, le système homogène complexe

$$\begin{array}{rcrcrcl} x & - & y & + & z & = & 0 \\ 3x & + & y & + & az & = & 0 \\ -x & - & 2y & - & z & = & 0, \end{array}$$

a-t-il des solutions non nulles? Dans ce cas, trouver les solutions.

12. Déterminer si le système homogène sur $\mathbb{C}$ a des solutions non nulles ou non:

$$\begin{array}{rcrcrcl} 3x & - & y & + & 2z & = & 0 \\ & & y & + & (1+i)z & = & 0 \\ 3x & & & + & (3+i)z & = & 0. \end{array}$$

13. Considérer le système homogène suivant:

$$\begin{array}{rrcrcrcl} x_1 & & + & 2x_3 & - & x_4 & = & 0 \\ x_1 & & - & x_3 & + & x_4 & = & 0 \\ & -x_2 & & & + & (1+a)x_4 & = & 0 \\ & a\,x_2 & & & & & = & 0. \end{array}$$

Donner les valeurs réelles de a pour ce système homogène ait des solutions non nulles.

14. Soit $A \in M_{m\times n}(K)$. Montrer que le système homogène $AX = 0$ a des solutions non nulles dans chacun des cas suivants:
(1) A a une colonne nulle.
(2) A a deux colonnes identiques.

15. Soit $A \in M_{m\times n}(K)$. Montrer les énoncés suivants:
(1) Si $m < n$, alors il existe une matrice non nulle B telle que $AB = 0$.
(2) S'il existe $C \in M_{n\times m}(K)$ telle que $CA = I_n$, alors $m \geq n$.
Indice: Appliquer la première partie.

16. Soient A, B, C des matrices sur K. Si le système homogène $AX = 0$ n'a pas de solutions non nulles, montrer que $AB = AC$ si et seulement si $B = C$.

17. Soit $A \in M_n(K)$. Montrer que A est inversible si et seulement si tout système d'équations linéaires ayant A pour matrice de coefficients est compatible. *Indice*: Utiliser le numéro 45 des Exercices 2.5.

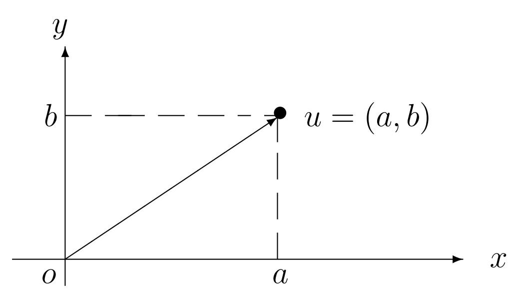
Chapitre IV: Espaces vectoriels

Beaucoup de quantités dans les applications, comme la chaleur et la température, peuvent être décrites par un seul scalaire. Mais certains d'autres quantités, comme la force et la vitesse, exigent plusieurs scalaires pour leur définition. On les appelle *quantités vectorielles*. On sait que les quantités vectorielles différentes possèdent des propriétes communes. Par exemple, une quantité peut être multipliée par un scalaire et deux quantités vectorielles de même genre peuvent être additionnées. Afin d'étudier les quantités vectorielles diverses en même temps, on introduit la notion d'espace vectoriel et on étudie celle-ci en général. Et ensuite, on peut utiliser les résultats sur les espaces vectoriels généraux dans des applications particuliers.

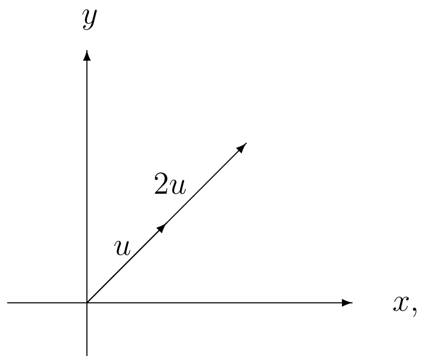
Partout dans ce chapitre, on se fixe K un corps.

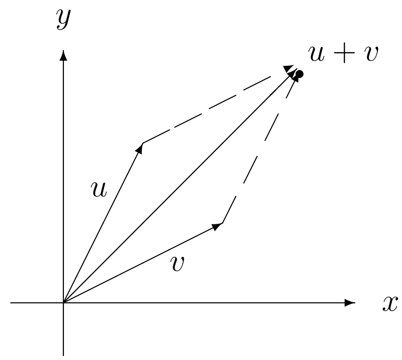
4.1. Définition et exemples

Avant introduire la notion abstraire d'un espace vectoriel, nous rappelons deux exemples d'espaces vectoriels réels. D'abord, le plan $\mathbb{R}^2$ se compose des vecteurs représentées par les couples (a, b), où $a, b \in \mathbb{R}$, illustré par le diagramme suivant:



Il y a deux opérations pour les vecteurs du plan: premièrement étant donnés un vecteur $u \in \mathbb{R}^2$ et un nombre $\alpha \in \mathbb{R}$, en multipliant u par α, on obtient un autre vecteur αu; et deuxièrement étant données deux vecteurs u, v, en les additionnant, on obtient un nouveau vecteur $u + v$, illustrés par les diagrammes suivants.





De même, on a l'espace usuel $\mathbb{R}^3 = \{(a, b, c), \mid a, b, c \in \mathbb{R}\}$. Il y a aussi deux opérations pour les vecteurs de $\mathbb{R}^3$ suivantes:

(1) Multiplication par un scalaire:

$$\alpha \cdot (a, b, c) = (\alpha a, \alpha b, \alpha c),\ \alpha \in \mathbb{R};$$

(2) Addition:

$$(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2).$$

Les opérations dans $\mathbb{R}^2$ et celles dans $\mathbb{R}^3$ satisfont aux axiomes communs. En généralisant ces axiomes, on obtient la notion d'espace vectoriel.

4.1.1. Définition. Soit K un corps, ses éléments appelés *scalaires*. Un ensemble non vide E, ses éléments appelés *vecteurs*, s'appelle *espace vectoriel* sur K (ou K-*espace vectoriel*) s'il est muni d'une multiplication par un scalaire

$$\cdot :\ K \times E \to E : (\alpha, u) \mapsto \alpha \cdot u$$

et d'une addition

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

telles que pour tous $u, v, w \in E$ et $\alpha, \beta \in K$,

(1) (commutativité) $u + v = v + u$.

(2) (associativité) $u + (v + w) = (u + v) + w$.

(3) Il existe un *vecteur nul*, noté 0_E, tel que $u + 0_E = u$, pour tout $u \in E$.

(4) Tout $u \in E$ admet un *opposé*, noté $-u$, tel que $u + (-u) = 0_E$.

(5) (associativité) $\alpha \cdot (\beta \cdot u) = (\alpha\beta) \cdot u$.

(6) (neutralité) $1_K \cdot u = u$.

(7) (distributivité par rapport aux scalaires) $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$.

(8) (distributivité par rapport aux vecteurs) $(\alpha+\beta)\cdot u = \alpha\cdot u + \beta\cdot u$.

Remarque. (1) Pour tout $u \in E$, $0_E + u = u$ et $(-u) + u = 0_E$.

(2) Pour $u, v, w \in E$, on écrit $(u+v)+w = u+v+w$ et $u - v = u + (-v)$.

(3) Un espace vectoriel E est dit *nul* si $E = \{0_E\}$.

(4) Un espace vectoriel *rationnel*, *réel* ou *complex* est un espace vectoriel sur $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, respectivement.

Exemple. (1) L'ensemble $E = \{0_K\}$ est un K-espace vectoriel, pour les opérations suivantes:

$$0_K + 0_K = 0_K, \;\; \alpha \cdot 0_K = 0_K, \text{ pour tout } \quad \alpha \in K.$$

On voit que F est nul. Essentiellement c'est le seul K-espace vectoriel nul.

(2) L'ensemble $M_{m\times n}(K) = \{(a_{ij})_{m\times n} \mid a_{ij} \in K\}$ est un K-espace vectoriel pour l'addition et la multiplication scalaire de matrices. Ici, le vecteur nul est la matrice nulle $0_{m\times n}$.

(3) En particulier, $K^n = \{(a_1, \ldots, a_n) \,|\, a_i \in K\}$ et

$$K^{(n)} = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \,|\, a_i \in K \right\}$$

sont des K-espaces vectoriels.

(4) Si $n = 1$, alors $K = K^1$ est un K-espace vectoriel. En particulier, $\mathbb{C}$ est un $\mathbb{C}$-espace vectoriel, noté ${}_{\mathbb{C}}\mathbb{C}$.

(5) L'ensemble $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ est aussi un $\mathbb{R}$-espace vectoriel, noté ${}_{\mathbb{R}}\mathbb{C}$, pour les opérations habituelles:

$$(a+bi) + (c+di) = (a+c) + (b+d)i; \quad \alpha(a+bi) = (\alpha a) + (\alpha b)i.$$

Remarquons que ${}_{\mathbb{C}}\mathbb{C}$ et ${}_{\mathbb{R}}\mathbb{C}$ sont éssentiellement différents, car ils n'ont pas le même ensemble de scalaires.

(6) Soit I un intervalle de l'axe réel. L'ensemble $C(I)$ des fonctions continues $f : I \to \mathbb{R}$ est un espace vectoriel sur $\mathbb{R}$ pour les opérations habituelles:

$$(f+g)(t) = f(t) + g(t), \quad (\alpha f)(t) = \alpha f(t), \quad \text{pour tout} \quad t \in I.$$

Ici, le vecteur nul est la fonction nulle $\mathbf{0}$ telle que $\mathbf{0}(t) = 0$, pour tout $t \in I$.

(7) L'ensemble $K_n[x] = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \,|\, a_i \in K\}$ est un K-espace vectoriel si, étant donnés $a \in K$ et

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}, g(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in K_n[x],$$

on définit les opérations suivantes:

$$\alpha \cdot f(x) = (\alpha a_0) + (\alpha a_1)x + \cdots + (\alpha a_{n-1})x^{n-1}$$

et

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_{n-1} + b_{n-1})x^{n-1}.$$

Ici, le vecteur nul est le polynôme nul $0 + 0x + \cdots + 0x^{n-1}$.

(8) L'ensemble $K[x] = \{a_0 + a_1x + \cdots + a_mx^m \,|\, m \geq 0, a_i \in K\}$ est un K-espace vectoriel pour les opérations définies comme ci-dessus.

Voici des propriétés élémentaires d'espaces vectoriels.

4.1.2. Proposition. Soit E un K-espace vectoriel avec $u, v, w \in E$ et $\alpha, \beta \in K$.
(1) E admet un seul vecteur nul.
(2) Si $u + v = u + w$, alors $v = w$.
(3) Tout vecteur a un seul opposé.
(4) $\alpha u = 0_E$ si et seulement si $\alpha = 0_K$ ou $u = 0_E$.
(5) $(-1_K)u = -u$ et $-(-u) = u$.
(6) $-(u + v) = -u - v$.
(7) $u + v = w$ si et seulement si $u = w - v$.

Démonstration. (1) Si 0 et $0'$ sont des vecteurs nuls, alors $0' = 0 + 0' = 0' + 0 = 0$.

(2) Supposons $u+v = u+w$. Alors $(-u)+(u+v) = (-u)+(u+w)$. D'après l'associativité, $((-u) + u) + v = ((-u) + u) + v$. Donc $0_E + v = 0_E + w$. Ainsi $v = w$. Par conséquent, (2) est valide.

(3) $0_Ku + 0_Ku = (0_K + 0_K)u = 0_Ku = 0_Ku + 0_E$. Donc $0_Ku = 0_E$. De même, $\alpha 0_E = 0_E$. Supposons maintenant que $\alpha u = 0_E$. Si $\alpha \neq 0_K$, alors α^{-1} existe. Or

$$u = 1_K \cdot u = (\alpha^{-1}\alpha)u = \alpha^{-1}(\alpha u) = \alpha^{-1}0_E = 0_E.$$

(4) On a $(-1_K)\,u + u = (-1_K) \cdot u + 1_K \cdot u = ((-1_K) + 1_K)u = 0_Ku = 0_E$. Ainsi $(-1_K)\,u = -u$. Ainsi $-(u + v) = (-1_K)(u + v) = (-1_K)u + (-1_K)v = -u - v$. Ceci achève la démonstration.

4.2. Bases

Partout dans cette section, on se fixe E un K-espace vectoriel.

4.2.1. Définition. Soient $u_1, \ldots, u_n \in E$. Un vecteur $u \in E$ est dit une *combinaison linéaire* de $u_1, \ldots, u_n$ s'il existe $\alpha_1, \ldots, \alpha_n \in K$, appelés *coefficients*, tels que

$$u = \alpha_1 u_1 + \cdots + \alpha_n u_n.$$

Remarque. Une combinaison linéaire d'un seul vecteur u est de la forme αu avec $\alpha \in K$, appelé aussi un *multiple* de u. En particulier, u est une combinaison linéaire de lui-même.

Exemple. (1) Le vecteur nul 0_E est une combinaison linéaire de n vecteurs quelconques.

(2) Dans l'espace vectoriel réel ${}_{\mathbb{R}}\mathbb{C}$, le nombre complexe i n'est pas une combinaison linéaire de 1, car $i \neq a \cdot 1$, pour tout $a \in \mathbb{R}$.

(3) Dans l'espace vectoriel complexe ${}_{\mathbb{C}}\mathbb{C}$, le nombre complexe i est une combinaison linéaire du nombre 1, car $i = i \cdot 1$, où i est un scalaire.

Exercice. Soit $C[0, 2\pi]$ l'espace réel des fonctions continues définies sur $[0, 2\pi]$. Vérifier que $f = t^2$ n'est pas une combinaison linéaire des fonctions $g = \sin t$ et $h = \cos t$.

Démonstration. Supposons au contraire que f est une combinaison linéaire de g, h. Alors il existe $\alpha, \beta \in \mathbb{R}$ tels que $f = \alpha \cdot g + \beta \cdot h$. Ainsi, pour tout $t \in [0, 2\pi]$, on obtient

$$f(t) = (\alpha \cdot g + \beta \cdot h)(t) = (\alpha \cdot g)(t) + (\beta \cdot h)(t) = \alpha \cdot g(t) + \beta \cdot h(t).$$

C'est-à-dire, $t^2 = \alpha \sin t + \beta \cos t$, pour tout $t \in [0, 2\pi]$. En prennant $t = 0$ et $t = \pi$, on obtient

$$\begin{array}{rcrcl} 0\alpha & + & \beta & = & 0 \\ 0\alpha & - & \beta & = & \pi^2. \end{array}$$

Ceci nous donne $\pi^2 = 0$, une contradiction. Donc la fonction t^2 n'est pas une combinaison linéaire des fonctions $\sin t, \cos t$.

En général, les coefficients d'une combinaison linéaire ne sont pas uniques. On étudiera quand les coefficients d'une combinaison linéaire de $u_1, \ldots, u_n$ sont uniques.

4.2.2. Définition. Soient $u_1, \ldots, u_n \in E$. On dit que $u_1, \ldots, u_n$ sont *linéairement dépendants* s'il existe $\alpha_1, \ldots, \alpha_n \in K$, non tous nuls, tels que

$$\alpha_1 u_1 + \cdots + \alpha_n u_n = 0_E;$$

et *linéairement indépendants* sinon, c'est-à-dire, si toute égalité

$$\alpha_1 u_1 + \cdots + \alpha_n u_n = 0_E,\ \alpha_i \in K,$$

entraîne que $\alpha_1 = \cdots = \alpha_n = 0_K$.

Remarque. En bref, une famille $\{u_1, \ldots, u_n\}$ de vecteurs de E est dite
(1) *liée* si $u_1, \ldots, u_n$ sont linéairement dépendants;
(2) *libre* si $u_1, \ldots, u_n$ sont linéairement indépendants.

Exemple. (1) Considérons l'espace vectoriel réel ${}_{\mathbb{R}}\mathbb{C}$. La famille $\{1, i\}$ est libre.
En effet, si $a, b \in \mathbb{R}$ tels que $a \cdot 1 + b \cdot i = 0$, alors $a + bi = 0$. D'où, $a = b = 0$.

(2) Considérons l'espace vectoriel complexe ${}_{\mathbb{C}}\mathbb{C}$. La famille $\{1, i\}$ est liée.
En effet, 1 et i sont deux scalaires non nuls tels que $1 \cdot 1 + i \cdot i = 0$.

(3) Considérons le K-espace vectoriel $M_{m\times n}(K)$. La famille $\{e_{ij} \mid i = 1, \ldots, m; j = 1, \ldots, n\}$ est libre, où e_{ij} désigne la matrice dont le (i, j)-terme est 1_K et tous les autres sont nuls.

En effet, supposons que $a_{ij} \in K$, $i = 1, \ldots, m; j = 1, \ldots, n$ sont tels que

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} \cdot e_{ij} = 0_{m\times n}.$$

Comme la somme du membre de gauche est la matrice $(a_{ij})_{m\times n}$, on obtient $(a_{ij})_{m\times n} = 0_{m\times n}$, c'est-à-dire, $a_{ij} = 0$, $i = 1, \ldots, m; j = 1, \ldots, n$.

(4) Considérons le K-espace vectoriel $K_n[x]$. La famille $\{1, x, \ldots, x^{n-1}\}$ est libre.

En effet, si $a_0, a_1, \ldots, a_{n-1} \in K$ sont tels que $a_0 \cdot 1 + a_1 \cdot x + \cdots + a_{n-1} \cdot x^{n-1} = 0$, alors $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} = 0$. D'après la définition, $a_0 = a_1 = \cdots = a_{n-1} = 0$.

Exercice. Considérons l'espace réel $C[0, 2\pi]$ des fonctions continues $f : [0, 2\pi] \to \mathbb{R}$. Montrer que chacune des familles suivantes est libre:
(1) $\{f = \sin t,\ g = \cos t\}$.
(2) $\{\sin t, \sin 2t, \ldots, \sin nt\}$ avec $n \geq 1$.

4.2.3. Proposition. Une famille $\{u_1, \ldots, u_n\}$ de vecteurs de E est libre si, et seulement si, toute combinaison linéaire u de $u_1, \ldots, u_n$ s'écrit d'une façon unique

$$u = \alpha_1 u_1 + \cdots + \alpha_n u_n,\ \alpha_1, \ldots, \alpha_n \in K.$$

Démonstration. Supposons que $\{u_1, \ldots, u_n\}$ est libre. Soit u une combinaison linéaire de $u_1, \ldots, u_n$. Posons $u = \alpha_1 u_1 + \cdots + \alpha_n u_n$, $\alpha_1, \ldots, \alpha_n \in K$. Si $\beta_1, \ldots, \beta_n \in K$ sont tels que $u = \beta_1 u_1 + \cdots + \beta_n u_n$, alors $(\alpha_1 - \beta_1)u_1 + \cdots + (\alpha_n - \beta_n)u_n = 0$. Comme la famille est libre, $\alpha_i - \beta_i = 0$, c'est-à-dire, $\alpha_i = \beta_i$, pour tout $1 \leq i \leq n$.

Réciproquement, supposons que $\{u_1, \ldots, u_n\}$ satisfait à la condition énoncée dans la proposition. Soit $\alpha_1 u_1 + \cdots + \alpha_n u_n = 0_E$, $\alpha_1, \ldots, \alpha_n \in K$. Comme $0_E = 0 \cdot u_1 + \cdots + 0 \cdot u_n$. Or l'unicité de l'expression implique $\alpha_i = 0$, $i = 1, \ldots, n$. Ainsi $\{u_1, \ldots, u_n\}$ est libre. Ceci achève la démonstration de la proposition.

Le résultat suivant nous dit comment déterminer une petite famille de vecteurs est liée ou libre.

4.2.4. Lemme. Soient deux vecteurs $u, v \in E$.

(1) La famille $\{u\}$ est liée si, et seulement si, $u = 0_E$;

(2) La famille $\{u, v\}$ est liée si et seulement si l'un de u, v est un multiple de l'autre.

Démonstration. (1) Si $u = 0_E$, comme $1_K \cdot u = 0_E$, on voit que $\{u\}$ est liée. Supposons que $u \neq 0_E$. Si $\alpha u = 0_E$, alors $\alpha = 0_K$. D'où, $\{u\}$ est libre.

(2) Supposons que $\{u, v\}$ est liée. Alors il existe des scalaires $\alpha, \beta \in K$, non tous nuls, tels que $\alpha u + \beta v = 0_E$. Si $\alpha \neq 0_K$, alors $u = (-\alpha^{-1}\beta)v$. Si $\beta \neq 0_K$, alors $v = (-\beta^{-1}\alpha)u$.

Supposons réciproquement que $u = \alpha v$ avec $\alpha \in K$. Alors $1_K \cdot u - \alpha v = 0_E$ avec $1_K \neq 0_K$. D'où, $\{u, v\}$ est liée. Cela s'achève la démonstration du lemme.

4.2.5. Lemme. Soient $\{u_1, \ldots, u_n\}$ une famille libre de vecteurs de E. Si $u \in E$, alors $\{u_1, \ldots, u_n, u\}$ est libre si, et seulement si, u n'est pas une combinaison linéaire de $u_1, \ldots, u_n$.

Démonstration. Supposons que $u = \alpha_1 u_1 + \cdots + \alpha_n u_n$ avec $\alpha_1, \ldots, \alpha_n \in K$. Alors

$$\alpha_1 u_1 + \cdots + \alpha_n u_n + (-1)u = 0_E.$$

Ainsi $\{u_1, \ldots, u_n, u\}$ est liée. Supposons maintenant que u n'est pas une combinaison linéaire de $u_1, \ldots, u_n$. Soient $\alpha_1, \ldots, \alpha_n, \alpha \in K$ tels que $\alpha_1 u_1 + \cdots + \alpha_n u_n + \alpha u = 0_E$. Si $\alpha \neq 0_K$, alors u est combinaison linéaire de $u_1, \ldots, u_n$, une contradiction. Ainsi $\alpha = 0_K$. D'où,

$$\alpha_1 u_1 + \cdots + \alpha_n u_n = 0_E.$$

Comme $\{u_1, \ldots, u_n\}$ est libre, $\alpha_1 = \cdots = \alpha_n = 0$. D'où $\{u_1, \ldots, u_n, u\}$ est libre. Ceci achève la démonstration.

Exercice. Considérons l'espace vectoriel réel $\mathbb{R}^3$. Augmenter la famille $\{(1, 0, 0)\}$ à une famille libre de 3 vecteurs.

4.2.6. Proposition. Soit $\mathcal{U} = \{u_1, \ldots, u_n\}$ une famille libre de vecteurs de E. Alors toutes les sous-familles de $\mathcal{U}$ sont libres; et en particulier,

(1) $u_i \neq 0_E$ pour tout $1 \leq i \leq n$; et

(2) $u_i \neq u_j$ pour tous $1 \leq, i, j \leq n$ avec $i \neq j$.

Démonstration. Soit $\mathcal{X}$ une sous-famille non vide de $\mathcal{U}$. Sans perdu de généralité, on peut supposer que $\mathcal{X} = \{u_1, \ldots, u_r\}$ avec $1 \leq r \leq n$. Si $\alpha_1, \ldots, \alpha_r \in K$ sont tels que $\alpha_1 u_1 + \cdots + \alpha_r u_r = 0_E$, alors $\alpha_1 u_1 + \cdots + \alpha_r u_r + 0u_{r+1} + \cdots + 0u_n = 0_E$. Comme $\mathcal{U}$ est libre, les coefficients sont tous nuls. En particulier, $\alpha_i = 0$ pour tout $1 \leq i \leq r$. Ceci montre que $\mathcal{X}$ est libre. La preuve de la proposition s'achève.

La proposition 4.2.6 conduit à la définition suivante.

4.2.7. Définition. Soit $\mathcal{U}$ une famille (finie ou infinie) non vide de vecteurs de E. On dit que $\mathcal{U}$ est *libre* si ses sous-familles finies sont toutes libres; et *liée* sinon.

Remarque. Par convention, la famille vide est libre.

Exemple. (1) Considérons le K-espace vectoriel $K[x]$ des polynômes sur K. La famille infinie $\mathcal{X} = \{1, x, x^2, \ldots, x^i, \ldots, \}$ est libre.

En effet, soit $\mathcal{U}$ une sous-famille finie de $\mathcal{X}$. Si $\mathcal{U}$ est vide, alors $\mathcal{U}$ est libre. Sinon, il existe un maximal $n \geq 0$ tel que $x^n \in \mathcal{U}$. On voit maintenant que $\mathcal{U} \subseteq \{1, x, \cdots, x^n\}$. Comme $\{1, x, \cdots, x^n\}$ est libre et finie, $\mathcal{U}$ est libre. Ceci montre que $\mathcal{X}$ est libre.

(2) De même, on peut vérifier que $\{\sin t, \sin 2t, \ldots, \sin nt, \ldots, \}$ est une famille infinie libre des vecteurs de l'espace vectoriel réel $C[0, 2\pi]$.

4.2.8. Définition. Soit E un K-espace vectoriel. Une famille $\mathcal{B}$ de vecteurs de E s'appelle une *base* de E si

(1) $\mathcal{B}$ est libre; et

(2) tout vecteur non nul de E est une combinaison linéaire d'un nombre fini de vecteurs de $\mathcal{B}$.

Remarque. (1) Si $E = 0$, alors la famille vide $\emptyset$ est la seule base de E.

(2) Si $E \neq 0$ dont $\mathcal{B}$ est une base, alors

  (a) $\mathcal{B} \neq \emptyset$;

  (b) $0_E \notin \mathcal{B}$;

  (c) les vecteurs de $\mathcal{B}$ sont deux à deux distincts;

  (d) tout vecteur de E est une combinaison linéaire d'un nombre fini de vecteurs de $\mathcal{B}$.

Exemple. (1) Le K-espace vectoriel $M_{m\times n}(K)$ a pour base, appelée *base canonique*, la famille $\mathcal{E} = \{e_{ij} \mid i = 1, \ldots, m; j = 1, \ldots, n\}$.

En effet, on a vu que $\mathcal{E}$ est libre. Maintenant, toute $A = (a_{ij})_{m\times n}$ s'écrit

$$A = \sum\nolimits_{1\leq i\leq m; 1\leq j\leq n} a_{ij}e_{ij}, \quad \text{où } a_{ij} \in \mathbb{R}.$$

Ainsi, $\mathcal{E}$ est une base de $M_{m\times n}(K)$.

(2) Le K-espace vectoriel K^n a pour base canonique la famille suivante:

$$\{e_1 = (1_K, 0, \cdots, 0),\ e_2 = (0, 1_K, \ldots, 0),\ \ldots,\ e_n = (0, \ldots, 0, 1_K)\}.$$

(3) Le K-espace vectoriel $K^{(n)}$ a pour base canonique la famille suivante:

$$\left\{ e_1 = \begin{pmatrix} 1_K \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 \\ 1_K \\ \vdots \\ 0 \end{pmatrix},\ \ldots,\ e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1_K \end{pmatrix} \right\}.$$

(4) Le K-espace vectoriel K a une base canonique $\{1_K\}$.

(5) L'espace vectoriel réel ${}_{\mathbb{R}}\mathbb{C}$ a pour base, appelée *base canonique*, la famille $\{1, i\}$.

En effet, on a vu que $\{1, i\}$ est libre. Or, tout $z = a + bi \in \mathbb{C}$ s'écrit $z = a \cdot 1 + b \cdot i$, où $a, b \in \mathbb{R}$. Par conséquent, $\{1, i\}$ est une base de ${}_{\mathbb{R}}\mathbb{C}$.

(6) Par contre, $\{1, i\}$ n'est une base de l'espace vectoriel complexe ${}_{\mathbb{C}}\mathbb{C}$.

En effet, on a vu que $\{1, i\}$ est une famille liée de vecetours de ${}_{\mathbb{C}}\mathbb{C}$.

(7) Le K-espace vectoriel $K_n[x] = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_i \in K\}$ a pour base, appelée *base canonique*, la famille $\{1, x, \ldots, x^{n-1}\}$.

En effet, on a vu que $\{1, x, \ldots, x^{n-1}\}$ est libre. En outre, tout

$$f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in K_n[x]$$

s'écrit $f = a_0 \cdot 1 + a_1 \cdot x + \cdots + a_{n-1} \cdot x^{n-1}$, où $a_0, a_1, \ldots, a_{n-1} \in K$. Ainsi, $\{1, x, \ldots, x^{n-1}\}$ est une base de $K_n[x]$.

(8) De même, le K-espace vectoriel $K[x]$ a pour base, appelée *base canonique*, la famille infinie $\{1, x, \ldots, x^n, \ldots, \}$.

On énonce maintenant le résultat fondamental suivant dont la démonstration est trop avancé pour ce cours.

4.2.9. Théorème. Tout espace vectoriel admet une base.

Il est à noter que, dans la plupart de cas, il est impossible de trouver une base explicite d'un espace vectoriel. Par exemple, on est incapable de trouver une base de l'espace vectoriel réel $C[0, 2\pi]$.

4.3. Matrices des coordonnées

Le but de cette section est d'appliquer la théorie de matrices à étudier les espaces vectoriels. Partout dans cette section, on se fixe E un K-espace vectoriel ayant une base finie. Dans ce cas, les bases de E seront considérées comme des familles ordonnées. Par exemple, le plan $\mathbb{R}^2$ a deux bases distinctes $\{e_1, e_2\}$ et $\{e_2, e_1\}$.

4.3.1. Définition. Soit $\{u_1, \ldots, u_n\}$ une base de E. D'après la proposition 4.2.3, tout $u \in E$ s'écrit d'une façon unique

$$(*) \qquad u = \alpha_1 u_1 + \cdots + \alpha_n u_n, \ \alpha_1, \ldots, \alpha_n \in K.$$

On appelle $\{\alpha_1, \ldots, \alpha_n\}$ les *coordonnées* de u dans la base $\{u_1, \ldots, u_n\}$.

Remarque. Si l'on considère $(u_1, \ldots, u_n)$ comme une matrice-ligne et met les coordonnées $\{\alpha_1, \ldots, \alpha_n\}$ en colonne

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in K^{(n)},$$

appelée la *colonne des coordonnées* de u dans la base $\{u_1, \ldots, u_n\}$, alors l'équation $(*)$ devient

$$u = (u_1, \ldots, u_n) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Ceci est illustrée par le diagramme suivant:

$$(u_1, \ldots, u_n) \xrightarrow{\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}} u.$$

Exercice. Considérons l'espace vectoriel réel $M_{2\times 3}(\mathbb{R})$ et le vecteur

$$A = \begin{pmatrix} 2 & 5 & 3 \\ 1 & 0 & 2 \end{pmatrix}.$$

Donner la colonne des coordonnées de
(1) dans la base canonique $\{e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}\}$;
(2) dans la base $\{e_{11}, e_{21}, e_{12}, e_{22}, e_{13}, e_{23}\}$.

Exercice. En sachant que $\{1 + x, 2 + x, 3 + x^2\}$ est une base de l'espace vectoriel réel $\mathbb{R}_3[x]$, trouver le polynôme dont la colonne des coordonnées dans cette base est

$$\begin{pmatrix} 4 \\ -2 \\ 3 \end{pmatrix}.$$

Si E est l'un des exemples d'espaces vectoriels ayant une base canonique, alors il est facile de trouver les coordonnées d'un vecteur dans la base canonique, appelés *coordonnées canoniques*. On va discuter plus tard comment trouver les coordonnées d'un vecteur dans une base non canonique. L'observation suivante sera pratique.

4.3.2. Lemme. (1) Si $u \in K^{(n)}$, alors sa colonne des coordonnées canoniques est u.
(2) Si $v \in K^n$, alors sa colonne des coordonnées canoniques est v^T.
Démonstration. (1) Soit

$$u = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^{(n)}.$$

Comme $u = a_1 e_1 + \cdots + a_n e_n$, la colonne des coordonnées de u dans $\{e_1, \ldots, e_n\}$ est

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = u.$$

(2) Soit $v = (b_1, \cdots, b_n) \in K^n$. Comme $v = b_1 e_1 + \cdots + b_n e_n$, la colonne des coordonnées de v dans $\{e_1, \ldots, e_n\}$ est

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = v^T.$$

Ceci achève la démonstration du lemme.

Le résultat suivant dit qu'un vecteur est uniquement déterminé par sa colonne des coordonnées dans une base.

4.3.3. Lemme. Soit $\{u_1, \ldots, u_n\}$ une base de E. Soient $u, v \in E$ dont les colonnes de coordonnées dans $\{u_1, \ldots, u_n\}$ sont A, B, respectivement.

(1) $u = v$ si, et seulement si, $A = B$.

(2) $u = 0_E$ si, et seulement si, $A = 0_{n\times 1}$.

Démonstration. Posons

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \; B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

D'après la définition, on a $u = a_1u_1 + \cdots + a_nu_n$ et $v = b_1u_1 + \cdots + b_nu_n$.

(1) En vue de l'unicité des coordonnées, $u = v$ si et seulement si $a_i = b_i$, $i = 1, \ldots, n$ si, et seulement si, $A = B$.

(2) La colonne des coordonnées de 0_E dans la base $\{u_1, \ldots, u_n\}$ est $0_{n\times 1}$. D'après la partie (1), $u = 0_E$ si et seulement si $A = 0_{n\times 1}$. Ceci achève la démonstration du lemme.

4.3.4. Lemme. Soit $\{u_1, \ldots, u_n\}$ une base de E. Soient $v_1, \ldots, v_m \in E$ dont les colonnes des coordonnées dans $\{u_1, \ldots, u_n\}$ sont $A_1, \ldots, A_m$, respectivement. Si $v = \alpha_1v_1 + \cdots + \alpha_mv_m$ avec $\alpha_1, \ldots, \alpha_m \in K$, alors la colonne des coordonnées de v dans $\{u_1, \ldots, u_n\}$ est

$$\alpha_1A_1 + \cdots + \alpha_mA_m.$$

Démonstration. Posons

$$A_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix},$$

c'est-à-dire, $v_j = \sum_{i=1}^n a_{ij}u_i$, $j = 1, \ldots, m$. Ceci donne

$$\alpha_1v_1 + \cdots + \alpha_mv_m = \sum_{j=1}^m \sum_{i=1}^n \alpha_j a_{ij} u_i = \sum_{i=1}^n \left(\sum_{j=1}^m \alpha_j a_{ij} \right) u_i = \sum_{i=1}^n \left(a_{i1}\alpha_1 + \cdots + \alpha_{im}\alpha_m \right) u_i.$$

D'où, la colonne de $\alpha_1v_1 + \cdots + \alpha_mv_m$ est donnée par

$$\begin{pmatrix} \alpha_1a_{11} + \cdots + \alpha_m\alpha_{1m} \\ \vdots \\ \alpha_1a_{n1} + \cdots + \alpha_ma_{nm} \end{pmatrix} = \alpha_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} + \cdots + \alpha_m \begin{pmatrix} a_{1m} \\ \vdots \\ a_{nm} \end{pmatrix} = \alpha_1A_1 + \cdots + \alpha_mA_m.$$

Ceci achève la démonstration du lemme.

Exercice. Considérons l'espace rationnel $\mathbb{Q}_3[x]$. Soit $f = f_1 - 3f_2 + 2f_3$, où

$$f_1 = 1 - 2x + x^2, f_2 = 3 + x - x^2, f_3 = x - x^2.$$

Donner la colonne des coordonnées canoniques de f.

Plus généralement, on a la notion suivante.

4.3.5. Définition. Soit $\{u_1, \ldots, u_n\}$ une base de E. Soient $v_1, \ldots, v_m \in E$ dont les colonne des coordonnées dans $\{u_1, \ldots, u_n\}$ sont $A_1, \ldots, A_m$ respectivement. La matrice

$$(A_1 \cdots A_m)_{n\times m}$$

s'appelle la *matrice des coordonnées* de la famille $\{v_1, \ldots, v_m\}$ dans la base $\{u_1, \ldots, u_n\}$, notée $P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_m\}}$.

Remarque. (1) Si l'on considère $(v_1, \ldots, v_m)$ et $(u_1, \ldots, u_n)$ comme des matrices-ligne formelles, alors

$$(v_1, \ldots, v_m) = (u_1, \ldots, u_n) P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_m\}}.$$

Ceci est illustré par le diagramme suivant:

$$(u_1, \cdots, u_n) \xrightarrow{P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_m\}}} (v_1, \cdots, v_m).$$

(2) $P_{\{u_1,\ldots,u_n\}}^{\{v\}}$ est la colonne des coordonnées de v dans $\{u_1, \ldots, u_n\}$.

Exercice. Soit $\{u_1, u_2, u_3\}$ une base de $\mathbb{R}^3$. Donner $P_{\{u_1,u_2,u_3\}}^{\{u_3,u_2\}}$.

Exercice. Considérons la base non canonique $\{e_{11}, e_{22}, e_{21}, e_{12}\}$ de l'espace réel $M_2(\mathbb{R})$. Trouver les matrices $A_1, A_2, A_3 \in M_2(\mathbb{R})$ telles que

$$P_{\{e_{11},e_{22},e_{21},e_{12}\}}^{\{A_1,A_2,A_3\}} = \begin{pmatrix} 1 & 5 & 7 \\ 4 & 1 & 3 \\ 3 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}.$$

Le résultat suivant est une conséquence immédiate du lemme 4.3.2.

4.3.6. Lemme. (1) Si $v_1, \ldots, v_m \in K^{(n)}$, alors la matrice des coordonnées canoniques de $\{v_1, \ldots, v_m\}$ est $(v_1 \cdots v_m)$.

(2) Si $w_1, \ldots, w_m \in K^n$, alors la matrice des coordonnées canoniques de $\{w_1, \ldots, w_m\}$ est $(w_1^T \cdots w_m^T)$.

Le résultat suivant dit comment utiliser matrices des coordonnées pour déterminer si l'un vecteur est une combinaison linéaire ou non d'une famille donnée de vecteurs.

4.3.7. Théorème. Soit $\{u_1, \ldots, u_n\}$ une base de E. Soient $v_1, \ldots, v_m; v \in E$ avec $A = P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_m\}}$ et $B = P_{\{u_1,\ldots,u_n\}}^{\{v\}}$.

(1) $v = \alpha_1 v_1 + \cdots + \alpha_m v_m$ avec $\alpha_1, \cdots, \alpha_m \in K$ si, et seulement si,

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

est une solution du système $AX = B$.

(2) v est une combinaison linéaire de $v_1, \ldots v_m$ si, et seulement si, $\mathrm{rg}(A) = \mathrm{rg}(A|B)$.

Démonstration. Posons $A = (A_1 \cdots A_m)$, où $A_j = P_{\{u_1,\ldots,u_n\}}^{\{v_j\}}$, $j = 1, \ldots, m$.

(1) D'après le lemme 4.3.3(1), $v = \alpha_1 v_1 + \cdots + \alpha_m v_m$ si, et seulement si, $P_{\{u_1,\ldots,u_n\}}^{\{v\}} = P_{\{u_1,\ldots,u_n\}}^{\{\alpha_1 v_1 + \cdots + \alpha_m v_m\}}$. En vertu du lemme 4.3.4, c'est équivalent à

$$B = \alpha_1 A_1 + \cdots + \alpha_m A_m = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix},$$

c'est-à-dire,

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

est une solution du système $AX = B$.

(2) D'après l'énoncé (1), v est une combinaison linéaire de $v_1, \ldots v_m$ si, et seulement si, $AX = B$ est compatible. D'après le théorème 3.12, ce dernier est équivalent à $\mathrm{rg}(A) = \mathrm{rg}(A|B)$. Ceci achève la démonstration du théorème.

Exercice. Considérer l'espace réel $\mathbb{R}^{(3)}$ et ses vecteurs

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \; v_2 = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \; v_3 = \begin{pmatrix} 3 \\ 2 \\ 2 \end{pmatrix}, \; v = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Déterminer si v est une combinaison linéaire ou non de v_1, v_2 et v_3.

Exercice. Considérer l'espace rationnel $\mathbb{Q}_3[x]$ et ses vecteurs

$$f_1 = 2 - x + x^2,\ f_2 = 1 + x - 2x^2,\ f = 3 + x + ax^2.$$

Trouver la valeur de a pour que f s'exprime comme une combinaison linéaire de f_1, f_2; et dans ce cas, donner une expression explicite.

Le résultat suivant nous dit comment utiliser matrice des coordonnées pour déterminer si une famille de vecteurs est libre ou liée.

4.3.8. Théorème. Soit $\{u_1, \ldots, u_n\}$ une base de E. Soient $v_1, \ldots, v_m \in E$ avec $A = P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_m\}}$. Les trois premières conditions suivantes sont équivalentes.

(1) $\{v_1, \ldots, v_m\}$ est libre.

(2) Le système homgogène $AX = 0$ n'a que la solution nulle.

(3) $\mathrm{rg}(A) = m$.

Par conséquent, si $m > n$, alors $\{v_1, \ldots, v_m\}$ est liée.

Démonstration. Remarquons que $P_{\{u_1,\ldots,u_n\}}^{\{0_E\}} = 0_{n\times 1}$. Or, $\{v_1, \ldots, v_m\}$ est liée si et seulement s'il existe $\alpha_1, \ldots, \alpha_n \in K$, non tous nuls, tels que $\alpha_1 u_1 + \cdots + \alpha_n u_n = 0_E$. D'après le théorème 4.3.7(1), cela est équivalent au fait que

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

est une solution non nulle du système homogène $AX = 0_{n\times 1}$. Ceci montre l'équivalence des énoncés (1) et (2). D'après le théorème 3.14(1), les énoncés (2) et (3) sont équivalents.

Supposons enfin que $m > n$. Alors $\mathrm{rg}(A) \le \min\{m, n\} = n < m$. D'après ce qu'on a montré, $\{v_1, \ldots, v_m\}$ est liée. Ceci achève la démonstration du théorème.

Exemple. Comme $\{1, i\}$ est une base de ${}_{\mathbb{R}}\mathbb{C}$. Tous les trois complexes sont linéairement dépendants sur $\mathbb{R}$.

Exercice. Soient $f_1 = 1 + 4x + 7x^2,\ f_2 = 2 + 5x + 8x^2,\ f_3 = 3 + 6x + 9x^2 \in \mathbb{Q}_3[x]$. Déterminer si $\{f_1, f_2, f_3\}$ est libre ou liée.

Le résultat suivant est un cas particulier des théorèmes 4.3.7 et 4.3.8.

4.3.9. Théorème. Soit $A \in M_{m\times n}(K)$.

(1) Les colonnes de A sont linéairement indépendantes si et seulement si $\mathrm{rg}(A) = n$.

(2) Un vecteur $B \in K^{(m)}$ est une combinaison linéaire des colonnes de A si et seulement si $\mathrm{rg}(A) = \mathrm{rg}(A \mid B)$.

Démonstration. Posons $A = (A_1 \cdots A_m)$, où $A_1, \ldots, A_n \in K^{(m)}$. Considérons la base canonique $\{e_1, \ldots, e_m\}$ de $K^{(m)}$. D'après le lemme 4.3.6(1), $P_{\{e_1,\ldots,e_m\}}^{\{A_1,\ldots,A_n\}} = A$.

(1) D'après le théorème 4.3.8(3), $\{A_1, \ldots, A_n\}$ est libre si et seulement si $\mathrm{rg}(A) = n$.

(2) D'après le lemme 4.3.2(1), $P_{\{e_1,\ldots,e_m\}}^{\{B\}} = B$. D'après le théorème 4.3.7(2), B est une combinaison linéaire de $A_1, \ldots, A_n$ si et seulement si $\mathrm{rg}(A) = \mathrm{rg}(A|B)$. Ceci achève la preuve du théorème.

Exercice. Considérons les vecteurs suivants:

$$v_1 = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}, v_3 = \begin{pmatrix} -2 \\ 3 \\ a \end{pmatrix} \in \mathbb{R}^{(3)}.$$

Donner les valeurs de a pour que $\{v_1, v_2, v_3\}$ est libre.

Exercice. Considérer l'espace réel $\mathbb{R}^3$ et ses vecteurs

$$u_1 = \begin{pmatrix} 2 \\ 3 \\ 2 \end{pmatrix},\ u_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix},\ u_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},\ u = \begin{pmatrix} 1 \\ 5 \\ 1 \end{pmatrix}.$$

Déterminer si u est une combinaison linéaire de u_1, u_2, u_3.

Le résultat suivant est une autre forme du lemme 4.3.4, qui donne une méthode pour trouver les coordonnées d'une combinaison linéaire d'une famille de vecteurs à l'aide de la matrice des coordonnées.

4.3.10. Proposition. Soit $\{u_1, \ldots, u_n\}$ une base de E. Soient $v_1, \ldots, v_m; v \in E$. Si

$$v = (v_1, \ldots, v_m) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

avec $\alpha_1, \ldots, \alpha_m \in K$, alors

$$P_{\{u_1,\ldots,u_n\}}^{\{v\}} = P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_m\}} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}.$$

Démonstration. Posant $P^{\{v_j\}}_{\{u_1,\ldots,u_n\}} = A_j$, on a $P^{\{v_1,\ldots,v_m\}}_{\{u_1,\ldots,u_n\}} = (A_1 \cdots A_m)$. Par hypothèse, $v = \alpha_1 v_1 + \cdots + \alpha_m v_m$. D'après la proposition 4.3.4 et le lemme 2.2.4(2),

$$P^{\{v\}}_{\{u_1,\ldots,u_n\}} = \alpha_1 A_1 + \cdots + \alpha_m A_m = (A_1 \cdots A_m) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = P^{\{v_1,\ldots,v_m\}}_{\{u_1,\ldots,u_n\}} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}.$$

Ceci achève la démonstration de la proposition.

Remarque. La proposition 4.3.10 est illustrée par le diagramme commutatif suivant:

$$\begin{tikzcd}
(u_1, \cdots, u_n) \arrow[r, "P^{\{v_1,\cdots,v_m\}}_{\{u_1,\cdots,u_n\}}"] \arrow[dr, "P^{\{v\}}_{\{u_1,\cdots,u_n\}}"'] & (v_1, \cdots, v_m) \arrow[d, "\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}"] \\
& v.
\end{tikzcd}$$

On conclut cette section par une propriété de matrices de coordonnées.

4.3.11. Lemme. Soit $\{u_1, \ldots, u_n\}$ une base de E. Si $A \in M_{n\times m}(K)$ et $B \in M_{m\times p}(K)$, alors

$$(u_1, \ldots, u_n)(AB) = ((u_1, \ldots, u_n)A)\, B.$$

Démonstration. On partage $B = (B_1 \ \cdots \ B_p)$ en colonnes. Si l'on pose

$$(v_1, \ldots, v_m) = (u_1, \ldots, u_n)A,$$

alors $A = P^{\{v_1,\ldots,v_m\}}_{\{u_1,\ldots,u_n\}}$. En outre, posons

$$(w_1, \ldots, w_p) = (v_1 \ldots v_m)B = ((u_1, \ldots, u_n)A)B.$$

Par définition, $w_j = (v_1, \ldots, v_m)B_j$. D'après la proposition 4.3.10,

$$P^{\{w_j\}}_{\{u_1,\ldots,u_n\}} = P^{\{v_1,\ldots,v_m\}}_{\{u_1,\ldots,u_n\}} B_j = AB_j, \quad j = 1, \ldots, p.$$

Ainsi $P^{\{w_1,\ldots,w_p\}}_{\{u_1,\ldots,u_n\}} = (AB_1 \cdots AB_p) = AB$. C'est-à-dire, $(w_1, \ldots, w_p) = (u_1, \ldots, u_n)(AB)$. Ceci achève la démonstration du lemme.

4.4. Dimension

Partout dans cette section, on se fixe E un K-espace vectoriel. D'après le théorème 4.2.9, E admet toujours des bases. Bien que les bases de E ne soient pas uniques en général, on a le résultat suivant.

4.4.1. Théorème. Toutes les bases de E ont le même nombre (peut-être l'infini) de vecteurs. Ce nombre commun s'appelle la *dimension* de E, noté $\dim(E)$.

Démonstration. Si $E = \{0_E\}$, alors la famille vide est la seule base de E. Supposons maintenant que E est non nul. Soient $\mathcal{U}$ et $\mathcal{B}$ deux bases de E, qui sont toutes non vides. Si $\mathcal{U}$ et $\mathcal{B}$ sont toutes infinies, alors le résultat est valide. Supposons que $\mathcal{U}$ ou $\mathcal{B}$ est fini, disons $|\mathcal{U}| = n > 0$. Si $|\mathcal{B}| > n$, on peut trouver des vecteurs distincts $v_1, \ldots, v_n, v_{n+1} \in \mathcal{B}$. D'après le théorème 4.3.8, $\{v_1, \ldots, v_{n+1}\}$ est liée. Par conséquent, $\mathcal{B}$ est liée, une contradiction. Donc $|\mathcal{B}| \leq n$. De même, $|\mathcal{U}| \leq |\mathcal{B}|$. D'où $|\mathcal{B}| = |\mathcal{U}|$. Ceci achève la démonstration.

Remarque. (1) $\dim(E) = 0$ si, et seulement si, $E = \{0_E\}$.

(2) On dit que E est de *dimension infinie* s'il admet une base infinie; et sinon, de *dimension finie*.

Exemple. (1) $\dim_{\mathbb{R}} \mathbb{C} = 2$ et $\dim_{\mathbb{C}} \mathbb{C} = 1$.

(2) Soit un entier $n \geq 1$. On a $\dim K_n[x] = \dim K^n = \dim K^{(n)} = n$.

(3) $K[x]$ est de dimension infinie car $\{1, x, \ldots, x^n, \ldots, \}$ est une base infinie.

Une base d'un espace vectoriel satisfait aux deux conditions énoncées dans la définition 4.2.8. Maintenant, On étudiera les familles de vecteurs qui ne satisfait qu'à une de ces deux conditions.

4.4.2. Lemme. Si E est de dimension $n \geq 0$, alors

(1) toute famille libre de n vecteurs de E est une base.

(2) toute famille de plus que n vecteurs de E est liée.

Démonstration. Supposons que $n = 0$. Alors $E = \{0_E\}$. Une famille de 0 vecteur est la famille vide, qui est la base de E. En outre, toute famille d'au moins un vecteur contient 0_E, qui est liée.

Supposons maintenant que $n > 0$. Alors E admet une base $\mathcal{B} = \{u_1, \ldots, u_n\}$. D'après le théorème 4.3.8, toute famille de plus que n vecteurs de E est liée.

Soit $\mathcal{V} = \{v_1, \ldots, v_n\}$ une famille libre de vecteurs de E. Si $\mathcal{V}$ n'est pas une base de E, alors il existe un vecteur $v_{n+1} \in E$, qui n'est pas une combinaison linéaire de $v_1, \ldots, v_n$.

D'après le lemme 4.2.5, $\{v_1, \ldots, v_n, v_{n+1}\}$ est une famille libre de $n+1$ vecteurs. Ceci contredit le théorème 4.3.8. La preuve du lemme s'achève.

Exemple. (1) Comme $\dim \mathbb{R}^2 = 2$, deux vecteurs non co-linéaires de $\mathbb{R}^2$ forment une base; et tous trois vecteurs de $\mathbb{R}^2$ sont linéairement dépendants.

(2) Comme $\dim \mathbb{R}^3 = 3$, trois vecteurs non co-planaires de $\mathbb{R}^3$ forment une base; et tous quatre vecteurs de $\mathbb{R}^3$ sont linéairement dépendants.

(3) Le K-espace $M_{m\times n}(K)$ est de dimension mn. Ainsi, toute famille de $mn+1$ matrices de type $m \times n$ est liée.

4.4.3. Proposition. Si E est de dimension finie, alors toute famille libre de vecteurs de E est contenue dans une base.

Démonstration. Supposons que $\dim(E) = n$. Soit $\mathcal{U} = \{v_1, \ldots, v_m\}$ une famille libre de vecteurs de E. D'après le lemme 4.3.2(2), $m \leq n$. On procède par récurrence sur $r = n - m$.

Supposons que $r = 0$, c'est-à-dire, $m = n$. D'après le lemme 4.4.2, $\mathcal{U}$ est une base de E.

Supposons que $r > 0$ et le résultat est vrai pour $r - 1$. D'après le théorème 4.4.1, $\mathcal{U}$ n'est pas une base de E. Donc il existe $v \in E$ qui n'est pas une combinaison linéaire de vecteurs de $\mathcal{U}$. D'après le lemme 4.2.5, $\mathcal{V} = \{v_1, \ldots, v_m, v\}$ est libre aevc $n - |\mathcal{V}| = r - 1$. D'après l'hypothèse de récurrence, $\mathcal{V}$, et donc $\mathcal{U}$, est contenue dans une base de E. Ceci achève la démonstration de la proposition.

Exercice. Considérons l'espace réel $\mathbb{C}$. Donner une base de $\mathbb{C}$ contenant $2 + 3i$.

4.4.4. Lemme. Soient $\{u_1, \ldots, u_n\}$ et $\{v_1, \ldots, v_m\}$ des familles de vecteurs de E. Si chacun v_i avec $1 \leq i \leq m$ est une combinaison linéaire de $u_1, \ldots, u_n$, alors toute combinaison linéaire de $v_1, \ldots, v_m$ est une combinaison linéaire de $u_1, \ldots, u_n$.

Démonstration. Supposons que $v_i = \sum_{j=1}^n \beta_{ij} u_j,\ \beta_{ij} \in K$. Si $u = \sum_{i=1}^m \alpha_i v_i,\ \alpha_i \in K$, alors $v = \sum_{j=1}^n (\sum_{i=1}^m \alpha_i \beta_{ij}) u_j$, ce qui est une combinaison linéaire de $u_1, \ldots, u_n$. Ceci achève la démonstration du lemme.

4.4.5. Proposition. Soit $\mathcal{U}$ une famille finie de vecteurs de E. Si tout vecteur de E est une combinaison linéaire de vecteurs de $\mathcal{U}$, alors $\mathcal{U}$ contient une base de E.

Démonstration. Si $E = \{0_E\}$, alors la famille vide est une base contenue dans $\mathcal{U}$.

Supposons maintenant que E est non nul. Alors $\mathcal{U}$ contient au moins un vecteur non nul u. D'après le lemme 4.2.5, $\{u\}$ est une sous-famille libre de $\mathcal{U}$. Soit n le plus grand nombre tel que $\mathcal{U}$ a une sous-famille libre $\mathcal{B} = \{u_1, \ldots, u_n\}$. On prétend que $\mathcal{B}$ est une base de E.

Si $\mathcal{U}$ a un vecteur v qui n'est pas une combinaison linéaire de $u_1, \ldots, u_n$, d'après le lemme 4.2.5, $\{u_1, \ldots, u_n, v\}$ est une sous-famille libre de $n+1$ vecteurs de $\mathcal{U}$. Ceci contredit la maximalité de n. Donc tout vecteur de $\mathcal{U}$ est une combinaison linéaire de $u_1, \ldots, u_n$. D'après le lemme 4.4.4, tout vecteur de E est une combinaison linéaire de $u_1, \ldots, u_n$. D'où, $\mathcal{B}$ est une base de E. Ceci achève la démonstration de la proposition.

Le résultat suivant est très pratique pour déterminer si une famille de vecteurs donnée est une base ou non.

4.4.6. Théorème. Soit E de dimension n ayant une base $\{u_1, \ldots, u_n\}$. Si $v_1, \ldots, v_n \in E$, les conditions suivantes sont équivalentes.

(1) $\{v_1, \ldots, v_n\}$ est une base.

(2) $\{v_1, \ldots, v_n\}$ est libre.

(3) Tout vecteur de E est une combinaison linéaire de $v_1, \ldots, v_n$.

(4) $P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_n\}}$ est inversible.

Démonstration. D'abord, par définition, l'énoncé (1) implique les énoncés (2) et (3). Supposons que l'énoncé (2) ou (3) est valide. D'après les propositions 4.4.3 et 4.4.4, il existe une base $\mathcal{B}$ de E telle que $\{v_1, \ldots, v_n\} \subseteq \mathcal{B}$, ou bien, $\mathcal{B} \subseteq \{v_1, \ldots, v_n\}$. Comme $\dim(E) = n$, on a $|\mathcal{B}| = n$. Ainsi $\{v_1, \ldots, v_n\} = \mathcal{B}$. En particulier, $\{v_1, \ldots, v_n\}$ est une base de E. Ceci montre l'équivalence des énoncés (1), (2) et (3).

Enfin, $\{v_1, \ldots, v_n\}$ est une base si et seulement si $\{v_1, \ldots, v_n\}$ est libre si et seulement si $P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_n\}}$ est de rang n si et seulement si $P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_n\}}$ est inversible. Ceci achève la démonstration du théorème.

Exercice. Vérifier laquelle des familles suivantes est une base de l'espace vectoriel donné.

(1) $\{v_1 = (1,2,1), v_2 = (2,1,3), v_3 = (3,3,4)\} \subseteq \mathbb{R}^3$.

(2) $\{f_1 = 1 + x, f_2 = 2 + x, f_3 = 3 + x + x^2\} \subseteq \mathbb{R}_3[x]$.

Exercice. Augmenter la famille $\{u_1 = (1,2,1), u_2 = (2,1,1)\}$ à une base de $\mathbb{R}^3$.

4.5. Matrice de passage

Partout dans cette section, on se fixe E un K-espace vectoriel de dimension finie.

4.5.1. Définition. Soient $\{u_1, \ldots, u_n\}$ et $\{v_1, \ldots, v_n\}$ deux bases de E. La matrice des coordonées de la famille $\{v_1, \ldots, v_n\}$ dans la base $\{u_1, \ldots, u_n\}$ s'appelle la *matrice de passage* de la base $\{u_1, \ldots, u_n\}$ vers la base $\{v_1, \ldots, v_n\}$, notée encore $P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_n\}}$.

Remarque. (1) D'après le théorème 4.4.6(4), toute matrice de passage est inversible.
(2) La matrice de passage d'une base $\{u_1, \ldots, u_n\}$ vers $\{u_1, \ldots, u_n\}$ est I_n.

Exemple. Considérons l'espace vectoriel réel $\mathbb{C}$ dont $\{1, i\}$ et $\{2 + 3i, 1 - 5i\}$ sont deux bases. La matrice de la famille $\{2 + 3i, 1 - 5i\}$ dans la base $\{1, i\}$ est

$$\begin{pmatrix} 2 & 1 \\ 3 & -5 \end{pmatrix} := A.$$

Par définition, A est la matrice de passage de la base $\{1, i\}$ vers la base $\{2 + 3i, 1 - 5i\}$.

Si E est l'un des espaces vectoriels de dimension finie ayant une base canonique, alors il est trivial de trouver les coodonnées d'un vecteur dans la base canonique. Le résultat suivant nous dit en particulier comment trouver les coordonnées d'un vecteur dans une base non canonique à l'aide de la matrice de passage.

4.5.2. Proposition. Soient $\{u_1, \ldots, u_n\}$ et $\{v_1, \ldots, v_n\}$ des bases de E. Soit P la matrice de passage de $\{u_1, \ldots, u_n\}$ vers $\{v_1, \ldots, v_n\}$. Si $\{w_1, \ldots, w_m\}$ est une famille ordonnée de vecteurs de E avec $A = P_{\{u_1,\ldots,u_n\}}^{\{w_1,\ldots,w_m\}}$, alors

$$P_{\{v_1,\ldots,v_n\}}^{\{w_1,\ldots,w_m\}} = P^{-1}A.$$

Ceci est illustrée par le diagramme suivant:

$$\begin{tikzcd} (u_1, \ldots, u_n) \arrow[r, "P"] \arrow[dr, "A"'] & (v_1, \ldots, v_n) \arrow[d, dotted, "P^{-1}A"] \\ & (w_1, \ldots, w_m). \end{tikzcd}$$

Démonstration. Par hypothèse, $(v_1, \ldots, v_n) = (u_1, \ldots, u_n)P$. D'où

$$(v_1, \ldots, v_n)P^{-1} = ((u_1, \ldots, u_n)P)P^{-1} = (u_1, \ldots, u_n)(PP^{-1}) = (u_1, \ldots, u_n).$$

Maintenant, comme $P_{\{u_1,\ldots,u_n\}}^{\{w_1,\ldots,w_m\}} = A$, on a

$$(w_1, \ldots, w_m) = (u_1, \ldots, u_n)A = ((v_1, \ldots, v_n)P^{-1})A = (v_1, \ldots, v_n)(P^{-1}A).$$

D'où, $P_{\{v_1,\ldots,v_n\}}^{\{w_1,\ldots,w_m\}} = P^{-1}A$. Ceci achève la démonstration de la proposition.

Remarque. Si $m = 1$, le résultat ci-dessus donne le changement des coordonnées d'un vecteur dans deux bases.

Exercice. Considérons l'espace rationnel $\mathbb{Q}_3[x]$. Trouver les coordonnées du polynôme $f = 4 + 5x + 3x^2$ dans la base $\{1 + x, 2 + x, 3 + x + x^2\}$.

Exercice. Soit θ un angle. Considérer les vecteurs du plan $\mathbb{R}^2$ suivants:

$$u_1 = (\cos\theta, \sin\theta),\ u_2 = (-\sin\theta, \cos\theta).$$

(1) Vérifier que $\{u_1, u_2\}$ est une base de $\mathbb{R}^2$.
(2) Trouver les coordonnées de $u = (a, b) \in \mathbb{R}^2$ dans $\{u_1, u_2\}$.

Si E est l'un d'espaces vectoriels de dimension finie ayant une base canonique, alors il est facile de trouver la matrice de passage de la base canonique vers une autre base. En appliquant la proposition 4.5.2 à une base de E, on a le résultat suivant, qui nous permettra de trouver la matrice de passage d'une base quelconque vers une autre base quelconque.

4.5.3. Corollaire. Soient $\{u_1, \ldots, u_n\}$, $\{v_1, \ldots, v_n\}$ et $\{w_1, \ldots, w_n\}$ des bases de E. Si P et Q sont les matrices de passage de $\{u_1, \ldots, u_n\}$ vers $\{v_1, \ldots, v_n\}$ et vers $\{w_1, \ldots, w_n\}$, alors la matrice de passage
(1) de $\{v_1, \ldots, v_n\}$ vers $\{u_1, \ldots, u_n\}$ est P^{-1}.
(2) de $\{v_1, \ldots, v_n\}$ vers $\{w_1, \ldots, w_n\}$ est $P^{-1}Q$, ce qui est illustrée par le diagram

$$\begin{tikzcd}
(u_1, \ldots, u_n) \arrow[r, "P"] \arrow[dr, "Q"'] & (v_1, \ldots, v_n) \arrow[d, dotted, "P^{-1}Q"] \\
& (w_1, \ldots, w_n).
\end{tikzcd}$$

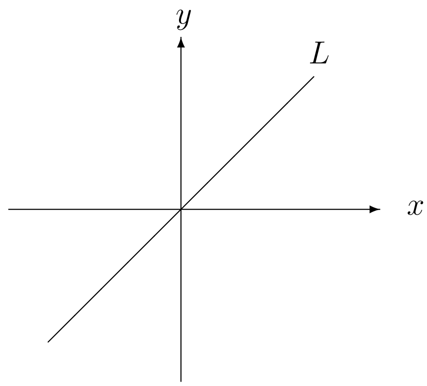
Exercice. Considérons les bases de l'espace réel $\mathbb{R}^3$ suivantes:

$$\{u_1 = (1,1,0),\ u_2 = (2,1,0), u_3 = (3,1,1)\}\,;\ \{v_1 = (0,1,1),\ v_2 = (1,0,1), v_3 = (1,1,0)\}\,.$$

Trouver la matrice de passage
(1) de $\{u_1, u_2, u_3\}$ vers la base canonique $\{e_1, e_2, e_3\}$;
(2) de $\{u_1, u_2, u_3\}$ vers $\{v_1, v_2, v_3\}$.

4.6. Sous-espaces vectoriels

On commence par un exemple. Considère la droite $L = \{(x, x) \mid x \in \mathbb{R}\}$ du plan illustré comme suit:



Il est évident que si $u, v \in L$ et $\alpha \in \mathbb{R}$, alors $u + v, \alpha u \in L$. Donc L est stable pour l'addition et la multiplication scalaire. Donc, L lui-même est un espace vectoriel réel.

Dès maintenant jusqu'à la fin de cette section, on se fixe E un espace vectoriel sur K.

4.6.1. Définition. Un sous-ensemble non vide F de E s'appelle *sous-espace vectoriel* (ou bien, *sous-espace*) si pour tous $u, v \in F$ et $\alpha \in \mathbb{R}$, on a

(1) $\alpha u \in F$;

(2) $u + v \in F$.

Remarque. (1) $\{0_E\}$ et E sont des sous-espaces de E, appelés les *sous-espaces triviaux.*

(2) Si F un sous-espace de E, alors F est un K-espace vectoriel muni des opérations induites de celles de E avec $0_F = 0_E$.

Exemple. On voit que $F = \big\{(x, y, 0) \in \mathbb{R}^3 \mid x, y \in \mathbb{R}\big\}$ est un sous-espace de $\mathbb{R}^3$.

Exercice. Vérifier si les sous-ensembles de $\mathbb{R}^2$ suivants sont des sous-espaces vectoriels.

(1) $F = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = -1\}$;

(2) $G = \{(n, n) \in \mathbb{R}^2 \mid n \in \mathbb{Z}\}$;

(3) $H = \{(x, y) \in \mathbb{R}^2 \mid x = 0 \text{ ou } y = 0\}$.

4.6.2. Proposition. Soit F un sous-ensemble non vide de E. Les conditions suivantes sont équivalentes.

(1) F est un sous-espace de E.

(2) Si $u, v \in F$ et $\alpha, \beta \in K$, alors $\alpha u + \beta v \in F$.

(3) Si $u_1, \cdots u_r \in F$ et $\alpha_1, \cdots \alpha_r \in K$, où $r \geq 1$, alors $\alpha_1 u_1 + \cdots \alpha_r u_r \in F$.

Démonstration. Supposons que l'énoncé (1) est vrai. Si $u, v \in E$ et $\alpha, \beta \in K$, alors $\alpha u, \beta v \in F$, et donc $\alpha u + \beta v \in F$.

Supposons que l'énoncé (2) est valide. Soient $u_1, \cdots u_r \in E$ et $\alpha_1, \cdots \alpha_r \in K$ avec $r \geq 1$. Si $r = 1$, alors $\alpha_1 u_1 = \alpha_1 u_1 + 0_K u_1 \in F$. Supposons que $r > 1$ et l'énoncé (3) est vrai pour $r - 1$. En particulier, $\alpha_1 u_1 + \cdots \alpha_{r-1} u_{r-1},\ \alpha_r u_r \in F$. D'où

$$\alpha_1 u_1 + \cdots \alpha_{r-1} u_{r-1} + \alpha_r u_r = 1 \cdot (\alpha_1 u_1 + \cdots \alpha_{r-1} u_{r-1}) + \alpha_r u_r \in E.$$

Supposons, enfin, que l'énoncé (3) est vrai. Si $u, v \in F$ et $\alpha \in K$, alors $\alpha u \in F$ et $u + v = 1_K \cdot u + 1_K \cdot v \in F$. Ceci achève la démonstration de la proposition.

4.6.3. Proposition. Si F est un sous-espace de E, alors $\dim(F) \leq \dim(E)$. En outre, si E est de dimension finie, alors $\dim(F) = \dim(E)$ si, et seulement si, $F = E$.

Démonstration. Si E est de dimension infinie, il est évident que $\dim(F) \leq \dim(E)$.

Supposons maintenant que $\dim(E) = n$. Si $\mathcal{U}$ est une base de F, alors $\mathcal{U}$ est une famille libre de vecteurs de E. D'après la proposition 4.4.3, $\mathcal{U} = \{u_1, \ldots, u_r\}$ avec $r \leq n$. D'où, $\dim(F) \leq \dim(E)$.

Supposons que $\dim(F) = \dim(E)$, c'est-à-dire, $r = n$. D'après le lemme 4.4.2, $\{u_1, \ldots, u_r\}$ est une base de E. Ainsi tout $u \in E$ s'écrit comme $u = \alpha_1 u_1 + \cdots + \alpha_n u_n$, $\alpha_i \in K$. Comme $u_i \in F$, d'après la proposition 4.6.2(3), $u \in F$. Ceci montre que $E \subseteq F$, et donc, $F = E$. La preuve de la proposition s'achève.

Remarque. La deuxième partie de la proposition 4.6.3 n'est pas vraie en général. Par exemple, considérons le K-espace $K[x]$. L'ensemble F des polynômes de degré paire est un sous-espace de $K[x]$ avec $\dim(F) = \dim K[x] = \infty$. Mais $F \neq K[x]$.

Exemple. (1) Si F est un sous-espace non trivial du plan $\mathbb{R}^2$, alors $0 < \dim(F) < 2$. D'où, $\dim(F) = 1$. C'est-à-dire, F est une droite.

(2) Si F est un sous-espace non trivial de $\mathbb{R}^3$, alors $0 < \dim(F) < 3$, et donc $\dim(F) = 1$ ou 2. C'est-à-dire, F est une droite ou un plan.

4.6.4. Proposition. Soit $\mathcal{U}$ une famille non-vide de vecteurs de E. L'ensemble

$$< \mathcal{U} >= \{u \in E \mid u = \alpha_1 + \cdots \alpha_r u_r; r \geq 1; u_1, \ldots, u_r \in \mathcal{U}; \alpha_1, \ldots, \alpha_r \in K\}$$

est le plus petit sous-espace de E contenant $\mathcal{U}$, appelé *sous-espace engendré* par $\mathcal{U}$.

Démonstration. Si $u \in \mathcal{U}$, alors $u = 1_K \cdot u \in < \mathcal{U} >$. D'où, $\mathcal{U}$ est contenu dans $< \mathcal{U} >$.

Soient $u, v \in < \mathcal{U} >$ et $\alpha, \beta \in K$. Comme u, v sont deux combinaisons linéaires de vecteurs de $\mathcal{U}$, d'après le lemme 4.4.4, $\alpha u + \beta v$ l'est aussi. C'est-à-dire, $\alpha u + \beta v \in < \mathcal{U} >$. D'après la proposition 4.6.2, $< \mathcal{U} >$ est un sous-espace de E.

Soit F un sous-espace de E contenant $\mathcal{U}$. Si $u \in < \mathcal{U} >$, alors $u = \alpha_1 + \cdots \alpha_r u_r$, où $\alpha_1, \ldots, \alpha_r \in K$ et $u_1, \ldots, u_r \in \mathcal{U}$. Comme $u_1, \ldots, u_r \in F$, d'après la proposition 4.6.2(3), $u \in F$. Cela montre que $< \mathcal{U} > \subseteq F$. La preuve de la proposition s'achève.

Remarque. (1) Comme $\{0_E\}$ est le plus petit sous-espace de E contenant la famille vide $\emptyset$, par convention, $< \emptyset > = \{0_E\}$.

(2) Si $\mathcal{U} = \{u_1, \ldots, u_n\}$, alors

$$< \mathcal{U} > = \{\alpha_1 u_1 + \cdots + \alpha_n u_n \mid \alpha_1, \ldots, \alpha_n \in K\} := < u_1, \ldots, u_n > .$$

(3) Si $E = < \mathcal{U} >$, on dit alors que $\mathcal{U}$ *engendre* E. En vertu de cette terminologie, une famille $\mathcal{B}$ de vecteurs de E est une base si et seulement si $\mathcal{B}$ est libre et $\mathcal{B}$ engendre E.

Exemple. (1) Si $u \in \mathbb{R}^3$ est non nul, alors $< u > = \{\alpha u \mid \alpha \in \mathbb{R}\}$ est la droite de $\mathbb{R}^3$ contenant u.

(2) Si $u, v \in \mathbb{R}^3$ ne sont pas colinéaires, alors $< u, v > = \{\alpha u + \beta v \mid \alpha, \beta \in \mathbb{R}\}$ est le plan contenant u et v.

Exercice. Considérons l'espace vectoriel réel $C[0, 2\pi]$. Vérifier, pour tout entier $n \geq 1$, que $\sin t \notin < 1, t, \ldots, t^{n-1} >$.

Le résultat suivant est utile pour le calcul de sous-espace Dans la pratique.

4.6.5. Corollaire. Soient $\mathcal{U}$ et $\mathcal{V}$ des familles de vecteurs de E, telles que tout vecteur de $\mathcal{V}$ est une combinaison linéaire de vecteurs de $\mathcal{U}$.

(1) $< \mathcal{V} > \subseteq < \mathcal{U} >$.

(2) Si $\mathcal{U} \subseteq \mathcal{V}$, alors $< \mathcal{U} > = < \mathcal{V} >$.

Démonstration. Par définition, $\mathcal{V} \subseteq < \mathcal{U} >$. Ainsi $< \mathcal{U} >$ est un sous-espace de E contenant $\mathcal{V}$. D'après la propsotion 4.6.4, $< \mathcal{V} > \subseteq < \mathcal{U} >$.

Supposons en outre que $\mathcal{U} \subseteq \mathcal{V}$. Alors $< \mathcal{V} >$ est un sous-espace de E contenant $\mathcal{U}$. D'après la propsotion 4.6.4, $< \mathcal{U} > \subseteq < \mathcal{V} >$. D'où $< \mathcal{U} > = < \mathcal{V} >$. Ceci achève la démonstration du corollaire.

Remarque. Si $F =< u_1, \ldots, u_{n-1}, u_n >$ avec u_n une combinaison linéaire de $u_1, \ldots, u_{n-1}$, alors $F =< u_1, \ldots, u_{n-1} >$.

On va étudier comment trouver une base pour un sous-espace engendré par une famille finie de vecteurs. Le résultat suivant est une conséquence immédiate de la définition d'une base.

4.6.6. Lemme. Soit $\mathcal{U}$ une famille de vecteurs de E. Alors $\mathcal{U}$ est une base de $< \mathcal{U} >$ si et seulement si $\mathcal{U}$ est libre.

Exemple. Considérons l'espace vectoriel réel $C[0, 2\pi]$.

(1) Soit $F =< \sin t, \cos t >$. Comme $\{\sin t, \cos t\}$ est libre, elle est une base de F,

(2) Soit $G =< \sin nt \mid n \in \mathbb{Z} >$. Comme $\{\sin nt \mid n \geq 1\}$ est libres, elle est une base infinie de G.

Si $F =< v_1, \cdots, v_m >$, d'après la proposition 4.4.5, $\{v_1, \ldots, v_m\}$ contient une base $\{v_{j_1}, \cdots, v_{j_r}\}$, avec $1 \leq j_1 < j_2 < \cdots < j_r \leq m$, de F. Le résultat suivant nous dit comment trouver ces indices $j_1, \ldots, j_r$.

4.6.7. Théorème. Soit F un sous-espace de E engendré par $v_1, \ldots, v_m$. Prenons une base $\{u_1, \ldots, u_n\}$ de E; et calculons $A = P_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots v_m\}}$, dont B est une forme échelonnée. Si les pivots de B se trouvent dans les colonnes $j_1, \cdots, j_r$, alors $\{v_{j_1}, \cdots, v_{j_r}\}$ est une base de F. En particulier, $\dim(F) = \mathrm{rg}(A)$.

Demonstration. Écrivons $A = (A_1 \cdots A_m)$, où $A_j = P_{\{u_1,\cdots,v_n\}}^{\{v_j\}}$. Écrivons $B = (B_1 \cdots B_n)$ en colonnes, dont les pivots se trouvent dans les colonnes $j_1, \ldots, j_r$. Considérons $B' = (B_{j_1}, \ldots, B_{j_r})$ et $(B' \mid B_j) = (B_{j_1}, \ldots, B_{j_r} \mid B_j)$, $j = 1, \ldots, m$. On voit que B' et $(B' \mid B_j)$ sont toutes échelonnées de rang r.

On prétend que $\{v_{j_1}, \ldots, v_{j_r}\}$ est une base de F. D'abord, $P_{\{u_1,\ldots,u_n\}}^{\{v_{j_1},\ldots,v_{j_r}\}} = (A_{j_1} \cdots A_{j_r}) = A'$. Comme A se réduit à B, on voit que A' se réduit à B'. D'où, $\mathrm{rg}(A') = r$. D'après le théorème 4.3.8(3), $\{v_{j_1}, \ldots, v_{j_r}\}$ est libre.

En outre, pour tout $1 \leq j \leq m$, comme $(A_1 \cdots A_m)$ se réduit à $(B_1 \cdots B_m)$, on voit que $(A' \mid A_j) = (A_1 \cdots A_m \mid A_j)$ se réduit à $(B_1 \cdots B_m \mid B_j) = (B' \mid B_j)$. En conséquence, $\mathrm{rg}(A' \mid A_j) = r = \mathrm{rg}(A')$. D'après le théorème 4.3.7(2), v_j est une combinaison linéaire de $v_{j_1}, \ldots, v_{j_r}$. D'après le corollaire 4.6.5(2), $F =< v_1, \ldots, v_m >=< v_{j_1}, \ldots, v_{j_r} >$. Ceci achève la démonstration du théorème.

Exercice. Trouver une base du sous-espace F de $\mathbb{Q}_4[x]$ engendré par

$$f_1 = 1 + x - 2x^2 + x^3, \; f_2 = 2 + 2x - 4x^2 + 2x^3, \; f_3 = 2 + x + 2x^3.$$

4.6.8. Définition. Les opérations suivantes sur une famille ordonnée $\{v_1, \ldots, v_m\}$ de vecteurs de E s'appelle les *opérations élémentaires*:

Type 1: Permuter deux vecteurs.

Type 2: Additionner à un vecteur un multiple d'un autre vecteur.

Type 3: Multiplier un vecteur par un scalaire non nul de K.

En outre, on dit qu'une famille ordonnée $\{v_1, \ldots, v_m\}$ se réduit à une autre famille ordonnée $\{w_1, \ldots, w_m\}$ si cette dernière est obtenue à partir de la première par une suite finie d'opérations élémentaires.

Remarque. Les opérations élémentaires sur les familles ordonnées de m vecteurs de E sont toutes inversibles.

4.6.9. Théorème. Soient $\mathcal{V} = \{v_1, \ldots, v_m\}$ et $\mathcal{W} = \{w_1, \ldots, w_m\}$ deux familles ordonnées de vecteurs de E. Si $\mathcal{V}$ se réduit à $\mathcal{W}$, alors $< \mathcal{V} >=< \mathcal{W} >$.

Démonstration. On peut supposer que $\mathcal{W}$ est obtenue à partir de $\mathcal{V}$ par une seule opération élémentaire T. Alors il est facile de voir que chacun des w_i est une combinaison linéaire de $v_1, \ldots, v_m$. D'où, $< \mathcal{W} >\subseteq< \mathcal{V} >$. D'autre part, comme $\mathcal{W}$ se réduit à $\mathcal{V}$ par T^{-1}, on a $< \mathcal{V} >\subseteq< \mathcal{W} >$. Donc, $< \mathcal{V} >=< \mathcal{W} >$. Ceci achève la démonstration.

4.6.10. Corollaire. Soit $\mathcal{V}$ une famille finie de vecteurs de E. Si $\mathcal{V}$ se réduit à une autre famille $\mathcal{W}$, alors $\mathcal{V}$ est une base de E si, et seulement si, $\mathcal{W}$ l'est.

Démonstration. Supposons que $\mathcal{V} = \{v_1, \ldots, v_n\}$ se réduit à $\mathcal{W} = \{w_1, \ldots, w_n\}$. Si $\mathcal{V}$ est une base de E, alors $\dim(E) = n$ et $< w_1, \ldots, w_n >=< v_1, \ldots, v_n >= E$. D'après le théorème 4.4.6(3), $\{w_1, \ldots, w_n\}$ est une base de E. Récirpqouement, si $\mathcal{W}$ est une base de E, comme $\mathcal{W}$ se réduit à $\mathcal{V}$, on a vu que $\mathcal{V}$ est une base de E. Ceci achève la démonstration du corollaire.

4.7. Sous-espaces associés à une matrice

L'objet de cette section est d'étudier trois sous-espaces associés à une matrice. En particulier, on montrera que les formes échelonnées d'une matrice donnée ont le même nombre de pivots, un résultat accepté sans démonstration dans la section 2.3.

4.7.1. Théorème. Soit $AX = 0$ un système homogène à n inconnues sur K. Alors l'ensemble $\mathcal{N}(A)$ des solutions de ce système est un sous-espace vectoriel de $K^{(n)}$. Afin de trouver une base de $\mathcal{N}(A)$, on réduit ce système à un système homogène échelonné $A'X = 0$.

1. Si le système échelonné n'a aucune inconnue libre, alors $\mathcal{N}(A)$ est nul. En particulier, $\mathcal{N}(A)$ a pour base l'ensemble vide.
2. Si le système échelonné admet s inconnues libres $x_{i_1}, x_{i_2}, \ldots, x_{i_s}$, alors $\mathcal{N}(A)$ a une base $\{u_1, u_2, \cdots, u_s\}$ trouvée de la façon suivante: on choisit s scalaires $a_1, a_2, \cdots, a_s \in K$, tous non nuls, et résout successivement le système échelonné

   (1) en posant $x_{i_1} = a_1,\ x_{i_2} = \cdots = x_{i_s} = 0$, ce qui donne la solution u_1;

   (2) en posant $x_{i_1} = 0, x_{i_2} = a_2, x_{i_3} = \cdots = x_{i_s} = 0$, ce qui donne la solution u_2;

   $\vdots$

   (s) en posant $x_{i_1} = \cdots = x_{i_{s-1}} = 0, x_{i_s} = a_s$, ce qui donne la solution u_s.

En tout cas, $\dim(\mathcal{N}(A)) = n - \mathrm{rg}(A)$, le nombre d'inconnues libres du système échelonné.

Démonstration. D'abord, il est facile de vérifier que $\mathcal{N}(A)$ est un sous-espace de $K^{(n)}$. Supposons que le système échelonné a s inconnues libres $x_{i_1}, x_{i_2}, \ldots, x_{i_s}$. On montrera que $\{u_1, u_2, \ldots, u_s\}$ est une base de $\mathcal{N}(A)$. Pour simplifier la notation, on suppose que les inconnues libres sont $x_{r+1}, x_{r+2}, \ldots, x_n$, c'est-à-dire, $i_j = r + j,\ j = 1, \ldots, s$. Alors u_j^T s'écrit $u_j^T = (b_{j1}, \ldots, b_{jr},\ 0, \ldots, 0,\ a_j,\ 0,\ \ldots,\ 0)$, $j = 1, \ldots, s$. Soient $\alpha_1, \ldots, \alpha_s \in K$ tels que $\sum_{j=1}^{s} \alpha_j u_j = 0$. Ceci donne

$$(\sum_{j=1}^{s} \alpha_j b_{j1},\ \ldots,\ \sum_{j=1}^{s} \alpha_j b_{jr},\ a_1\alpha_1,\ a_2\alpha_2,\ \ldots,\ a_s\alpha_s) = (0, \ldots, 0, 0, 0, \ldots, 0).$$

Ainsi $\alpha_j = 0$ car $a_j \neq 0$, pour tout $1 \leq j \leq s$. Par conséquent, $\{u_1, u_2, \ldots, u_s\}$ est libre. Enfin, soit $u \in \mathcal{N}(A)$, et posons $u^T = (\lambda_1, \ldots, \lambda_r, \lambda_{r+1}, \lambda_{r+2}, \ldots, \lambda_n)$, $\lambda_i \in K$. Donc u est la solution telle que $x_{r+k} = \lambda_{r+k}$, $k = 1, \ldots, s$. D'autre part, $\lambda_{r+1} a_1^{-1} u_1 + \cdots + \lambda_n a_s^{-1} u_s$ est aussi une solution telle que $x_{r+k} = \lambda_{r+k}$, $k = 1, \ldots, s$. Ainsi $u = \lambda_{r+1} a_1^{-1} u_1 + \cdots + \lambda_n a_s^{-1} u_s$. Ceci montre que $\{u_1, \ldots, u_s\}$ est une base de $\mathcal{N}(A)$. La preuve s'achève.

Remarque. On appelle $\mathcal{N}(A)$ l'*espace-solution* du système homogène $AX = 0$, ou bien, le *noyau* de la matrice A.

Exemple. Trouver une base de l'espace-solution du système homogène réel suivant:

$$\begin{array}{ccccccccccccc}
2x_1 & + & x_2 & - & x_3 & + & 2x_4 & - & x_5 & + & 3x_6 & = & 0 \\
4x_1 & + & 2x_2 & - & x_3 & + & 5x_4 & + & 3x_5 & + & 5x_6 & = & 0 \\
2x_1 & + & x_2 & - & x_3 & + & 2x_4 & & & + & 5x_6 & = & 0.
\end{array}$$

4.7.2. Définition. Soit $A \in M_{m\times n}(K)$. On définit

(1) *espace-colonne* de A, noté $\mathcal{C}(A)$, comme étant le sous-espace vectoriel de $K^{(m)}$ engendré par les colonnes de A;

(2) *espace-ligne* de A, noté $\mathcal{L}(A)$, comme étant le sous-espace vectoriel de K^n engendré par les lignes de A s'appelle.

4.7.3. Proposition. Un système $AX = B$ est compatible si et seulement si $B \in \mathcal{C}(A)$.

Démonstration. Écrivons $A = (A_1 \cdots A_n)$ en colonnes. Alors $\mathcal{C}(A) =< A_1, \cdots, A_n >$. Or, le système est compatible si et seulement si, il existe $\alpha_1, \ldots, \alpha_n \in K$, tels que

$$B = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \alpha_1 A_1 + \cdots + \alpha_n A_n,$$

si et seulement si $B \in \mathcal{C}(A)$. Ceci achève la démonstration de la proposition.

4.7.4. Lemme. Soient A, B des matrices sur K. Si A se réduit à B par des opérations élémentaires sur les lignes, alors $\mathcal{L}(A) = \mathcal{L}(B)$.

Démonstration. Soient $A_1, \ldots, A_m$ les lignes de A, et $B_1, \ldots, B_m$ les lignes de B. Si A se réduit à B, alors la famille $\{A_1, \ldots, A_m\}$ se réduit à la famille $\{B_1, \ldots, B_m\}$. D'après le théorème 4.6.9, $< A_1, \ldots, A_m >=< B_1, \ldots, B_m >$. C'est-à-dire, $\mathcal{L}(A) = \mathcal{L}(B)$. Ceci achève la démonstration.

4.7.5. Lemme. Soit A une matrice échelonnée sur K. Les lignes non nulles de A forment une base de $\mathcal{L}(A)$. En particulier, $\dim\mathcal{L}(A)$ est égal au nombre de pivots de A.

Démonstration. On procède par récurrence sur r, le nombre de pivots de A. Si $r = 0$, alors A est nulle, et donc $\mathcal{L}(A)$ est nul. Dans ce cas, la famille des lignes non nulles de A est vide, qui est la base de $\mathcal{L}(A)$.

Supposons maintenant que $r \geq 1$ et le résultat est vrai pour $r-1$. Soient $A_1, \ldots, A_{r-1}, A_r$ avec $0 < r \leq m$ les lignes non nulles de A. Il est évident que $\mathcal{L}(A) =< A_1, \ldots, A_{r-1}, A_r >$. En outre, la matrice

$$B = \begin{pmatrix} A_2 \\ \vdots \\ A_r \end{pmatrix}$$

est échelonnée n'ayant aucune ligne nulle. Par l'hypothèse de récurrence, $\{A_2, \ldots, A_r\}$ est une base de $\mathcal{L}(B)$. En particulier, $\{A_2, \ldots, A_r\}$ est une famille libre. Soit a_{1,j_1} le pivot de la première ligne de A. Alors la j_1-ième composante de A_1 est non nul et cela de A_i est nulle pour $i = 2, \ldots, r$. Ceci implique que A_1 n'est pas une combinaison linéaire de $A_2, \ldots, A_r$.

D'après le lemme 4.2.5, $\{A_1, A_2, \ldots, A_r\}$ est libre, et donc une base de $\mathcal{L}(A)$. Ceci achève la démonstration.

Maintenant, on est capable de donner la démonstration du théorème 2.3.5.

4.7.6. Proposition. Si A est une matrice sur K, alors les forme échelonnées de A ont le même nombre de pivots, et ce nombre commun est égal à $\dim \mathcal{L}(A)$.

Démonstration. Soit B une forme échelonnée de A. D'après le lemme 4.7.4, $\mathcal{L}(A) = \mathcal{L}(B)$. En particulier, $\dim\mathcal{L}(A) = \dim\mathcal{L}(B)$. D'après le lemme 4.7.5, ce dernier est égal au nombre de pivots de B. La preuve de la proposition s'achève.

4.7.7. Théorème. Si A est une matrice sur K, alors

$$\dim \mathcal{C}(A) = \text{rg}(A) = \dim \mathcal{L}(A).$$

Démonstration. Il suffit de montrer la première égalité. Partageons $A = (A_1 \cdots A_n)$ en colonnes. Alors $\mathcal{C}(A) =< A_1, \ldots, A_n >$. En outre, A est la matrice des coordonnées de $\{A_1, \ldots, A_n\}$ dans la base canonique. D'après le théorème 4.6.7, $\dim\mathcal{C}(A) = \text{rg}(A)$. Ceci achève la démonstration du théorème.

On va utiliser le théorème ci-haut pour montrer le résultat suivant qui a été établi dans le chapitre III.

4.7.8. Corollaire. Un système d'équations linéaires $AX = B$ est compatible si, et seulement si, $\text{rg}(A) = \text{rg}(A \mid B)$.

Démonstration. On partage $A = (A_1 \cdots A_n)$ en colonnes. Alors

$$\mathcal{C}(A) =< A_1, \cdots, A_n >\subseteq< A_1, \cdots, A_n, B >= \mathcal{C}(A \mid B).$$

Or le système $AX = B$ est compatible si, et seulement si, $B \in \mathcal{C}(A)$ si, et seulement si, $< A_1, \cdots, A_n >=< A_1, \cdots, A_n, B >$ si, et seulement si, $\dim \mathcal{C}(A) = \dim \mathcal{C}(A|B)$, c'est-à-dire, $\text{rg}(A) = \text{rg}(A|B)$. Ceci achève la démonstration du corollaire.

4.7.9. Proposition. Si A est une matrice sur K, alors $\text{rg}(A) = \text{rg}(A^T)$.

Démonstration. Soient $A_1, \cdots, A_m$ les lignes de A. Alors $A_1^T \cdots A_m^T$ sont les colonnes de A^T. Ainsi $\mathcal{L}(A) =< A_1, \cdots, A_m >$ et $\mathcal{C}(A^T) =< A_1^T, \cdots, A_n^T >$. D'après la proposition 4.4.5, $\mathcal{L}(A)$ a une base $\{A_{j_1}, \cdots, A_{j_r}\}$ avec $1 \le j_1 < \cdots < j_r \le n$. On prétend que $\left\{A_{j_1}^T, \cdots, A_{j_r}^T\right\}$ est une base de $\mathcal{C}(A^T)$.

D'abord, supposons que $\alpha_1 A_{j_1}^T + \cdots + \alpha_r A_{j_r}^T = \mathbf{0}$, $\alpha_i \in K$. En transposant deux côtés, d'après la proposition 2.1.11, on obtien $\alpha_1 A_{j_1} + \cdots + \alpha_r A_{j_r} = \mathbf{0}$. Ainsi $\alpha_1 = \cdots = \alpha_r = 0$. Ceci montre que $\left\{A_{j_1}^T, \cdots, A_{j_r}^T\right\}$ est libre.

Ensuite, pour tout $u \in \mathcal{C}(A^T)$, on a $u^T \in \mathcal{L}(A)$. Ainsi, $u^T = \beta_1 A_{j_1} + \cdots + \beta_r A_{j_r}$, $\beta_i \in K$. D'où, $u = (u^T)^T = \alpha_1 A_{j_1}^T + \cdots + \alpha_r A_{j_r}^T$. Ceci montre que $\left\{A_{j_1}^T, \cdots, A_{j_r}^T\right\}$ est une base de $\mathcal{C}(A^T)$. Par conséquent, $\mathrm{rg}(A^T) = \dim \mathcal{C}(A^T) = r = \dim \mathcal{L}(A) = \mathrm{rg}(A)$. Ceci achève la preuve du corollaire.

4.7.10. Proposition. Si $A \in M_{m\times n}(K)$ et $B \in M_{n\times p}(K)$, alors

$$\mathrm{rg}(AB) \leq \min\{\mathrm{rg}(A), \mathrm{rg}(B)\}.$$

Démonstration. On partage $B = (B_1, \ldots, B_p)$ en colonnes. D'après le lemme 2.2.5(2), $AB = (AB_1 \cdots AB_p)$, et donc $\mathcal{C}(AB) =< AB_1, \ldots, AB_p >$. En vertu du lemme 2.2.4(2), on voit que $AB_j \in \mathcal{C}(A)$, $j = 1, \cdots, p$. D'après le corollaire 4.6.5(1), $\mathcal{C}(AB) \subseteq \mathcal{C}(A)$. D'après le théorème 4.7.7 et la proposition 4.6.3, $\mathrm{rg}(AB) = \mathrm{dim}\mathcal{C}(AB) \leq \mathrm{dim}\mathcal{C}(A) = \mathrm{rg}(A)$. En outre, d'après la proposition 4.7.9 et ce qu'on a montré, on a

$$\mathrm{rg}(AB) = \mathrm{rg}(AB)^T = \mathrm{rg}(B^T A^T) \leq \mathrm{rg}(B^T) = \mathrm{rg}(B).$$

Ceci achève la démonstration de la proposition.

4.7.11. Théorème. Soit $A \in M_n(K)$. Les conditions suivantes sont équivalentes:
(1) A est inversible.
(2) Les lignes de A sont linéairement indépendantes.
(3) Les colonnes de A sont linéairement indépendantes.

Démonstration. En vertu des théorèmes 4.3.9(1) et 2.4.8, on obtien l'équivalence de (1) et (3). Par définition, $\mathcal{L}(A) =< A_1, \ldots, A_n >$ avec $A_1, \ldots, A_n$ les lignes de A. Maintenant, A est inversible, si et seulement si $\mathrm{rg}(A) = n$, si et seulement si, $\dim \mathcal{L}(A) = \dim(K^n)$ si, et seulement si, $< A_1, \ldots, A_n >= K^n$ si, et seulement si, $\{A_1, \ldots, A_n\}$ est libre d'après le théorème 4.4.6. La preuve du théorème s'achève.

4.8. Intersection et somme de sous-espaces

Partout dans cette section, on se fixe E un espace vectoriel sur K. On étudiera les opérations sur les sous-espaces de E.

4.8.1. Proposition. Soient $F_1, F_2, \ldots, F_r$ des sous-espaces de E.

(1) L'intersection $\cap_{i=1}^r F_i$ est un sous-espace de E.

(2) La somme $\sum_{i=1}^r F_i = \{u_1 + u_2 + \cdots + u_r \mid u_i \in F_i\}$ est un sous-espace de E.

Démonstration. (1) D'abord, $0_E \in \cap_{i=1}^r F_i$ car $0_E \in F_i$, pour tout $1 \leq i \leq r$. Si $u, v \in \cap_{i=1}^r F_i$ et $\alpha, \beta \in K$, alors $u, v \in F_i$, pour tout $1 \leq i \leq r$. Comme F_i est un sous-espace, $\alpha u + \beta v \in F_i$ pour tout $1 \leq i \leq r$. Donc $\alpha u + \beta v \in \cap_{i=1}^r F_i$. Ceci montre que $\cap_{i=1}^r F_i$ est un sous-espace de E.

(2) D'abord, $0_E = 0_E + 0_E + \cdots + 0_E$, $0_E \in F_i$ entraîne que $0_E \in \sum_{i=1}^r F_i$. Si $u, v \in \sum_{i=1}^r F_i$ et $\alpha, \beta \in K$, alors $u = u_1 + \cdots + u_r, v = v_1 + \cdots + v_r$ avec $u_i, v_i \in F_i$. Donc $\alpha u + \beta v = (\alpha u_1 + \beta v_1) + \cdots + (\alpha u_n + \beta v_n)$. Comme F_i est un sous-espace, $\alpha u_i + \beta v_i \in F_i$. Ainsi $\alpha u + \beta v \in \sum_{i=1}^r F_i$. Ceci achève la démonstration.

Remarque. Par contre, la réunion de sous-espaces n'est pas nécessairement un sous-espace.

Exercice. Considérons les sous-espaces de l'espace réel $\mathbb{Q}_4[x]$ suivants:

$$F =< f_1 = 1 + 2x - x^2, f_2 = 1 - x + x^2 - x^3, f_3 = 2 + x - x^2 + x^3 >$$

et

$$G =< g_1 = 1 - x^3, g_2 = 2 + x - 2x^3, g_3 = 1 + 2x - 2x^2 + 2x^3 > .$$

Trouver l'intersection de F et G.

Exercice. Considérons les matrices rationnelles suivantes:

$$A = \begin{pmatrix} 1 & 4 & 2 \\ 1 & 3 & 1 \\ -2 & -4 & 0 \\ 1 & 4 & 2 \end{pmatrix}, \ B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \\ 3 & 2 & 3 \\ 2 & 1 & 4 \end{pmatrix}.$$

Trouver une base de $\mathcal{C}(A) \cap \mathcal{C}(B)$.

Le résultat suivant est utile Dans la pratique.

4.8.2. Lemme. Si $\mathcal{U}$ et $\mathcal{V}$ sont des familles de vecteurs de E, alors

$$< \mathcal{U} > + < \mathcal{V} > = < \mathcal{U} \cup \mathcal{V} > .$$

Démonstration. D'abord, $< \mathcal{U} > \subseteq < \mathcal{U} \cup \mathcal{V} >$ et $< \mathcal{V} > \subseteq < \mathcal{U} \cup \mathcal{V} >$. Ainsi $< \mathcal{U} > + < \mathcal{V} > \subseteq < \mathcal{U} \cup \mathcal{V} >$. Comme $\mathcal{U} \cup \mathcal{V} \subseteq < \mathcal{U} > + < \mathcal{V} >$, d'après le corollaire

4.6.5(1), $<\mathcal{U}\cup\mathcal{V}>\subseteq<\mathcal{U}>+<\mathcal{V}>$. Ceci montre que $<\mathcal{U}\cup\mathcal{V}>=<\mathcal{U}>+<\mathcal{V}>$. La preuve s'achève.

Exercice. Considérons les matrices suivantes:

$$A=\begin{pmatrix} 1 & 1 & -2 & 1 \\ 4 & 3 & -4 & 4 \\ 2 & 1 & 0 & 2 \end{pmatrix}, \quad B=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 3 & 2 & -2 & 3 \\ 2 & 1 & -3 & 2 \end{pmatrix}$$

Trouver une base de $\mathcal{L}(A)+\mathcal{L}(B)$.

Le résultat suivant nous dit le lien entre la dimension de la somme et celle de l'intersection.

4.8.3. Formule de Grassmann. Si F et G sont des sous-espaces de dimension finie de E, alors $F+G$ est de dimension finie et

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

Démonstration. Étant un sous-espace de F et de G, d'après la proposition 4.6.3, $F\cap G$ admet une base finie $\{v_1,\ldots,v_s\}$. D'après la proposition 4.4.3, $\{v_1,\ldots,v_s\}$ se plonge en une base $\{v_1,\ldots,v_s,v_{s+1},\cdots,v_p\}$ de F et en une base $\{v_1,\cdots,v_s,w_{s+1},\cdots,w_q\}$ de G. On prétend que $\{v_1,\cdots,v_s,v_{s+1},\cdots,v_p,w_{s+1},\cdots,w_q\}$ est une base de $F+G$. En effet, d'après le lemme 4.8.2,

$$\begin{aligned} F+G &= <v_1,\cdots,v_s,v_{s+1},\cdots,v_p>+<v_1,\cdots,v_s,w_{s+1},\cdots,w_q> \\ &= <\{v_1,\cdots,v_s,v_{s+1},\cdots,v_p\}\cup\{v_1,\cdots,v_s,w_{s+1},\cdots,w_q\}> \\ &= <v_1,\cdots,v_s,v_{s+1},\cdots,v_p,w_{s+1},\cdots,w_q>. \end{aligned}$$

Supposons que $\sum_{i=1}^p\alpha_iv_i+\sum_{j=s+1}^q\beta_jw_j=0_E$. Alors $\sum_{i=1}^p\alpha_iv_i=-\sum_{j=s+1}^q\beta_jw_j\in F\cap G$. D'où, $\sum_{i=1}^s\alpha_iv_i+\sum_{i=s+1}^p\alpha_iv_i=\sum_{i=1}^s\gamma_iv_i,\ \gamma_i\in K$. Donc

$$\sum_{i=1}^s(\alpha_i-\gamma_i)v_i+\sum_{i=s+1}^p\alpha_iv_i=0_E.$$

Comme $\{v_1,\ldots,v_s,\ldots,v_p\}$ est libre, $\alpha_i=0$, $i=s+1,\ldots,p$. Par conséquent, $\sum_{i=1}^s\alpha_iv_i+\sum_{j=s+1}^q\beta_jw_j=0_E$. Comme $\{v_1,\ldots,v_s,w_{s+1},\ldots,w_q\}$ est libre, on voit que $\alpha_i=0$ et $\beta_j=0$ pour tous $1\le i\le s$ et $s+1\le j\le q$. Ainsi $\{v_1,\cdots,v_s,v_{s+1},\cdots,v_p,w_{s+1},\cdots,w_q\}$ est libre. Ceci établit notre énoncé. Par conséquent,

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

Ceci achève la démonstration.

Exemple. Si P_1, P_2 sont deux plans de l'espace réel $\mathbb{R}^3$ passant par l'origine, alors $P_1 \cap P_2 \neq 0$.

Exercice. Considérons les matrices suivantes:

$$A = \begin{pmatrix} 1 & 1 & -2 & 1 \\ 4 & 3 & -4 & 4 \\ 2 & 1 & 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 3 & 2 & -2 & 3 \\ 2 & 1 & -3 & 2 \end{pmatrix}$$

Trouver la dimension de $\mathcal{L}(A) \cap \mathcal{L}(B)$.

En général, un vecteur $u \in \sum_{i=1}^r F_i$ peut s'écrire de plusieurs façon sous la forme $u = \sum_{i=1}^r u_i,\ u_i \in F_i$.

4.8.4. Théorème. Soient $F_1, \ldots, F_r$ des sous-espaces de E et $F = \sum_{i=1}^r F_i$. Les conditions suivantes sont équivalentes:

(1) Tout $u \in F$ s'écrit d'une façon unique $u = u_1 + \cdots + u_r,\ u_i \in F_i$.

(2) Toute équalité $u_1 + \cdots + u_r = 0_E,\ u_i \in F_i$, entaîne que $u_1 = \cdots = u_r = 0$.

(3) $F_i \cap (\sum_{1 \leq j \leq r,\, j \neq i} F_j) = \{0_E\}$, pour $i = 1, \ldots, r$.

Dans ce cas, on dit que F est la somme *directe* des F_i et on écrit $F = \oplus_{i=1}^r F_i$.

Démonstartion. Supposons que (1) est vrai et que $u_1 + \cdots + u_r = 0_E,\ u_i \in F_i$. Mais $0_E = 0_E + \cdots + 0_E,\ 0_E \in F_i$. Par l'unicité, $u_i = 0_E$ pour tout $1 \leq i \leq r$. Ceci montre que l'énoncé (1) implique l'énoncé (2).

Supposons que (2) est vrai. Soit $u_i \in F_i \cap (F_1 + \cdots + F_{i-1} + F_{i+1} + \cdots + F_r)$. Alors $u_i = u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_r,\ u_j \in F_j$. Donc $u_1 + \cdots + u_{i-1} + (-u_i) + u_{i+1} + \cdots + u_r = 0_E$. Ainsi $-u_i = 0_E$ et donc $u_i = 0_E$. Par conséquent, $F_i \cap (F_1 + \cdots + F_{i-1} + F_{i+1} + \cdots + F_r) = \{0_E\}$. Ceci montre que l'énoncé (2) implique l'énoncé (3).

Enfin supposons que l'énoncé (3) est vrai. Soit $u \in \sum_{i=1}^r F_i$, qui s'écrit $u = \sum_{i=1}^r u_i = \sum_{i=1}^r v_i$ avec $u_i, v_i \in F_i$. Alors pour tout $1 \leq i \leq r$,

$$u_i - v_i = \sum\nolimits_{1 \leq j \leq r,\, j \neq i} (v_j - u_j) \in F_i \cap (F_1 + \cdots + F_{i-1} + F_{i+1} + \cdots + F_r) = \{0_E\}.$$

Ainsi $u_i = v_i$, pour tout $1 \leq i \leq r$. Ceci achève la démonstration.

Remarque. (1) Si $r = 1$, alors $F = F_1$ est une somme direct par définition.

(2) Si $r = 2$, alors la somme $F_1 + F_2$ est directe si et seulement si $F_1 \cap F_2 = 0$. Mais ce n'est pas vrai si $r > 2$.

Exemple. (1) Si $F_1 = \{(x,0,0) | x \in \mathbb{R}\}$, $F_2 = \{(0,y,0) \,|\, y \in \mathbb{R}\}$, $F_3 = \{(0,0,z) \mid z \in \mathbb{R}\}$, alors $\mathbb{R}^3 = F_1 \oplus F_2 \oplus F_3$.

(2) Si $E_1 = \{(x,0,z) \mid x, z \in \mathbb{R}\}$ et $E_2 = \{(0,y,z) \mid y, z \in \mathbb{R}\}$, alors $\mathbb{R}^3 = E_1 + E_2$. Mais cette somme n'est pas directe.

Exercice. Considérons l'espace vectoriel réel $C[0, 2\pi]$ et ses deux sous-espaces $F =< 1, t, \cdots, t^n >$ avec $n \geq 1$ et $G =< \sin t, \sin 2t, \ldots, \sin mt >$ avec $m \geq 1$. Montrer que $F + G = F \oplus G$.

Démonstration. Soit $f \in F \cap G$. C'est-à-dire,

$$f = a_0 + a_1 t + \cdots + a_n t^n = b_1 \sin t + b_2 \sin 2t + \cdots + b_m \sin mt; \qquad \text{où } a_i, b_j \in \mathbb{R}.$$

On voit que $f^{(2n)} = 0$. De l'autre côté, comme $(\sin kt)^{(2n)} = (-1)^n k^{2n} \sin kt$, pour $k = 1, 2, \ldots, m$, on obtient

$$\sum_{k=1}^{m} k^{2n} (-1)^n b_k \sin kt = 0.$$

Comme $\{\sin t, \sin 2t, \ldots, \sin mt\}$ est libre, on a $k^{2n}(-1)^n b_k = 0$, et donc, $b_k = 0$, pour $k = 1, 2, \ldots, m$. Ainsi, $f = 0$. C'est-à-dire, $F \cap G = 0$.

4.8.5. Proposition. Soit $F = F_1 + \cdots + F_r$ avec $r \geq 3$, où $F_1, \ldots, F_r$ sont des sous-espaces vectoriels de E. Pour tout $1 \leq s < r$, posons $G_s = F_1 + \cdots + F_s$ et $H_s = F_{r+1} + \cdots + F_r$. Les conditions suivantes sont équivalentes:

(1) $F = \oplus_{i=1}^r F_i$.

(2) $G_s = \oplus_{i=1}^s F_i$, $H_s = \oplus_{i=s+1}^r F_i$ et $F = G_s \oplus H_s$, pour tout s avec $1 \leq s < r$.

(3) $G_s = \oplus_{i=1}^s F_i$, $H_s = \oplus_{i=s+1}^r F_i$ et $F = G_s \oplus H_s$, pour un certain s avec $1 \leq s < r$.

Démonstration. D'abord, on voit aisément que $F = G_s + H_s$ pour tout $1 \leq s < r$. Supposons que la somme $F = \oplus_{i=1}^r F_i$. Soit s un entier avec $1 \leq s < r$. Si $u_1 + \cdots + u_s = 0_E$, $u_i \in F_i$, $i = 1, \cdots, s$, alors $u_1 + \cdots + u_s + 0_E + \cdots + 0_E = 0_E$. Ainsi $u_i = 0_E$, $i = 1, \ldots, s$. C'est-à-dire, $G_s = \oplus_{i=1}^s F_i$. De même, $H_s = \oplus_{i=s+1}^r F_i$. De plus, supposons que $u + v = 0_E$, où $u \in G_s$ et $v \in H_s$. Alors $u = u_1 + \cdots + u_s$ et $v = u_{s+1} + \cdots u_r$, où $u_i \in F_i$, $i = 1, \ldots, r$. Ceci donne $0 = u + v = u_1 + \cdots + u_s + u_{s+1} + \cdots + u_r$. Comme la somme $\sum_{i=1}^r F_i$ est directe, on a $u_i = 0_E$, $i = 1, \ldots, r$. D'où $u = 0_E$ et $v = 0_E$. Donc $F = G_s \oplus H_s$. Ceci montre que l'énoncé (1) implique l'énoncé (2). Il est trivial que l'énoncé (2) implique l'énoncé (3).

Supposons enfin que l'énoncé (3) est vrai. Si $(u_1 + \cdots + u_s) + (u_{s+1} + \cdots + u_r) = 0_E$, où $u_i \in F_i$, $i = 1, \ldots, r$, alors $u_1 \cdots + u_s = 0_E$ et $u_{s+1} + \cdots + u_r = 0_E$ car la somme $G_s + H_s$ est directe. Comme la somme $\sum_{i=1}^s F_i$ est directe, on a $u_1 = \cdots = u_s = 0_E$. Et comme la somme $\sum_{i=s+1}^{r} F_i$ est directe, on a $u_{s+1} = \cdots = u_r = 0_E$. Ceci montre que la somme $\sum_{i=1}^{r} F_i$ est directe. Ceci achève la démonstration.

4.8.6. Lemme. Une famille $\{u_1, \ldots, u_r\}$ de vecteurs non nuls de E est libre si, et seulement si,

$$< u_1, \ldots, u_r > = < u_1 > \oplus \cdots \oplus < u_r > .$$

Démonstration. D'après le lemme 4.8.2, $< u_1, \ldots, u_r > = < u_1 > + \cdots + < u_r >$. La somme est directe si et seulement si toute égalité $v_1 + \cdots + v_r = 0_E$, où $v_i \in < u_i >$, entraîne que les v_i sont tous nuls. Cette condition est équivalent à dire que toute égalité $\alpha_1 u_1 + \cdots + \alpha_i u_r = 0_E$ avec $\alpha_i \in K$ entraîne que les α_i sont tous nuls, c'est-à-dire, $\{u_1, \ldots, u_r\}$ est libre. Ceci achève la démonstration.

4.8.7. Corollaire. Soit E de dimension finie. Si F est un sous-espace vectoriel de E, alors il existe un sous-espace vectoriel G de E tel que $E = F \oplus G$. Dans ce cas, on appelle G un *complément* de F dans E.

Démonstration. Si $F = E$, alors on prend $G = \{0_E\}$. Si $F = \{0_E\}$, on prend alors $G = E$. Supposons que F est un sous-espace propre de E. Prenons une base $\{u_1, \ldots, u_r\}$ de F, qui se prolonge en une base $\{u_1, \ldots, u_r, u_{r+1}, \ldots, u_n\}$ de E. D'après le lemme 4.8.6, $E = < u_1 > \oplus \cdots \oplus < u_r > \oplus < u_{r+1} > \oplus \cdots \oplus < u_n >$. D'après la proposition 4.8.5(2),

$$\begin{aligned} E &= (< u_1 > + \cdots + < u_r >) \oplus (< u_{r+1} > + \cdots + < u_n >) \\ &= < u_1, \ldots, u_r > \oplus < u_{r+1}, \ldots, u_n > . \end{aligned}$$

Posant $G = < u_{r+1}, \ldots, u_n >$, on a le résultat. Ceci achève la démonstration.

Remarque. Un sous-espace de E peut avoir une infinité de compléments dans E.

Exercice. Considéreons la matrice rationnelle suivante:

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

Trouver un complément de $\mathcal{L}(A)$ dans $\mathbb{R}^4$.

4.8.8. Théorème. Soit $F = F_1 + \cdots + F_r$, où les F_i sont des sous-espaces de dimension finie de E. Alors $F = F_1 \oplus \cdots \oplus F_r$ si, et seulement si, $\dim(F) = \dim(F_1) + \cdots + \dim(F_r)$; et dans ce cas, si $\mathcal{B}_i$ est une base de F_i, $i = 1, \cdots, r$, alors $\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_r$ est une base de F.

Démonstartion. Le théorème est évidemment valide pour $r = 1$. Supposons que $r \geq 2$. Si $r = 2$, alors $F = F_1 \oplus F_2$ si, et seulement si, $F_1 \cap F_2 = 0$ si, et seulement si, $\dim(F_1 \cap F_2) = 0$ si, et seulement si, $\dim(F) = \dim(F_1) + \dim(F_2)$.

Supposons que $r > 2$ et le théorème est vrai pour $r - 1$. On veut montrer le théorème pour r. Supposons premièrement que $F = F_1 \oplus \cdots \oplus F_r$. Posons $G = F_1 + \cdots + F_{r-1}$. D'après la proposition 4.8.5, $G = \oplus_{i=1}^{r-1} F_i$ et $F = G \oplus F_r$. D'après le théorème de Grassmann et l'hypothèse de récurrence, $\dim(F) = \dim(G) + \dim(F_r) = \sum_{i=1}^{r} \dim(F_i)$.

Supposons réciproquement que $\dim(F) = \sum_{i=1}^{r} \dim(F_i)$. Prennant une base $\mathcal{B}_i$ de F_i, pour $i = 1, \cdots, r$, on obtien $F =< \mathcal{B}_1 > + \cdots + < \mathcal{B}_r > =< \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_r >$. D'après la proposition 4.4.5, $\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_r$ contient une base $\mathcal{B}$ de F. De l'autre côté, $|\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_r| \leq |\mathcal{B}_1| + \cdots + |\mathcal{B}_r| = \dim(F) = |\mathcal{B}|$, et donc, $\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_r = \mathcal{B}$, une base de F. D'après le lemme 4.8.6 et la proposition 4.8.5(2), $F =< \mathcal{B}_1 > \oplus \cdots \oplus < \mathcal{B}_r > = F_1 \oplus \cdots \oplus F_r$. La preuve du théorème s'achève.

Exercice. Vérifier que $\mathbb{R}^3 = F_1 \oplus F_2 \oplus F_3$, où

$$F_1 = \{(x, x, 0) \mid x \in \mathbb{R}\}, F_2 = \{(0, y, y) \mid y \in \mathbb{R}\}, F_3 = \{(0, 0, z) \mid z \in \mathbb{R}\}.$$

Exercice. Considérons les sous-espaces de $\mathbb{R}^3$ suivants:

$$E_1 = \{(x, x, 0) \mid x \in \mathbb{R}\}, E_2 = \{(2y, 3y, 0) \mid y \in \mathbb{R}\}, E_3 = \{(z, -z, 0) \mid z \in \mathbb{R}\}.$$

Vérifier si la somme $E_1 + E_2 + E_3$ est directe ou non.

4.9. Exercices

1. Soit K un corps et E un K-espace vectoriel non nul. Montrer premièment que E est infini lorsque K est infini, et ensuite donner un contre exemple pour illustrer que ce n'est pas vrai si K est fini.

2. Dans chacun des cas suivants, déterminer si $\mathbb{R} \times \mathbb{R} = \{(x_1, x_2) \mid x_1, x_2 \in \mathbb{R}\}$ est un espace vectoriel sur $\mathbb{R}$ ou non pour les opérations données:

   (1) $\quad (x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2), \quad \alpha \cdot (x, y) = (\alpha x, 0), \quad \alpha \in \mathbb{R}.$

   (2) $\quad (x_1, x_2) + (y_1, y_2) = (x_1 - y_1, x_2 + y_2), \quad \alpha \cdot (x, y) = (\alpha x, \alpha y), \quad \alpha \in \mathbb{R}.$

3. Considérer le K-espace vectoriel $K_5[x]$ avec $K = \mathbb{Z}_7$ et les vecteurs

$$f_2 = 2 + 3x^2 - 4x^4; f_1 = 3 + 2x + x^3 + x^4 \; f_3 = 5x + 6x^2 - 2x^3.$$

Dans chacun des cas suivants, exprimer f comme une combinaison linéaire de f_1, f_2, et f_3 si possible, et donner une justification si impossible.

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

4. Considérer l'espace vectoriel réel $C[0, 2\pi]$ des fonctions continues définies sur $[0, 2\pi]$.
   (1) Vérifier, pour tout $n \geq 1$, que la famille $\{\cos t, \ldots, \cos nt\}$ est libre.
   (2) Déterminer si la fonction t est une combinaison linéaire ou non de $\sin t$, $\sin 2t$, et $\sin 3t$.

5. Considérer l'espace vectoriel réel $\mathbb{C}$. Déterminer $2 - 3i$ et $3 + 5i$ sont linéairement dépendants ou indépendants.

6. Soit E un espace vectoriel réel. Si $\{u_1, u_2, u_3\}$ est une famille libre de vecteurs de E, montrer que $\{3u_1,\ 2u_1 - u_2, u_1 + u_3\}$ est aussi libre.

7. Soit E un K-espace vectoriel. Si $\{u_1, \cdots, u_n\}$ est une famille libre de vecteurs de E, montrer que $\{a_1u_1, \cdots, a_nu_n\}$ est aussi libre, où $a_1, \cdots, a_n \in K$ sont tous non nuls.

8. Soit $C(\mathbb{R})$ l'espace vectoriel réel des fonctions continues réelles.
   (1) Vérifier que $\{e^t, e^{2t}, e^{3t}\}$ est une famille libre de vecteurs de $C(\mathbb{R})$.
   (2) Vérifier que si la fonction $t + 1$ est une combinaison linéaire ou non de e^t, e^{2t}, e^{3t}.
   Indice: Utiliser la dérivation.

9. Considérer l'espace vectoriel réel $C[0, 1]$ des fonctions continues définies sur $[0, 1]$.
   (1) Déterminer les fonctions $t + 1$, $t + 2$, et $t + 3$ sont linéairement dépendantes ou indépendantes.
   (2) Montrer que les fonctions $1, t, \ldots, t^n$ avec $n \geq 1$ sont linéairement indépendantes.
   (3) Déduire avec justification que $C[0, 1]$ est de dimension finie ou infinie.

10. Considérer les vecteurs suivants de l'espace vectoriel rationnel $\mathbb{Q}^{(4)}$:

$$u_1 = \begin{pmatrix} 1 \\ 4 \\ -5 \\ 2 \end{pmatrix}, \; u_2 = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 1 \end{pmatrix}, \; v = \begin{pmatrix} 2 \\ 18 \\ a \\ 9 \end{pmatrix}, \; w = \begin{pmatrix} 3 \\ 2 \\ a \\ b \end{pmatrix}.$$

(1) Donner la valeur de a pour que u_1, u_2, v soient linéairement dépendants.

(2) Pour quelles valeurs de a et b, peut-on exprimer w comme une combinaison linéaire de u_1, u_2? Et trouver une telle expression dans les cas possibles.

11. Soit E un K-espace vectoriel. Montrer qu'une famille $\{u_1, \ldots, u_n\}$ de vecteurs de E est liée si, et seulement si, il existe un indice i, avec $1 \leq i \leq n$, tel que u_i est une combinaison linéaire de $u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n$.

12. Dans chacune des parties suivantes, déterminer si la famille de vecteurs de $\mathbb{R}^{(4)}$ est liée ou libre; et si elle est liée, écrire un vecteur comme une combinaison linéaire des autres; et sinon, augmenter la famille à une famille libre de 4 vecteurs.

$$(1)\ \left\{\begin{pmatrix} 1 \\ 3 \\ -1 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 8 \\ -5 \\ 7 \end{pmatrix}, \begin{pmatrix} 2 \\ 9 \\ 4 \\ 23 \end{pmatrix}\right\}; \quad (2)\ \left\{\begin{pmatrix} 1 \\ -2 \\ 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ -3 \end{pmatrix}, \begin{pmatrix} 3 \\ -6 \\ 1 \\ 4 \end{pmatrix}\right\}.$$

13. Considérer l'espace réel $\mathbb{R}_3[x]$ et les vecteurs suivants:

$$f_1 = 1 - x + x^2,\ f_2 = 2 + 3x - x^2, f_3 = x + x^2.$$

(1) Vérifier, d'après la définition, que $\{f_1, f_2, f_3\}$ est une base de $\mathbb{R}_3[x]$.

(2) Trouver la colonne des coordonnées de $2 - x + 3x^2$ dans cette base.

14. Considérer l'espace réel ${}_{\mathbb{R}}\mathbb{C}$.

(1) Vérifier, d'après la définition, que $\{7 + 5i, 3 - 2i\}$ est une base de $\mathbb{C}$.

(2) Trouver la matrices des coordonnées de la famille $\{1 + i, 2 - i, 3 + i\}$ dans cette base ci-haut mentionnée.

15. Considérer l'espace vectoriel rationnel $\mathbb{Q}_3[x]$. Dans chacun des cas suivants, trouver la matrice des coordonnées de la famille dans la base canonique $\{1, x, x^2\}$, et en déterminer si la famille est libre ou liée.

(1) $\{1 + x, 2 + x\}$.

(2) $\{2 + x, 3 + x, 4 + 5x + 6x^2\}$.

(3) $\{5 + 6x - x^2, 2 - 3x + 5x^2, 7 + 3x + 4x^2\}$.

16. Considérer l'espace vectoriel réel $M_2(\mathbb{R})$ des matrices carrées réelles d'ordre 2 et sa base canonique $\{e_{11}, e_{12}, e_{21}, e_{22}\}$.

(1) Trouver la matrice des coordonnées de la famille suivante dans la base canonique:

$$A_1 = \begin{pmatrix} 2 & -3 \\ 6 & 2 \end{pmatrix}, \ A_2 = \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix}, A_3 = \begin{pmatrix} 3 & 3 \\ 1 & 5 \end{pmatrix}.$$

(2) Déterminer si la famille en partie (1) est liée ou libre.

(3) Donner les valeurs de a et b telles que la matrice A est une combinaison linéaire de A_1, A_2, A_3, où

$$A = \begin{pmatrix} a+3 & 1 \\ 5 & 2+b \end{pmatrix}.$$

(4) Trouver la famille dont la matrice des coordonnées dans la base canonique est comme ci-dessous:

$$\begin{pmatrix} 2 & -1 & \sqrt{2} & 0 & 1 \\ 2 & 1 & 5 & \sqrt{7} & 3 \\ 3 & 5 & -1 & 4 & 2 \\ 1 & 0 & 3 & 0 & 7 \end{pmatrix}.$$

17. Considérer l'espace vectoriel rationnel $\mathbb{Q}_4[x]$. Dans chacun des cas suivants, trouver la matrice de la famille dans la base canonique, et en déterminer si la famille est une base de $\mathbb{Q}_4[x]$ ou non.

(1) $\{3 + 2x - 5x^2 + 2x^3, -2 + x^2 - 3x^3, x^2 + x^3, 4 - x + 3x^2\}$.

(2) $\{1 + x + x^2 + x^3, 1 + x^2 + x^3, 1 + x + x^2, 6 + 4x + 6x^2 + 3x^3\}$.

18. Considérer l'espace vectoriel rationnel $\mathbb{Q}_4[x]$.

(1) Vérifier que la famille $\{2 - x + 3x^2 - x^3,\ 1 + x - x^2 + 2x^3\}$ est libre et prolonger cette famille en une base de $\mathbb{Q}_4[x]$.

(2) Pour quelles valeurs de a, les vecteurs suivants forme-t-ils une base de $\mathbb{Q}_4[x]$?

$$1 + x + x^2 + x^3, 1 + 2x + x^2 + x^3, 2x + ax^2, 1 + 3x + (a+2)x^3.$$

19. Considérer l'espace vectoriel réel $\mathbb{R}_{n+1}[x]$ des polynômes sur $\mathbb{R}$ de degré inférieur ou égal à n. Soit $f \in \mathbb{R}_{n+1}[x]$ de degré n. Montrer que f, $f^{(1)}$, $f^{(2)}$, $\ldots$, $f^{(n)}$, où $f^{(i)}$ est la i-ième dérivée de f, forment une base de $\mathbb{R}_{n+1}[x]$.

20. Soit E un espace vectoriel sur K. Montrer qu E est de dimension infinie si, et seulement si, il existe une famille infinie libre de vecteurs de E.

21. Vérifier que $\{1, \quad 1-x, \quad (1-x)^2\}$ est une base de l'espace vectoriel $\mathbb{R}_3[x]$, et trouver les coordonnées de $6-5x+2x^2$ dans cette base.

22. Considérer les familles de vecteurs de l'espace vectoriel réel $\mathbb{R}^4$ suivantes:

$$\mathcal{U} = \{(1,1,1,0),\ (1,1,0,1),\ (1,0,1,1),\ (0,1,1,1)\}$$

et

$$\mathcal{V} = \{(1,1,0,0),\ (1,0,1,0),\ (0,1,1,0),\ (0,0,1,1)\}.$$

(1) Montrer que $\mathcal{U}$, ainsi que $\mathcal{V}$, est une base de $\mathbb{R}^4$.

(2) Trouver la matrice de passage de $\mathcal{U}$ vers $\mathcal{V}$.

(3) Trouver la colonne des coordonnées de $(2,1,3,4)$ dans $\mathcal{U}$ et celle dans $\mathcal{V}$.

23. Dans chacun de cas suivants, déterminer si l'ensemble donné est un sous-espace de $\mathbb{R}^2$ ou non:

(1) $F_1 = \{(a,b) \in \mathbb{R}^2 \mid b = 2a\}$.

(2) $F_2 = \{(a,b) \in \mathbb{R}^2 \mid b = a^2\}$.

(3) $F_3 = \{(a,b) \in \mathbb{R}^2 \mid (a-b)^2 = 2a+b\}$.

24. Montrer que $F = \{\lambda + (2\lambda - 3\mu)x + (\lambda+\mu)x^2 \mid \lambda, \mu \in \mathbb{R}\}$ est un sous-espace de l'espace vectoriel réel $\mathbb{R}_3[x]$ et donner une base de F.

25. Soit $n \geq 1$ un entier. Déterminer lesquels des ensembles suivants sont sous-espaces de l'espace vectoriel $M_n(K)$ des matrices carrées d'ordre n.

(1) L'ensemble des matrices diagonales d'ordre n.

(2) L'ensemble des matrices d'ordre n ayant nulle trace.

(3) L'ensemble des matrices carrées non inversibles d'ordre n. *Indice*: Distinguer les cas où $n = 1$ et $n > 1$.

26. Soient $S_n(K)$ et $A_n(K)$ les sous-ensembles de $M_n(K)$ des matrices symétriques et des matrices anti-symétriques, respectivement.

(1) Montrer que $S_n(K)$ et $A_n(K)$ sont des sous-espaces vectoriels de $M_n(K)$.

(2) Trouver une base de $S_n(K)$.

(3) Donner une base de $A_n(K)$ en supposant que $1_K + 1_K \neq 0_K$.

27. Soit E un espace vectoriel sur K avec $u, v, w \in E$. Si $u+v+w = 0$, montrer que $<u,v> = <u,w>$.

28. Considérer l'espace vectoriel réel $C(\mathbb{R})$ des fonctions réelles continues. Soient $\lambda_1, \cdots, \lambda_n$, avec $n \geq 1$, des nombres réels deux à deux distincts.
   (1) Vérifier que les fonctions $e^{\lambda_1 t}, \ldots, e^{\lambda_n t}$ sont linéairement indépendantes dans $C(\mathbb{R})$.
   (2) Déterminer si la fonction $t+1$ appartient ou non au sous-espace vectoriel de $C(\mathbb{R})$ engendré par les fonctions $e^{\lambda_1 t}, \ldots, e^{\lambda_n t}$.

29. Soit E un espace vectoriel. Soient $\mathcal{U} = \{u_1, \ldots, u_r\}$ et $\mathcal{V} = \{v_1, \ldots, v_s\}$ deux familles de vecteurs de E telles que tout vecteur de $\mathcal{V}$ est une combinaison linéaire de vecteurs de $\mathcal{U}$.

   (1) Si $s = r$ et $\mathcal{V}$ est libre, montrer que $\mathcal{U}$ est libre.

   (2) Si $s > r$, montrer que $\mathcal{V}$ est liée.

   Indice: Considérer le sous espace $< \mathcal{U} >$.

30. Considérer l'espace vectoriel réel $C(\mathbb{R})$ des fonctions continues définies sur $\mathbb{R}$. Soit F le sous-espace engendré par les fonctions $\sin x, \sin 2x$ et $\sin 3x$. Soient $f_1 = \sin x + \sin 2x + \sin 3x$, $f_2 = \sin x - \sin 2x + 2\sin 3x$ et $f_3 = 2\sin x + \sin 2x - 3\sin 3x$.

   (1) Vérifier que $\{\sin x, \sin 2x, \sin 3x\}$ est une base de F.
   (2) Montrer que $\{f_1,\ f_2,\ f_3\}$ est également une base de F.
   (3) Donner la matrice de passage de $\{f_1, f_2, f_3\}$ à $\{\sin x, \sin 2x, \sin 3x\}$.
   (4) Trouver les coordonnées de $f = 3\sin x - \sin 2x + 4\sin 3x$ dans la base $\{f_1, f_2, f_3\}$.

31. Trouver une base du sous-espace de l'espace vectoriel réel $\mathbb{R}^4$ engendré par les vecteurs $(1, 1, 1, 2)$, $(2, 1, 0, 1)$, $(3, 1, 1, 2)$, et $(3, 2, 1, 3)$.

32. Donner une base du sous-espace de l'espace vectoriel réel $\mathbb{R}_5[x]$ engendré par les polynômes $1+x-x^2+x^4$, $x+x^2+x^3-x^4$,$1+2x+x^3$,$x+x^2+x^3+x^4$, et $1+3x+x^2+2x^3+x^4$.

33. Donner une base du sous-espace F de l'espace vectoriel réel $\mathbb{R}^4$ suivant:

$$F = \{(a+b, a-b, a-c, b-c) \mid a, b, c \in \mathbb{R}\}.$$

34. Donner une base du sous-espace F de l'espace vectoriel réel $M_2(\mathbb{R})$ suivant:

$$F = \left\{ \begin{pmatrix} a+2b+c & a+3b+2c \\ a+b & a+2b+c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}.$$

35. Soient $\mathcal{U}$ et $\mathcal{V}$ deux familles ordonnées finies de vecteurs d'un espace vectoriel E. Si $\mathcal{U}$ se réduit à $\mathcal{V}$ par une suite finie d'opérations élémentaires, montrer que $\mathcal{U}$ est libre si, et seulement si, $\mathcal{V}$ l'est.

36. Trouver une base de l'espace-solution du système homogène suivant:

$$\begin{array}{rcrcrcrcl} 3x_1 & + & 3x_2 & + & 5x_3 & & & = & 0 \\ x_1 & + & x_2 & + & 3x_3 & + & 2x_4 & = & 0 \\ 2x_1 & + & 2x_2 & + & 4x_3 & + & x_4 & = & 0 \\ 5x_1 & + & 5x_2 & + & 9x_3 & + & x_4 & = & 0. \end{array}$$

37. Dans chacun des cas suivants, montrer que $1 \le \dim \mathcal{N}(A) \le 2$ et trouver les valeurs de a pour que $\dim \mathcal{N}(A) = 1$.

$$(1) \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 3 & 2 & 4 \\ 3 & 4 & 3 & a \end{pmatrix}. \qquad\qquad (2) \quad \begin{pmatrix} 1 & 0 & -1 & 0 \\ 2 & 1 & 1 & 1 \\ 3 & 1 & 0 & a \end{pmatrix}.$$

38. Soit $AX = B$ un système d'équations linéaires dont u_0 est une solution. Montrer que l'ensemble des solutions de ce système est donné par

$$\mathcal{S} = \{u_0 + u \mid u \in \mathcal{N}(A)\}.$$

39. Considérer la matrice réelle suivante:

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

Donner une base pour chacun de $\mathcal{C}(A)$, $\mathcal{L}(A)$ et $\mathcal{N}(A)$.

40. Montrer que $A \in M_n(K)$ est inversible si et seulement si $\operatorname{rg}(AB) = \operatorname{rg}(B)$ pour toute matrice B de n lignes.

41. Soient $A \in M_{m\times n}(K)$ et $B \in M_{n\times p}(K)$. Si $AB = 0$, montrer que $\operatorname{rg}(A) + \operatorname{rg}(B) \le n$.
Indice: Vérifier que $\mathcal{C}(B)$ est un sous-espace vectoriel de $\mathcal{N}(A)$.

42. Soit $A \in M_{m\times n}(K)$. Montrer que
   (1) Si $m > n$, alors les lignes de A sont linéairement dépendantes.
   (2) Si $m < n$, alors les colonnes de A sont linéairement dépendantes.
   (3) Si AA^T est inversible, alors $\mathrm{rg}(A) = m$.

43. Soient A, B des matrices sur K. Si $B = PAQ$ avec P, Q inversibles, montrer que $\mathrm{rg}(B) = \mathrm{rg}(A)$. *Indice*: Utiliser la proposition 4.7.10.

44. Soient $A \in M_{m\times n}(K)$ et $B \in M_{m\times p}(K)$. Montrer qu'il existe $C \in M_{n\times p}(K)$ telle que $AC = B$ si et seulement si $\mathrm{rg}(A) = \mathrm{rg}(A|B)$.

45. Considérer deux sous-espaces de l'espace vectoriel réel $\mathbb{R}_4[x]$ suivants:
$$< 1 + x^3, x - x^2, 2 - x + x^2 + 2x^3 >$$
et
$$< 1 - x + x^2 + x^3, x^2 - x^3, 1 - x + 2x^3 > .$$
Trouver une base de leur somme, et calculer leur intersection.

46. Si F et G sont des sous-espaces d'un espace vecotirel E, montrer que $< F \cup G >= F + G$.

47. Considérer les matrices réelles suivantes:
$$A = \begin{pmatrix} 1 & 2 & 0 \\ -1 & 0 & -2 \\ 2 & -1 & 5 \\ 1 & 0 & -1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 4 & 3 \\ -1 & -2 & -1 \\ 2 & 0 & 2 \\ 1 & 1 & -1 \end{pmatrix}$$
Trouver une base pour chacun de $\mathcal{C}(A) \cap \mathcal{C}(B)$ et $\mathcal{C}(A) + \mathcal{C}(B)$, et déterminer si la somme est directe ou non.

48. Considérer les systèmes homogènes réels suivants:
$$\begin{array}{rcrcrcl} x & + & y & - & z & = & 0 \\ x & - & 3y & + & z & = & 0 \\ x & - & y & & & = & 0 \end{array} \qquad \text{et} \qquad \begin{array}{rcrcrcl} x & - & y & + & z & = & 0 \\ 3x & - & 3y & + & 3z & = & 0 \\ 5x & - & 5y & + & 5z & = & 0. \end{array}$$
Trouver une base pour l'intersection ainsi que la somme de leur espaces-solutions, et déterminer si la somme est directe ou non.

49. Soit E un K-espace vectoriel ayant pour sous-espaces F_1, F_2 et F_3.
   (1) Montrer que $F_1 \cap F_2 + F_1 \cap F_3 \subseteq F_1 \cap (F_2 + F_3)$.

(2) A-t-on l'inclusion contraire?

50. Soient A et B deux matrices de type $m \times n$ sur K. Si le rang de A ainsi que celui de B est inférieur à $\frac{n}{2}$, montrer qu'il existe une matrice non nulle C de type $n \times 1$ sur K telle que $AC = BC = 0$. *Indice*: Utiliser la formule de Grassmann.

51. Soient $S_n(K)$ et $T_n(K)$ les sous-espace vectoriels de $M_n(K)$ des matrices symétriques et des matrices triangulaires supérieures.
    (1) Trouver la dimension de chacun de $S_n(K)$, $T_n(K)$, et $S_n(K) \cap T_n(K)$.
    (2) Vérifier que $M_n(K) = S_n(K) + T_n(K)$.
    (3) Déterminer si la somme $M_n(K) = S_n(K) + T_n(K)$ est directe ou non.

52. Considérer les matrices réelles suivantes:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 2 \\ 2 & 1 & 3 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 3 & 3 & 1 & 2 \\ 4 & 4 & 2 & 2 \end{pmatrix}.$$

Vérifier que la somme $\mathcal{L}(A) + \mathcal{L}(B)$ est directe.

53. Considérer l'espace vectoriel réel $\mathbb{R}^3$. Montrer que $\mathbb{R}^3 = F_1 \oplus F_2 \oplus F_3$, où

$$F_1 = \{(x, x, 0) \mid x \in \mathbb{R}\}, \; F_2 = \{(x, 0, x) \mid x \in \mathbb{R}\}, \; F_3 = \{(0, x, x) \mid x \in \mathbb{R}\}.$$

54. Considérer l'espace vectoriel complex $M_n(\mathbb{C})$, avec $n \geq 1$, des matrices carrées complexes d'ordre n. Montrer que $M_n(\mathbb{R}) = S_n(\mathbb{R}) \oplus A_n(\mathbb{R})$, où $S_n(\mathbb{C})$ est le sous-espace vectoriel des matrices symétriques, et $A_n(\mathbb{C})$ est le sous-espace vectoriel des matrices antisymétriques.

55. Soit $M_2(\mathbb{R})$ l'espace vectoriel réel des matrices carrées réelles d'ordre 2. Soient

$$F = \left\{ \begin{pmatrix} a & 2a+b \\ -b & -a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \text{ et } G = \left\{ \begin{pmatrix} a & 3a+b \\ -b & b-2a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

Vérifier que F et G sont des sous-espaces de $M_2(\mathbb{R})$ tels que $M_2(\mathbb{R}) = F \oplus G$.

56. Conisdérer l'espace vectoriel réel $\mathbb{R}_5[x]$. Soit F le sous-espace vectoriel de $\mathbb{R}_5[x]$ engendré par les vecteurs $f_1 = 1 + x - x^2 - x^3 + x^4$, $f_2 = 2 - x + x^2 + 3x^4$, $f_3 = x + x^2 - x^3$, $f_4 = 3 + 2x + 2x^2 - 2x^3 + 4x^4$, et $f_5 = 5 + x + 3x^2 - 2x^3 + 7x^4$. Trouver un complément de F dans $\mathbb{R}_5[x]$.

57. Soit E un K-espace vectoriel, et soit $E_1 \oplus \cdots \oplus E_r$ une somme directe de sous-espaces de E. Soit $\mathcal{F}_i$ une famille de vecteurs de E_i, $i = 1, \ldots, r$. Montrer que $\mathcal{F}_1 \cup \cdots \cup \mathcal{F}_r$ est libre si, et seulement si, $\mathcal{F}_i$ est libre pour tout $1 \leq i \leq r$.

Chapitre V: Applications linéaires d'espaces vectoriels

On a étudié des propriétés élémentaires d'espaces vectoriels. Dans la plupart de cas, on doit étudier la relation entre deux espaces vectoriels sur un même corps. Ceci sera donnée par les applications linéaires d'un espace vectoriel dans un autre, qui conservent la structure d'espace vectoriel.

Partout dans ce chapitre, on se fixe K un corps, et E, F des espaces vectoriels sur K.

5.1. Applications linéaires

Tout d'abord, on rappelle la notion d'application d'ensembles. Soient X et Y deux ensembles. Une *application* T de X dans Y est une règle qui associe à chaque élément $x \in X$ un élément unique $y \in Y$, où y s'appelle l'*image* de x par T noté $y = T(x)$; et x, un *antécédent* de y. Une telle application est notée $T : X \to Y : x \mapsto T(x)$.

Soit $T : X \to Y$ une application. On appelle l'*image* de X par T l'ensemble

$$\operatorname{Im}(T) = \{y \in Y \mid y = T(x) \text{ pour un certain } x \in X\}.$$

On dit que T est *injective* si tout $y \in Y$ admet au plus un antécédent; *surjective* si $\operatorname{Im}(T) = Y$; et *bijective* si T est à la fois injective et surjective. Par exemple, l'*application identité* $\mathbb{1}_X : X \to X : x \mapsto x$ est bijective. Si T est bijective, alors tout $y \in Y$ a exactement un antécédent noté $T^{-1}(y)$. Dans ce cas,

$$T^{-1} : Y \to X : y \mapsto T^{-1}(y)$$

est une application bijective appelée l'*inverse* de T. On dit que deux applications T_1 et T_2 de X dans Y sont *égales* si $T_1(x) = T_2(x)$ pour tout $x \in X$. Si $S : Y \to Z$ est une autre application, alors $ST : X \to Z : x \mapsto S(T(x))$ est une application de X dans Z, appelée le *composé* de T et S. La composition d'applications est associative. On voit aisément que $\mathbb{1}_Y T = T \mathbb{1}_X = T$ et $T^{-1}T = \mathbb{1}_X$ et $TT^{-1} = \mathbb{1}_Y$ lorsque $T : X \to Y$ est bijective.

Dès maintenant, on étudiera les applications entre des espaces vectoriels qui sont compatibles avec la structure d'espace vectoriel.

5.1.1. Définition. Soient E, F des K-espaces vectoriels. Une application $T : E \to F$ est dite *linéaire* si, pour tous $u, v \in E$, on a

(1) $T(\alpha u) = \alpha T(u)$,
(2) $T(u+v) = T(u) + T(v)$.

Remarque. Si $T : E \to F$ est linéaire, alors $T(0_E) = 0_F$.

Exemple. (1) L'application nulle $\mathbf{0} : E \to F : u \mapsto 0_F$ et l'application identitée $\mathbb{1}_E : E \to E : u \mapsto u$ sont linéaires.

(2) Soit $D^\infty[a,b]$ l'espace vectoriel réel des fonctions infiniment différentiables définies sur l'intervalle $[a,b]$. L'opérateur différentiel suivant est linéaire:

$$\partial : D^\infty[a,b] \to D^\infty[a,b] : f(t) \mapsto \frac{df(t)}{dt}.$$

(3) L'application suivante est linéaire :

$$T : M_{m\times n}(K) \to M_{n\times m}(K) : A \mapsto A^T.$$

(4) L'application suivante n'est pas linéaire :

$$\sin x : \ \mathbb{R} \to \mathbb{R} : t \mapsto \sin t.$$

(5) Considérons le $\mathbb{R}$-espace $E = \mathbb{R}^2$ et le $\mathbb{C}$-espace $F = \mathbb{C}^2$. L'application

$$T : \mathbb{R}^2 \to \mathbb{C}^2 : (a,b) \mapsto (a,b)$$

n'est pas linéaire parce que E et F ne sont pas d'espaces vectoriels sur le même corps.

5.1.2. Proposition. Une application $T : E \to F$ est linéaire si, et seulement si,

$$T(\alpha u + \beta v) = \alpha T(u) + \beta T(v),$$

pour tous $u, v \in E$, et $\alpha, \beta \in K$.

Démonstration. Supposons que T est linéaire. Pour tous $u, v \in E, \alpha, \beta \in K$, on a

$$T(\alpha u + \beta v) = T(\alpha u) + T(\beta v) = \alpha T(u) + \beta T(v).$$

Réciproquement supposons que T satisfait à la condition. Alors

$$T(u+v) = T(1\cdot u) + T(1\cdot v) = 1\cdot T(u) + 1\cdot T(v)$$

et

$$T(\alpha u) = T(\alpha u + 0\cdot 0_E) = \alpha T(u) + 0\cdot T(0_E) = \alpha T(u).$$

Ainsi T est linéaire. Ce qui achève la démonstration.

Exemple. Soit $A \in M_{m\times n}(K)$. Alors les applications suivantes sont linéaires :

$$T_A : K^{(n)} \to K^{(m)} : v \mapsto Av \quad \text{et} \quad S_A : K^m \to K^n : u \mapsto uA.$$

En effet, pour tous $u, v \in K^m$ et $\alpha, \beta \in K$, on a

$$(\alpha u + \beta v)A = \alpha(uA) + \beta(vA).$$

On déduit par récurrence le résultat suivant de la proposition 5.1.2.

5.1.3. Corollaire. Si $T : E \to F$ est linéaire, alors

$$T(\alpha_1 u_1 + \cdots + \alpha_n u_n) = \alpha_1 T(u_1) + \cdots + \alpha_n T(u_n)$$

pour tous $u_i \in E$ et $\alpha_i \in K,\ i = 1, \ldots, n.$

5.1.4. Proposition. Si E a une base finie $\{u_1, \cdots, u_n\}$ alors, pour tous $v_1, \ldots, v_n \in F$, il existe une et une seule application linéaire $T : E \to F$ telle que $T(u_i) = v_i, i = 1, \ldots, n.$

Démonstration. Tout $u \in E$ s'écrit uniquement $u = \alpha_1 u_1 + \cdots + \alpha_n u_n,\ \alpha_i \in K$. Définissons une application $T : E \to F$ par $T(\alpha_1 u_1 + \cdots + \alpha_n u_n) = \alpha_1 v_1 + \cdots + \alpha_n v_n$. Alors T est linéaire telle que $T(u_i) = T(1 \cdot u_i) = 1 \cdot v_i = v_i, i = 1, \ldots, n$. En outre, supposons que $S : E \to F$ est linéaire telle que $S(u_i) = v_i,\ i = 1, \cdots, n$. Alors, pour tout $u = \sum_{i=1}^n \alpha_i u_i \in E$, on a $S(u) = \sum_{i=1}^n \alpha_i S(u_i) = \sum_{i=1}^n \alpha_i T(u_i) = T(u)$. D'où, $S = T$. Ceci achève la démonstration.

Exemple. (1) Considérons la base canonique $\{e_1, e_2\}$ de $\mathbb{R}^2$ et les vecteurs

$$f_1 = 1 + 2x + 3x^2, f_2 = 2 + 4x + 6x^2$$

de $\mathbb{R}_3[x]$. Alors l'application linéaire $T : \mathbb{R}^2 \to \mathbb{R}_3[x]$ telle que $T(e_i) = f_i, i = 1, 2$ est définie par $T((a, b)) = af_1 + bf_2 = (a + 2b) + (2a + 4b)x + (3a + 6b)x^2$, pour tout $(a, b) \in \mathbb{R}^2$.

(2) Considérons les espaces vectoriels $\mathbb{R}_3[x]$ et ${}_{\mathbb{R}}\mathbb{C}$. Trouver une application linéaire $T : \mathbb{R}_3[x] \to {}_{\mathbb{R}}\mathbb{C}$ telle que $T(1 + x^2) = T(-1 + x) = 1 + i$ et $T(x - x^2) = 1 - i$.

Solution. D'abord, les polynômes $f_1 = 1 + x^2, f_2 = -1 + x, f_3 = x - x^2$ forment une base de $\mathbb{R}_3[x]$. La matrice de passage de la base canonique $\{1, x, x^2\}$ à la base $\{f_1, f_2, f_3\}$ est

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

Soit $a+bx+cx^2$ un polynôme quelconque. Comme sa colonne dans $\{1,x,x^2\}$ est $(a,b,c)^T$, sa colonne dans $\{f_1,f_2,f_3\}$ est

$$P^{-1}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \frac{1}{2}\begin{pmatrix} a-b+c \\ a+b+c \\ a+b-c \end{pmatrix}.$$

Ceci implique que

$$a+bx+cx^2 = \frac{a-b+c}{2}f_1 + \frac{a+b+c}{2}f_2 + \frac{a+b-c}{2}f_3.$$

Ainsi l'application linéaire cherchée est définie par

$$\begin{array}{rcl} T(a+bx+cx^2) & = & \frac{a-b+c}{2}\,T(f_1) + \frac{a+b+c}{2}\,T(f_2) + \frac{a+b-c}{2}\,T(f_3) \\ & = & \frac{a-b+c}{2}\,(1+i) + \frac{a+b+c}{2}\,(1+i) + \frac{a+b-c}{2}\,(1-i) \\ & = & \frac{3a+b+c}{2} + \frac{a-b+3c}{2} i. \end{array}$$

On désignera par $\mathcal{L}(E,F)$ l'ensemble des applications linéaires de E dans F. On montrera que $\mathcal{L}(E,F)$ est un K-espace vectoriel.

5.1.5. Proposition. Soient $T,S \in \mathcal{L}(E,F)$ et $\alpha \in K$. Alors les applications

$$\alpha T : E \to F : u \mapsto \alpha T(u) \quad \text{et} \quad T+S : E \to F : u \mapsto T(u)+S(u)$$

sont linéaires.

Démonstration. Pour tous $u,v \in E, \beta,\gamma \in K$,

$$\begin{array}{rcl} (\alpha T)(\beta u+\gamma v) & = & \alpha T(\beta u+\gamma v) = \alpha[\beta T(u)+\gamma T(v)] \\ & = & \beta\alpha T(u)+\gamma\alpha T(v) = \beta(\alpha T)(u)+\gamma(\alpha T)(u) \\ (T+S)(\beta u+\gamma v) & = & T(\beta u+\gamma v)+S(\beta u+\gamma v) \\ & = & \beta T(u)+\gamma T(v)+\beta S(u)+\gamma S(v) \\ & = & \beta[T(u)+S(u)]+\gamma[T(v)+S(v)] \\ & = & \beta(T+S)(u)+\gamma(T+S)(v). \end{array}$$

Donc αT et $T+S$ sont linéaires. Ceci achève la démonstration.

Exemple. Considérons les applications T et S de $\mathbb{R}^2$ dans $\mathbb{R}^3$ définies par

$$T(x,y) = (x-y, x+y, y) \quad \text{et} \quad S(x,y) = (2x+y, x+3y, 0).$$

Alors $4T+5S$ est une application linéaire de $\mathbb{R}^2$ dans $\mathbb{R}^3$ telle que

$$(4T+5S)(x,y) = (4T)(x,y)+(5S)(x,y) = 4T(x,y)+5S(x,y) = (14x+y, 9x+19y, 4y).$$

5.1.6. Lemme. Soient $T, S, T' \in \mathcal{L}(E, F)$ et $\alpha, \beta \in K$. Alors

(1) $T + S = S + T$;	(2) $(T + S) + T' = T + (S + T')$;
(3) $1_K T = T$;	(4) $\alpha(\beta T) = (\alpha\beta)T$;
(5) $\alpha(T + S) = \alpha T + \alpha S$;	(6) $(\alpha + \beta)T = \alpha T + \beta T$.

Démonstration. La démonstration est une vérification de routine. À titre d'exemple, on montrera (5). Pour tout $u \in E$,

$$\begin{aligned} (\alpha(T + S))\,(u) &= \alpha\left((T + S)(u)\right) \\ &= \alpha(T(u) + S(u)) = \alpha T(u) + \alpha S(u) \\ &= (\alpha T)(u) + (\alpha S)(u) \\ &= (\alpha T + \alpha S)(u). \end{aligned}$$

Ainsi $\alpha(T + S) = \alpha T + \alpha S$. Ceci achève la démonstration.

5.1.7. Théorème. Muni des opérations définies dans la Proposition 5.1.5, $\mathcal{L}(E, F)$ est un K-espace vectoriel.

Démonstration. D'abord $0 : E \to F : u \mapsto 0_F$ est linéaire. Ainsi $\mathcal{L}(E, F)$ est non vide. Pour tout $T \in \mathcal{L}(E, F)$, l'application $-T : E \to F : u \mapsto -T(u)$ est linéaire telle que $T + (-T) = 0$. Il suit du lemme 5.1.6 que les autres axiomes de K-espace vectoriel sont aussi satisfaits. Ceci achève la démonstration.

5.1.8. Proposition. Soient $T : E \to F$ et $S : F \to G$ des applications linéaires de K-espaces vectoriels. Alors ST est linéaire. En outre,

(1) Pour tout $T' \in \mathcal{L}(E, F)$, $S(T + T') = ST + ST'$.

(2) Pour tout $S' \in \mathcal{L}(F, G)$, $(S + S')T = ST + S'T$.

Démonstration. Pour tous $u, v \in E, \alpha, \beta \in K$,

$$\begin{aligned} (ST)(\alpha u + \beta v) &= S[T(\alpha u + \beta v)] = S[\alpha T(u) + \beta T(v)] \\ &= \alpha S(T(u)) + \beta S(T(v)) = \alpha(ST)(u) + \beta(ST)(v). \end{aligned}$$

Donc ST est linéaire. En outre pour tout $u \in E$,

$$\begin{aligned} (S(T + T'))\,(u) &= S\left((T + T')(u)\right) \\ &= S\left(T(u) + T'(u)\right) \\ &= S(T(u)) + S(T'(u)) \\ &= (ST)(u) + (ST')(u). \end{aligned}$$

Ainsi $S(T+T') = ST+ST'$. De même, $(S+S')T = ST+S'T$. Ceci achève la dḿonstration.

Exemple. Considérons les applications linéaires

$$T : \mathbb{R} \to \mathbb{R}^2 : x \mapsto (x, x) \quad \text{et} \quad S : \mathbb{R}^2 \to \mathbb{R}^3 : (x, y) \mapsto (x + y, x - y, 0).$$

Alors $ST :\ \mathbb{R} \to \mathbb{R}^3 : x \mapsto (2x, 0, 0)$.

5.2. Isomorphismes

Le but de cette section est d'étudier premièrement plus de propriétés d'une application linéaire d'espaces vectoriels, et de trouver ensuite quand deux espaces vectoriels sont éssentiellement identiques. On commence par deux sous-espaces vectoriels associés à une application linéaire $T : E \to F$. Si $\mathcal{U}$ est une famille de vecteurs de E, on note $T(\mathcal{U}) = \{T(u) \mid u \in \mathcal{U}\}$, une famille de vecteurs de F.

5.2.1. Proposition. Soit $T \in (E, F)$.
(1) $\mathrm{Im}(T) = \{v \in F \,|\, v = F(u)$ pour un certain $u \in E\}$ est un sous-espace de F.
(2) $\mathrm{Ker}(T) = \{u \in E \,|\, T(u) = 0_F\}$ est un sous-espace de E, appelé *noyau* de T.

Démonstration. (1) Soient $v_1, v_2 \in \mathrm{Im}\,(T)$ et $\alpha_1, \alpha_2 \in K$. Alors $v_i = T(u_i)$ avec $u_i \in E,\ i = 1, 2$. Ainsi $\alpha_1 v_1 + \alpha_2 v_2 = T(\alpha_1 u_1 + \alpha_2 u_2) \in \mathrm{Im}\,(T)$. Donc $\mathrm{Im}(T)$ est un sous-espace de F.

(2) Soient $u, v \in \mathrm{Ker}\,(T)$ et $\alpha, \beta \in K$. Alors $T(u) = T(v) = 0_F$. Or $T(\alpha u + \beta v) = \alpha T(u) + \beta T(v) = 0_F$. Ainsi $\alpha u + \beta v \in \mathrm{Ker}\,(T)$. Ce qui implique que $\mathrm{Ker}(T)$ est un sous-espace de E. Ceci achève la dḿonstration.

Exemple. (1) Considérons la projection du plan sur l'axe des x

$$p : \mathbb{R}^2 \to \mathbb{R}^2 : (x, y) \mapsto (x, 0).$$

Alors $\mathrm{Ker}(p) = \{(0, y) \mid y \in \mathbb{R}\}$, l'axe des y; et $\mathrm{Im}(p) = \{(x, 0) \mid x \in \mathbb{R}\}$, l'axe des x.

(2) Soit $D^\infty[a, b]$ l'espace vectoriel réel des fonctions infiniment différentiables définies sur l'intervalle $[a, b]$. Considérons

$$\partial : D^\infty[a, b] \to D^\infty[a, b] : f(t) \mapsto \frac{df(t)}{dt}.$$

Alors $\mathrm{Ker}(\partial) = \{f(t) = c \mid c \in \mathbb{R}\}$ et $\mathrm{Im}(\partial) = D^\infty[a, b]$. En effet, $\partial(f(t)) = 0$ si et seulement si $f(t)$ est une fonction constante. Et si $f \in D^\infty[a, b]$, alors $g(t) = \int_a^t f(x)dx \in D^\infty[a, b]$ est telle que $\partial(g) = f$.

(3) Considérons l'application linéaire $T : K^{(n)} \to K^{(m)} : u \mapsto Au$, où $A \in M_{m\times n}(K)$. Pour tout $u \in K^{(n)}$, on a $u \in \mathrm{Ker}(T)$ si et seulement si $Au = 0$ si et seulement si $u \in \mathcal{N}(A)$. D'où $\mathrm{Ker}(T) = \mathcal{N}(A)$. Plus précisément, considérons l'application suivante:

$$T : \mathbb{R}^{(3)} \to \mathbb{R}^{(3)} : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 3x_1 - 3x_2 + 3x_3 \\ 3x_1 - 3x_2 + 3x_3 \\ 6x_1 - 6x_3 + 6x_4 \end{pmatrix}.$$

On voit aisément que pour tout $u \in \mathbb{R}^{(3)}$, $T(u) = Au$ avec

$$A = \begin{pmatrix} 3 & -3 & 3 \\ 3 & -3 & 3 \\ 6 & -6 & 6 \end{pmatrix}.$$

Or $\mathrm{Ker}(T)$ est l'espace-solution du système $AX = 0$. Remarquons que A se réduit à la matrice échelonnée suivante:

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

Donc $\mathrm{Ker}(T)$ est de dimension 2 et on trouve une base comme suit:

$$\left\{(1,1,0)^T,\ (-1,0,1)^T\right\}.$$

On étudiera comment déterminer l'image d'une application linéaire.

5.2.2. Proposition. Soit $E =< \mathcal{U} >$, où $\mathcal{U}$ est une famille de vecteurs de E. Si $T \in \mathcal{L}(E,F)$, alors $\mathrm{Im}(T) =< T(\mathcal{U}) >$. Par conséquent, T est surjective si, et seulement si, $F =< T(\mathcal{U}) >$.

Démonstration. Comme $T(\mathcal{U}) \subseteq \mathrm{Im}(T)$, on a $< T(\mathcal{U}) >\subseteq \mathrm{Im}(T)$. D'autre part, si $v \in \mathrm{Im}(T)$, alors $v = T(w)$ avec $w \in E$. Or w s'écrit $w = \alpha_1 u_1 + \cdots + \alpha_n u_n,\ u_i \in \mathcal{U},\ \alpha_i \in K$. Donc $v = T(w) = \alpha_1 T(u_1) + \cdots + \alpha_n T(u_n) \in< T(\mathcal{U}) >$. Ce qui montre $\mathrm{Im}(T) \subseteq< T(\mathcal{U}) >$. Ainsi $\mathrm{Im}(T) =< T(\mathcal{U}) >$. Ceci achève la démonstration.

Exemple. Soit $A \in M_{m\times n}(K)$. Considérons l'application linéaire

$$T : K^{(n)} \to K^{(m)} : u \mapsto Au.$$

Soit $\{e_1, \cdots, e_n\}$ la base canonique de $K^{(n)}$. Pour tout $1 \le j \le n$, on voit que $T(e_j) = Ae_j$ est la j-ième colonne de A. Comme $K^{(n)} =< e_1, \cdots, e_n >$, d'après la proposition 5.2.2, on a

$$\mathrm{Im}(T) =< T(e_1), \cdots, T(e_n) >= \mathcal{C}(A).$$

Plus précisément, considérons l'application linéaire:

$$T : \mathbb{R}^{(3)} \to \mathbb{R}^{(3)} : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 3x_1 - 3x_2 + 3x_3 \\ 3x_1 - 3x_2 + 3x_3 \\ 6x_1 - 6x_2 + 6x_3 \end{pmatrix}.$$

On a

$$\mathrm{Im}(T) =< T(e_1),\ T(e_2),\ T(e_3) >=< (3,3,6)^T, (-3,-3,-6)^T, (3,3,6)^T >=< (3,3,6)^T > .$$

En particulier $\mathrm{Im}(T)$ est dimension 1. Ainsi $\mathrm{Im}(T) \neq \mathbb{R}^{(3)}$, et donc T n'est pas surjective.

Le résultat suivant dit que l'image d'une famille liée par une application linéaire est toujours liée.

5.2.3. Lemme. Soit $T \in \mathcal{L}(E, F)$, et soit $\mathcal{U}$ une famille de vecteurs de E.
(1) Si $T(\mathcal{U})$ est libre, alors $\mathcal{U}$ est libre.
(2) Si T est injective, alors $\mathcal{U}$ est libre si et seulement si $T(\mathcal{U})$ est libre.

Démonstration. (1) Supposons que $T(\mathcal{U})$ est libre. Si $\alpha_1 u_1 + \cdots + \alpha_n u_n = 0_E,\ u_i \in \mathcal{U}, \alpha_i \in K$, alors $\alpha_1 T(u_1) + \cdots + \alpha_n T(u_n) = 0_F$. Comme $\{T(u_1), \ldots, T(u_n)\}$ est libre, $\alpha_1 = \cdots = \alpha_n = 0$. Donc $\mathcal{U}$ est libre.

(2) Supposons que T est injective et $\mathcal{U}$ est libre. Si $\alpha_1 T(u_1) + \cdots + \alpha_n T(u_n) = 0_F, \alpha_i \in K, u_i \in \mathcal{U}$, alors $T(\alpha_1 u_1 + \cdots + \alpha_n u_n) = T(0_E)$. D'où, $\alpha_1 u_1 + \cdots + \alpha_n u_n = 0_E$, puisque T est injective. Ainsi $\alpha_1 = \cdots = \alpha_n = 0$, car $\{u_1, \ldots, u_n\}$ est libre. Ceci montre que $T(\mathcal{U})$ est libre. Le preuve du lemme s'achève.

Exemple. Considérons $u_1 = (a_1, a_2, 1, 0),\ u_2 = (b_1, b_2, 0, 1) \in \mathbb{R}^4$. Alors $\{u_1, u_2\}$ est libre pour tous $a_1, a_2, b_1, b_2 \in \mathbb{R}$. En effet,

$$T : \mathbb{R}^4 \to \mathbb{R}^2 : (x_1, x_2, x_3, x_4) \mapsto (x_3, x_4)$$

est une application linéaire telle que $T(u_1) = (1, 0)$ et $T(u_2) = (0, 1)$. Comme $\{(1, 0), (0, 1)\}$ est libre, d'après le lemme 5.2.3(1), $\{u_1, u_2\}$ est libre.

On donne maintenant un critère pour qu'une application linéaire soit injective.

5.2.4. Proposition. Soient $T \in \mathcal{L}(E, F)$ et $\mathcal{B}$ une base de E. Alors les conditions suivantes sont équivalentes:
(1) T est injective.

(2) $\operatorname{Ker}(T) = 0$.

(3) La famille $T(\mathcal{B})$ est libre.

Démonstration. Supposons que T est injective. Si $u \in \operatorname{Ker}(T)$, alors $T(u) = 0_F = T(0_E)$. Ainsi $u = 0_E$ d'après l'injectivité de T. Par conséquent, $\operatorname{Ker}(T) = 0$.

Supposons que $\operatorname{Ker}(T) = 0$. Soient $v_1, \ldots, v_r \in T(\mathcal{B})$, c'est-à-dire, $v_i = T(u_i)$ avec $u_i \in \mathcal{B}$, $i = 1, \ldots, r$. Si $\alpha_1 v_1 + \cdots + \alpha_r v_r = 0_F$, $\alpha_i \in K$, alors $T(\alpha_1 u_1 + \cdots + \alpha_r u_r) = 0_F$, c'est-à-dire, $\alpha_1 u_1 + \cdots + \alpha_r u_r \in \operatorname{Ker}(T)$. Comme $\operatorname{Ker}(T) = \{0_E\}$ par l'hypothèse, $\alpha_1 u_1 + \cdots + \alpha_r u_r = 0_E$. Comme $\mathcal{B}$ est libre, $\alpha_i = 0$, $i = 1, \ldots, r$. Ceci montre que $T(\mathcal{B})$ est libre.

Supposons enfin que $T(\mathcal{B})$ est libre. Soient $u, v \in E$ tels que $T(u) = T(v)$. Écrivons $u = \sum_{i=1}^n \alpha_i u_i, v = \sum_{i=1}^n \beta_i u_i,\ \alpha_i, \beta_i \in K, u_i \in \mathcal{B}$. Alors

$$\sum_{i=1}^n (\alpha_i - \beta_i) T(u_i) = \sum_{i=1}^n \alpha_i T(u_i) - \sum_{i=1}^n \beta_i T(u_i) = T(u) - T(v) = 0_F.$$

Comme $\{T(u_1), \ldots, T(u_n)\}$ est libre, on a $\alpha_i - \beta_i = 0$, $i = 1, \ldots, n$. Ainsi $u = v$. Ceci montre que T est injective. Ceci achève la démonstration.

Remarque. Il suit de la proposition 5.2.4 que $\dim(E) \leq \dim(F)$ lorsqu'il existe une application linéaire injective $T : E \to F$.

Exemple. L'application linéaire suivante

$$T : \mathbb{R}^{(3)} \to \mathbb{R}^{(3)} : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 3x_1 - 3x_2 + 3x_3 \\ 3x_1 - 3x_2 + 3x_3 \\ 6x_1 - 6x_3 + 6x_4 \end{pmatrix}$$

n'est pas injective car $\operatorname{Ker}(T)$ est non nul.

5.2.5. Définition. On dit que $T \in \mathcal{L}(E, F)$ est un *isomorphisme* si T est bijective.

Exemple. (1) L'application identitée $\mathbb{1} : E \to E : u \mapsto u$ est un isomorphisme.

(2) Si E ou F est non nul, alors l'application nulle de E dans F n'est pas un isomorphisme.

(3) L'application $T : M_{m\times n}(K) \to M_{n\times m}(K) : A \mapsto A^T$ est un isomorphisme. En particulier, l'application linéaire suivante est un isomorphisme :

$$S : K^n \to K^{(n)} : (a_1, \ldots, a_n) \mapsto \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

5.2.6. Proposition. Une application linéaire $T : E \to F$ est un isomorphisme si et seulement s'il existe une application linéaire $S : F \to E$ telle que $ST = \mathbb{1}_E$ et $TS = \mathbb{1}_F$. Dans ce cas, $S = T^{-1}$ est également un isomorphisme.

Démonstration. Supposons que T est un isomorphisme. Alors T est bijective. Ainsi $T^{-1} : F \to E$ est une application telle que $T^{-1}T = \mathbb{1}_E$ et $TT^{-1} = \mathbb{1}_F$. Il reste de montrer que T^{-1} est linéaire. Soient $v_1, v_2 \in F$ et $\alpha_1, \alpha_2 \in K$. Posons $u_i = T^{-1}(v_i) \in E$, $i = 1, 2$. D'après la définition, $T(u_i) = v_i, i = 1, 2$. Or

$$T(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1 T(u_1) + \alpha_2 T(u_2) = \alpha_1 v_1 + \alpha_2 v_2.$$

D'après la définition de T^{-1}, on a

$$T^{-1}(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 u_1 + \alpha_2 u_2 = \alpha_1 T^{-1}(v_1) + \alpha_2 T^{-1}(v_2).$$

Ainsi T^{-1} est linéaire.

Réciproquement supposons que $S : F \to E$ est une application linéaire telle que $ST = \mathbb{1}_E$ et $TS = \mathbb{1}_F$. Pour tout $v \in F$, $S(v) \in E$ est tel que $T(S(v)) = (TS)(v) = \mathbb{1}_F(v) = v$. Ce qui montre que T est surjective. Or supposons que $T(u_1) = T(u_2)$ avec $u_i \in E$, $i = 1, 2$. Alors $S(T(u_1)) = S(T(u_2))$, c'est-à-dire, $(ST)(u_1) = (ST)(u_2)$. Donc $u_1 = u_2$ comme $ST = \mathbb{1}_E$. Ceci implique que T est injective. Par conséquent, T est un isomorphisme. Enfin $T(S(v)) = v$ pour tout $v \in F$ entraîne que $S(v) = T^{-1}(v)$ pour tout $v \in F$. Ainsi $S = T^{-1}$. Ceci achève la démonstration.

5.2.7. Corollaire. Soit $\{u_1, \ldots, u_n\}$ une base de E. Alors l'application

$$T : K^{(n)} \to E : \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \mapsto (u_1, \ldots, u_n) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

est un isomorphisme.

Démonstration. Il est évident que T est linéaire. Or pour tout $u \in E$, posons $S(u)$ la colonne de u dans $\{u_1, \ldots, u_n\}$. D'après le lemme 4.3.2(3), l'application

$$S : E \to K^{(n)} : u \mapsto S(u)$$

est linéaire. On vérifie aisément que $ST = \mathbb{1}_{K^{(n)}}$ et $TS = \mathbb{1}_E$. Ainsi T est un isomorphisme. Ceci achève la démonstration.

5.2.8. Proposition. Soit $\mathcal{B}$ une base de E. Si $T \in \mathcal{L}(E, F)$, alors T est un isomorphisme si, et seulement si, $T(\mathcal{B})$ est une base de F.

Démonstration. D'après la définition, T est un isomorphisme si, et seulement si, T est injective et surjective si, et seulement si, $T(\mathcal{B})$ est libre et $F =< T(\mathcal{B}) >$ si, et seulement si, $T(\mathcal{B})$ est une base F. Ceci achève la démonstration.

5.2.9. Corollaire. Soit $T : E \to F$ un isomorphisme. Si $\mathcal{B}$ est une famille de vecteurs de E, alots $\mathcal{U}$ est une base de E si, et seulement si, $T(\mathcal{B})$ est une base de F.

Démonstration. Si $\mathcal{B}$ est une base de E, alors $T(\mathcal{B})$ est une base de F d'après la proposition 5.2.8.

Réciproquement supposons que $T(\mathcal{B})$ est une base de F. Alors $\mathcal{B}$ est libre car $T(\mathcal{B})$ est libre. Ensuite pour tout $u \in E$, on a $T(u) = \alpha_1 T(u_1) + \cdots \alpha_n T(u_n)$ avec $u_i \in \mathcal{B},\ \alpha_i \in K$ car $F =< T(\mathcal{B}) >$. Ainsi $T(u) = T(\alpha_1 u_1 + \cdots + \alpha_n u_n)$. Ce qui donne $u = \alpha_1 u_1 + \cdots + \alpha_n u_n$ car T est injective. Par conséquent, $\mathcal{B}$ est une base de E. Ceci achève la démonstration.

On dit que E et F sont *isomorphes*, noté $E \cong F$, s'il existe un isomorphisme $T : E \to F$. Dans ce cas, on peut identifier E avec F en identifiant $u \in E$ avec $T(u) \in F$.

Exemple. On a vu que $K^{(n)} \cong K^n$, pour tout $n \geq 1$.

5.2.10. Proposition. La relation d'isomorphisme de K-espaces vectoriels est une relation d'équivalence.

Démonstration. D'abord, $E \cong E$ car $\mathbb{1}_E : E \to E$ est un isomorphisme.

Ensuite supposons que $E \cong F$. Alors il existe un isomorphisme $T : E \to F$. Ainsi $T^{-1} : F \to E$ est également un isomorphisme. Donc $F \cong E$.

Enfin supposons que $E \cong F$ et $F \cong G$. Alors il existent des isomorphismes $T : E \to F$ et $S : F \to G$. On sait que $ST : E \to G$ est une application linéaire. De plus, S^{-1} et T^{-1} sont des isomorphismes, et $(ST)(T^{-1}S^{-1}) = S(TT^{-1})S^{-1} = S\mathbb{1}_F S^{-1} = SS^{-1} = \mathbb{1}_G$. De même, $(T^{-1}S^{-1})(ST) = \mathbb{1}_E$. Ainsi $ST : E \to G$ est un isomoprhisme, et donc $E \cong G$. Ceci achève la démonstration.

Il suit du corollaire 5.2.9 que deux K-espaces vectoriels isomorphes ont même dimension. La réciproque est vraie si l'un d'eux est de dimension finie.

5.2.11. Théorème. Soient E, F deux K-espaces vectoriels. Si E est de dimension finie, alors $E \cong F$ si, et seulement si, $\dim(E) = \dim(F)$.

Démonstration. La suffisance suit immédiatement du corollaire 5.2.9. Supposons maintenant que $\dim(E) = \dim(F) = n$. Alors $E \cong K^{(n)}$ et $F \cong K^{(n)}$. Ainsi $E \cong F$. Ceci achève la démonstration.

Remarque. Le résultat ci-dessus nous dit qu'un espace vectoriel de dimension finie est déterminé, à isomorphisme près, par sa dimension. Ainsi K^n est essentiellement le seul K-espace vectoriel de dimension n.

Exemple. ${}_{\mathbb{R}}\mathbb{C} \cong \mathbb{R}^2$ et $K_n[x] \cong K^{(n)}$, pour tout $n \geq 1$.

5.3. Représentation matricielle d'applications linéaires

Cette section a pour but de représenter les applications linéaires d'espaces vectoriels de dimension finie par les matrices. Ce qui nous permet d'étudier les applications linéaires en appliquant les propriétés de matrices.

Partout dans cette section, on se fixe E et F deux K-espace vectoriels de dimension finie.

5.3.1. Définition. Soient $\{u_1, \ldots, u_n\}$ une base de E et $\{v_1, \ldots, v_m\}$ une base de F. Si $T \in \mathcal{L}(E, F)$, alors $\{T(u_1), \ldots, T(u_n)\}$ est une famille de vecteurs de F. On appelle

$$P_{\{v_1,\ldots,v_m\}}^{\{T(u_1),\ldots,T(u_n)\}}$$

la *matrice* de T dans les bases $\{u_1, \ldots, u_n\}$ et $\{v_1, \ldots, v_m\}$, notée $[T]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}}$. Remarquons que

$$(T(u_1), \ldots, T(u_n)) = (v_1, \ldots, v_m)[T]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}}.$$

Exemple. (1) $[\mathbf{0}]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}} = 0_{m\times n}$ et $[\mathbb{1}_E]_{\{u_1,\ldots,u_n\}}^{\{u_1,\ldots,u_n\}} = I_n$.

(2) Soit $T \in \mathcal{L}(\mathbb{R}^3, \mathbb{R}^2)$ définie par $T(a_1, a_2, a_3) = (a_1+2a_2-a_3, 2a_1-a_2+a_3)$. Considérons la base $\{u_1 = (0, 1, 1),\ u_2 = (1, 0, 1),\ u_3 = (1, 1, 0)\}$ de $\mathbb{R}^3$, et la base $\{v_1 = (1, 1), v_2 = (1, -1)\}$ de $\mathbb{R}^2$. Alors

$$\begin{array}{rcrcrcr} T(u_1) & = & (1,0) & = & \frac{1}{2}v_1 & + & \frac{1}{2}v_2 \\ T(u_2) & = & (0,3) & = & \frac{3}{2}v_1 & - & \frac{3}{2}v_2 \\ T(u_3) & = & (3,1) & = & 2v_1 & + & v_2 \end{array}$$

Donc la matrice de T dans ces bases est

$$[T] = \begin{pmatrix} \frac{1}{2} & \frac{3}{2} & 2 \\ \frac{1}{2} & -\frac{3}{2} & 1 \end{pmatrix}.$$

(3) Une matrice $A \in M_{m\times n}(K)$ définit deux applications linéaires

$$T_A : K^{(n)} \to K^{(m)} : v \mapsto Av; \quad S_A : K^m \to K^n : u \mapsto uA.$$

On voit que la matrice de T_A dans les bases canoniques est A, mais celle-ci de S_A est A^T.

Le résultat suivant dit qu'une application linéaire est uniquement déterminée par sa matrice.

5.3.2. Proposition. Soient $\{u_1, \ldots, u_n\}$ une base de E et $\{v_1, \ldots, v_m\}$ une base de F. Si $T, S \in \mathcal{L}(E, F)$, alors $T = S$ si, et seulement si,

$$[T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}} = [S]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}}.$$

Démonstration. Il suffit de montrer la suffisance. Si $[T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}} = [S]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}}$, alors

$$(T(u_1), \ldots, T(u_n)) = (S(u_1), \ldots, S(u_n)),$$

c'est-à-dire, $T(u_i) = S(u_i)$ $i = 1, \ldots, n$. D'après la proposition 5.1.4, $T = S$. Ceci achève la démonstration.

Le résultat suivant nous permet de déterminer si une application d'espaces vectoriels de dimension finie est linéaire ou non.

5.3.3. Proposition. Soient $\{u_1, \ldots, u_n\}$ une base de E et $\{v_1, \ldots, v_m\}$ une base de F. Une application $T : E \to F$ est linéaire si et seulement s'il existe une matrice $A = (a_{ij})_{m\times n}$ sur K telle que, pour tous $x_1, \ldots, x_n \in K$, on a

$$T(x_1u_1 + \cdots + x_nu_n) = (a_{11}x_1 + \cdots + a_{1n}x_n)v_1 + \cdots + (a_{m1}x_1 + \cdots + a_{mn}x_n)v_m.$$

C'est-à-dire, $P^{\{T(u)\}}_{\{v_1,\ldots,v_m\}} = AP^{\{u\}}_{\{u_1,\ldots,u_n\}}$, pour tout $u \in E$. Dans ce cas, $A = [T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}}$.

Démonstration. On commence par la necessité. Supposons que T est linéaire et posons $A = (a_{ij})_{m\times n} = [T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}}.$ Par définition, $(T(u_1), \ldots, T(u_n)) = (v_1, \ldots, v_m)A$, c'est-à-dire, $T(u_j) = \sum_{i=1}^m a_{ij}v_i,\ j = 1, \ldots, n$. Si $u = \sum_{j=1}^n x_ju_j \in E$, alors

$$\begin{aligned} T(u) &= \textstyle\sum_{j=1}^n x_j\, T(u_j) = \sum_{j=1}^n x_j(\sum_{i=1}^m a_{ij}v_i) \\ &= \textstyle\sum_{j=1}^n \sum_{i=1}^m a_{ij}x_jv_i = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij}x_j\right) v_i\,. \end{aligned}$$

Supposons réciproquement que T satisfait à la condition énoncée dans la proposition. Si $u = \sum_{j=1}^n x_ju_j,\ v = \sum_{i=1}^n y_ju_j \in E$ et $\alpha, \beta \in K$, alors $\alpha u + \beta v = \sum_{j=1}^n (\alpha x_j + \beta y_j)$ et donc

$$\begin{aligned} T(\alpha u + \beta v) &= \textstyle\sum_{i=1}^n \left(\sum_{j=1}^m a_{ij}(\alpha x_j + \beta y_j)\right) v_i \\ &= \textstyle\alpha \sum_{i=1}^n \left(\sum_{j=1}^m a_{ij}x_j\right) v_i + \beta \sum_{i=1}^n \left(\sum_{j=1}^m a_{ij}y_j\right) v_i \\ &= \alpha\, T(u) + \beta\, T(v)\,. \end{aligned}$$

Ainsi T est linéaire. De plus, la colonne de u_j dans $\{u_1, \ldots, u_n\}$ est $e_j \in K^{(n)}$. Ainsi la colonne de $T(u_j)$ dans $\{v_1, \ldots, v_m\}$ est Ae_j, la j-ième colonne de A. Ceci implique que A est la matrice de $\{T(u_1), \ldots, T(u_n)\}$ dans $\{v_1, \ldots, v_m\}$, c'est-à-dire, la matrice de T dans les bases $\{u_1, \ldots, u_n\}$ et $\{v_1, \ldots, v_m\}$. Ceci achève la démonstration.

Remarque. D'après le résultat précédent, si $T : E \to F$ est linéaire, alors T est donnée par

$$T : E \to F : (u_1, \ldots, u_n)B \mapsto (v_1, \ldots, v_m)AB.$$

Exemple. (1) On se fixe un angle θ. La rotation $\rho_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ d'angle θ est linéaire et sa matrice dans les bases canoniques est

$$A(\theta) := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Par conséquent, ρ_θ est de la forme suivante:

$$\rho_\theta : \mathbb{R}^2 \to \mathbb{R}^2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Démonstration. Pour tout $u \in \mathbb{R}^2$, il existe $r \geq 0$ et un angle ϕ tels que

$$u = \begin{pmatrix} r\cos\phi \\ r\sin\phi \end{pmatrix}.$$

D'après la définition,

$$\begin{aligned} \rho_\theta(u) &= \begin{pmatrix} r\cos(\phi+\theta) \\ r\sin(\phi+\theta) \end{pmatrix} = \begin{pmatrix} r\cos\theta\cos\phi - r\sin\theta\sin\phi \\ r\sin\theta\cos\phi + r\cos\theta\sin\phi \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} r\cos\phi \\ r\sin\phi \end{pmatrix} \\ &= A(\theta)u. \end{aligned}$$

D'où, on obtient l'énoncé.

(2) L'application $T : \mathbb{R}_4[x] \to \mathbb{R}_3[x]$ définie par

$$T(a_0 + a_1x + a_2x^2 + a_3x^3) = (2a_0 + a_1 + 3a_3) + (a_1 + 2a_2 + 2a_4)x + (3a_0 + 2a_1 + a_2)x^2$$

est linéaire et

$$[T]^{\{1,x,x^2,x^3\}}_{\{1,x,x^2\}} = \begin{pmatrix} 2 & 1 & 0 & 3 \\ 0 & 1 & 2 & 2 \\ 3 & 2 & 1 & 0 \end{pmatrix}.$$

(3) L'application $T : \mathbb{R}^2 \to \mathbb{R}^3 : (x, y) \mapsto (x + 2y - 1, x - y, y)$ n'est pas linéaire.

Le résultat suivant nous dit comment trouver l'image d'une application linéaire à l'aide de sa matrice.

5.3.4. Théorème. Soient $\{u_1, \ldots, u_n\}$ une base de E et $\{v_1, \ldots, v_m\}$ une base de F. Soit $T \in \mathcal{L}(E, F)$ avec $A = [T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}}$.

(1) $\dim(\mathrm{Im}(T)) = \mathrm{rg}(A)$.

(2) Un vecteur $v \in F$ appartient à $\mathrm{Im}(T)$ si, et seulement si, $P^{\{v\}}_{\{v_1,\ldots,v_m\}}$ appartient à l'espace-colonne $\mathcal{C}(A)$ de A.

Démonstration. Soit $A = (A_1 \cdots A_n)$, où $A_j = P^{\{T(u_j)\}}_{\{v_1,\ldots,v_m\}}$, $j = 1, \ldots, n$. Comme $E =< u_1, \ldots, u_n >$, on a $\mathrm{Im}(T) =< T(u_1), \ldots, T(u_n) >$. D'après le théorème 4.6.8,

$$\dim(\mathrm{Im}(T)) = \mathrm{rg}(P^{\{T(u_1),\ldots,T(u_n)\}}_{\{v_1,\ldots,v_m\}}) = \mathrm{rg}(A).$$

En outre, pour tout $v \in F$, on voit que $v \in \mathrm{Im}(T)$ si et seulement si v est combinaison linéaire de $T(u_1)$, ..., $T(u_n)$, si et seulement si, le système

$$P^{\{T(u_1),\ldots,T(u_n)\}}_{\{v_1,\ldots,v_m\}} X = P^{\{v\}}_{\{v_1,\ldots,v_m\}}$$

est compatible d'après le théorème 4.3.7, si et seulement si, $P^{\{v\}}_{\{v_1,\ldots,v_m\}} \in \mathcal{C}(A)$ d'après la proposition 4.7.3. Ceci achève la démonstration du théorème.

Remarque. On appelle *rang* de T la dimension de $\mathrm{Im}(T)$, et noté $\mathrm{rg}(T)$.

Exemple. Considérons l'application linéaire $T : \mathbb{R}_3[x] \to \mathbb{R}_4[x]$ telle que

$$T(1) = 1 + 2x + 3x^2 + 6x^3,\; T(x) = 2 + 3x + 5x^2 + 10x^3,\; T(x^2) = 3 + x + 4x^2 + 8x^3.$$

(1) Déterminer si $x + x^2 - x^3$ appartient à $\mathrm{Im}(T)$ ou non.

(2) Trouver une base pour $\mathrm{Im}(T)$.

Solution. D'abord, on trouve la matrice de T dans les bases canoniques comme suit:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 5 & 4 \\ 6 & 10 & 8 \end{pmatrix}.$$

(1) D'après le théorème 5.3.4, $x+x^2-x^3 \in \text{Im}(T)$ si et seulement si $(0,1,1,-1)^T \in \mathcal{C}(A)$. On échelonne la matrice

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 2 & 3 & 1 & 1 \\ 3 & 5 & 4 & 1 \\ 6 & 10 & 8 & -1 \end{array}\right) \Longrightarrow \left(\begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 0 & 1 & 5 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

On en déduit que $(0,1,1,-1)^T \notin \mathcal{C}(A)$. Ainsi $x+x^2-x^3 \notin \text{Im}(T)$.

(2) Pour trouver une base de $\text{Im}(T)$, on sait que $\text{Im}(T) = < T(1), T(x), T(x^2) >$. Comme

$$P_{\{1,x,x^2,x^3\}}^{\{T(1),T(x),T(x^2)\}} = A \Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

on voit que $\{T(1) = 1+2x+3x^2+6x^3,\ T(x) = 2+3x+5x^2+10x^3\}$ est une base de $\text{Im}(T)$.

Le résultat suivant nous dit comment trouver le noyau d'une application linéaire à l'aide de sa matrice.

5.3.5. Théorème. Soient $\{u_1, \ldots, u_n\}$ une base de E et $\{v_1, \ldots, v_m\}$ une base de F. Soit $T \in \mathcal{L}(E,F)$ avec $A = [T]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}}$.

(1) Un vecteur $u \in E$ appartient à $\text{Ker}(T)$ si, et seulement si, $P_{\{u_1,\ldots,u_n\}}^{\{u\}}$ appartient au noyau $\mathcal{N}(A)$ de A.

(2) Si $\{S_1, \ldots, S_r\}$ est une base de $\mathcal{N}(A)$ et $w_j = (u_1, \ldots, u_n)S_j$, $j = 1, \ldots, r$, alors $\{w_1, \ldots, w_r\}$ est une base de $\text{Ker}(T)$. En particulier, $\dim(\text{Ker}(T)) = \dim\mathcal{N}(A)$.

Démonstration. (1) Par définition, $u \in \text{Ker}(T)$ si, et seulement si, $T(u) = 0_F$ si, et seulement si, $P_{\{v_1,\ldots,v_m\}}^{\{T(u)\}} = 0_{m\times 1}$ si, et seulement si, $AP_{\{u_1,\ldots,u_n\}}^{\{u\}} = 0_{m\times 0}$ d'après la proposition 5.3.3, c'est-à-dire, $P_{\{u_1,\ldots,u_n\}}^{\{u\}} \in \mathcal{N}(A)$.

(2) D'après l'énoncé (1), l'application

$$\Psi : \mathcal{N}(A) \to \text{Ker}(T) : S \mapsto (v_1, \ldots, v_m)S$$

est surjective, qui est aussi injective car $\{v_1, \ldots, v_m\}$ est libre. En outre, Ψ est linéaire, et donc un isomorphisme. Or, l'énoncé (2) suit de la proposition 5.2.8. Ceci achève la démonstration.

Exemple. Considérons l'application linéaire $T : \mathbb{R}_3[x] \to \mathbb{R}_4[x]$ telle que

$$T(1) = 1 + 2x + 3x^2 + 6x^3,\ T(x) = 2 + 3x + 5x^2 + 10x^3,\ T(x^2) = 3 + x + 4x^2 + 8x^3.$$

Alors

$$[T]^{\{1,x,x^2\}}_{\{1,x,x^2,x^3\}} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 5 & 4 \\ 6 & 10 & 8 \end{pmatrix}.$$

Pour trouver une base de $\mathrm{Ker}(T)$, on trouve que $\left\{(7,-5,1)^T\right\}$ est une base de l'espace-solution de $AX = 0$. Posons $f = 7 - 5x + x^2$. Alors $\{f\}$ est une base de $\mathrm{Ker}(T)$.

Le résultat suivant donne le lien enter les dimensions de l'image et du noyau d'une application linéaire.

5.3.6. Corollaire. Si $T \in \mathcal{L}(E,F)$, alors $\dim(E) = \dim(\mathrm{Im}(T)) + \dim(\mathrm{Ker}(T))$.

Démonstration. Soient $\{u_1, \ldots, u_n\}$ une base de E et $\{v_1, \ldots, v_m\}$ une base de F. Soit $T \in \mathcal{L}(E,F)$ avec $A = [T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}}$. D'après les théorèmes 5.3.4 et 5.3.5, $\dim(\mathrm{Im}(T)) = \mathrm{rg}(A)$ et

$$\dim(\mathrm{Ker}(T)) = \dim \mathcal{N}(A) = n - \mathrm{rg}(A),$$

où la deuxième égalité suit du théorème 4.8.1. Ainsi

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

Ceci achève la démonstration.

Exemple. Considérons la projection $p : \mathbb{R}^2 \to \mathbb{R}^2 : (x,y) \mapsto (x,0)$. Alors

$$\dim(\mathrm{Ker}(p)) + \dim(\mathrm{Im}(p)) = 2 = \dim(\mathbb{R}^2).$$

Le résultat suivant nous donne une caractérisation de l'injectivité et de la surjectivité d'une application linéaire en terme du rang de sa matrice.

5.3.7. Proposition. Soient $\{u_1, \ldots, u_n\}$ une base de E et $\{v_1, \ldots, v_m\}$ une base de F. Soient $T \in \mathcal{L}(E,F)$ et $A = [T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}}$.

(1) T est injective si et seulement si $\mathrm{rg}(A) = n$.

(2) T est surjective si et seulement si $\mathrm{rg}(A) = m$.

(3) T est un isomorphisme si et seulement si A est inversible.

Démonstration. (1) T est injective si et seulement si $\mathrm{Ker}(T) = 0$ si et seulement si $\dim(\mathrm{Ker}(T)) = 0$ si et seulement si $\dim(E) - \mathrm{rg}(A) = 0$, c'est-à-dire, $\mathrm{rg}(A) = n$.

(2) T est surjective si et seulement si $\mathrm{Im}(T) = F$ si et seulement si $\dim(\mathrm{Im}(T)) = \dim(F)$ si et seulement si $\mathrm{rg}(A) = m$.

(3) T est un isomorphisme si et seulement si T est injective et surjective si et seulement si $\mathrm{rg}(A) = n = m$ si et seulement si A est inversible. Ceci achève la démonstration.

Remarque. Soit $T : E \to F$ une application linéaire. On voit que $\dim(E) \leq \dim(F)$ si T est injective, et $\dim(E) \geq \dim(F)$ si T est surjective.

Exemple. (1) Considérons l'application linéaire $T : \mathbb{R}_4[x] \to \mathbb{R}_3[x]$ telle que

$$T(1) = 1 + 2x + 3x^2,\ T(x) = 2 + 3x + 5x^2, T(x^2) = 3 + 5x + x^2 \text{ et } T(x^3) = 1 + x^2.$$

Alors la matrice de T dans les bases canoniques est

$$A = \begin{pmatrix} 1 & 2 & 3 & 1 \\ 2 & 3 & 5 & 0 \\ 3 & 5 & 1 & 2 \end{pmatrix}.$$

On voit que $\mathrm{rg}(A) = 3$. Ainsi T est surjective et non injective.

(2) Considérons l'application linéaire

$$T : \mathbb{R}^4 \to M_2(\mathbb{R}) : (a_1, a_2, a_3, a_4) \mapsto \begin{pmatrix} a_1 + 2a_3 & 2a_2 + a_4 \\ 2a_1 + a_4 & 3a_2 + 2a_3 \end{pmatrix}.$$

On veut montrer que T est un isomorphisme. Considérons la base canonique $\{e_1, e_2, e_3, e_4\}$ de $\mathbb{R}^4$ et la base de canonique $\{e_{11}, e_{12}, e_{21}, e_{22}\}$ de $M_2(\mathbb{R})$. Alors

$$[T]_{\{e_{11},e_{12},e_{21},e_{22}\}}^{\{e_1,e_2,e_3,e_4\}} = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 \\ 2 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

On voit que cette matrice est de rang 4, et donc inversible. Ceci montrer que T est un isomorphisme.

5.3.8. Lemme. Soient $\{u_1, \ldots, u_n\}$ une base de E et $\{v_1, \ldots, v_m\}$ une base de F. Si $T, S \in \mathcal{L}(E, F)$ et $\alpha, \beta \in K$, alors

$$[\alpha T + \beta S]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}} = \alpha[T]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}} + \beta[S]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}}.$$

Démonstration. Posons $A = [T]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}}$ et $B = [S]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}}$. Alors $(T(u_1),\ldots,T(u_n)) = (v_1,\ldots,v_m)A$ et $(S(u_1),\ldots,S(u_n)) = (v_1,\ldots,v_m)B$. Or

$$\begin{aligned} & ((\alpha T+\beta S)(u_1),\ldots,(\alpha T+\beta S)(u_n)) \\ = \ & (\alpha T(u_1)+\beta S(u_1),\ldots,\alpha T(u_n)+\beta S(u_n)) \\ = \ & \alpha(T(u_1),\ldots,T(u_n))+\beta(S(u_1),\ldots,S(u_n)) \\ = \ & \alpha(v_1,\ldots,v_m)A+\beta(v_1,\ldots,v_m)B \\ = \ & (v_1,\ldots,v_m)(\alpha A+\beta B). \end{aligned}$$

Par conséquent, $[\alpha T+\beta S]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}} = \alpha A+\beta B$. Ceci achève la démonstration.

Exemple. Considérons $T, S \in \mathcal{L}(\mathbb{R}^4, M_{2\times 2}(\mathbb{R}))$ définies respectivement par

$$T(a_1,a_2,a_3,a_4) = \begin{pmatrix} a_1+2a_3 & 2a_2+a_4 \\ 2a_1+a_4 & 3a_2+2a_3 \end{pmatrix}, \ S(a_1,a_2,a_3,a_4) = \begin{pmatrix} a_1+a_3 & a_2+a_4 \\ a_1+a_4 & a_2+a_3 \end{pmatrix}.$$

On sait que les matrices de T et S dans les bases canoniques sont respectivement

$$A = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 \\ 2 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Ainsi

$$[3T-2S]_{\{e_{11},e_{12},e_{21},e_{22}\}}^{\{e_1,e_2,e_3,e_4\}} = 3A-2B = \begin{pmatrix} 1 & 0 & 4 & 0 \\ 0 & 4 & 0 & 7 \\ 4 & 0 & 0 & 4 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

5.3.9. Lemme. Soient $\{u_1,\ldots,u_n\}$ une base de E et $\{v_1,\ldots,v_m\}$ une base de F. Pour toute $A \in M_{m\times n}(K)$, il existe une unique $T \in \mathcal{L}(E,F)$ telle que $[T]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}} = A$.

Démonstration. Posons $(w_1,\ldots,w_n) = (v_1,\ldots,v_m)A$. D'après la proposition 5.1.4, il existe une unique $T \in \mathcal{L}(E,F)$ telle que $T(u_i) = w_i, i = 1,\ldots,n$. Or

$$(T(u_1),\ldots,T(u_n)) = (w_1,\ldots,w_n) = (v_1,\ldots,v_m)A.$$

Par conséquent, $[T]_{\{v_1,\ldots,v_m\}}^{\{u_1,\ldots,u_n\}} = A$. Ceci achève la démonstration.

Exemple. Trouver $T \in \mathcal{L}(\mathbb{R}^3, \mathbb{R}_2[x])$ dont la matrice dans les bases canoniques est

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

Solution. Soient $\{e_1, e_2, e_3\}$ la base canonique de $\mathbb{R}^3$ et $\{1, x\}$ la base canonique de $\mathbb{R}_2[x]$. Par l'hypothèse, $(T(e_1), T(e_2), T(e_3)) = (1, x)A = (1+4x, 2+5x, 3+6x)$, c'est-à-dire, $T(e_1) = 1 + 4x, T(e_2) = 2 + 5x$ et $T(e_3) = 3 + 6x$. Ainsi pour tout $u = (a, b, c) \in \mathbb{R}^3$, $T(u) = aT(e_1) + bT(e_2) + cT(e_3) = (a + 2b + 3c) + (4a + 5b + 6c)x$.

5.3.10. Théorème. Soient $\dim E = n$ et $\dim F = m$. Alors $\mathcal{L}(E, F) \cong M_{m\times n}(K)$. En particulier, $\dim\mathcal{L}(E, F) = mn$.

Démonstration. On se fixe une base $\{u_1, \ldots, u_n\}$ de E et une base $\{v_1, \ldots, v_m\}$ de F. Considérons l'application suivante

$$\Phi : \mathcal{L}(E, F) \to M_{m\times n}(K) : T \mapsto [T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}}.$$

Alors Φ est linéaire d'après le lemme 5.3.9 et bijective d'après le lemme 5.3.10. Ainsi Φ est un isomorphisme. Ceci achève la démonstration.

5.3.11. Théorème. Soient E, F et G des K-espaces vectoriels ayant pour base $\{u_1, \ldots, u_n\}$, $\{v_1, \ldots, v_m\}$, et $\{w_1, \ldots, w_p\}$, respectivement. Si $T \in \mathcal{L}(E, F)$ et $S \in \mathcal{L}(F, G)$, alors

$$[ST]^{\{u_1,\ldots,u_n\}}_{\{w_1,\ldots,w_p\}} = [S]^{\{v_1,\ldots,v_m\}}_{\{w_1,\ldots,w_p\}} \cdot [T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}}.$$

Démonstration. Posons $[S]^{\{v_1,\ldots,v_m\}}_{\{w_1,\ldots,w_p\}} = A$ et $[T]^{\{u_1,\ldots,u_n\}}_{\{v_1,\ldots,v_m\}} = B = (B_1 \cdots B_n)$, où $B_i = P^{\{T(u_i)\}}_{\{v_1,\ldots,v_m\}}$, $i = 1, \ldots, n$. Alors $P^{\{S(T(u_i))\}}_{\{w_1,\ldots,w_p\}} = AB_i$, $i = 1, \ldots, n$. Donc

$$[ST]^{\{u_1,\ldots,u_n\}}_{\{w_1,\ldots,w_p\}} = P^{\{S(T(u_1),\ldots,S(T(u_n))\}}_{\{w_1,\ldots,w_p\}} = (AB_1, \cdots, AB_n) = AB.$$

Ceci achève la démonstration.

Exemple. Considérons les applications linéaires d'espaces réels suivantes:

$$T : \mathbb{R}_2[x] \to \mathbb{R}^2 : a + bx \mapsto (2a + b, a - 3b),$$

et

$$S : \mathbb{R}^2 \to \mathbb{C} : (x, y) \mapsto (x + y) + (3x - y)i.$$

Alors

$$[T]_{\{e_1,e_2\}}^{\{1,x\}} = \begin{pmatrix} 2 & 1 \\ 1 & -3 \end{pmatrix} \quad \text{et} \quad [S]_{\{1,i\}}^{\{e_1,e_2\}} = \begin{pmatrix} 1 & 1 \\ 3 & -1 \end{pmatrix}.$$

Ainsi

$$[ST]_{\{1,i\}}^{\{1,x\}} = [S][T] = \begin{pmatrix} 1 & 1 \\ 3 & -1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & -3 \end{pmatrix} = \begin{pmatrix} 3 & -2 \\ 5 & 6 \end{pmatrix}.$$

Cela veut dire que ST est définie par

$$ST : \mathbb{R}_2[x] \to \mathbb{C} : a + bx \mapsto (3a - 2b) + (5a + 6b)i.$$

5.3.12. Corollaire. Soit $T : E \to F$ est un isomorphisme. Si $\{u_1, \ldots, u_n\}$ est une base de E et $\{v_1, \ldots, v_n\}$ est une base de F, alors

$$[T^{-1}]_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_n\}} = \left([T]_{\{v_1,\ldots,v_n\}}^{\{u_1,\ldots,u_n\}}\right)^{-1}.$$

Démonstration. Posons $A = [T]_{\{v_1,\ldots,v_n\}}^{\{u_1,\ldots,u_n\}}$ et $B = [T^{-1}]_{\{u_1,\ldots,u_n\}}^{\{v_1,\ldots,v_n\}}$. Comme $T^{-1}T = \mathbb{1}_E$ et $[\mathbb{1}_E]_{\{u_1,\ldots,u_n\}}^{\{u_1,\ldots,u_n\}} = I_n$, d'après le théorème 5.3.11, on a $BA = I_n$. De même, $AB = I_n$. Ceci achève la démonstration.

Exemple. Considérons l'application linéaire suivante:

$$T : \mathbb{R}_2[x] \to \mathbb{R}^2 : a + bx \mapsto (2a + b, a - 3b).$$

On voit que

$$[T]_{\{e_1,e_2\}}^{\{1,x\}} = \begin{pmatrix} 2 & 1 \\ 1 & -3 \end{pmatrix}.$$

Comme $[T]$ est inversible, T est un isomorphisme et

$$[T^{-1}]]_{\{1,x\}}^{\{e_1,e_2\}} = ([T]_{\{e_1,e_2\}}^{\{1,x\}})^{-1} = \begin{pmatrix} 2 & 1 \\ 1 & -3 \end{pmatrix}^{-1} = \frac{1}{7}\begin{pmatrix} 3 & 1 \\ 1 & -2 \end{pmatrix},$$

c'est-à-dire,

$$T^{-1} : \mathbb{R}^2 \to \mathbb{R}_2[x] : (a, b) \mapsto \frac{3a + b}{7} + \frac{a - 2b}{7}x.$$

5.4. Endomorphismes d'espaces vectoriels

Soit E un K-espace vectoriel. Une application linéaire $T : E \to E$ s'appelle *endomorphisme* de E; et *automorphisme* de E si T est un isomorphisme. Par exemple, l'application nulle $\mathbf{0} : E \to E : u \mapsto 0_E$ est un endomorphisme de E, et l'application identité $\mathbb{1}_E$ de E est un automorphisme de E. Désignerons par $\mathrm{End}(E)$ l'ensemble des endomorphismes de E qui, d'après le théorème 5.1.7, est un espace vectoriel sur K. Le but de cette section est étudier, à l'aide de la théorie des matrices, les endomorphismes d'un espace vectoriel de dimension finie.

5.4.1. Théorème. Soit E un K-espace vectoriel de dimension finie. Les conditions suivantes sont équivalentes pour $T \in \mathrm{End}(E)$.

(1) T est un automorphisme.

(2) T est injective.

(3) T est surjective.

Démonstration. Comme E est de dimension finie, $\dim(E) = \dim(\mathrm{Ker}(T)) + \dim(\mathrm{Im}(T))$. Or T est injective si, et seulement si, $\dim(\mathrm{Ker}(T)) = 0$ si, et seulement si, $\dim(E) = \dim(\mathrm{Im}(T))$ si, et seulement si, $\mathrm{Im}(T) = E$ si, et seulement si, T est surjective. Ceci achève la démonstration.

Exemple. Comme

$$\partial : D^\infty[a,b] \to D^\infty[a,b] : f(t) \mapsto \frac{df(t)}{dt}$$

est un endomorphisme de $D^\infty[a,b]$, qui est surjectif et non injectif. Par conséquent, $D^\infty[a,b]$ est de dimension infinie.

5.4.2. Définition. Soit $\{u_1, \ldots, u_n\}$ une base de E. Pour $T \in \mathrm{End}\,(E)$, on définit la *matrice* de T dans $\{u_1, \ldots, u_n\}$, notée $[T]_{\{u_1,\ldots,u_n\}}$, comme étant la matrice de la famille $\{T(u_1), \ldots, T(u_n)\}$ dans cette base. Ainsi

$$(T(u_1), \ldots, T(u_n)) = (u_1, \ldots, u_n)[T]_{\{u_1,\ldots,u_n\}}.$$

Exemple. (1) $[\mathbf{0}_E]_{\{u_1,\ldots,u_n\}} = 0_{n\times n}$ et $[\mathbb{1}_E]_{\{u_1,\ldots,u_n\}} = I_n$.

(3) Soit $A \in M_{n\times n}(K)$. Alors la matrice de

$$T_A : K^{(n)} \to K^{(n)} : v \mapsto Av$$

dans la base canonique est A. Et la matrice de

$$S_A : K^n \to K^n : u \mapsto uA$$

dans la base canonique est A^T.

On voit que si $T \in$End(E), alors $T^2 = TT \in$End(E). En général on définit $T^0 = \mathbb{1}_E$ et $T^n = TT^{n-1}$ pour tout $n \geq 1$. Le résultat suivant suit de la proposition 5.3.3, le corollaire 5.3.7, la proposition 5.3.12 et le corollaire 5.3.13.

5.4.3. Théorèm. Soit $T \in \text{End}(E)$. Si $\{u_1, \dots, u_n\}$ est une base de E, alors
(1) $P^{\{T(u)\}} = [T]_{\{u_1,\dots,u_n\}} P^{\{u\}}_{\{u_1,\dots,u_n\}}$, pour tout $u \in E$.
(2) T est un automorphisme si et seulement si $[T]_{\{u_1,\dots,u_n\}}$ est inversible.
(3) $[T^r]_{\{u_1,\dots,u_n\}} = \big([T]_{\{u_1,\dots,u_n\}}\big)^r$, pour tout $r \geq 0$.
(4) $[T^r]_{\{u_1,\dots,u_n\}} = \big([T]_{\{u_1,\dots,u_n\}}\big)^r$, pour tout entier r lorsque T est un automorphisme.

Exemple. On voit aisément que la rotation ρ_θ du plan d'angle θ est un automorphisme et $\rho_\theta^n = \rho_{n\theta}$, pour tout entier n. Or

$$[\rho_\theta]_{\{e_1,e_2\}} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

et

$$[\rho_{n\theta}]_{\{e_1,e_2\}} = \begin{pmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{pmatrix}.$$

D'après le théorème 5.4.3(4), on a

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^n = \begin{pmatrix} \cos n\theta & \sin n\theta \\ -\sin n\theta & \cos n\theta \end{pmatrix}.$$

Le résultat suivant nous dit comment sont reliées les matrices d'un endomorphisme dans deux bases différentes.

5.4.4. Théorème. Soit $T \in \text{End}(E)$. Si P est la matrice de passage d'une base $\{u_1, \dots, u_n\}$ de E vers une autre base $\{v_1, \dots, v_n\}$, alors

$$[T]_{\{v_1,\dots,v_n\}} = P^{-1}[T]_{\{u_1,\dots,u_n\}}P.$$

Démonstration. Posons $A = [T]_{\{u_1,\dots,u_n\}}$. Soit $P = (P_1 \cdots P_n)$ partagée en colonnes. Alors $v_j = (u_1, \dots, u_n)P_j$, et donc d'après le théo̊eme 5.4.3, $P^{T(v_j)}_{\{u_1,\dots,u_n\}} = AP_j$, $j = 1, \dots, n$. Ainsi $P^{\{T(v_1),\dots,T(v_n)\}}_{\{u_1,\dots,u_n\}} = (AP_1 \cdots AP_n) = AP$. D'où

$$\begin{aligned} (T(v_1), \dots, T(v_n)) &= (u_1, \dots, u_n)(AP) \\ &= ((v_1, \dots, v_n)P^{-1})(AP) \\ &= (v_1, \dots, v_n)(P^{-1}AP). \end{aligned}$$

Ainsi $[T]_{\{v_1,\ldots,v_n\}} = P^{-1}AP$. Ceci achève la démonstration.

Exemple. Considérons l'endomorphisme ∂ de l'espace vectoriel réel $\mathbb{R}_3[x]$ défini par $\partial(a+bx+cx^2) = b+2cx$.

(1) Trouver la matrice de ∂ dans la base $\{2+x, 3+x, 4+5x+6x^2\}$.

(2) Trouver les coordonnées de $\partial(a+bx+cx^2)$ dans la base $\{2+x, 3+x, 4+5x+6x^2\}$.

Solution. On voit que la matrice de ∂ dans la base canonique $\{1, x, x^2\}$ est

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix},$$

et la matrice de passage de $\{1, x, x^2\}$ vers $\{2+x, 3+x, 4+5x+6x^2\}$ est

$$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 1 & 5 \\ 0 & 0 & 6 \end{pmatrix}.$$

(1) Donc la matrice de ∂ dans la base $\{2+x, 3+x, 4+5x+6x^2\}$ est

$$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 1 & 5 \\ 0 & 0 & 6 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 2 & 3 & 4 \\ 1 & 1 & 5 \\ 0 & 0 & 6 \end{pmatrix} = \begin{pmatrix} -1 & -1 & 31 \\ 1 & 1 & -19 \\ 0 & 0 & 0 \end{pmatrix}.$$

(2) La colonnes de coordonnées de $f = a+bx+cx^2$ dans $\{2+x, 3+x, 4+5x+6x^2\}$ est

$$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 1 & 5 \\ 0 & 0 & 6 \end{pmatrix}^{-1} \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Ainsi la colonne de $\partial(f)$ dans la base $\{2+x, 3+x, 4+5x+6x^2\}$ est

$$\begin{pmatrix} -1 & -1 & 31 \\ 1 & 1 & -19 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 2 & 3 & 4 \\ 1 & 1 & 5 \\ 0 & 0 & 6 \end{pmatrix}^{-1} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 & -1 & 6 \\ 0 & 1 & -4 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} -b+6c \\ b-4c \\ 0 \end{pmatrix}.$$

5.4.5. Définition. On dit que $A, B \in M_n(K)$ sont *semblables*, notée $A \sim B$, s'il existe une matrice inversible P telle que $A = P^{-1}BP$.

5.4.6. Proposition. La relation de semblable de matrices de $M_n(K)$ est une relation d'équivalence.

Démonstration. Soient $A, B, C \in M_n(K)$.

(1) Comme $A = I_n^{-1} A I_n$, on a $A \sim A$.

(2) Si $A \sim B$, alors $A = P^{-1}BP$ avec P inversible. Alors $B = PAP^{-1} = Q^{-1}AQ$ avec $Q = P^{-1}$ inversible. Donc $B \sim A$.

(3) Si $A \sim B$ et $B \sim C$, alors $A = P^{-1}BP$ et $B = Q^{-1}CQ$. Alors QP est inversible telle que $A = (QP)^{-1}C(QP)$. Ainsi $A \sim C$.

Le Théorème 5.4.4 nous dit que les matrices d'un endomorphisme dans deux bases sont semblables. Réciproquement, on a le résultat suivant.

5.4.7. Proposition. Soient T un endomorphisme de E et A la matrice de T dans une base $\{u_1, \ldots, u_n\}$ de E. Si B est une matrice semblable à A, alors il existe une base $\{v_1, \ldots, v_n\}$ de E dans laquelle la matrice de T est B.

Démonstration. Par l'hypothèse, $B = P^{-1}AP$ avec P inversible. Posons $(v_1, \ldots, v_n) = (u_1, \ldots, u_n)P$. Alors $\{v_1, \ldots, v_n\}$ est une base de E et P est la matrice de passage de $\{u_1, \ldots, u_n\}$ vers $\{v_1, \ldots, v_n\}$. D'après le théorème 5.4.4, la matrice de T dans $\{v_1, \ldots, v_n\}$ est $P^{-1}AP = B$. Ceci achève la démonstration.

Exemple. Considérons l'endomorphisme $T : \mathbb{R}_2[x] \to \mathbb{R}_2[x]$ défini par

$$T(a + bx) = (a + b) + (-2a + 4b)x.$$

Alors la matrice de T dans $\{1, x\}$ est

$$\begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix}.$$

Or

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

Posons

$$(f_1, f_2) = (1, x) \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = (1 + x, 1 + 2x).$$

Alors la matrice de T dans la base $\{1+x, 1+2x\}$ est

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

Selon le Théorème 5.4.4 et la proposition 5.4.7, le problème de trouver une base dans laquelle la matrice d'un endomorphisme est le plus simple se ramène au problème de trouver une matrice le plus simple qui est semblable à une matrice carrée. On discutera ce problème dans le cours MAT253.

5.5. Exercices

1. Soit $M \in M_n(K)$ non nulle. Laquelle(s) parmi les applications $T : M_n(K) \to M_n(K)$ suivantes est linéaire et pourquoi?

   (1) $T(A) = MA$; (2) $T(A) = M + A$.

2. Dans chacun des cas suivants, déterminer si l'application est linéaire ou non:

   (1) $T : \mathbb{R}^2 \to \mathbb{R}^2 : (x, y) \mapsto (x + y, y^2)$.
   (2) $\cos : \mathbb{R} \to \mathbb{R} : t \mapsto \cos t$.

3. Considérer les espaces vectoriels réels $\mathbb{R}^3$ et $\mathbb{R}^4$.

   (1) Vérifier que les vecteurs $u_1 = (-1, 1, 1)$, $u_2 = (1, 2, 1)$, $u_3 = (0, 1, 2)$ forment une base de $\mathbb{R}^3$.
   (2) Trouver une application linéaire $T : \mathbb{R}^3 \to \mathbb{R}^4$ telle que $T(u_1) = T(u_2) = T(u_3) = (1, 0, 2, 1)$.
   (3) Déterminer s'il existe ou non une application linéaire $S : \mathbb{R}^3 \to \mathbb{R}^4$ telle que $S(u_1) = S(u_2) = (1, 2, 0, 1)$, $S(u_3) = (1, 0, 1, 1)$ et $S(-1, 0, 1) = (1, 0, 1, 0)$.

4. Soient $T_1, T_2 : \mathbb{R}^2 \to \mathbb{R}^3$ et $S : \mathbb{R}^3 \to \mathbb{R}_2[x]$ des applications linéaires définies par $T_1(a, b) = (2a - b, a, a + b)$, $T_2(a, b) = (a - 3b, b, 2a + 5b)$ et $S(a, b, c) = (a - b + c) + (2a + 3b - c)x$. Calculer $S(6T_1 - 9T_2)$.

5. Soit $E = E_1 \oplus E_2$. Pour tout $u = u_1 + u_2$, $u_1 \in E_1$ et $u_2 \in E_2$, définir $p(u) = u_1$. Montrer que p est une application linéaire surjective de E sur E_1.

6. Soient n, m deux entiers avec $n > m > 0$. Soient $u_i = (a_{i1}, \ldots, a_{im},\ a_{i,m+1}, \ldots, a_{in}) \in K^n$ et $v_i = (a_{i1}, \ldots, a_{im}) \in K^{n-m}$ pour $i = 1, \ldots, r$. Montrer, en construisant une application linéaire de K^n dans K^{n-m}, que si $v_1, \ldots, v_r$ sont linéairement indépendants, alors $u_1, \ldots, u_r$ sont également linéairement indépendants.

7. Dans chacun des cas suivants, trouver une base de $\mathrm{Ker}(T)$ et une base de $\mathrm{Im}(T)$, et déterminer si T est injective ou surjective.

(1) $T : \mathbb{R}^{(4)} \to \mathbb{R}^{(3)} : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + 2x_2 + x_4 \\ 2x_1 + 3x_2 + x_3 \\ x_1 + 3x_3 + x_4 \end{pmatrix}.$

(2) $T : \mathbb{R}^{(4)} \to \mathbb{R}^{(3)} : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + 2x_2 + x_4 \\ 2x_1 + 3x_2 + x_3 \\ 3x_1 + 5x_2 + 3x_3 + x_4 \end{pmatrix}.$

8. Soient E et F deux K-espaces vectoriels de dimension finie avec $T \in \mathcal{L}(E, F)$. Montrer les énoncés suivants:
(1) T est injective si et seulement s'il existe $S \in \mathcal{L}(F, E)$ telle que $ST = \mathbb{1}_E$.
(2) T est surjective si et seulement s'il existe $S \in \mathcal{L}(F, E)$ telle que $TS = \mathbb{1}_F$.

9. Considérer l'application linéaire

$$T : M_{2\times 2}(\mathbb{R}) \to M_{2\times 2}(\mathbb{R}) : A \mapsto AM - MA; \qquad \text{où} \qquad M = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}.$$

Trouver une base pour $\mathrm{Ker}(T)$ et une pour $\mathrm{Im}(T)$.

10. Dans chacun des cas suivants, trouver une base pour $\mathrm{Ker}(T)$ et une pour $\mathrm{Im}(T)$.

(1) $\quad T : \mathbb{R}^{(4)} \to \mathbb{R}^{(3)} : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}.$

(2) $\quad T \in \mathcal{L}(\mathbb{R}_4[x], \mathbb{R}_3[x])$ dont la matrice dans les bases canoniques est

$$A = \begin{pmatrix} 1 & 2 & 3 & -1 \\ 3 & 1 & 2 & 1 \\ 4 & 3 & 5 & 0 \end{pmatrix}.$$

11. Soit $T : E \to F$ une application linéaire de K-espaces vectoriels de dimension finie.
    (1) Supposons que T est surjective. Montrer que F est isomorphe à un complément de $\mathrm{Ker}(T)$ et en déduire que $\dim(F) \leq \dim(E)$.
    (2) Supposons que T est injective. Montrer que E est isomorphe à $\mathrm{Im}(T)$ et en déduire que $\dim(E) \leq \dim(F)$.

12. Soit $T \in \mathcal{L}(\mathbb{R}^3,\ \mathbb{R}^{(3)})$ dont la matrice dans les bases canoniques est A. Dans chacun des cas suivants, déterminer si T est un isomorphisme ou non; et si oui, trouver la matrice de son inverse dans les bases canoniques.

$$(1) \quad A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}; \qquad\qquad (2) \quad A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 3 \\ 1 & 1 & 2 \end{pmatrix}.$$

13. Soient $T : E \to F$ et $S : F \to G$ des applications linéaires de K-espaces vectoriels de dimension finie.
    (1) Si T est surjective, montrer que $\mathrm{rg}(ST) = \mathrm{rg}(S)$.
    (2) Si S est injective, montrer que $\mathrm{rg}(ST) = \mathrm{rg}(T)$.

14. Soient E et F des K-espaces vectoriels de dimension finie. Si $T \in \mathcal{L}(E, F)$ est de rang $r > 0$, montrer qu'il existe une base $\{u_1, \ldots, u_m\}$ de E et une base $\{v_1, \ldots, v_n\}$ de F dans lesquelles la matrice de T est de la forme

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

15. Dans chacun des cas suivants, montrer que l'application T est un isomorphisme:
    (1) $T : \mathbb{R}_n[x] \to \mathbb{R}^n : f \mapsto (f(0), f(1), \ldots, f(n-1))$.
    (2) $S : \mathbb{R}_n[x] \to \mathbb{R}_n[x] : f(x) \mapsto f(x + \alpha)$, où $\alpha \in \mathbb{R}$.

16. Pour tout $n \geq 1$, construire un isomorphisme $K^n \to K_n[x]$.

17. Considérer l'application linéaire $T : \mathbb{Q}_3[x] \to \mathbb{Q}_3[x]$ définie par

$$T(a_0 + a_1 x + a_2 x^2) = (a_0 + 2a_1 + 3a_2) + (2a_0 - a_1 + a_2)x + (3a_0 + a_1 + 4a_2)x^2.$$

    (a) Trouver la matrice de T dans la base canonique $\{1, x, x^2\}$.

(b) Déterminer si T est un automorphisme ou non.

(c) Trouver la matrice de T dans la base $\{1+x-x^2, 2-x+x^2, x+3x^2\}$.

(d) Trouver les coordonnées de $T(2-3x-x^2)$ dans $\{1+x-x^2, 2-x+x^2, x+3x^2\}$.

18. Soit $A \in M_n(K)$. Montrer que

$$T_A : K^{(n)} \to K^{(n)} : u \mapsto Au$$

est un automorphisme de $K^{(n)}$ si et seulement si A est inversible.

19. Soit T un endomorphisme de $\mathbb{Q}^3$ dont la matrice dans la base canonique est

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

(1) Vérifier que T est un automorphisme.

(2) Trouver la matrice de T^{-1} dans la base $\{(1,0,1),\ (1,1,0),\ (0,1,1)\}$.

20. Soit T un endomorphisme d'un K-espace vectoriel de dimension finie E. Montrer les énoncés suivants.

(1) Si $T^2 = T$, alors $E = \operatorname{Im}(T) \oplus \operatorname{Ker}(T)$.

(2) Si $T^3 = T$, alors $E = E_{-1} \oplus E_0 \oplus E_1$, où $E_\lambda = \{u \in E \mid T(u) = \lambda u\}$, $\lambda = -1, 0, 1$.

21. Considérer l'espace $K[x]$ des polynômes sur K.

(1) Trouver un endomorphisme de E qui est surjectif et non injectif.

(2) Trouver un endomorphisme de E qui est injectif et non surjectif.

22. Soient A et B deux matrices carrées semblables. Montrer les énoncés suivants.

(1) A et B ont le même rang.

(2) A est inversible si, et seulement si, B l'est.

(3) A est nilpotente si, et seulement si, B l'est.

23. Un endomorphisme T de E est dit *nilpotent* si $T^r = \mathbf{0}$ pour un certain entier $r > 0$. Si E est de dimension finie, montrer que T est nilpotent si, et seulement si, la matrice de T dans une base de E est nilpotente.

24. Soit $A \in M_2(K)$ non nulle telle que $A^2 = 0$. Montrer que A est semblable à la matrice suivante

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Indice: Considérer l'application linéaire $T_A : K^2 \to K^2 : u \mapsto Au$. Trouver premièrement un vecteur u tel que $Au \neq 0$, et ensuite, montrer que $\{u, Au\}$ est une base de K^2.