

MAT 153: Introduction à l'algèbre linéaire I

Chapitre I: Corps

Les objets d'étude d'algèbre sont des systèmes algébriques, c'est-à-dire, les ensembles dans lesquels on peut effectuer des opérations arithmétiques. Les premiers 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 du développement des nombres. Considérons l'ensemble des nombres naturels

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

ce qui est muni d'une addition et d'une multiplication, c'est-à-dire, pour tous $a, b \in \mathbb{N}$, on a $a + b, ab \in \mathbb{N}$. Mais, \mathbb{N} n'est pas stable pour la soustraction. Par exemple, $1 - 2 \notin \mathbb{N}$, car $2 + n \neq 1$ pour tout $n \in \mathbb{N}$. Après l'introduction de nombres négatifs, nous avons l'ensemble des nombres entiers

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

dans lequel on peut effectuer l'addition, la soustraction et la multiplication. Mais, 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

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

dans lequel on peut effectuer l'addition, la soustraction, la multiplication et la division. Mais, il n'est pas stable pour les limites. Par exemple,

$$\lim_{n \rightarrow \infty} \sum_{k=0}^n \frac{1}{k!} = e,$$

ce qui n'est pas rationnel. En introduisant les nombres irrationnels, on obtient l'ensemble des nombres réels \mathbb{R} , c'est-à-dire, l'union des nombres rationnels et des nombres irrationnels. Alors \mathbb{R} est stable pour toutes les opérations ci-haut mentionnées. Cependant, \mathbb{R} n'est pas

stable pour l'extraction de racine. Par exemple, $\sqrt{-1} \notin \mathbb{R}$. En effet, pour tout $a \in \mathbb{R}$, on a $a^2 \geq 0$. En particulier, $a^2 \neq -1$. Pour obtenir un ensemble des nombres stable pour toutes les opérations arithmétiques ci-haut mentionnées, 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 *unité imaginaire*;
- (2) le nombre réel a s'appelle *partie réelle* de z , notée $a = \operatorname{Re}(z)$;
- (3) le nombre réel b s'appelle *partie imaginaire* de z , notée $b = \operatorname{Im}(z)$.

En outre, deux nombres complexes $a + bi$ et $c + di$ sont dits *égaux* si $a = c$ et $b = d$.

Notation. L'ensemble des nombres complexes sera noté $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$.

Remarque. (1) Si $\operatorname{Re}(z) = 0$, 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 réel est un nombre complexe dont la partie imaginaire est nulle. Par conséquent, $\mathbb{R} \subseteq \mathbb{C}$.

Exemple. (1) $2 + 3i, 4 + 1i, \sqrt{2} + 0i, 0 + \sqrt{5}i, 0 + 0i, (-6) + (-7)i \in \mathbb{C}$.

(2) $\operatorname{Re}(\sqrt{2} + 0i) = \sqrt{2}$ et $\operatorname{Im}(\sqrt{2} + 0i) = 0$.

(3) $\operatorname{Re}((-6) + (-7)i) = -6$ et $\operatorname{Im}((-6) + (-7)i) = -7$.

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

Solution. Soient $a, b \in \mathbb{R}$ tels que $(a^2 - a) + (a + b^2)i = i$. Par définition, on a

$$\operatorname{Re}[(a^2 - a) + (a + b^2)i] = \operatorname{Re}(i) \text{ et } \operatorname{Im}[(a^2 - a) + (a + b^2)i] = \operatorname{Im}(i).$$

C'est-à-dire, $a^2 - a = 0$ et $a + b^2 = 1$. Comme $a(a - 1) = 0$, on a $a = 0$ ou $a - 1 = 0$. Si $a = 0$, alors $b = \pm 1$. Sinon, $a = 1$. Ainsi $b^2 = 0$, et donc $b = 0$. En conclusion, les couples (a, b) qu'on cherche sont les suivants:

$$a = 0, b = 1; a = 0, b = -1; a = 1, b = 0.$$

On définira les opérations arithmétiques sur 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. Pour tous $a, b \in \mathbb{R}$, on a

$$a + bi = (a) + (bi).$$

Exemple. $(\sqrt{2} + 3i) + (2 + (-4)i) = (\sqrt{2} + 2) + (3 + (-4))i = (2 + \sqrt{2}) + (-1)i.$

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 $z_1, z_2, \dots, z_n \in \mathbb{C}$ avec $n > 2$, on définit

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

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

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

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

Démonstration. Il est évident 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 de la proposition.

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

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

Exemple. $-0 = 0$ et $-(2 + (-3)i) = (-2) + (-(-3))i = (-2) + 3i.$

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

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

Soit v_1 un autre nombre complexe tel que $w + v_1 = z$. Alors $w + v_1 = w + v$. D'après la loi de simplification, on a $v_1 = v$. Ceci montre l'unicité de v . La preuve de la proposition s'achève.

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 $a + (-b)i = (a) - (bi)$. Par exemple, $5 + (-3)i = 5 - 3i$.

Exemple.

$$(\sqrt{2} + 3i) - (2 + 4i) = (\sqrt{2} - 2) + (3 - 4)i = (\sqrt{2} - 2) + (-1)i = (\sqrt{2} - 2) + (-i).$$

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

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

Remarque. (1) Si $a, b \in \mathbb{R}$, alors $a \cdot b = ab$.

(2) S'il n'y a aucun risque de confusion, on écrit $z \cdot w = zw$.

(3) Si $a, b \in \mathbb{R}$, alors $a + bi = (a) + (b \cdot i)$.

Exemple. (1) $i \cdot i = (0 + 1i)(0 + 1i) = (0 \cdot 0 - 1) + (0 \cdot 1 + 1 \cdot 0)i = -1$.

(2) $(2 + 3i)(4 - 5i) = 23 + 2i$. Remarquons que

$$(2 + 3i)(4 - 5i) \neq (2 \cdot 4) + (3 \cdot (-5))i.$$

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) $(-1) \cdot z = -z$.
- (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 quatre énoncés découlent facilement des propriétés des nombres réels. On vérifiera seulement les trois derniers énoncés.

(5) On a $z + (-1) \cdot z = 1 \cdot z + (-1) \cdot z = [(1 + (-1))] \cdot z = 0 \cdot z = 0$. Par définition, $(-1) \cdot z = -z$.

(6) Posons $z = a + bi$ et $w = c + di$, où $a, b, c, d \in \mathbb{R}$. Par définition, on a

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

Supposons que $z = 0$. Par définition, $a = b = 0$. D'où, $ac - bd = 0$ et $ad + bc = 0$. Par définition, $z \cdot w = 0$. Si $w = 0$, alors $z \cdot w = w \cdot z = 0$. Ceci montre la nécessité.

Pour la suffisance, supposons que $z \cdot w = 0$ et $z \neq 0$. Par définition,

$$(*) \quad ac - bd = 0 \text{ et } ad + bc = 0.$$

D'où, $a^2c - abd = 0$ et $bad + b^2c = 0$. D'où, $(a^2 + b^2)c = 0$.

Maintenant, comme $z \neq 0$, on a $a \neq 0$ ou $b \neq 0$. Comme a, b sont réels, $a^2 + b^2 > 0$. En particulier, $a^2 + b^2 \neq 0$. Comme $(a^2 + b^2)c = 0$, on voit que $c = 0$. En vue des équations (*), on voit que $bd = 0$ et $ad = 0$. Ainsi, $(a^2 + b^2)d = 0$. Encore comme $a^2 + b^2 \neq 0$, on a $d = 0$. 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 $i \cdot i = -1$.

(2) En particulier, $r(a + bi) = (ra) + (rb)i$, pour tout $r \in \mathbb{R}$.

(3) Pour $z, w, v \in \mathbb{C}$, grâce à l'associativité, on peut définir

$$zvw := z(wv).$$

(4) En général, pour $z_1, z_2, \dots, z_n \in \mathbb{C}$ avec $n > 2$, on définit

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

Exemple. En utilisant la distributivité, on trouve

$$(2 + 3i)(3 - 2i) = 2(3 - 2i) + (3i)(3 - 2i) = 6 - 4i + 9i - 6i^2 = 6 + 5i - 6(-1) = 12 + 5i.$$

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 $q = \frac{w}{z}$.

Exemple. Comme $(2 + 3i)(3 - 2i) = 12 + 5i$, on a

$$3 - 2i = \frac{12 + 5i}{2 + 3i} \quad \text{et} \quad 2 + 3i = \frac{12 + 5i}{3 - 2i}.$$

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 particulier où z est réel.

1.1.10. Lemme. Soient $w, z \in \mathbb{C}$ avec z non nul.

(1) Si $w = a + bi$ et $z = r$ avec $a, b, r \in \mathbb{R}$, alors

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

(2) Si $v \in \mathbb{C}$ est non nul, alors $\frac{w}{z}$ existe si, et seulement si, $\frac{wv}{zv}$ existe. Et dans ce cas,

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

Démonstration. (1) D'après la proposition 1.1.8(3), on a

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

D'où,

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

(2) Supposons que $v \neq 0$. D'après la proposition 1.1.8(6), $zv \neq 0$. Si $q \in \mathbb{C}$, alors $q = \frac{w}{z}$ si, et seulement si, $w = zq$. Comme $v \neq 0$, on voit que $w = zq$ si, et seulement si, $wv = (zq)v = (zv)q$, c'est-à-dire,

$$q = \frac{wv}{zv}.$$

Ceci achève la démonstration du lemme.

Exemple.

$$\frac{2 - \sqrt{6}i}{\sqrt{2}} = \frac{2}{\sqrt{2}} - \frac{\sqrt{6}}{\sqrt{2}}i = \sqrt{2} - \sqrt{3}i.$$

Exercice. Calculer $\frac{3+i}{i}$.

Solution. Remarquons que $i \cdot i = -1 \in \mathbb{R}$. D'après le lemme 1.1.10(1), on a

$$\frac{(3+i) \cdot i}{i \cdot i} = \frac{-1+3i}{-1} = 1-3i.$$

D'après le lemme 1.1.10(2), on a

$$\frac{3+i}{i} = \frac{(3+i) \cdot i}{i \cdot i} = 1-3i.$$

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 par

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

Exemple.

$$\overline{2-3i} = 2+3i, \quad \overline{-\sqrt{2}+\sqrt{3}i} = -\sqrt{2}-\sqrt{3}i.$$

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) $z = 0$ si, et seulement si, $\bar{z} = 0.$
- (6) $z = \bar{z}$ si, et seulement si, $z \in \mathbb{R}.$

Démonstration. On ne montrera que les énoncés (4) et (6), car les autres énoncés sont faciles à vérifier.

(4) D'après la définition, on a

$$z \cdot \bar{z} = (a^2 - b(-b)) + (a(-b) + ba)i = (a^2 + b^2) + (-ab + ab)i = a^2 + b^2.$$

(6) Si $z = a + bi \in \mathbb{R}$, alors $b = 0$, et donc $z = a$. D'où, $\bar{z} = a - bi = a - 0i = a = z$. 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 de la proposition.

1.1.13. Proposition. Soient $z = a + bi, w = c + di \in \mathbb{C}$. Si $z \neq 0$, alors $\frac{w}{z}$ 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. Si $z \neq 0$, alors $\bar{z} \neq 0$ tel que

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

Or, d'après le lemme 1.1.10(2), on a

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

Ceci achève la démonstration.

Exemple.

$$\frac{3 + 5i}{2 - 3i} = \frac{(2 + 3i)(3 + 5i)}{(2 + 3i)(2 - 3i)} = \frac{6 + 9i + 10i - 15}{2^2 + 3^2} = \frac{-9 + 19i}{13} = -\frac{9}{13} + \frac{19}{13}i.$$

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

Exemple. L'inverse de $1 + i$ est

$$\frac{1}{1 + i} = \frac{1}{2} - \frac{i}{2}.$$

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'après la définition, $z \cdot z^{-1} = z \cdot \frac{1}{z} = 1$. 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,

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

Ceci achève la démonstration de la proposition.

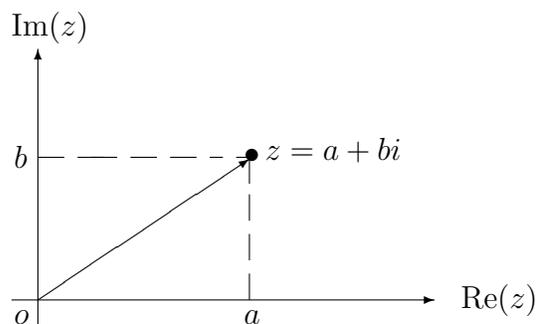
Exercice. Trouver l'inverse de $(2 + i)(3 - i)$.

Solution. D'après le lemme 1.1.15(3), on a

$$((2 + i)(3 - i))^{-1} = (2 + i)^{-1}(3 - i)^{-1} = \frac{1}{2 + i} \times \frac{1}{3 - i} = \frac{7}{50} - \frac{1}{50}i.$$

1.2. Représentation géométrique

Il est bien connu que les nombres réels peuvent être représentés par les points d'un axe. Le but de cette section est de représenter les nombres complexes d'une façon géométrique. Comme un nombre complexe dépend de deux variables indépendantes, c'est-à-dire, 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 $\text{Re}(z)$, et l'axe vertical est appelé *axe imaginaire*, noté $\text{Im}(z)$. 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.



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

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

ce qui est la racine carrée 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 .

Exemple. $|\sqrt{2} - 2i| = \sqrt{\sqrt{2}^2 + (-2)^2} = \sqrt{6}$.

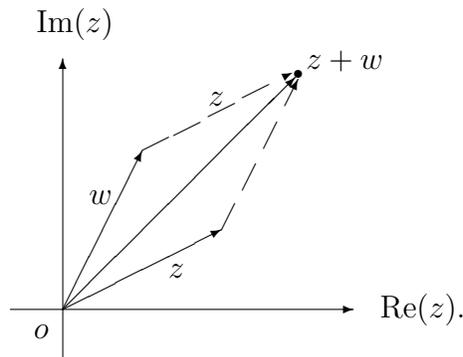
1.2.2. Lemme. Soient $z, w \in \mathbb{C}$.

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

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

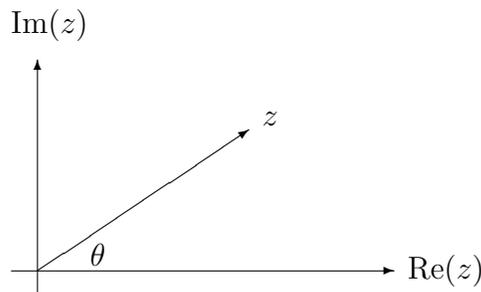
Démonstration. Posant $z = a + bi$, on a $|z| = \sqrt{a^2 + b^2}$. Alors $|z| = 0$ si, et seulement si, $|z|^2 = 0$ si, et seulement si, $a^2 + b^2 = 0$ si, et seulement si, $a^2 = 0$ et $b^2 = 0$ si, et seulement si, $a = 0$ et $b = 0$ si, et seulement si, $z = 0$. Ceci établit l'énoncé (1).

Ensuite, remarquons que la somme $z + w$ est représentée par la somme des vecteurs représentant z et w , illustré comme suit:



D'où, $|z + w| \leq |z| + |w|$. Ceci achève la démonstration.

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 $\theta = \text{Arg}(z)$, ce qui est illustré par



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 $k \in \mathbb{Z}$.

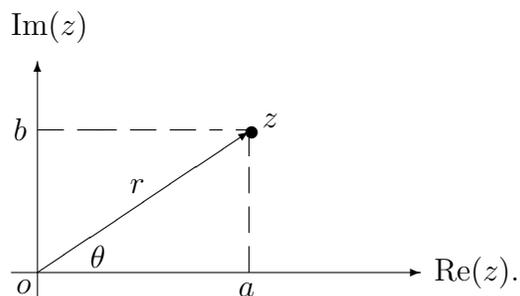
(2) Comme $\frac{\pi}{2}$ est un argument de i , l'angle $2k\pi + \frac{\pi}{2}$ l'est aussi, pour tout $k \in \mathbb{Z}$.

1.2.4. Proposition. 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 *forme polaire* de z .

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



Considérons le triangle droit de sommets $0, a$ et z . Par définition, $\cos \theta$ est le rapport entre la longueur du côté adjacent à θ et la longueur de l'hypoténuse. Et $\sin \theta$ est le rapport entre la longueur du côté opposé à θ et la longueur de l'hypoténuse. C'est-à-dire,

$$\cos \theta = \frac{a}{r}; \quad \sin \theta = \frac{b}{r}.$$

Ceci nous donne $a = r \cos \theta$ et $b = r \sin \theta$. Par conséquent,

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

La preuve de la proposition 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 $a, b \in \mathbb{R}$, s'appelle *forme algébrique* de z , ce qui est unique.

Exemple. Comme 1 et i sont de module 1 et ont pour argument 0 et $\frac{\pi}{2}$, respectivement, on voit que

$$1 = 1(\cos 0 + i \sin 0); \quad i = 1 \cdot (\cos \frac{\pi}{2} + i \sin \frac{\pi}{2})$$

sont formes polaires de 1 et de i , respectivement.

On étudiera comment trouver une forme polaire d'un nombre complexe non nul. Pour ce but, on fera 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 $k \in \mathbb{Z}$.

Exemple. (1) $\cos(\frac{\pi}{2} + \theta) = \cos \frac{\pi}{2} \cos \theta - \sin \frac{\pi}{2} \sin \theta = -\sin \theta$.

(2) $\sin(\frac{\pi}{2} + \theta) = \sin \frac{\pi}{2} \cos \theta + \cos \frac{\pi}{2} \sin \theta = \cos \theta$.

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

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

En outre, θ est un angle tel que

$$\cos \theta = \frac{r \cos \theta}{r} = \frac{a}{r}$$

et

$$\sin \theta = \frac{r \sin \theta}{r} = \frac{b}{r}.$$

Par définition, 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

$$r(\cos \theta + i \sin \theta) = s(\cos \phi + i \sin \phi)$$

si, et seulement si, $r = s$ et $\phi - \theta = 2k\pi$, pour un certain entier k .

Exemple. (1) On voit que

$$\sqrt{2}\left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3}\right), 3\left(\cos\left(-\frac{\pi}{5}\right) + i \sin\left(-\frac{\pi}{5}\right)\right)$$

sont des complexes sous la forme polaire.

(2) Aucun de complexes

$$(-2) \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right), 3 \left(\cos \frac{\pi}{3} - i \sin \frac{\pi}{3} \right), 4 \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{2} \right), 0 \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right)$$

n'est sous la forme polaire.

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) $\cos(\pi - \theta) = -\cos \theta;$ $\sin(\pi - \theta) = \sin \theta;$
- (2) $\cos(\pi + \theta) = -\cos \theta;$ $\sin(\pi + \theta) = -\sin \theta;$
- (3) $\cos(2\pi - \theta) = \cos \theta;$ $\sin(2\pi - \theta) = -\sin \theta.$

Exemple.

- (1) $(-2) \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right) = 2 \left(\cos(\pi + \frac{\pi}{3}) + i \sin(\pi + \frac{\pi}{3}) \right) = 2 \left(\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} \right).$
- (2) $5 \left(-\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) = 5 \left(\cos(\pi - \frac{\pi}{4}) + i \sin(\pi - \frac{\pi}{4}) \right) = 5 \left(\cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4} \right).$
- (3) $3 \left(\cos \frac{\pi}{6} - i \sin \frac{\pi}{6} \right) = 3 \left(\cos(-\frac{\pi}{6}) + i \sin(-\frac{\pi}{6}) \right).$

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

1.2.8. Théorème. 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

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

3. Un argument θ de z sera donné par

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

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

Exercice. Trouver une forme polaire de z , où

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

Solution. (1) $r = \sqrt{1^2 + 1^2} = \sqrt{2}$ et $\cos \phi = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$, $\sin \phi = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$. Donc $\phi = \frac{\pi}{4}$. Comme $a > 0$ et $b > 0$, on voit que ϕ est un argument de z . Ainsi

$$1 + i = \sqrt{2}(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})$$

est une forme polaire de z .

(2) $r = \sqrt{1^2 + (-\sqrt{3})^2} = 2$ et $\cos \phi = \frac{1}{2}$, $\sin \phi = \frac{\sqrt{3}}{2}$. Donc $\phi = \frac{\pi}{3}$. Comme $a > 0$ et $b < 0$, $\theta = 2\pi - \phi = \frac{5\pi}{3}$ est un argument de z . Ainsi

$$1 - \sqrt{3}i = 2 \left(\cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3} \right)$$

est une forme polaire de z .

La forme polaire facilite les opérations arithmétiques des nombres complexes.

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

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

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

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) et (3).

(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, $v = \frac{z}{w}$. Ceci achève la démonstration de la proposition.

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

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

Solution. On a vu que

$$1+i = \sqrt{2}(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4}), \quad 1-\sqrt{3}i = 2(\cos(-\frac{\pi}{3}) + i \sin(-\frac{\pi}{3})).$$

(1) D'après la proposition 1.2.9(2), on a premièrement

$$\frac{1+i}{1-\sqrt{3}i} = \frac{\sqrt{2}}{2} \left(\cos(\frac{\pi}{4} - (-\frac{\pi}{3})) + i \sin(\frac{\pi}{4} - (-\frac{\pi}{3})) \right) = \frac{\sqrt{2}}{2} (\cos \frac{7\pi}{12} + i \sin \frac{7\pi}{12}),$$

et ensuite,

$$(1+i)(1-\sqrt{3}i) = 2\sqrt{2} \left(\cos(\frac{\pi}{4} - \frac{\pi}{3}) + i \sin(\frac{\pi}{4} - \frac{\pi}{3}) \right) = 2\sqrt{2} \left(\cos(-\frac{\pi}{12}) + i \sin(-\frac{\pi}{12}) \right).$$

(2) D'après la partie (1), on a

$$(1+i)(1-\sqrt{3}i) = 2\sqrt{2} \left(\cos \frac{\pi}{12} - i \sin \frac{\pi}{12} \right) = (2\sqrt{2}) \cos \frac{\pi}{12} - (2\sqrt{2} \sin \frac{\pi}{12}) i.$$

De l'autre côté, à l'aide de la forme algébrique, on a

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

D'où,

$$2\sqrt{2} \cos \frac{\pi}{12} = 1 + \sqrt{3}; \quad -2\sqrt{2} \sin \frac{\pi}{12} = 1 - \sqrt{3}.$$

Par conséquent,

$$\cos \frac{\pi}{12} = \frac{1+\sqrt{3}}{2\sqrt{2}} = \frac{\sqrt{2}+\sqrt{6}}{4}; \quad \sin \frac{\pi}{12} = \frac{1-\sqrt{3}}{-2\sqrt{2}} = \frac{\sqrt{6}-\sqrt{2}}{4}.$$

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

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

$$(1) \quad |zw| = |z| \cdot |w|; \quad (2) \quad \text{Arg}(zw) = \text{Arg}(z) + \text{Arg}(w);$$

$$(3) \quad \left| \frac{z}{w} \right| = \frac{|z|}{|w|}; \quad (4) \quad \text{Arg} \left(\frac{z}{w} \right) = \text{Arg}(z) - \text{Arg}(w).$$

On définira les puissances d'un nombre complexe comme suit.

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 $z = r(\cos \theta + i \sin \theta)$, un nombre complexe 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 montrera 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

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

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

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

Enfin, pour tout $n \geq 1$,

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

Ceci achève la démonstration du théorème.

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

Solution. On a vu que $1 + i$ pour forme polaire

$$1 + i = \sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right).$$

D'après le théorème de de Moirve, on a

$$\begin{aligned} (1 + i)^{101} &= \sqrt{2}^{101} \left(\cos \frac{101}{4}\pi + i \sin \frac{101}{4}\pi \right) \\ &= 2^{50} \sqrt{2} \left[\cos \left(\frac{5\pi}{4} + 24\pi \right) + i \sin \left(\frac{5\pi}{4} + 24\pi \right) \right] \\ &= 2^{50} \sqrt{2} \left(\cos \frac{5\pi}{4} + i \sin \frac{5\pi}{4} \right) \\ &= 2^{50} \sqrt{2} \left(-\frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \right) = -2^{50} - 2^{50}i. \end{aligned}$$

1.2.13. Définition. Soient $z \in \mathbb{C}$ et $n \geq 1$ un entier. Si $w \in \mathbb{C}$ tel que $w^n = z$, alors w s'appelle *racine n -ième* de z ; et *racine carrée* ou *cubique* de z au cas $n = 2$ ou 3 respectivement.

Remarque. Pour tout $n \geq 1$, le complexe nul 0 a une seule racine n -ième, c'est-à-dire, 0 .

Exemple. Comme $i^2 = (-i)^2 = -1$, on voit que i et $-i$ sont deux racines carrées de -1 .

Afin de montrer que tout nombre complexe admet des racines n -ièmes, on rappelle le résultat bien connu suivant.

1.2.14. Lemme. Soit $n \geq 1$ un entier. Si $r \in \mathbb{R}^+$, alors il existe un unique $s \in \mathbb{R}^+$ tel que $s^n = r$. Ainsi, s est la seule racine n -ième réelle positive de r , et on note $s = \sqrt[n]{r}$.

Démonstration. Considérons la fonction $f(x) = x^n - r$ définie sur l'intervalle $[0, +\infty[$. 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, $f'(x) = nx^{n-1} > 0$ pour tout $x > 0$. Ainsi, $f(x)$ est strictement croissante 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 $\sqrt[n]{1} = 1$.

Pour étudier les racines n -ièmes de complexes en général, on acceptera sans preuve le résultat sur les entiers suivant, appelé *algorithme de division*.

1.2.15. Théorème. Soient a, b des entiers. Si $b > 0$, alors il existe deux entiers uniques q et r tels que

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

Remarque. (1) Les entiers q et r dans le théorème 1.2.15 s'appellent *quotient* et *reste*, respectivement, de a divisé par b . On note $q = q_b(a)$ et $r = r_b(a)$.

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

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

Solution. D'abord, en divisant 19 par 5 , on a $19 = 5 \times 3 + 4$. Donc

$$-19 = 5 \times (-3) - 4 = 5 \times (-3) - 5 + (5 - 4) = 5 \times (-4) + 1.$$

Ainsi $q_5(-19) = -4$ et $r_5(-19) = 1$.

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

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

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

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, \dots, 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

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

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, \dots, 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 $\phi = \frac{\theta + 2k\pi}{n} + 2q\pi$. D'après la proposition 1.2.5(4),

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

Ceci achève la démonstration du théorème.

Exercice. Trouver les racines carrées de i .

Solution. On écrit i sous forme polaire $i = 1 \cdot (\cos \frac{\pi}{2} + i \sin \frac{\pi}{2})$. D'après la proposition 1.2.16, les racines carrées de i sont

$$z_0 = \sqrt{1} \left(\cos \frac{\pi/2 + 0}{2} + i \sin \frac{\pi/2 + 0}{2} \right) = \cos \frac{\pi}{4} + i \sin \frac{\pi}{4} = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}$$

et

$$z_1 = \sqrt{1} \left(\cos \frac{\pi/2 + 2\pi}{2} + i \sin \frac{\pi/2 + 2\pi}{2} \right) = \cos \frac{5\pi}{4} + i \sin \frac{5\pi}{4} = -\frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2}.$$

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

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

qui partagent le cercle unité en secteurs égaux d'angle $\frac{2\pi}{n}$.

Démonstration. On a $1 = 1 \cdot (\cos 0 + i \sin 0)$. D'après le théorème 1.2.16, les racines n -ièmes de 1 sont

$$\cos \frac{0 + 2k\pi}{n} + i \sin \frac{0 + 2k\pi}{n} = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n},$$

pour $k = 0, 1, \dots, n - 1$. La preuve du corollaire s'achève.

Remarque. Pour tout entier $n \geq 1$, on appelle

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

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

Exemple. Les racines cubiques de l'unité sont

$$\cos 0 + i \sin 0 = 1; \quad \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i; \quad \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

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 *exponentielle* d'un nombre complexe z par

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

On accepte sans preuve le résultat suivant.

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

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 $z = r(\cos \theta + i \sin \theta)$, un complexe sous la forme polaire. D'après la proposition 1.2.18(2), on a

$$z = r e^{i\theta},$$

appelé *formule d'Euler* de z .

Exemple. (1) $1 - \sqrt{3}i = 2 \left(\cos\left(-\frac{\pi}{3}\right) + i \sin\left(-\frac{\pi}{3}\right) \right) = 2e^{-\frac{\pi}{3}i}$.

(2) $1 + i = \sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) = \sqrt{2} e^{\frac{\pi}{4}i}$.

(3) Les racines n -ièmes de l'unité sont

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

1.3. Corps

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

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

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

et d'une multiplication

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

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 un *zéro*, noté 0_K , tel que $a + 0_K = a$ pour tout $a \in K$.
- (4) Tout $a \in K$ a un *opposé*, noté $-a$, 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 *identité*, noté 1_K , avec $1_K \neq 0_K$, tel que $1_K \cdot a = a$ pour tout $a \in K$.
- (8) Tout $a \in K$ avec $a \neq 0_K$ admet un *inverse*, noté a^{-1} , tel que $a \cdot a^{-1} = 1_K$.

Les deux opérations sont compatibles:

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

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, par exemple, 0_K et 1_K .

- (2) Un corps K a un seul zéro et un seul identité.
- (3) 0_K est un opposé de 0_K ; et 1_K est un inverse de 1_K .
- (4) Pour $a, b \in K$, on définit *différence* entre a et b par

$$a - b = a + (-b).$$

- (5) Grâce à l'associativité, pour $a, b, c \in K$, on peut définir

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

- (6) En générale, pour a_1, a_2, \dots, a_n avec $n > 2$, on définit

$$a_1 + a_2 + \dots + a_n = (\dots((a_1 + a_2) + a_3) + \dots + a_{n-1}) + a_n.$$

Exemple. (1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps pour l'addition et la multiplication usuelles.

(2) \mathbb{Z} n'est pas un corps pour les opérations usuelles.

Le résultat suivant ramasse des 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) Par définition, 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.

Dès maintenant, on étudiera plus 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, les deux conditions suivantes sont satisfaites.

- (1) $1 \in K$.

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

Dans ce cas, K s'appelle *corps de nombres*.

Démonstration. La nécessité 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

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

et d'une multiplication

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

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

Démonstration. Soient $x = a + b\sqrt{2}, y = c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Alors

$$x \pm y = (a \pm c) + (b \pm d)\sqrt{2}, \quad xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Supposons maintenant que $y \neq 0$, c'est-à-dire, $c \neq 0$ ou $d \neq 0$. On veut montrer que $c - d\sqrt{2} \neq 0$. C'est vrai lorsque $d = 0$, car $c \neq 0$ dans ce cas. Considérons le cas où $d \neq 0$. Si $c - d\sqrt{2} = 0$, alors $\sqrt{2} = \frac{c}{d} \in \mathbb{Q}$, une contradiction. Donc $c - d\sqrt{2} \neq 0$ dans tous les cas. Par conséquent, $y(c - d\sqrt{2}) = c^2 - 2d^2 \neq 0$. Or

$$\frac{x}{y} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

D'après la proposition 1.3.3, $\mathbb{Q}[\sqrt{2}]$ est un corps. Ceci achève la démonstration.

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

Démonstration. Par définition, $1 \in K$. 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 $\mathbb{Z} \subseteq K$.

En outre, pour tous $m, n \in \mathbb{Z}$ avec $n \neq 0$, on a $\frac{m}{n} = mn^{-1} \in K$. D'où, $\mathbb{Q} \subseteq K$. Ceci achève la démonstration de la proposition.

Remarque. La proposition 1.3.4 dit que \mathbb{Q} est le plus petit corps de nombres.

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. Il est connu que 1 et n sont toujours diviseurs positifs de n . Si n n'a aucun d'autre diviseur positif, on dit alors que n est *premier*. Par exemple, 2, 3, 5, 7, 11, 13, et 17 sont premiers, mais 1, 4, 6, et 9 ne le sont pas.

On accepte sans preuve le résultat suivant.

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

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

Dans ce cas, $r_t = 1$. En outre, $r_i = px_i + ay_i$, avec $x_i, y_i \in \mathbb{Z}$, pour $i = 2, \dots, t$. En particulier,

$$px_t + ay_t = 1.$$

Remarque. Cette méthode pour résoudre l'équation entière

$$ax + by = 1$$

s'appelle *algorithme d'Euclide*.

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

$$29x + 11y = 1.$$

Solution. On effectue les divisions suivantes:

$$29 = 11 \times 2 + 7; \quad (1)$$

$$11 = 7 \times 1 + 4; \quad (2)$$

$$7 = 4 \times 1 + 3; \quad (3)$$

$$4 = 3 \times 1 + 1. \quad (4)$$

Ceci donne

$$\begin{aligned} 7 &\stackrel{(1)}{=} 29 \times 1 + 11 \times (-2); \\ 4 &\stackrel{(2)}{=} 29 \times (-1) + 11 \times 3; \\ 3 &\stackrel{(3)}{=} 29 \times 2 + 11 \times (-5); \\ 1 &\stackrel{(4)}{=} 29 \times (-3) + 11 \times 8. \end{aligned}$$

Le résultat suivant sera pratique dans le calcul du reste.

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 $r_p(b) = s$. Alors, $a = pc + r$ et $b = pd + s$, où $c, d \in \mathbb{Z}$.

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

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

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

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

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

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

Exemple. On sait que $r_5(157) = 2$ et $r_5(674) = 4$. D'après le lemme 1.3.6, on a

$$r_5(175 + 673) = r_5(2 + 4) = 1,$$

et

$$r_5(175 \times 673) = r_5(2 \times 4) = 3.$$

1.3.7. Théorème. Si p un nombre premier, alors

$$\mathbb{Z}_p = \{0, 1, \dots, p - 1\}$$

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. L'associativité de l'addition \oplus et celle de la multiplication \odot découlent du lemme 1.3.6. Soient $a, b, c \in \mathbb{Z}_p$.

(1) On a $a \oplus b = r_p(a + b) = r_p(b + a) = b \oplus a$ et $a \odot b = r_p(ab) = r_p(ba) = b \odot a$.

(2) De plus, $a \oplus 0 = r_p(a + 0) = a$ et $a \odot 1 = r_p(a \cdot 1) = a$.

(3) Si $a = 0$, alors $-a = 0 \in \mathbb{Z}_p$. Sinon, $0 < a < p$. 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, $-a = p - a \in \mathbb{Z}_p$.

(4) 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 $y = pq + r$, $0 \leq r < p$. 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 $0 \neq a \in \mathbb{Z}_p$,

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

(2) si $px + ay = 1$ avec $x, y \in \mathbb{Z}$, alors $a^{-1} = r_p(y)$.

On remarque que la théorie des corps finis est appliquée dans la 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. Calculer l'inverse de 7 dans le corps \mathbb{Z}_{19} .

Solution. D'abord, on résout l'équation $7x + 19y = 1$. À l'aide de l'algorithme d'Euclide, on trouve

$$7 \times (-8) + 3 \times 19 = 1.$$

Donc l'inverse de 7 dans \mathbb{Z}_{19} est le reste de -8 par 19. Comme $-8 = (-1) \times 19 + 11$, on a $7^{-1} = 11$.

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

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

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

Exemple. Dans le corps \mathbb{Z}_{19} , on a $7^{-1} = 11$. Par conséquent, $7^{-2} = 11^2 = 7$ et $7^{-3} = 7^{-2} \cdot 7^{-1} = 7 \cdot 11 = 1$.

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

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

où $n(\geq 0)$ est un entier, et $a_0, a_1, \dots, a_n \in K$.

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

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

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

Le produit de deux polynômes est défini ci-dessous.

1.4.2. Définition. Soient $f(x) = a_n x^n + \dots + a_1 x + a_0$ et $g(x) = b_m x^m + \dots + b_1 x + b_0$ deux polynômes sur K . On définit leur produit comme suit:

$$f(x)g(x) = c_{n+m}x^{n+m} + c_{n+m-1}x^{n+m-1} + \dots + c_1x + c_0,$$

où

$$c_k = \sum_{i+j=k} a_i b_j, \quad k = 0, 1, \dots, n+m.$$

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

Exemple. (1) Considérons deux polynômes $f(x) = 2x^3 - 3x + 2$ et $g(x) = 3x + 2$ sur \mathbb{Z}_5 . Alors

$$f(x)g(x) = (2x^3 - 3x + 2) \cdot (3x) + (2x^3 - 3x + 2) \cdot 2 = x^4 + 4x^3 + x^2 + 4.$$

(2) Pour $\alpha \in \mathbb{C}$, on voit aisément que

- (i) $(x + \alpha)(x - \alpha) = x^2 - \alpha^2$;
- (ii) $(x + \alpha)^2 = x^2 + 2\alpha x + \alpha^2$.

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

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

On appelle a racine de $f(x)$ lorsque $f(a) = 0_K$.

Notre but est de trouver, si possible, les racines d'un polynôme.

Exemple. (1) Considérons le polynôme réelle $f(x) = 3x^2 + 6$. Pour tout $a \in \mathbb{R}$, on a $f(a) = 3a^2 + 6 \geq 6$. En particulier, $f(a) \neq 0$. Ainsi, $f(x)$ n'a aucune racine dans \mathbb{R} .

(2) Considérons le polynôme complexe $f(x) = 3x^2 + 6$. On a

$$f(\sqrt{2}i) = 3(\sqrt{2}i)^2 + 6 = 3 \cdot 2 \cdot i^2 + 6 = -6 + 6 = 0.$$

Ainsi, $\sqrt{2}i$ est une racine de $f(x)$ dans \mathbb{C} . De même, on voit que $-\sqrt{2}i$ est aussi une racine complexe de $f(x)$.

(3) Considérons $h(x) = x^2 + 1$ sur $\mathbb{Z}_3 = \{0, 1, 2\}$. Comme $h(0) = 1$, $h(1) = 2$ et $h(2) = 2$, on voit que $h(x)$ n'a aucune racine dans \mathbb{Z}_3 .

Le résultat suivant est évident.

1.4.4. Lemme. Considérons un polynôme sur K comme suit:

$$f(x) = ax + b.$$

Si $a \neq 0$, alors $f(x)$ a une et une seule racine $c = -(a^{-1}b)$.

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

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

Solution. D'après le lemme 1.4.4, $f(x)$ a une seule racine

$$a = -(7^{-1} \cdot 3) = -(11 \cdot 3) = -14 = 5.$$

1.4.5. Lemme. Soit $f(x) = g(x)h(x)$, avec $g(x), h(x)$ des polynômes sur K . Alors $a \in K$ est une racine de $f(x)$ si, et seulement si, a est une racine de $g(x)$ ou $h(x)$.

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 sur \mathbb{Z}_{11} suivant:

$$f(x) = (x - 5)(x + 7).$$

Solution. D'après le lemme 1.4.4, la racine de $x - 5$ est 5, et celle de $x + 7$ est $-7 = 4$. D'après le lemme 1.4.5, les racines de $f(x)$ dans \mathbb{Z}_{11} sont 5 et 4.

Pour trouver les racines d'un polynôme, on réduit le degré du polynôme en utilisant le résultat suivant, dont la preuve est omise.

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 .

Remarque. On applique la proposition 1.4.6 pour trouver les racines d'un polynôme sur un corps fini par essai et erreur.

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

Solution. D'abord, $f(1) = 0$. En divisant $f(x)$ par $x - 1$, on trouve

$$f(x) = (x - 1)g(x), \text{ où } g(x) = x^3 + x^2 + 2x + 2.$$

Comme $g(-1) = 0$, en divisant $g(x)$ par $x + 1$, on trouve $g(x) = (x + 1)(x^2 + 2)$. Cela donne

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

Comme $a^2 + 2 \neq 0$ pour tout $a \in \mathbb{Z}_5$, on trouve $x^2 + 2$ n'a aucune racine dans \mathbb{Z}_5 . En conclusion, les racines de $f(x)$ dans \mathbb{Z}_5 sont 1 et 4.

Dès 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, \dots, 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 *algébriquement clos*.

Exemple. Soit $f(x)$ le polynôme complexe de degré 3 à coefficient directeur 3, dont les racines en comptant multiplicités sont $2 - i$, $2 - i$, et $3 + 2i$. Alors

$$f(x) = 3(x - (2 - i))^2(x - (3 + 2i)) = 3x^3 - 21x^2 + (57 - 6i)x - (52 - 18i).$$

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 , $k = 0, 1, \dots, n - 1$, où

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

est la racine n -ième primitive de l'unité. D'après le théorème 1.4.7, ils sont les seules racines de $f(x)$. Comme le coefficient directeur de $f(x)$ est 1, on a

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

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 complexe quadratique

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

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

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

Démonstration.

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

Ceci achève la démonstration de la proposition.

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

Solution. D'abord, $\Delta = 2^2 - 4 \cdot 3 \cdot 1 = -8$. Or $\sqrt{-8} = \sqrt{8 \cdot (-1)} = \sqrt{8}\sqrt{-1} = 2\sqrt{2}i$.

Donc les racines du polynôme sont

$$x_1 = \frac{-2 + 2\sqrt{2}i}{2 \cdot 3} = -\frac{1}{3} + \frac{\sqrt{2}}{3}i, \quad x_2 = \frac{-2 - 2\sqrt{2}i}{2 \cdot 3} = -\frac{1}{3} - \frac{\sqrt{2}}{3}i.$$

Ainsi

$$3x^2 + 2x + 1 = 3(x - x_1)(x - x_2) = (3x + 1 - \sqrt{2}i)(x + \frac{1}{3} + \frac{\sqrt{2}}{3}i).$$

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 est un entier et un diviseur de a_0 .

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

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

D'où,

$$a^n = b(-a_{n-1}a^{n-1} - \cdots + a_1b^{n-2}a - a_0b^{n-1}).$$

Ainsi, b divise a^n . Comme $\text{pgcd}(a, b) = 1$, on a $\text{pgcd}(a^n, b) = 1$. Ainsi $b = 1$, c'est-à-dire, $q = a \in \mathbb{Z}$. En outre, d'après l'égalité (*), on a

$$a_0 = a(-a^{n-1} - a_{n-1}a^{n-2} - \cdots - a_1).$$

D'où, a est un diviseur de a_0 . Ceci achève la démonstration de la proposition.

Exercice. Factoriser le polynôme rationnel

$$f(x) = x^3 - 4x^2 + x + 6.$$

Solution. D'abord, les diviseurs de 6 sont $\pm 1, \pm 2, \pm 3, \pm 6$. Par essai-erreur, on trouve que $f(-1) = 0$. En divisant $f(x)$ par $x - (-1) = x + 1$, on trouve

$$f(x) = (x + 1)(x^2 - 5x + 6).$$

En appliquant la proposition 1.4.8, on obtient

$$x^2 - 5x + 6 = (x - 2)(x - 3).$$

D'où

$$f(x) = (x + 1)(x - 2)(x - 3).$$

1.5. Exercices

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

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

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

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:

$$(1) \quad (2 + i)(2 - i); \quad (2) \quad \frac{2 - 2i}{1 + i}; \quad (3) \quad -3 \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right).$$

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. Dans chacun des cas suivants, trouver une forme du complexe donner.

$$(1) \quad z = -1; \quad (2) \quad w = -i.$$

9. Mettre premièrement sous la forme polaire et ensuite sous la formule d'Euler chacun des nombres complexes suivants:

$$(1) \quad \frac{1 + \sqrt{3}i}{2}; \quad (2) \quad \frac{-1 + \sqrt{3}i}{3}; \quad (3) \quad -2 \left(\cos \frac{\pi}{6} + i \sin \frac{\pi}{6} \right).$$

10. 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.

11. Dans chacun des cas suivants, calculer en utilisant la forme polaire et mettre le résultat final sous la forme algébrique:

$$(1) \quad (1 - i)^{100}; \quad (2) \quad \left(\frac{1 + \sqrt{3}i}{1 - i} \right)^{20}; \quad (3) \quad \frac{(-1 + \sqrt{3}i)^{15}}{(1 - i)^{20}} + \frac{(-1 - \sqrt{3}i)^{15}}{(1 + i)^{20}}.$$

12. Montrer, pour tout entier $n \geq 1$, les énoncés suivants:

$$(1) \quad (1+i)^n = \sqrt{2}^n \left(\cos \frac{n\pi}{4} + i \sin \frac{n\pi}{4} \right); \quad (2) \quad (\sqrt{3}-i)^n = 2^n \left(\cos \frac{n\pi}{6} - i \sin \frac{n\pi}{6} \right).$$

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

14. 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 $n \geq 0$.

15. Montrer les égalités trigonométriques suivantes:

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

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.

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

17. (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-ièmes de l'unité.

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

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

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

19. 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.

20. Montrer, pour tout angle θ , que

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

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

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

22. Considérer $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. En sachant que $\sqrt{2}, \sqrt{5}, \sqrt{10} \notin \mathbb{Q}$,

(1) vérifier que $\mathbb{Q}[\sqrt{5}]$ est un corps de nombres;

(2) calculer $\frac{1 - \sqrt{5}}{2 + \sqrt{5}}$;

(3) vérifier que $\sqrt{2} \notin \mathbb{Q}[\sqrt{5}]$.

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

24. En sachant que 101 est premier, à l'aide de l'algorithme d'Euclide, trouver des entiers x, y tels que

$$101x + 35y = 1.$$

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

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c).$$

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

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

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

31. 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.

32. Trouver les racines des polynômes suivants:

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

(2) $x^4 + (1 - i)$. *Indice:* Utiliser le théorème 1.2.16.

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

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

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

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

Indice: Remarquer premièrement que $x^6 - 4x^3 + 1 = (x^3 - 2)^2 - 3$, et ensuite appliquer le numéro 17.

35. 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.

36. Soit un polynôme sur un corps K suivant:

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n).$$

Montrer que les racines de $f(x)$ dans K sont a_1, a_2, \dots, a_n . *Attention.* Il faut, en particulier, vérifier qu'il n'y pas d'autres racines que a_1, \dots, a_n .

Chapitre II: Matrices

Le but de ce chapitre est d'introduire les opérations arithmétiques sur les matrices et étudier leurs propriétés. 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 rectangulaire de mn éléments de K rangés sur m lignes et n colonnes comme suit:

$$\begin{array}{cccc} C_1 & C_2 & \cdots & C_n \\ \left(\begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{array} \right) & \begin{array}{l} L_1 \\ L_2 \\ \\ L_m \end{array} \end{array}$$

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

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

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

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

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

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

Une matrice sur \mathbb{Q} (respectivement, \mathbb{R}, \mathbb{C}) s'appelle *rationnelle* (respectivement, *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 les opérations arithmétiques sur 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 des opérations suivantes:

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

Exemple. Sur le corps \mathbb{Z}_5 , on a

- (1) $-\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} -2 & -1 \\ -0 & -3 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 0 & 2 \end{pmatrix};$
- (2) $2^{-1} \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} = 3 \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 \cdot 2 & 3 \cdot 1 \\ 3 \cdot 0 & 3 \cdot 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix};$
- (3) $\begin{pmatrix} 2 & 3 & 1 \\ 1 & 3 & 1 \end{pmatrix} - \begin{pmatrix} 4 & 2 & 1 \\ 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 2-4 & 3-2 & 1-1 \\ 1-3 & 3-4 & 1-2 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 0 \\ 3 & 4 & 4 \end{pmatrix}.$

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. (1) Grâce à l'associativité, pour $A, B, C \in M_{m \times n}(K)$, on peut définir

$$A + B + C = (A + B) + C.$$

(2) En générale, pour $A_1, \dots, A_r \in M_{m \times n}(K)$ avec $r > 2$, on définit

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

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

$$(a_1 \ a_2 \ \cdots \ a_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n =: \sum_{k=1}^n a_k b_k.$$

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

$$c_{ij} = (a_{i1} \ a_{i2} \ \cdots \ a_{in}) \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{pmatrix} = a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{in} b_{nj} =: \sum_{k=1}^n a_{ik} b_{kj},$$

pour tous $i = 1, \dots, m; j = 1, \dots, p$.

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 $AB \in M_n(K)$.

Exemple (1) Dans le calcul de la note finale du MAT153, les pondérations des devoirs, de l'examen intra et de l'examen final sont 15%, 35% et 50%, respectivement. Si les notes des devoirs, de l'examen intra et de l'examen final d'un étudiant sont 80, 56 et 75 respectivement, alors sa note finale est donnée par

$$80 \times 0,15 + 56 \times 0,35 + 75 \times 0,5 = (80, 56, 75) \begin{pmatrix} 0,15 \\ 0,35 \\ 0,50 \end{pmatrix}.$$

(2) Considérons les matrices complexes

$$A = \begin{pmatrix} 2 + 3i & 3 - i & \sqrt{2} \\ -2 & 3i & 0 \\ 1 + 2i & \sqrt{3} + i & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 2 - i & 2 - 3i \\ 0 & 3 + i \\ 3i & \sqrt{2} \end{pmatrix}.$$

Alors le (1,2)-terme de AB est le produit de la première ligne de A et la deuxième colonne de B , c'est-à-dire,

$$(2 + 3i \ 3 - i \ \sqrt{2}) \begin{pmatrix} 2 - 3i \\ 3 + i \\ \sqrt{2} \end{pmatrix} = (2 + 3i)(2 - 3i) + (3 - i)(3 + i) + \sqrt{2}\sqrt{2} = 25.$$

En outre, le (3,1)-terme de AB est le produit de la troisième ligne de A et la première colonne de B , c'est-à-dire,

$$(1 + 2i\sqrt{3} + i2) \begin{pmatrix} 2 - i \\ 0 \\ 3i \end{pmatrix} = 4 + 9i.$$

(3) Le produit suivant n'est pas défini.

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

(4)

$$\begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & -5 \\ -3 & 4 \end{pmatrix} \neq \begin{pmatrix} 2 \cdot 1 & 3 \cdot (-5) \\ 4 \cdot (-3) & 1 \cdot 4 \end{pmatrix}.$$

Pour définir une matrice identité, il est commode d'introduire le *symbole de Kronecker* δ_{ij} avec $i, j \in \mathbb{N}$ sur K , 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 la *matrice identité* d'ordre n comme étant

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

2.1.5. Proposition. Les énoncés suivants sont valides.

- (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. On ne vérifie que les deux premiers énoncés, car les preuves des autres énoncés sont faciles et laissées comme exercices.

(1) Posons $A = (a_{ij})_{m \times n}$. Par définition, $I_m = (\delta_{ij})_{m \times m}$ et $I_n = (\delta_{ij})_{n \times n}$. D'abord, on a $I_m A = (d_{ij})_{m \times n}$, où

$$d_{ij} = \sum_{k=1}^m \delta_{ik} a_{kj} = \sum_{k \neq i} \delta_{ik} a_{kj} + \delta_{ii} a_{ij} = \sum_{k \neq i} 0_K \cdot a_{kj} + 1_K \cdot a_{ij} = a_{ij},$$

pour tous $i = 1, \dots, m; j = 1, \dots, n$. Ainsi $I_m A = A$. Ensuite, on a $A I_n = (f_{ij})_{m \times n}$, où

$$f_{ij} = \sum_{k=1}^n a_{ik} \delta_{kj} = \sum_{k \neq j} a_{ik} \delta_{kj} + a_{ij} \delta_{jj} = \sum_{k \neq j} 0_K \cdot a_{ik} + a_{ij} \cdot 1_K = a_{ij},$$

pour tous $i = 1, \dots, m; j = 1, \dots, n$. Ainsi, $A I_n = A$.

(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

$$d_{il} = \sum_{k=1}^m a_{ik} b_{kl}, \quad i = 1, \dots, p; l = 1, \dots, n.$$

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 $1 \leq k \leq m$ et $1 \leq j \leq q$. 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 $(AB)C = A(BC)$. Ceci achève la démonstration de la proposition.

Remarque. (1) Si AB et BC sont définis, grâce à l'associativité, on peut définir

$$ABC := (AB)C.$$

(2) En générale, si A_1, \dots, A_r avec $r > 2$, sont des matrices telles que $A_i A_{i+1}$ est défini, pour $i = 1, \dots, r-1$, alors on définit

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

(3) La multiplication matricielle n'est pas commutative. Par exemple,

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}, \quad \text{mais} \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(4) Le produit AB peut être nul sans que A ou B soit nulle. Par exemple,

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0+0 & 0+0 \\ 0+0 & 0+0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Exemple. D'après la proposition 2.1.5(3), on a

$$\begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} = \frac{1}{2} \cdot \frac{\sqrt{2}}{2} \begin{pmatrix} \sqrt{3} & -1 \\ 1 & \sqrt{3} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \frac{\sqrt{2}}{4} \begin{pmatrix} \sqrt{3}-1 & -\sqrt{3}-1 \\ \sqrt{3}+1 & \sqrt{3}-1 \end{pmatrix}.$$

2.1.6. Puissance. Soit A une matrice carrée d'ordre n 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, $(AB)^r \neq A^r B^r$.

Exemple. (1) Pour tout entier $r \geq 0$, on voit que $I_n^r = I_n$.

(2) Sur le corps \mathbb{Z}_5 , on a

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

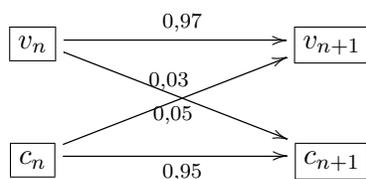
Exercice. Supposons que le nombre de résidents au Québec est constant et que chaque année, 3% des habitants en ville déménagent à la campagne et 5% des habitants à la campagne déménagent en ville. Vérifier que

$$\begin{pmatrix} v_n \\ c_n \end{pmatrix} = \begin{pmatrix} 0,97 & 0,05 \\ 0,03 & 0,95 \end{pmatrix}^n \begin{pmatrix} v_0 \\ c_0 \end{pmatrix},$$

où v_n et c_n avec $n \geq 0$, sont les nombres de résidents en ville et à la campagne n ans après cette année, respectivement.

Démonstration. Chaque année, 97% des habitants en ville restent en ville, et 95% des habitants à la campagne restent à la campagne. Pour tout $n \geq 0$, on a un diagramme comme

suit:



Ceci nous donne

$$v_{n+1} = 0,97 v_n + 0,05 c_n$$

$$c_{n+1} = 0,03 v_n + 0,95 c_n.$$

C'est-à-dire,

$$\begin{pmatrix} v_n \\ c_n \end{pmatrix} = \begin{pmatrix} 0,97 v_{n-1} + 0,05 c_{n-1} \\ 0,03 v_{n-1} + 0,95 c_{n-1} \end{pmatrix} = \begin{pmatrix} 0,97 \\ 0,03 \end{pmatrix} v_{n-1} + \begin{pmatrix} 0,05 \\ 0,95 \end{pmatrix} c_{n-1} = \begin{pmatrix} 0,97 & 0,05 \\ 0,03 & 0,95 \end{pmatrix} \begin{pmatrix} v_{n-1} \\ c_{n-1} \end{pmatrix}.$$

En particulier, on a

$$\begin{pmatrix} v_1 \\ c_1 \end{pmatrix} = \begin{pmatrix} 0,97 & 0,05 \\ 0,03 & 0,95 \end{pmatrix} \begin{pmatrix} v_0 \\ c_0 \end{pmatrix};$$

$$\begin{pmatrix} v_2 \\ c_2 \end{pmatrix} = \begin{pmatrix} 0,97 & 0,05 \\ 0,03 & 0,95 \end{pmatrix} \begin{pmatrix} v_1 \\ c_1 \end{pmatrix} = \begin{pmatrix} 0,97 & 0,05 \\ 0,03 & 0,95 \end{pmatrix}^2 \begin{pmatrix} v_0 \\ c_0 \end{pmatrix}.$$

En général, on a

$$\begin{pmatrix} v_n \\ c_n \end{pmatrix} = \begin{pmatrix} 0,97 & 0,05 \\ 0,03 & 0,95 \end{pmatrix}^n \begin{pmatrix} v_0 \\ c_0 \end{pmatrix}.$$

2.1.7. Définition. Une matrice carrée A d'ordre n est dite *nilpotente* si $A^r = 0_{n \times n}$ pour un certain entier $r \geq 1$.

Exemple. (1) La matrice nulle est nilpotente.

(2) La matrice rationnelle

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

est nilpotente. En effet,

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

Exercice. Vérifier que la matrice

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

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

Démonstration. En effet, on a vu que $A^4 = I$. Supposons au contraire que A est nilpotente, disons $A^r = 0$ pour un certain $r > 0$. Alors $A^{4r} = (A^4)^r = I^r = I$. Mais $A^{4r} = (A^r)^4 = 0^4 = 0$, une contradiction.

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 $D = \text{diag} \{d_{11}, \dots, d_{nn}\}$.

Exemple. (1) Toute matrice identité I_n est diagonale.

(2) Les matrices suivantes sont diagonales

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & \sqrt{5} \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

2.1.9. Proposition. Soient $D_1 = \text{diag} \{a_1, a_2, \dots, a_n\}$ et $D_2 = \text{diag} \{b_1, b_2, \dots, b_n\}$ des matrices diagonales sur K .

(1) $D_1 + D_2 = \text{diag} \{a_1 + b_1, a_2 + b_2, \dots, a_n + b_n\}$.

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

Démonstration. L'énoncé (1) est évident. D'après la définition, $D_1 D_2 = (c_{ij})_{n \times n}$, où

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

Ceci achève la démonstration.

Exemple. Considère les matrices diagonales sur \mathbb{Z}_3 :

$$D_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On a

$$D_1 + D_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad D_1 D_2 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

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

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 .

Exercice. À l'aide de la remarque ci-haut, trouver les transposées des matrices

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \end{pmatrix}; \quad B = \begin{pmatrix} 2 & 3 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}.$$

Solution. En transposant les lignes de A , on obtient

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

Ensuite, en transposant les colonnes de B , on obtient

$$\begin{pmatrix} 2 & 3 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 2 & 3 & 5 \\ 3 & 4 & 6 \end{pmatrix}.$$

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 $(AB)^T = B^T A^T$.

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 $1 \leq i \leq m$ et $1 \leq j \leq p$. Donc, $(AB)^T = (c'_{ij})_{p \times m}$ avec $c'_{ij} = c_{ji}$ pour tous $1 \leq i \leq p$ et $1 \leq j \leq m$.

D'autre part, $A^T = (a'_{ik})_{n \times m}$ avec $a'_{ik} = a_{ki}$ pour tous $1 \leq i \leq n$ et $1 \leq k \leq m$ et $B^T = (b'_{kj})_{p \times n}$ avec $b'_{kj} = b_{jk}$ pour tous $1 \leq k \leq p$ et $1 \leq j \leq n$. Donc $B^T A^T = (d_{ij})_{p \times m}$, 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 $1 \leq i \leq p$ et $1 \leq j \leq m$. Ainsi $B^T A^T = (AB)^T$. Ceci achève la démonstration de la proposition.

Exemple. Soient

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

On a

$$A^T = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad B^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \quad AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Maintenant,

$$B^T A^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = (AB)^T.$$

Remarquons que

$$A^T B^T = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

D'où, $(AB)^T \neq A^T B^T$.

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 $1 \leq i, j \leq n$;
- (2) *antisymétrique* si $A^T = -A$, ou bien, si $a_{ij} = -a_{ji}$ pour tous $1 \leq i, j \leq n$.

Remarque. (1) Une matrice diagonale est symétrique.

(2) La diagonale d'une matrice anti-symétrique sur \mathbb{C} est nulle. Mais c'est pas nécessairement vrai si le corps est fini. Par exemple, la matrice sur \mathbb{Z}_2 suivante est anti-symétrique:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Exemple. (1) Considérons les matrices suivantes:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 4 \\ 3 & 4 & 6 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 4 \\ 3 & -4 & 6 \end{pmatrix}.$$

On voit que

$$A^T = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 4 \\ 3 & 4 & 6 \end{pmatrix} = A \text{ et } B^T = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & -4 \\ 3 & 4 & 6 \end{pmatrix} \neq B.$$

Ainsi, A est symétrique et B ne l'est pas.

(2) Considérons les matrices suivantes:

$$C = \begin{pmatrix} 0 & 2 & 3 \\ -2 & 0 & -4 \\ -3 & 4 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 2 & 3 \\ -2 & 0 & 4 \\ -3 & -4 & 0 \end{pmatrix}.$$

On voit que

$$C^T = \begin{pmatrix} 0 & -2 & -3 \\ 2 & 0 & 4 \\ 3 & -4 & 0 \end{pmatrix} = -C \text{ et } D^T = \begin{pmatrix} 1 & -2 & -3 \\ 2 & 0 & -4 \\ 3 & 4 & 0 \end{pmatrix} \neq -D.$$

Ainsi, C est antisymétrique et D ne l'est pas.

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

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

Exemple. (1) $\text{tr}(0_{n \times n}) = 0_K$.

(2) On a, sur le corps \mathbb{Z}_3 ,

$$\text{tr} \begin{pmatrix} 0 & 2 & 1 \\ 1 & 1 & 2 \\ 0 & 2 & 2 \end{pmatrix} = 0 + 1 + 2 = 1 + 2 = 0.$$

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

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

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

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

Démonstration. On ne montrera que l'énoncé (1), car l'énoncé (2) est évident. 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

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

et

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

Donc $\text{tr}(AB) = \text{tr}(BA)$. 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 nuls, 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 un r -uplet (n_1, \dots, n_r) , avec $r \geq 1$ et $n_1, \dots, n_r > 0$, tel que $n = n_1 + n_2 + \dots + n_r$.

Exemple. On obtient des partages de 5 comme suit:

$$5; (4, 1); (1, 4); (3, 2); (2, 3); (3, 1, 1); (1, 3, 1); (1, 1, 1, 1, 1).$$

2.2.2. Définition. Soit $A = (a_{ij})_{m \times n} \in M_{m \times n}(K)$. Soient (m_1, \dots, m_r) un partage de m ; et (n_1, \dots, n_s) un partage de n . Posons $\hat{m}_0 = 0$ et $\hat{m}_p = \hat{m}_{p-1} + m_p$, en outre, $\hat{n}_0 = 0$ et $\hat{n}_q = \hat{n}_{q-1} + n_q$, pour $p = 1, \dots, r$; $q = 1, \dots, s$. Considérons les sous-matrices de A suivantes:

$$A_{pq} = (a_{ij})_{\hat{m}_{p-1} < i \leq \hat{m}_p; \hat{n}_{q-1} < j \leq \hat{n}_q}, p = 1, \dots, r; q = 1, \dots, s.$$

Cela donne un partage de A 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 (i, j) -bloc, pour $i = 1, \dots, r; j = 1, \dots, t$.

Remarque. Dans une matrice partagée,

- (1) les blocs dans la même colonne de blocs ont le même nombre de colonnes;
- (2) les blocs dans la même ligne de blocs ont le même nombre de lignes.

Exemple. Les matrices suivantes sont partagées en blocs:

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

Le résultat suivant dit comment utiliser la partage de matrices pour calculer le produit de matrices, dont la preuve est omise.

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 $1 \leq i \leq r; 1 \leq k \leq s; 1 \leq j \leq t$;
- (2) $AB = (C_{ij})_{r \times t}$, où

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

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

Exemple.

$$\left(\begin{array}{ccc|cc} 1 & -1 & 3 & 1 & 0 \\ 2 & 0 & -1 & 0 & 1 \\ \hline 1 & 2 & 3 & 2 & 0 \\ 2 & 3 & 4 & 5 & 3 \end{array} \right) \left(\begin{array}{cc|ccc} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{array} \right) = \left(\begin{array}{cc|ccc} 1 & 0 & 1 & -1 & 3 \\ 0 & 1 & 2 & 0 & -1 \\ \hline 2 & 0 & 1 & 2 & 3 \\ 5 & 3 & 2 & 3 & 4 \end{array} \right)$$

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, L_2, \dots, L_m sont les lignes de A , alors

$$(b_1 b_2 \cdots b_m)A = b_1 L_1 + b_2 L_2 + \cdots + b_m L_m.$$

(2) Si C_1, C_2, \dots, C_n sont les colonnes de A , alors

$$A \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = a_1 C_1 + a_2 C_2 + \dots + a_n C_n.$$

Démonstration. (1) On applique théorème 2.2.3 en partageant la matrice-ligne en colonnes et A en lignes comme suit:

$$(b_1 \ b_2 \ \dots \ b_m)A = (\ b_1 \ | \ b_2 \ | \ \dots \ | \ b_m \) \begin{pmatrix} \frac{L_1}{} \\ \frac{L_2}{} \\ \vdots \\ \frac{L_m}{} \end{pmatrix} = b_1 L_1 + b_2 L_2 + \dots + b_m L_m.$$

(2) On applique théorème 2.2.3 en partageant A en colonnes et la matrice-colonne en lignes comme suit:

$$A \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = (\ C_1 \ | \ C_2 \ | \ \dots \ | \ C_n \) \begin{pmatrix} \frac{a_1}{} \\ \frac{a_2}{} \\ \vdots \\ \frac{a_n}{} \end{pmatrix} = a_1 C_1 + a_2 C_2 + \dots + a_n C_n.$$

Ceci achève la démonstration du lemme.

Exemple.

$$(4i, 0) \begin{pmatrix} 3i & -3 & 1+i \\ 4 & i & \sqrt{2} \end{pmatrix} = (4i)(3i, -3, 1+i) + 0(4, i, \sqrt{2}) = (-12, -12i, -4 + 4i).$$

Le résultat suivant nous dit que le calcul du produit de deux matrices quelconques se ramène aux cas traités dans le lemme 2.2.4.

2.2.5. Lemme. Soient $A \in M_{m \times n}(K)$ et $B \in M_{n \times p}(K)$.

(1) Si B_1, B_2, \dots, B_p sont les colonnes de B , alors $AB = (AB_1, AB_2, \dots, AB_p)$.

(2) Si A_1, A_2, \dots, A_m sont les lignes de A , alors

$$AB = \begin{pmatrix} A_1 B \\ A_2 B \\ \vdots \\ A_m B \end{pmatrix}.$$

Démonstration. Pour montrer l'énoncé (1), on partage A en un seul bloc et B en colonnes ($B_1 \cdots B_p$). Pour montrer l'énoncé (2), on partage A en lignes et B un seul bloc. Maintenant, le résultat suit immédiatement du théorème 2.2.3. Ceci achève la démonstration du lemme.

Exemple.

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

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 2 & 0 & 1 \\ 0 & 4 & -1 \end{pmatrix} = \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right).$$

2.2.6. Corollaire. Soient e_1, \dots, e_m les lignes de I_m , et soient e'_1, \dots, e'_n les colonnes de I_n . Si $A \in M_{m \times n}(K)$, alors

- (1) $e_i A$ est la i -ième ligne de A , pour $i = 1, \dots, m$;
- (2) $A e'_j$ est la j -ième colonne de A , pour $j = 1, \dots, n$;
- (3) $e_i A e'_j$ est le (i, j) -terme de A , pour $i = 1, \dots, m$ et $j = 1, \dots, n$.

Démonstration. Soient L_1, \dots, L_m les lignes et C_1, \dots, 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 $e_i A = L_i$, $i = 1, \dots, m$. En outre, on a

$$(C_1 \cdots C_n) = A = A I_n = A(e'_1, \dots, e'_n) = (A e'_1, \dots, A e'_n).$$

D'où $A e'_j = C_j$, $j = 1, \dots, n$. Ceci montre les énoncés (1) et (2).

Enfin, écrivons $A = (a_{ij})_{m \times n}$ avec $a_{ij} \in K$. D'après l'énoncé (1), $e_i A = L_i = (a_{i1}, \dots, a_{in})$, et d'après l'énoncé (2), $L_i e'_j$ est la j -ième colonne de L_i , c'est-à-dire, a_{ij} . Ceci achève la démonstration du corollaire.

Exemple.

$$(0 \ 1 \ 0 \ 0) \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \\ 4 & 5 & 6 \end{pmatrix} = (1 \ 2 \ 3), \quad \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 4 \\ 6 \end{pmatrix}.$$

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

2.2.7. Corollaire. Soit A une matrice de type $m \times n$ sur K .

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

$$A \begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix} = (a_1 C_1, \dots, a_n C_n).$$

(2) Si L_1, \dots, 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 $\text{diag}\{a_1, \dots, a_n\} = (a_1 e'_1 \ \cdots \ a_n e'_n)$. 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.

Exemple.

$$\begin{pmatrix} 3i & -3 & 1+i \\ 4 & i & \sqrt{2} \end{pmatrix} \begin{pmatrix} i & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix} = \begin{pmatrix} -3 & -9 & \sqrt{2} + \sqrt{2}i \\ 4i & 3i & 2 \end{pmatrix}.$$

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 carrée est diagonale si, et seulement si, elle est triangulaire supérieure et triangulaire inférieure.

Exemple. Considérons les matrices suivantes:

$$\begin{pmatrix} 2 & 0 & 0 \\ -3 & -1 & 0 \\ 5 & 2 & -3 \end{pmatrix}, \quad \begin{pmatrix} \sqrt{3} & 0 & 34 & 95 \\ 0 & 1+i & 0 & 5 \\ 0 & 0 & -3 & 2 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Alors la première est triangulaire inférieure, et la deuxième est triangulaire supérieure.

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:

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

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

$$A^2 = \begin{pmatrix} B^2 & BC \\ 0 & 0 \end{pmatrix}, \quad A^3 = \begin{pmatrix} B^3 & B^2C \\ 0 & 0 \end{pmatrix}, \quad \dots, \quad A^i = \begin{pmatrix} B^i & B^{i-1}C \\ 0 & 0 \end{pmatrix}.$$

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.

Exemple. Considérons la matrice

$$A = \begin{pmatrix} 0 & \sqrt{2} & 3 & 5 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & \sqrt{3} \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

D'après la proposition 2.2.9, $A^4 = 0_{4 \times 4}$.

2.3. Rang

Le but de cette section est d'introduire la notion du rang d'une matrice. On commence par les matrices échelonnées et les opérations élémentaires sur les lignes de matrices.

2.3.1. Définition. Soit A une matrice sur K de lignes L_1, \dots, L_m . On dit que A est *échelonnée* si, pour tout $i = 2, \dots, m$, la condition suivante est vérifiée:

Si L_i est non nulle dont le premier terme non nul se trouve dans la colonne j_i , alors L_{i-1} est non nulle donc le premier terme se trouve dans la colonne j_{i-1} avec $j_{i-1} < j_i$.

Dans ce cas, le premier terme non nul d'une ligne non nulle s'appelle *pivot* de cette ligne.

Remarque. Soit A une matrice échelonnée de type $m \times n$.

- (1) Une ligne nulle de A ne contient aucun pivot.
- (2) Chaque ligne, ainsi que chaque colonne, contient au plus un pivot. Par conséquent, le nombre de pivots de A est plus petit ou égal à $\min\{m, n\}$.

Exemple. (1) Une matrice-ligne est échelonnée.

(2) Une matrice nulle est échelonnée sans pivot.

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

(4) Les matrices suivantes sont échelonnées dont les pivots sont encadrés.

$$\begin{pmatrix} 0 & \boxed{1} \\ 0 & 0 \end{pmatrix}; \begin{pmatrix} \boxed{1} & 1 & 3 & 0 \\ 0 & \boxed{1} & 1 & -9 \\ 0 & 0 & \boxed{7} & 2 \end{pmatrix}; \begin{pmatrix} 0 & \boxed{3} & 2 & 1 & 0 \\ 0 & 0 & 0 & \boxed{5} & 0 \\ 0 & 0 & 0 & 0 & \boxed{-7} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}; \begin{pmatrix} \boxed{3} & 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & \boxed{9} & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

(5) Les matrices suivantes ne sont pas échelonnées:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 3 & 0 & 1 & 2 \\ 0 & 9 & 0 & 1 \\ 0 & 8 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{pmatrix}.$$

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 autre matrice B si cette dernière est obtenue à partir de la première par une suite finie d'opérations élémentaires sur les lignes.

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

Exemple.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \xrightarrow{L_2 \leftrightarrow L_3} \begin{pmatrix} 1 & 2 & 3 \\ 7 & 8 & 9 \\ 4 & 5 & 6 \end{pmatrix} \xrightarrow{2L_2} \begin{pmatrix} 1 & 2 & 3 \\ 14 & 16 & 18 \\ 4 & 5 & 6 \end{pmatrix} \xrightarrow{L_1 - 2L_3} \begin{pmatrix} -7 & -8 & -9 \\ 14 & 16 & 18 \\ 4 & 5 & 6 \end{pmatrix}.$$

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 $L_i \leftrightarrow L_j$ avec $i \neq j$, 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 $a^{-1}L_i$.

Démonstration. Soient A_1, A_2, \dots, A_m les lignes de A .

(1) On voit que

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} \xrightarrow{L_i \leftrightarrow L_j} \begin{pmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_i \\ \vdots \\ A_m \end{pmatrix} \begin{matrix} \leftarrow i\text{-ième} \\ \leftarrow j\text{-ième} \end{matrix} \xrightarrow{L_i \leftrightarrow L_j} \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} = A.$$

(2) On voit que

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} \xrightarrow{L_i + aL_j} \begin{pmatrix} A_1 \\ \vdots \\ A_i + aA_j \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} \xrightarrow{L_i - aL_j} \begin{pmatrix} A_1 \\ \vdots \\ A_i + aA_j - aA_j \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} = A.$$

(3) On voit que

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} \xrightarrow{aL_i} \begin{pmatrix} A_1 \\ \vdots \\ aA_i \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} \xrightarrow{a^{-1}L_i} \begin{pmatrix} A_1 \\ \vdots \\ a^{-1}(aA_i) \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} = A.$$

La preuve du lemme s'achève.

Exemple.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 7 & 8 & 9 & 12 \end{pmatrix} \xrightarrow{L_2 \leftrightarrow L_3} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 7 & 8 & 9 & 12 \\ 4 & 5 & 6 & 7 \end{pmatrix} \xrightarrow{L_2 \leftrightarrow L_3} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 7 & 8 & 9 & 12 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 7 & 8 & 9 & 12 \end{pmatrix} \xrightarrow{3L_2} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 12 & 15 & 18 & 21 \\ 7 & 8 & 9 & 12 \end{pmatrix} \xrightarrow{\frac{1}{3}L_2} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 7 & 8 & 9 & 12 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 7 & 8 & 9 & 12 \end{pmatrix} \xrightarrow{L_2 - 4L_1} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -3 & -6 & -9 \\ 7 & 8 & 9 & 12 \end{pmatrix} \xrightarrow{L_2 + 4L_1} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 7 & 8 & 9 & 12 \end{pmatrix}.$$

2.3.4. Proposition. Soient $A, B, C \in M_{m \times n}(K)$.

- (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 $A = 0_{m \times n}$ si, et seulement si, $B = 0_{m \times n}$.

Démonstration. Les deux premiers énoncés sont évidents. Et l'énoncé (3) est une conséquence immédiate du lemme 2.3.3.

Supposons enfin 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 de la proposition.

On a maintenant le résultat fondamental suivant, dont la preuve est omise.

2.3.5. Théorème. Toute matrice A sur K se réduit à une matrice échelonnée, appelée *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 le plus entier tel que la s -ième colonne est non nulle. En échangeant deux lignes si nécessaire, on peut supposer que $a_{1s} \neq 0$. En effectuant les opérations $L_2 - a_{1s}^{-1}a_{2s}L_1, \dots, L_m - a_{1s}^{-1}a_{ms}L_1$ 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 B , 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 , dont les pivots se trouvent dans les $n-s$ dernières colonnes. Maintenant, en effectuant les mêmes opérations élémentaires sur les $m-1$ dernières lignes de B , on obtient la matrice

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

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

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

Exemple.

$$(1) \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 7 & 8 & 9 & 12 \end{pmatrix} \xrightarrow[L_3-7L_1]{L_2-4L_1} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -3 & -6 & -9 \\ 0 & -6 & -12 & -16 \end{pmatrix} \xrightarrow{L_3-2L_2} \begin{pmatrix} \boxed{1} & 2 & 3 & 4 \\ 0 & \boxed{-3} & -6 & -9 \\ 0 & 0 & 0 & \boxed{2} \end{pmatrix}.$$

$$(2) \quad \begin{pmatrix} 0 & 2 & 4 & 2 & 10 \\ 0 & 1 & 2 & 2 & 7 \\ 0 & 1 & 2 & 1 & 5 \end{pmatrix} \xrightarrow{\frac{1}{2}L_1} \begin{pmatrix} 0 & 1 & 2 & 1 & 5 \\ 0 & 1 & 2 & 2 & 7 \\ 0 & 1 & 2 & 1 & 5 \end{pmatrix} \xrightarrow[L_3-L_1]{L_2-L_1} \begin{pmatrix} 0 & \boxed{1} & 2 & 1 & 5 \\ 0 & 0 & 0 & \boxed{1} & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

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

Remarque. Le rang d'une matrice échelonnée est le nombre de pivots, ou bien, le nombre de lignes non nulles.

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

Exercice. Trouver le rang de la matrice sur \mathbb{Z}_5 suivante:

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

Solution. On a

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 2 & 3 \\ 4 & 0 & 1 & 1 \end{pmatrix} \xrightarrow[L_3-4L_1]{L_2-2L_1} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 0 \\ 0 & 2 & 4 & 0 \end{pmatrix} \xrightarrow{L_3-L_2} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}.$$

Ainsi le rang de A est égal à 2.

2.3.7. Lemme. Soit A une matrice de type $m \times n$ sur K .

- (1) $\text{rg}(A) \leq \min\{m, n\}$.
- (2) $\text{rg}(A) = 0$ si, et seulement si, $A = 0_{m \times n}$.
- (3) Si A se réduit à B , alors $\text{rg}(A) = \text{rg}(B)$.
- (4) Si B est obtenue à partir de A en supprimant des lignes nulles, alors $\text{rg}(A) = \text{rg}(B)$.

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, $\text{rg}(A) \leq \min\{m, n\}$.

(2) Supposons que $\text{rg}(A) = 0$. Alors E n'a aucun pivot, c'est-à-dire, E est nulle. Comme A se réduit à E , d'après la proposition 2.3.4(4), A est nulle.

(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 $\text{rg}(B) = \text{rg}(A)$.

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

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

Ceci achève la démonstration du lemme.

Exercice. Calculer le rang de la matrice suivante

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 \\ 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & 0 \\ 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Solution. D'après le lemme 2.3.7(4), le rang de A est égal au rang de la matrice suivante:

$$B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 \end{pmatrix}.$$

Cette dernière se réduit à la matrice échelonnée suivante:

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

D'après le lemme 2.3.7(3), $\text{rg}(B) = \text{rg}(C) = 2$. D'où, $\text{rg}(A) = 2$.

On donnera une interprétation algébrique d'opérations élémentaires. Pour ce faire, on a besoin de la notion suivante.

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:

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

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

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

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

Exemple. En effectuant les opérations élémentaires $L_3 + 2L_1, (-3)L_2$ et $L_1 \leftrightarrow L_2$ à partir de I_3 , on obtient trois matrices élémentaires comme suit:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} = E_{31}(2); \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_2(-3); \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_{1,2}.$$

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 d'ordre m correspondante.

Démonstration. Soit A une matrice de lignes A_1, A_2, \dots, A_m . Soit e_i la i -ième ligne de I_m . D'après le corollaire 2.2.6(1), on voit que

$$E_{i,j}A = \begin{pmatrix} e_1 \\ \vdots \\ e_j \\ \vdots \\ e_i \\ \vdots \\ e_m \end{pmatrix} A = \begin{pmatrix} e_1A \\ \vdots \\ e_jA \\ \vdots \\ e_iA \\ \vdots \\ e_mA \end{pmatrix} = \begin{pmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_i \\ \vdots \\ A_m \end{pmatrix} \begin{matrix} \leftarrow i\text{-ième} \\ \\ \leftarrow j\text{-ième} \\ \\ \end{matrix}.$$

De la même façon, on trouve que

$$E_{ij}(a)A = \begin{pmatrix} e_1 \\ \vdots \\ e_i + ae_j \\ \vdots \\ e_m \end{pmatrix} A = \begin{pmatrix} e_1A \\ \vdots \\ e_iA + ae_jA \\ \vdots \\ e_mA \end{pmatrix} = \begin{pmatrix} A_1 \\ \vdots \\ A_i + aA_j \\ \vdots \\ A_m \end{pmatrix} \leftarrow i\text{-ième}.$$

$$E_i(a)A = \begin{pmatrix} e_1 \\ \vdots \\ ae_i \\ \vdots \\ e_m \end{pmatrix} A = \begin{pmatrix} e_1 A \\ \vdots \\ ae_i A \\ \vdots \\ e_m A \end{pmatrix} = \begin{pmatrix} A_1 \\ \vdots \\ aA_i \\ \vdots \\ A_m \end{pmatrix}.$$

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, \dots, E_2, E_1 telles que

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

Exemple.

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \xrightarrow{L_2 - 3L_1} \begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix} \xrightarrow{-\frac{1}{2}L_2} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \xrightarrow{L_1 - 2L_2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ainsi

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

2.4. Matrices inversibles

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 et égaux, A et B devraient être carrées de même ordre. Même si A est carrée d'ordre n et non nulle, il n'y a pas nécessairement une matrice B telle que $AB = BA = I_n$. Par exemple,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \neq I_2$$

pour tous $a, b, c, d \in K$.

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 s'appelle *inverse* de A , noté $B = A^{-1}$.

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

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

Ceci achève la démonstration du lemme.

Exemple. (1) I_n est inversible et $0_{n \times n}$ ne l'est pas.

(2) Comme

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

et

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

on a, par définition, que

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

(3) Comme on a vu, la matrice

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

n'est pas inversible.

(4) Considérons les matrices suivantes:

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

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

2.4.2. Lemme. (1) Si $A \in M_n(K)$ est inversible, alors A n'a ni ligne nulle ni colonne nulle; et en outre,

$$(A^{-1})^{-1} = A; (A^T)^{-1} = (A^{-1})^T.$$

(2) Si $A_1, \dots, A_r \in M_n(K)$ sont toutes inversibles, alors

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

Démonstration. (1) Supposons que $A \in M_n(K)$ est inversible. Si la i -ième ligne A_i de A est nulle, d'après le lemme 2.2.5, la i -ième ligne de AA^{-1} est égale à $A_i A^{-1} = 0$, ce qui est absurde. D'une façon similaire, A n'a aucune colonne nulle.

Et comme $A^{-1} \cdot A = A \cdot A^{-1} = I$, on voit que A^{-1} est inversible et $(A^{-1})^{-1} = A$. Enfin, comme $I = I^T = (A^{-1} \cdot A)^T = A^T(A^{-1})^T$ et $(A^{-1})^T A^T = I$, on voit que A^T est inversible et $(A^T)^{-1} = (A^{-1})^T$.

(2) Si $r = 2$, on a alors

$$(A_2^{-1}A_1^{-1})(A_1A_2) = A_2^{-1}(A_1^{-1}A_1)A_2 = A_2^{-1}IA_2 = A_2^{-1}A_2 = I.$$

De même, $(A_1A_2)(A_2^{-1}A_1^{-1}) = I$. Ainsi A_1A_2 est inversible avec

$$(A_1A_2)^{-1} = A_2^{-1}A_1^{-1}.$$

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 du lemme.

Exemple. On a vu que

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

D'après le lemme 2.4.2, on a

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^{-1} = \left(\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \right)^{-1} \right)^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

et

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}^{-1} &= \left(\left(\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^T \right)^{-1} \right)^{-1} = \left(\left(\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^{-1} \right)^T \right)^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

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. Si $AB = C$, alors $A^{-1}(AB) = A^{-1}C$. Donc $(A^{-1}A)B = A^{-1}C$. Ainsi $B = A^{-1}C$. Ceci montre l'énoncé (1). De même, si $BA = C$, alors $B = CA^{-1}$.

Si $AB = 0$, d'après l'énoncé (1), $B = A^{-1}0 = 0$. Ceci montre l'énoncé (3).

Si $AB = AC$, alors $A(B - C) = 0$. D'après l'énoncé (3), $B - C = 0$. C'est-à-dire, $B = C$. Ceci achève la démonstration du lemme.

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) D'après le lemme 2.3.3(1), $E_{i,j}$ se réduit à I_n par l'opération $L_i \leftrightarrow L_j$. Et d'après la proposition 2.3.9, $E_{i,j}E_{i,j} = I_n$. Par définition, $E_{i,j}^{-1} = E_{i,j}$.

(2) Pour tout $a \in K$, d'après le lemme 2.3.3(2), $E_{ij}(a)$ se réduit à I_n par l'opération $L_i - aL_j$. D'après la proposition 2.3.9, $E_{ij}(-a)E_{ij}(a) = I_n$. Remplaçant a par $-a$, on trouve $E_{ij}(-(-a))E_{ij}(-a) = I_n$, c'est-à-dire, $E_{ij}(a)E_{ij}(-a) = I_n$. D'où, $(E_{ij}(a))^{-1} = E_{ij}(-a)$.

(3) D'après le lemme 2.3.3(3), $E_i(a)$ se réduit à I_n par l'opération $a^{-1}L_i$. D'après la proposition 2.3.9, $E_i(a^{-1})E_i(a) = I_n$. Remplaçant a par a^{-1} , on trouve $E_i((a^{-1})^{-1})E_i(a^{-1}) = I_n$, c'est-à-dire, $E_i(a)E_i(a^{-1}) = I_n$. D'où, $(E_i(a))^{-1} = E_i(a^{-1})$. Ceci achève la démonstration.

Remarque. D'après le lemme 2.4.2(2), un produit de matrices élémentaires est inversible.

Exemple.

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

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

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 est inversible.

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, \dots, 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 du corollaire.

Exercice. Déterminer si la matrice suivante est inversible ou non:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 4 & 6 & 8 \end{pmatrix}.$$

Solution. On voit que

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 4 & 6 & 8 \end{pmatrix} \xrightarrow{L_3 - L_1} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 3 & 4 & 5 \end{pmatrix} \xrightarrow{L_3 - L_2} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 0 & 0 & 0 \end{pmatrix} =: B$$

Ayant une ligne nulle, B est non inversible. D'après le corollaire 2.4.5, A est non inversible.

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

Démonstration. Supposons que $\text{rg}(A) = n$. Alors $n \leq \min\{m, n\} \leq m$. Par définition, les n pivots de A se trouvent dans les premières n lignes. Soient $a_{1j_1}, a_{2j_2}, \dots, a_{nj_n}$ les pivots. Comme $1 \leq j_1 < j_2 < \dots < j_n \leq n$, on trouve $j_1 = 1, j_2 = 2, \dots, j_n = n$. C'est-à-dire, $a_{11}, a_{22}, \dots, a_{nn}$ sont les pivots. Ceci achève la démonstration du lemme.

Exemple. Voici une matrice échelonnée dont chaque colonne admet un pivot

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 9 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

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 des pivots à partir du dernier pivot.

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

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

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

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

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

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

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.

Exemple.

$$\begin{pmatrix} 1 & 2 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \xrightarrow{2^{-1}L_3} \begin{pmatrix} 1 & 2 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{\begin{matrix} L_2 - L_3 \\ L_1 + 2L_1 \end{matrix}} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{L_1 - 2L_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

2.4.8. Théorème. Soit $A \in M_n(K)$. Les conditions suivantes sont équivalentes:

- (1) A est inversible.
- (2) $\text{rg}(A) = n$.
- (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, $\text{rg}(A) = n$.

Supposons que $\text{rg}(A) = n$. 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, \dots, 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.

Exemple. (1) On effectue des réductions suivantes:

$$C = \begin{pmatrix} 1 & 2 & -2 \\ 1 & 3 & -1 \\ 2 & 1 & -5 \end{pmatrix} \xrightarrow[L_3-2L_1]{L_2-L_1} \begin{pmatrix} 1 & 2 & -2 \\ 0 & 1 & 1 \\ 0 & -3 & -1 \end{pmatrix} \xrightarrow{L_3+3L_2} \begin{pmatrix} 1 & 2 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix},$$

Ainsi $\text{rg}(C) = 3$. D'après le théorème 2.4.8, C est inversible.

(2) On effectue des réductions suivantes:

$$D = \begin{pmatrix} 1 & 2 & -2 \\ 1 & 3 & -1 \\ 2 & 5 & -3 \end{pmatrix} \xrightarrow[L_3-2L_1]{L_2-L_1} \begin{pmatrix} 1 & 2 & -2 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow{L_3-L_2} \begin{pmatrix} 1 & 2 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

Ainsi $\text{rg}(D) = 2 < 3$. D'après le théorème 2.4.8, D est non inversible.

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

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

Solution. On effectue des réductions suivantes:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \xrightarrow{L_2-3L_1} \begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix} \xrightarrow{-\frac{1}{2}L_2} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \xrightarrow{L_1-2L_2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ceci donne l'égalité suivante:

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

Ainsi

$$\begin{aligned} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & -\frac{1}{2} \end{pmatrix}^{-1} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

2.4.9. Théorème. Soient 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, \dots, 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 $(I_n | C)$. En outre, $(E_r \cdots E_1)A = I_n$ et $C = (E_r \cdots E_1)B$. Ainsi, $E_r \cdots E_1 = A^{-1}$, et donc, $C = A^{-1}B$. 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

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

Solution. On doit échelonner $(A | B)$ et $(A | I_2)$. Pour ce faire, on peut échelonner une matrice $(A | B | I_2)$ comme suit:

$$\begin{aligned} (A | B | I_2) &= \left(\begin{array}{cc|ccc|cc} 1 & 2 & 2 & 3 & 4 & 1 & 0 \\ 3 & 4 & 1 & 2 & 0 & 0 & 1 \end{array} \right) \xrightarrow{L_2-3L_1} \left(\begin{array}{cc|ccc|cc} 1 & 2 & 2 & 3 & 4 & 1 & 0 \\ 0 & -2 & -5 & -7 & -12 & -3 & 1 \end{array} \right) \\ &\xrightarrow{-\frac{1}{2}L_2} \left(\begin{array}{cc|ccc|cc} 1 & 2 & 2 & 3 & 4 & 1 & 0 \\ 0 & 1 & \frac{5}{2} & \frac{7}{2} & 6 & \frac{3}{2} & -\frac{1}{2} \end{array} \right) \xrightarrow{L_1-2L_2} \left(\begin{array}{cc|ccc|cc} 1 & 0 & -3 & -4 & -8 & -2 & 1 \\ 0 & 1 & \frac{5}{2} & \frac{7}{2} & 6 & \frac{3}{2} & -\frac{1}{2} \end{array} \right). \end{aligned}$$

Alors $(A | B)$ et $(A | I_2)$ s'échelonnent respectivement aux matrices suivantes:

$$\left(\begin{array}{cc|ccc} 1 & 0 & -3 & -4 & -8 \\ 0 & 1 & \frac{5}{2} & \frac{7}{2} & 6 \end{array} \right) \text{ et } \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array} \right).$$

D'où,

$$A^{-1}B = \begin{pmatrix} -3 & -4 & -8 \\ \frac{5}{2} & \frac{7}{2} & 6 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}.$$

2.5. Exercices

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

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

2. Considérer les matrices sur le corps \mathbb{Z}_{19} suivantes:

$$A = \begin{pmatrix} 1 & 3 & 5 & 7 & 9 & 11 \\ 0 & 2 & 4 & 6 & 8 & 10 \\ 1 & 6 & 5 & 8 & 9 & 12 \\ 13 & 5 & 7 & 9 & 11 & 17 \end{pmatrix}; \quad B = \begin{pmatrix} 3 & 2 & 1 & 9 \\ 0 & 2 & 4 & 6 \\ 1 & 5 & 7 & 8 \\ 5 & 9 & 2 & 15 \\ 5 & 7 & 9 & 11 \\ 7 & 11 & 0 & 13 \end{pmatrix}.$$

Trouver le $(4, 3)$ -terme du produit AB .

3. Calculer les produits de matrices complexes suivants:

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

$$(2) \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{10}} & \frac{1}{\sqrt{15}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{10}} & -\frac{1}{\sqrt{15}} \\ 0 & \frac{2}{\sqrt{10}} & \frac{3}{\sqrt{15}} \\ 0 & \frac{2}{\sqrt{10}} & -\frac{2}{\sqrt{15}} \end{pmatrix} \begin{pmatrix} \frac{2}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{5}{\sqrt{10}} & \frac{2}{\sqrt{10}} \\ 0 & 0 & \frac{3}{\sqrt{15}} \end{pmatrix}.$$

4. 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 $B \neq C$.

5. Considérer les matrices rationnelles suivantes:

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

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

6. Supposer que le nombre de résidents du Québec est constant; et chaque année, 2% des habitants en ville déménagent à la campagne, et 4% des habitants à la campagne déménagent en ville. Si les nombres de personnes qui habitaient en ville et à la campagne en 2000 étaient 5 millions et 2 millions respectivement, quels seront les nombres de personnes qui habiteront en ville et à la campagne en 2003?

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

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

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

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

8. (1) Montrer, pour toute matrice $A \in M_n(K)$ et tout entier $r > 0$, que

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

Indice: Utiliser la partie (1) du numéro 7.

(2) Vérifier que la matrice rationnelle A est nilpotente, où

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

(3) Calculer la matrice rationnelle B^r , où $r > 2$ et

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

Indice: Remarquer que $B = I_3 + A$ et appliquer les parties (1) et (2).

9. 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

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

10. (1) Considérer deux matrices symétriques suivantes:

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

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

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

11. 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.

12. 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.

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

14. 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 .

15. À l'aide de la multiplication par blocs, calculer le produit suivant:

$$\begin{pmatrix} 2 & 3 & 17 & 2 & 5 & 2 \\ 5 & 6 & 0 & 13 & 3 & 1 \\ 0 & 4 & 7 & 6 & 0 & 3 \\ 13 & 0 & 0 & 7 & 0 & 7 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

16. À l'aide des lemmes 2.2.4 et 2.2.5, donner la deuxième ligne, ainsi que la troisième colonne, du produit de matrices complexes suivant :

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

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

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

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

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

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

19. 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 $i \neq j$.
20. Soit $A = (a_{ij})_{n \times n}$ une matrice carrée d'ordre n sur K . Montrer, pour tous $x_1, \dots, x_n; y_1, \dots, y_n \in K$, que

$$(x_1, \dots, x_n)A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \sum_{1 \leq i, j \leq n} a_{ij} x_i y_j.$$

21. 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

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

22. 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.

23. 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 précédent.

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

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

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

26. Considérer la matrice carrée sur K d'ordre $n + 1$ suivante :

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

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

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

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

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

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

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

29. Soient $A = (A_1 \cdots A_n)$ et $B = (B_1 \cdots B_n)$ deux matrices sur K 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 $j_1, \dots, j_r \in \{1, \dots, n\}$. Si A se réduit à B , montrer que A' se réduit à B' . *Indice:* Utiliser le numéro précédent et appliquer la multiplication par blocs.

30. 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.

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

32. Dans chacun des cas suivants, vérifier la matrice est élémentaire en indiquant l'opération élémentaire à laquelle la matrice correspond, et donner l'inverse de la matrice à l'aide du lemme 2.4.4.

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

33. Soit une matrice diagonale $D = \{a_1, \dots, a_n\}$, où $a_1, \dots, a_n \in K$. Montrer que D est inversible si et seulement si a_1, \dots, a_n sont tous non nuls; et dans ce cas, trouver D^{-1} . *Indice:* Appliquer le lemme 2.4.2 pour la première partie; et appliquer la proposition 2.1.9(2) pour la deuxième partie.

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

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

35. 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.

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

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

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

37. 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 $B = PA$.

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

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

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

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

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

40. Trouver une matrice X telle que

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

41. 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 .

42. 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.

43. 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 $C_i = A^{-1}B_i$, $i = 1, \dots, r$.

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

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

45. 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 $(I - A)^{-1} = I + A + \dots + A^{r-1}$.

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

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

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

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

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

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

48. 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 $i = 1, \dots, n$, montrer que A est inversible. *Indice:* Procéder par récurrence en utilisant le numéro 45.

49. 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 .

50. 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 des sciences et du génie se ramènent au problème de la résolution de systèmes d'équations linéaires. Dans ce chapitre, on étudiera les propriétés et la résolution des 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:

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

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

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

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 des 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. (1) Considérons un système de deux équations linéaires à deux inconnues x et y sur \mathbb{R} suivant:

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

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

(2) Considérons le système sur \mathbb{Z}_3 comme suit:

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

On vérifie facilement que $(0, 0)$, $(2, 1)$ et $(1, 2)$ sont des solutions de ce système.

(3) Le système complexe

$$\begin{aligned}\sqrt{2}x + (1+i)y &= 1 \\ x + (1-i)y &= 0 \\ 0y &= 0\end{aligned}$$

est équivalent au système

$$\begin{aligned}\sqrt{2}x + (1+i)y &= 1 \\ x + (1-i)y &= 0.\end{aligned}$$

(4) Le système rationnel suivant est incompatible:

$$\begin{aligned}x + y &= 1 \\ x + y &= 2.\end{aligned}$$

(5) Les équations suivantes ne sont pas linéaires:

$$(a) \quad x + y^2 = 1; \quad (b) \quad |x| + 2y = 2; \quad (c) \quad \cos x + \sin x = 1.$$

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

3.2. Définition. Soit un système d'équations linéaires sur K :

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

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 *matrice de coefficients* et *matrice augmentée* du système respectivement.

Remarque. (1) Un système d'équations linéaires est uniquement déterminé par sa matrice augmentée.

Démonstration. Un n -uplet (s_1, s_2, \dots, s_n) avec $s_i \in K$, est une solution du système (*) si, et seulement si,

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

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,

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

si, et seulement si,

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

est une solution de l'équation matricielle (**). Ceci achève la démonstration du lemme.

Exemple. Le système complexe d'équations linéaires

$$\begin{array}{rclcl} 2x & & - & z & = & 1 - i \\ x & - & 2y & & = & 1 + i \\ 2x & & - & 2z & = & 5 + i \\ & & & 0z & = & 0 \end{array}$$

est équivalent à l'équation matricielle

$$\begin{pmatrix} 2 & 0 & -1 \\ 1 & -2 & 0 \\ 2 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 - i \\ 1 + i \\ 5 + i \\ 0 \end{pmatrix}.$$

On vérifie que

$$\begin{pmatrix} -\frac{3}{2} - \frac{3}{2}i \\ -\frac{5}{4} - \frac{5}{4}i \\ -4 - 2i \end{pmatrix}$$

est une solution de l'équation matricielle, et donc

$$\left(-\frac{3}{2} - \frac{3}{2}i, -\frac{5}{4} - \frac{5}{4}i, -4 - 2i \right)$$

est une solution du système complexe.

Dès maintenant, un système de m équations linéaires à n inconnues sur K 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 $m \times 1$ sur K . 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;
- (2) trouver toutes les solutions s'il est compatible.

On commence par un cas spécial où la matrice des coefficients d'un système est inversible.

3.4. Proposition. Soit un système d'équations linéaires

$$AX = B,$$

où $A \in M_n(K)$ et $B \in M_{n \times 1}(K)$. 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 démonstration de la proposition.

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

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

Solution. D'après l'hypothèse, on a

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 3 & -1 & 1 \\ 1 & 4 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 6 \\ 0 \\ -6 \end{pmatrix}.$$

Pour vérifier A est inversible et trouver la solution, on doit échelonner A et $(A \mid B)$. Pour ce faire, on échelonne $(A \mid B)$ comme suit:

$$\left(\begin{array}{ccc|c} 1 & -1 & 1 & 6 \\ 3 & -1 & 1 & 0 \\ 1 & 4 & -1 & -6 \end{array} \right) \Rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & -3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 11 \end{array} \right).$$

En particulier, A s'échelonne à

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

D'où, $\text{rg}(A) = 3$, et donc, A est inversible. D'après la proposition 3.4, le système a une seule solution donnée par

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A^{-1}B = \begin{pmatrix} -3 \\ 2 \\ 11 \end{pmatrix}.$$

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

3.5. Définition. Un système d'équations linéaires

$$AX = B$$

est dit *échelonné* si $(A \mid B)$ est échelonnée. Dans ce cas, une inconnue du système est dite *libre* si aucun de ses coefficients n'est un pivot.

Exemple. (1) Le système

$$\begin{array}{rcccccc} 2x_1 & + & x_2 & - & x_3 & + & 2x_4 & - & x_5 & = & 0 \\ & & & & 5x_3 & + & x_4 & + & 5x_5 & = & -1 \\ & & & & & & 7x_4 & & & = & -8 \end{array}$$

est échelonné, car la matrice augmentée

$$\left(\begin{array}{ccccc|c} 2 & 1 & -1 & 2 & -1 & 0 \\ 0 & 0 & 5 & 1 & 5 & -1 \\ 0 & 0 & 0 & 7 & 0 & -8 \end{array} \right)$$

est échelonnée. On voit que les inconnues libres sont x_2 et x_5 .

(2) Le système

$$0x_1 + 3x_2 - 4x_3 - 5x_4 + x_5 = 1$$

est échelonné dont les inconnues libres sont x_1, x_3, x_4 et x_5 .

(3) Le système

$$\begin{array}{rcccccc} x & - & 2y & + & z & = & 3 \\ & & 5y & - & 5z & = & -15 \\ & & & & -2z & = & -4 \end{array}$$

est échelonné n'ayant aucune inconnue libre.

(4) Les systèmes suivants ne sont pas échelonnés.

$$\begin{array}{rcccc} x & + & y & - & z & = & 0 \\ & & 3y & + & z & = & 1 \\ & & y & + & z & = & 3, \end{array} \quad \begin{array}{rcccc} x & + & y & - & z & = & 0 \\ & & 3y & + & z & = & 5 \\ & & 2x & & + & z & = & 3. \end{array}$$

3.6. Lemme. Soit un système échelonné d'équations linéaires à n inconnues:

$$AX = B.$$

Alors les énoncés suivants sont valides.

- (1) A est échelonnée, dont les pivots sont des pivots de $(A | B)$.
- (2) $\text{rg}(A) \leq \text{rg}(A | B)$ et $\text{rg}(A) \leq n$.
- (3) $\text{rg}(A) < \text{rg}(A | B)$ si, et seulement si, B contient un pivot de $(A | B)$;
- (4) Le nombre d'inconnues libres du système est égal à $n - \text{rg}(A)$.

Démonstration. Posons $A = (a_{ij})_{m \times n}$ et $B = (b_i)_{m \times 1}$. Soient A_1, \dots, A_m les lignes de A . Alors les lignes de $(A | B)$ sont $(A_1 | b_1), \dots, (A_m | b_m)$.

(1) Supposons que $A_i \neq 0$, dont le premier terme non nul est a_{i,j_i} avec $j_i \leq n$. Alors $(A_i | b_i) \neq 0$, dont le pivot est aussi a_{i,j_i} . Comme $(A | B)$ est échelonnée, $(A_{i-1} | b_{i-1}) \neq 0$, 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 premier terme non nul est $a_{i-1,j_{i-1}}$ avec $j_{i-1} < j_i$. Ceci montre que A est échelonnée, dont les pivots sont des pivots de $(A | B)$.

(2) D'après l'énoncé (1), $\text{rg}(A) \leq \text{rg}(A | B)$. Comme A a n colonnes, $\text{rg}(A) \leq n$.

(3) Si B contient un pivot de $(A | B)$, alors $(A | B)$ a un pivot de plus que A . D'où, $\text{rg}(A) < \text{rg}(A | B)$. Supposons réciproquement que $\text{rg}(A) < \text{rg}(A | B)$. Alors $(A | B)$ a une ligne non nulle $(A_r | b_r)$, dont le pivot n'est pas un pivot de A , et donc, ce pivot est b_r . C'est-à-dire, B contient un pivot de $(A | B)$.

(4) Il est évident que $n = s + t$, où s est le nombre d'inconnues libres et t est le nombre d'inconnues non libres. Par définition, une inconnue x_j avec $1 \leq j \leq n$ est non libre si, et seulement si, la j -ième colonne de A contient un pivot. 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 $\text{rg}(A) < \text{rg}(A | B)$. Posons $B = (b_i)_{n \times 1}$. D'après le lemme 3.6(3), B contient un pivot, disons b_r , de $(A | B)$. Alors la r -ième ligne de $(A | B)$ est de la forme $(0 \cdots 0 | b_r)$, c'est-à-dire, la r -ième équation du système est de la forme

$$0x_1 + \cdots + 0x_n = b_r.$$

Comme $b_r \neq 0$, cette équation n'a aucune solution; et donc, le système n'a aucune solution. Ceci achève la démonstration du lemme.

Exemple. Considérons le système échelonné suivant:

$$\begin{array}{rclcl} 2x & - & y & - & 2z & = & 1 \\ & & 2y & - & 3z & = & 0 \\ & & & & 0z & = & 2 \\ & & & & 0z & = & 0. \end{array}$$

La matrice augmentée est

$$(A | B) = \left(\begin{array}{ccc|c} 2 & -1 & -2 & 1 \\ 0 & 2 & -3 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{array} \right).$$

Comme $\text{rg}(A) = 2 < 3 = \text{rg}(A \mid B)$, d'après la proposition 3.7, le système est incompatible.

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

3.8. Lemme. Soit un système échelonné de m équations linéaires à n inconnues

$$AX = B.$$

Si $\text{rg}(A) = \text{rg}(A \mid B) = n$, alors le système admet une et une seule solution, ce qui peut être trouvée par substitution à partir de la dernière équation non nulle.

Démonstration. Supposons que $\text{rg}(A) = \text{rg}(A \mid B) = n$. En particulier, aucune inconnue n'est libre. En outre, A est échelonnée de n pivots. D'après le lemme 2.4.6, les pivots de A sont $a_{11}, a_{22}, \dots, a_{nn}$. Comme B ne contient aucun pivot de $(A \mid B)$, le système est de la forme

$$\begin{array}{rcccccl} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ & & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & \ddots & & & & \vdots \\ & & & & & & a_{nn}x_n & = & b_n \\ & & & & & & 0 & = & 0 \\ & & & & & & & & \vdots \\ & & & & & & 0 & = & 0. \end{array}$$

Ceci est évidemment équivalent au système échelonné suivant:

$$\begin{array}{rcccccl} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ & & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & \ddots & & & & \vdots \\ & & & & & & a_{nn}x_n & = & b_n. \end{array}$$

Comme $a_{11}, a_{22}, \dots, a_{nn}$ sont tous non nuls, la matrice des coefficients de ce dernier système est inversible. D'après la proposition 3.4, il admet une seule solution. D'après la dernière équation, on trouve $x_n = a_{nn}^{-1}b_n$. En substituant x_n par la valeur $a_{nn}^{-1}b_n$ dans la deuxième dernière équation, on peut trouver la valeur pour x_{n-1} . En continuant de cette manière, on peut trouver la solution du système original. Ceci achève la démonstration du lemme.

Exercice. Résoudre le système sur \mathbb{Z}_5 suivant:

$$\begin{aligned}2x - y + z &= 1 \\ y - z &= 3 \\ 3z &= 2 \\ 0z &= 0.\end{aligned}$$

Solution. À partir de la troisième équation non nulle, on trouve $z = 3^{-1} \cdot 2 = 2 \cdot 2 = 4$. En substituant $z = 4$ dans la deuxième équation, on trouve $y = 3 + z = 3 + 4 = 2$. Enfin, on substitue $z = 4$ et $y = 2$ dans la première équation, on trouve

$$2x = 1 + y - z = 1 + 2 - 4 = 1 + 2 + 1 = 4.$$

D'où, $x = 2$. Donc le système admet une seule solution $(2, 2, 4)$.

On étudiera comment résoudre les systèmes échelonnés ayant plusieurs solutions. Étant donné un ensemble \mathcal{S} , on désigne par $|\mathcal{S}|$ le nombre d'éléments de \mathcal{S} . On considère le produit cartésien de s copies de K suivant:

$$K^s = \{(\lambda_1, \dots, \lambda_s) \mid \lambda_j \in K\}.$$

Si K est fini, alors K^s est également fini avec $|K^s| = |K|^s$.

Exemple. Comme $\mathbb{Z}_2 = \{0, 1\}$, on a

$$\mathbb{Z}_2^3 = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (1, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1), (1, 1, 1)\}.$$

Ainsi $|\mathbb{Z}_2^3| = 8 = |\mathbb{Z}_2|^3$.

On acceptera sans preuve le résultat suivant.

3.9. Théorème. Soit un système échelonné d'équations linéaires à n inconnues

$$AX = B$$

tel que $\text{rg}(A) = \text{rg}(A|B) < n$. Si x_{j_1}, \dots, x_{j_s} sont les inconnues libres, alors le système admet plusieurs solutions, qui sont en bijection avec les éléments de K^s de la façon suivante :

Étant donné $(\lambda_1, \dots, \lambda_s) \in K^s$, on pose $x_{j_l} = \lambda_l$, $l = 1, \dots, s$, et déplace les termes $a_{i,j_l} \lambda_j$ 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 qui correspond à $(\lambda_1, \dots, \lambda_s)$.

Exercice. Résoudre le système rationnel suivant:

$$\begin{aligned} 0x_1 + 2x_2 - x_3 + x_4 &= 1 \\ x_3 - 2x_4 &= 1. \end{aligned}$$

Solution. Considérons la matrice augmentée

$$(A | B) = \left(\begin{array}{cccc|c} 0 & 2 & -1 & 1 & 1 \\ 0 & 0 & 1 & -2 & 1 \end{array} \right).$$

Le système est échelonné dont les inconnues libres sont x_1 et x_4 . Comme $\text{rg}(A) = \text{rg}(A|B) = 2$, les solutions sont en bijection avec les éléments de \mathbb{Q}^2 . À titre d'exemple, on trouvera la solution qui correspond au couple $(2, 3) \in \mathbb{Q}^2$. En posant $x_1 = 2$ et $x_4 = 3$, on obtient le système suivant:

$$\begin{aligned} 2x_2 - x_3 &= -2 \\ x_3 &= 7. \end{aligned}$$

Étant échelonné sans inconnue libre, ce système a une seule solution. En résolvant ce système, on obtient $x_3 = 7$ et $x_2 = \frac{5}{2}$. Donc, $(2, \frac{5}{2}, 7, 3)$ est la solution du système original qui correspond au couple $(2, 3)$.

En général, étant donné un couple quelconque $(\lambda, \mu) \in \mathbb{Q} \times \mathbb{Q}$, on pose $x_1 = \lambda$ et $x_4 = \mu$ et déplace les termes contenant λ, μ à droite. Ceci nous donne un système échelonné sans inconnues libres comme suit:

$$\begin{aligned} 2x_2 - x_3 &= 1 - \mu \\ x_3 &= 1 + 2\mu. \end{aligned}$$

En résolvant ce dernier par substitution, on trouve $x_3 = 1 + 2\mu$ et $x_2 = 1 + \frac{\mu}{2}$. Par conséquent, l'ensemble des solutions du système original est

$$\left\{ (\lambda, 1 + \frac{\mu}{2}, 1 + 2\mu, \mu) \mid \lambda, \mu \in \mathbb{Q} \right\}.$$

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 .

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.

Exemple.

$$\begin{array}{rcl} x + 2y + 3z = 1 & & x + 2y + 3z = 1 \\ 4x + 5y + 6z = 2 & \xrightarrow{\substack{E_2 - 4E_1 \\ E_3 - 7E_1}} & -3y - 6z = -2 \\ 7x + 8y + 9z = 3 & & -6y - 12z = -4 \end{array}$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 4 & 5 & 6 & 2 \\ 7 & 8 & 9 & 3 \end{array} \right) \xrightarrow{\substack{L_2 - 4L_1 \\ L_3 - 7L_1}} \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & -3 & -6 & -2 \\ 0 & -6 & -12 & -4 \end{array} \right).$$

On voit que la nouvelle matrice partagée 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, qui se réduit au système $A'X = B'$. Alors $(A|B)$ se réduit à $(A'|B')$. D'après le corollaire 2.3.10, il existe une matrice inversible P telle que $(A'|B') = P(A|B) = (PA|PB)$. Ceci donne $A' = PA$ et $B' = PB$. Soit S une matrice de type $n \times 1$. Comme P est inversible, $AS = B$ 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 *élimination de Gauss*.

Exercice. Résoudre, par l'élimination de Gauss, le système suivant sur \mathbb{Z}_5 :

$$\begin{array}{rcl} x_2 - x_3 + x_4 & = & 0 \\ 2x_1 - x_2 + 3x_3 - x_4 & = & 1 \\ x_1 + x_2 & & + x_4 = 3 \\ 3x_1 - 3x_2 + x_3 - 3x_4 & = & 4. \end{array}$$

Solution. On échelonne la matrice augmentée comme suit:

$$\begin{aligned}
(A | B) & \xrightarrow{L_1 \leftrightarrow L_3} \begin{pmatrix} 1 & 1 & 0 & 1 & | & 3 \\ 2 & -1 & 3 & -1 & | & 1 \\ 0 & 1 & -1 & 1 & | & 0 \\ 3 & -3 & 1 & -3 & | & 4 \end{pmatrix} \xrightarrow{\substack{L_2 - 2L_1 \\ L_3 - 3L_1}} \begin{pmatrix} 1 & 1 & 0 & 1 & | & 3 \\ 0 & -3 & 3 & -3 & | & 0 \\ 0 & 1 & -1 & 1 & | & 0 \\ 0 & -1 & 1 & -1 & | & 0 \end{pmatrix} \\
& \xrightarrow{-\frac{1}{3}L_2} \begin{pmatrix} 1 & 1 & 0 & 1 & | & 3 \\ 0 & -1 & 1 & -1 & | & 0 \\ 0 & 1 & -1 & 1 & | & 0 \\ 0 & -1 & 1 & -1 & | & 0 \end{pmatrix} \xrightarrow{\substack{L_3 + L_2 \\ L_4 - L_2}} \begin{pmatrix} 1 & 1 & 0 & 1 & | & 3 \\ 0 & -1 & 1 & -1 & | & 0 \\ 0 & 0 & 0 & 0 & | & 0 \\ 0 & 0 & 0 & 0 & | & 0 \end{pmatrix}
\end{aligned}$$

La dernière matrice représente le système échelonné suivant:

$$\begin{aligned}
x_1 + x_2 + x_4 &= 3 \\
-x_2 + x_3 - x_4 &= 0 \\
0 &= 0 \\
0 &= 0.
\end{aligned}$$

Remarquons que x_3 et x_4 sont les inconnues libres. Donc le système a 5^2 solutions. Pour tout $(\lambda, \mu) \in \mathbb{Z}_5 \times \mathbb{Z}_5$, posons $x_3 = \lambda$ et $x_4 = \mu$. On a un système sans inconnues libres:

$$\begin{aligned}
x_1 + x_2 &= 3 - \mu \\
-x_2 &= -\lambda + \mu.
\end{aligned}$$

En résolvant ce dernier par substitution à partir de la dernière équation, on trouve que

$$x_2 = \lambda - \mu, \quad x_1 = 3 + \lambda - 2\mu, \quad x_3 = \lambda, \quad x_4 = \mu; \quad \lambda, \mu \in \mathbb{Z}_5.$$

Par conséquent, l'ensemble des solutions du système original est

$$\{(3 - \lambda, \lambda - \mu, \lambda, \mu) \mid \lambda, \mu \in \mathbb{Z}_5\}.$$

3.12. Théorème. Soit un système d'équations linéaires sur K à n inconnues

$$AX = B.$$

Alors le système est compatible si, et seulement si, $\text{rg}(A) = \text{rg}(A | B)$. Plus précisément, on a les énoncés suivants.

(1) Si $\text{rg}(A) < \text{rg}(A | B)$, alors le système est incompatible.

(2) Si $\text{rg}(A) = \text{rg}(A \mid B) = n$, alors le système admet une seule solution.

(3) Si $\text{rg}(A) = \text{rg}(A \mid B) < n$, alors les solutions du système sont en bijection avec les éléments de K^s , où $s = n - \text{rg}(A)$. 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 $(C \mid D)$ une forme échelonnée de $(A \mid B)$. 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), $\text{rg}(A \mid B) = \text{rg}(C \mid D)$ et $\text{rg}(A) = \text{rg}(C)$. 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:

$$\begin{aligned} x + y - z &= 1 \\ x + 2y + az &= 2 \\ 2x + ay + 2z &= 3. \end{aligned}$$

Solution. On échelonne la matrice augmentée comme suit:

$$\left(\begin{array}{ccc|c} 1 & 1 & -1 & 1 \\ 1 & 2 & a & 2 \\ 2 & a & 2 & 3 \end{array} \right) \Rightarrow \left(\begin{array}{ccc|c} 1 & 1 & -1 & 1 \\ 0 & 1 & a+1 & 1 \\ 0 & 0 & (3-a)(a+2) & 3-a \end{array} \right) =: (A' \mid B').$$

Pour toute valeur de a , on voit que $(A' \mid B')$ est échelonnée, et donc

$$2 \leq \text{rg}(A) \leq \text{rg}(A \mid B) \leq 3.$$

(1) Le système n'a aucune solution si, et seulement si, $\text{rg}(A) < \text{rg}(A \mid B)$ si, et seulement si, $\text{rg}(A) = 2$ et $\text{rg}(A \mid B) = 3$ si, et seulement si, $(3-a)(a+2) = 0$ et $3-a \neq 0$ si, et seulement si, $a = -2 = 5$.

(2) Le système n'a qu'une solution si, et seulement si, $\text{rg}(A) = 3$ si, et seulement si, $(3-a)(a+2) \neq 0$ si, et seulement si, $a \in \{0, 1, 2, 4, 6\}$.

(3) Le système a au moins deux solutions si, et seulement si, $\text{rg}(A) = \text{rg}(A \mid B) < 3$ si, et seulement si, $\text{rg}(A) = \text{rg}(A \mid B) = 2$ si, et seulement si, $(3-a)(a+2) = 0$ et $3-a = 0$ si, et seulement si, $a = 3$. Dans ce cas, le système échelonné $A'X = B'$ a une seule inconnue libre. Comme $|\mathbb{Z}_7| = 7$, le système original admet 7 solutions.

Pour résumer, le système original admet

- (a) aucune solution si $a = 5$;
- (b) une seule solution si $a \in \{0, 1, 2, 4, 6\}$;

(c) 7 solutions si $a = 3$.

On conclut cette section par un genre spécial de systèmes d'équations linéaires tel que défini si-dessous, qui sert à déterminer si des vecteurs d'un espace vectoriel sont linéairement dépendants ou linéairement indépendants.

3.13. Définition. Un système d'équations linéaires

$$AX = B$$

est dit *homogène* si $B = 0$, c'est-à-dire, les termes constants sont tous nuls. Dans ce cas, $X = 0_{n \times 1}$ est toujours une solution, appelée la *solution nulle*, de ce système.

Il s'agit d'un problème très important de savoir quand un système homogène a des solutions non nulles.

3.14. Théorème. Soit un système homogène de m équations linéaires à n inconnues

$$AX = 0.$$

(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 système admet toujours des solutions non nulles.

Démonstration. On a $\text{rg}(A) = \text{rg}(A \mid 0)$. Si $\text{rg}(A) = n$, d'après le théorème 3.12(2), le système a une seule solution, ce qui doit être la solution nulle.

Si $\text{rg}(A) < n$, d'après le théorème 3.12(3), le système a plusieurs solutions dont au moins une est non nulle.

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 démonstration du théorème.

Exemple. Le système

$$\begin{aligned} \sqrt{2}x - (1+i)y - z &= 0 \\ (1-i)x + \sqrt{3}y + z &= 0 \end{aligned}$$

a des solutions non nulles.

Exercice. Pour quelle valeur de a , le système homogène

$$\begin{aligned} x - 2y + z &= 0 \\ x + y + 3z &= 0 \\ 3x + 5y + 5z &= 0 \\ 2x + 4y + az &= 0, \end{aligned}$$

a-t-il des solutions non nulles?

Solution. On échelonne la matrice des coefficients comme suit:

$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 3 & 5 & 5 \\ 2 & 4 & a \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 2 & 1 \\ 0 & -1 & 2 \\ 0 & 0 & a-2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Donc le système a des solutions non nulles si, et seulement si, la matrice des coefficients est de rang inférieur que 3 si, et seulement si, $a = 2$.

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 le théorème 3.14(1), 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 du corollaire.

Exercice. Considérer le système complexe homogène

$$\begin{aligned} (\sqrt{2} - \sqrt{3}i)x + (2 - i)y &= 0 \\ (2 + i)x + (\sqrt{2} + \sqrt{3}i)y &= 0. \end{aligned}$$

A-t-il des solutions non nulles?

Solution. Comme

$$A = \begin{pmatrix} \sqrt{2} - \sqrt{3}i & 2 - i \\ 2 + i & \sqrt{2} + \sqrt{3}i \end{pmatrix} \Rightarrow \begin{pmatrix} 5 & (2\sqrt{2} + \sqrt{3}) + (2\sqrt{3} - \sqrt{2})i \\ 5 & (2\sqrt{2} + \sqrt{3}) + (2\sqrt{3} - \sqrt{2})i \end{pmatrix},$$

on voit que $\text{rg}(A) = 1$. Ainsi A est non inversible. D'après le corollaire 3.15, le système a des solutions nulles.

3.16. Exercices

1. Résoudre, en trouvant l'inverse de la matrice de coefficients, le système d'équations linéaires sur \mathbb{C} suivant:

$$\begin{aligned}x - y &= 1 + i \\x + y + 3z &= i \\y + z &= 2 - i.\end{aligned}$$

2. Résoudre, par l'élimination de Gauss, les systèmes sur \mathbb{C} suivants:

$$(1) \quad \begin{aligned}x_1 - x_2 + x_3 &= 6 \\x_1 + x_2 + 2x_3 &= 8 \\2x_1 - 3x_2 - x_3 &= 1;\end{aligned}$$

$$(2) \quad \begin{aligned}x_1 - 3x_2 + x_3 &= 6 \\2x_1 + x_2 - 3x_3 &= 2i \\x_1 + (1+i)x_2 - 4x_3 &= 0.\end{aligned}$$

3. Résoudre, par l'élimination de Gauss, le système sur \mathbb{Z}_5 suivant:

$$\begin{aligned}x_1 + 2x_2 - x_3 + 2x_4 &= 0 \\2x_1 + 4x_2 - x_3 + 3x_4 &= 1 \\x_1 + 2x_2 - 2x_3 + 3x_4 &= 4 \\x_1 + 2x_2 + x_4 &= 1.\end{aligned}$$

4. Résoudre, par l'élimination de Gauss, le système sur \mathbb{Z}_3 suivant:

$$\begin{aligned}x_1 + 2x_2 + x_4 &= 0 \\2x_1 + 2x_2 + x_3 &= 1 \\x_1 + x_3 + 2x_4 &= 1.\end{aligned}$$

5. Soient P_1, P_2 , et P_3 les plans affines définis par les équations cartésiennes $x + 2y + z = 1$, 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.

$$(1) \quad \begin{aligned}x - 2y + z &= 6 \\3x + y - z &= 7 \\-x + y + az &= 6;\end{aligned}$$

$$(2) \quad \begin{aligned} x + 2y - 3z &= a \\ 2x + 6y - 11z &= b \\ x - 2y + 7z &= c. \end{aligned}$$

7. Donner, selon les valeurs réelles de a , le nombre de solutions du système réel suivant:

$$\begin{aligned} x + y + (1 - 2a)z &= 2(1 + a) \\ (1 + a)x - (1 + a)y + (2 + a)z &= 0 \\ 2x - 2ay + 3z &= 2(1 + a). \end{aligned}$$

8. Donner, selon les valeurs de a, b , le nombre de solutions du système rationnel suivant:

$$\begin{aligned} x + y &= 2 \\ x + ay &= 2b + 1. \end{aligned}$$

9. Considérer le système d'équations linéaires sur \mathbb{Z}_{11} suivant:

$$\begin{aligned} x + 2y + 2z &= 1 \\ 2x + 5y + az &= 1 \\ 3x + ay + 6z &= 5. \end{aligned}$$

Déterminer les valeurs de a pour lesquelles le système

(1) n'a pas de solution;

(2) ait une seule solution.

(3) ait plusieurs de solutions; et dans ce cas, donner le nombre de solutions.

10. Déterminer si le système homogène suivant admet ou non des solutions non nulles.

$$\begin{aligned} x_1 - 3x_2 + 6x_3 - 3x_4 &= 0 \\ x_2 - x_3 + x_4 &= 0 \\ 2x_1 - x_2 + 3x_3 - x_4 &= 0 \\ 4x_1 + 4x_2 + x_4 &= 0. \end{aligned}$$

11. Pour quelle valeur complexe de a , le système homogène complexe

$$\begin{aligned} x - y + z &= 0 \\ 3x + y + az &= 0 \\ -x - 2y - z &= 0, \end{aligned}$$

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:

$$\begin{aligned} 3x - y + 2z &= 0 \\ y + (1+i)z &= 0 \\ 3x + (3+i)z &= 0. \end{aligned}$$

13. Considérer le système homogène suivant:

$$\begin{aligned} x_1 + 2x_3 - x_4 &= 0 \\ x_1 - x_3 + x_4 &= 0 \\ -x_2 + (1+a)x_4 &= 0 \\ ax_2 &= 0. \end{aligned}$$

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 la matrice des coefficients est compatible.

Indice: Pour la suffisance, appliquer le numéro 51 des Exercices 2.5 en considérant les systèmes $AX = e_j$, où e_j est la j -ième colonne de I_n .

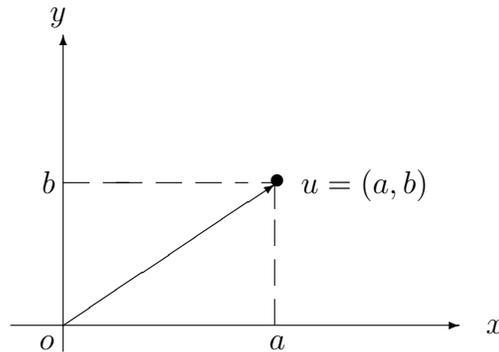
Chapitre IV: Espaces vectoriels

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 propriétés communes. Par exemple, une quantité vectorielle 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 abstraite 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 particulières.

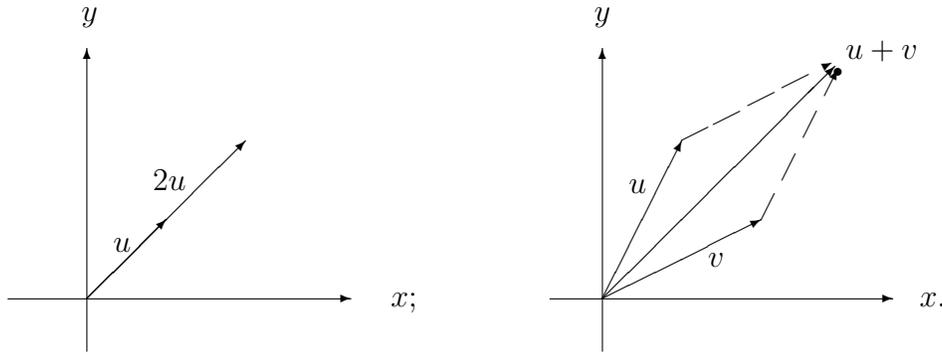
Partout dans ce chapitre, on se fixe K un corps.

4.1. Définition et exemples

Avant introduire la notion abstraite d'un espace vectoriel, nous rappelons deux exemples d'espaces vectoriels réels. D'abord, le plan \mathbb{R}^2 se compose des vecteurs représentés 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 donné 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 deuxièmement 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) $\alpha \cdot (a, b, c) = (\alpha a, \alpha b, \alpha c)$, $\alpha \in \mathbb{R}$;
- (2) $(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$.

Les opérations dans \mathbb{R}^2 et celles dans \mathbb{R}^3 satisfont aux axiomes communs. En généralisant ces axiomes, on obtient la notion abstraite 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

$$\cdot : K \times E \rightarrow E : (\alpha, u) \mapsto \alpha \cdot u$$

et d'une addition

$$+ : E \times E \rightarrow E : (u, v) \mapsto u + v$$

qui satisfont, pour tous $u, v, w \in E$ et $\alpha, \beta \in K$, aux huit axiomes suivants:

- (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 à l'addition de vecteurs) $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$.
- (8) (distributivité par rapport à l'addition de scalaires) $(\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u$.

En outre, E est dit *nul* si $E = \{0_E\}$. Dans le cas où $K = \mathbb{Q}$, \mathbb{R} ou \mathbb{C} , on dit brièvement que E est un espace vectoriel *rationnel*, *réel* ou *complexe*, respectivement.

Remarque. (1) Pour tout $u \in E$, on a

$$0_E + u = u; \quad (-u) + u = 0_E.$$

(2) Pour $u, v \in E$, on définit la *différence* entre u et v par

$$u - v := u + (-v).$$

(3) Pour $u, v, w \in E$, on définit

$$u + v + w := (u + v) + w.$$

(4) En général, pour $u_1, u_2, \dots, u_n \in E$ avec $n > 2$, on définit

$$u_1 + u_2 + \dots + u_n := (\dots((u_1 + u_2) + u_3) + \dots + u_{n-1}) + u_n.$$

Exemple. (1) $E = \{0_K\}$ est un K -espace vectoriel nul, pour les opérations suivantes:

$$0_K + 0_K = 0_K, \quad \alpha \cdot 0_K = 0_K, \quad \text{pour tout } \alpha \in K.$$

Essentiellement, c'est le seul K -espace vectoriel nul.

(2) Étant donnés des entiers $m, n \geq 1$, on voit que

$$M_{m \times n}(K) = \{(a_{ij})_{m \times n} \mid a_{ij} \in K\}$$

est un K -espace vectoriel pour l'addition et la multiplication par un scalaire sur les matrices. Dans ce cas, le vecteur nul est la matrice nulle $0_{m \times n}$.

(3) En particulier, $K^n = \{(a_1, \dots, a_n) \mid a_i \in K\}$ et

$$K^{(n)} = \left\{ \left(\begin{array}{c} a_1 \\ \vdots \\ a_n \end{array} \right) \mid a_i \in K \right\}$$

sont des K -espaces vectoriels, pour tout $n \geq 1$.

(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) De l'autre côté, $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ est aussi un \mathbb{R} -espace vectoriel, noté ${}_{\mathbb{R}}\mathbb{C}$, pour les opérations habituelles:

$$\alpha(a + bi) = (\alpha a) + (\alpha b)i; \quad (a + bi) + (c + di) = (a + c) + (b + d)i.$$

Remarquons que ${}_{\mathbb{C}}\mathbb{C}$ et ${}_{\mathbb{R}}\mathbb{C}$ sont essentiellement différents. En effet, ils n'ont pas le même ensemble des scalaires.

(6) Soit I un intervalle de l'axe réel \mathbb{R} . L'ensemble $C(I)$ des fonctions continues

$$f : I \rightarrow \mathbb{R} : t \mapsto f(t)$$

est un espace vectoriel réel pour les opérations usuelles telles, pour tous $f, g \in C(I)$ et $\alpha \in \mathbb{R}$, que

$$f + g : I \rightarrow \mathbb{R} : t \mapsto (f + g)(t) := f(t) + g(t)$$

et

$$\alpha \cdot f : I \rightarrow \mathbb{R} : t \mapsto (\alpha \cdot f)(t) := \alpha f(t).$$

Dans ce cas, le vecteur nul est la fonction nulle

$$\mathbf{0} : I \rightarrow \mathbb{R} : t \mapsto 0.$$

C'est-à-dire, $\mathbf{0}(t) = 0$, pour tout $t \in I$.

(7) L'ensemble de polynômes sur K de degré $< n$

$$K_n[x] = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_i \in K\}$$

est un K -espace vectoriel pour les opérations usuelles suivantes:

$$(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) + (b_0 + b_1x + \cdots + b_{n-1}x^{n-1}) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_{n-1} + b_{n-1})x^{n-1}.$$

et

$$\alpha \cdot (a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) = (\alpha a_0) + (\alpha a_1)x + \cdots + (\alpha a_{n-1})x^{n-1}, \text{ où } \alpha \in \mathbb{R}$$

Dans ce cas, le vecteur nul est le polynôme nul $0 + 0x + \cdots + 0x^{n-1}$.

(8) L'ensemble de tous les polynômes sur K

$$K[x] = \{a_0 + a_1x + \cdots + a_mx^m \mid m \geq 0, a_i \in K\}$$

est un K -espace vectoriel pour les opérations telles que définies ci-dessus.

Voici des propriétés élémentaires d'espaces vectoriels.

4.1.2. Proposition. Soit E un K -espace vectoriel. Les énoncés suivants sont valides pour tous $u, v, w \in E$ 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 $u = 0_E$.

$$(5) \quad (-1_K) \cdot u = -u.$$

$$(6) \quad -(-u) = u.$$

$$(7) \quad -(u + v) = -u - v.$$

$$(8) \quad u + v = w \text{ si, et seulement si, } u = w - v.$$

Démonstration. (1) Si 0 et $0'$ sont des vecteurs nuls de E , alors $0' = 0 + 0' = 0' + 0 = 0$.

(2) Supposons $u + v = u + w$. Alors $(-u) + (u + v) = (-u) + (u + w)$. D'après l'associativité, $((-u) + u) + v = ((-u) + u) + w$. Donc $0_E + v = 0_E + w$. Ainsi $v = w$. Par conséquent, (2) est valide.

(3) Si $u + u' = 0_E$, alors $u + u' = u + (-u)$. D'après l'énoncé (2), on a $u' = -u$.

(4) $0_K u + 0_K u = (0_K + 0_K)u = 0_K u = 0_K u + 0_E$. Donc $0_K u = 0_E$. De même, $\alpha 0_E = 0_E$. Supposons maintenant que $\alpha u = 0_E$. Si $\alpha \neq 0_K$, alors α^{-1} existe. Or

$$u = 1_K \cdot u = (\alpha^{-1} \alpha)u = \alpha^{-1}(\alpha u) = \alpha^{-1}0_E = 0_E.$$

(5) On a $(-1_K)u + u = (-1_K) \cdot u + 1_K \cdot u = ((-1_K) + 1_K)u = 0_K u = 0_E$. Ainsi $(-1_K)u = -u$.

(6) Comme $(-u) + u = 0_E$, d'après l'énoncé (3), on a $u = -(-u)$.

(7) D'après l'énoncé (5), on a $-(u + v) = (-1_K)(u + v) = (-1_K)u + (-1_K)v = (-u) + (-v) = -u - v$.

(8) Si $u + v = w$, alors $w - v = (u + v) + (-v) = u + (v + (-v)) = u + 0_E = u$. Réciproquement, si $u = w - v$, alors $u + v = (w + (-v)) + v = w + ((-v) + v) = w + 0_E = w$. La preuve de la proposition s'achève.

4.2. Bases

Partout dans cette section, on se fixe E un K -espace vectoriel.

4.2.1. Définition. Soient $u_1, \dots, u_n \in E$. Un vecteur $u \in E$ s'appelle *combinaison linéaire* de u_1, \dots, u_n s'il existe $\alpha_1, \dots, \alpha_n \in K$, tels que

$$u = \alpha_1 u_1 + \dots + \alpha_n u_n.$$

Dans ce cas, on appelle $\alpha_1, \dots, \alpha_n$ *coefficients* de u dans u_1, \dots, u_n .

Remarque. (1) Le vecteur nul 0_E est toujours combinaison linéaire de u_1, \dots, u_n , car

$$0_E = 0_K \cdot u_1 + \dots + 0_K \cdot u_n, \text{ où } 0_K \in K.$$

(2) Si $n = 1$, alors u est une combinaison linéaire de u_1 si $u = \alpha u_1$, pour un certain $\alpha \in K$. Dans ce cas, u s'appelle aussi *multiple* de u_1 .

(3) Tout vecteur u est une combinaison linéaire de lui-même, car $u = 1_K \cdot u$.

Exemple. (1) Dans l'espace vectoriel réel ${}_{\mathbb{R}}\mathbb{C}$, le vecteur i n'est pas une combinaison linéaire du vecteur 1. En effet, $i \neq a \cdot 1$, pour tout scalaire $a \in \mathbb{R}$.

(2) Dans l'espace vectoriel complexe ${}_{\mathbb{C}}\mathbb{C}$, le nombre complexe i est une combinaison linéaire du nombre 1. En effet, $i = i \cdot 1$, où $i \in \mathbb{C}$ est un scalaire.

(4) Considérons des matrices rationnelles

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 2 & 3 & 4 \\ 0 & 1 & 0 \end{pmatrix}; u = \begin{pmatrix} 3 \\ -2 \\ 1 \end{pmatrix}.$$

Remarquons que les colonnes de A sont des vecteurs

$$A_1 = \begin{pmatrix} 1 \\ 3 \\ 2 \\ 0 \end{pmatrix}, A_2 = \begin{pmatrix} 2 \\ 4 \\ 3 \\ 1 \end{pmatrix}, A_3 = \begin{pmatrix} 3 \\ 5 \\ 4 \\ 0 \end{pmatrix} \in \mathbb{Q}^{(4)}.$$

D'après le lemme 2.2.4(2), on a

$$Au = 3 \cdot A_1 + (-2) \cdot A_2 + 1 \cdot A_3,$$

ce qui est une combinaison linéaire des colonnes de A .

On a une autre interprétation de combinaisons linéaires. Considérons l'équation

$$x_1 u_1 + \cdots + x_n u_n = u,$$

où $u_1, \dots, u_n; u \in E$. Alors u est une combinaison linéaire de u_1, \dots, u_n si, et seulement si, cette équation admet une solution.

Exercice. Considérer l'espace vectoriel réel $M_2(\mathbb{R})$. Montrer que tout vecteur est une combinaison linéaire de vecteurs suivants:

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Preuve. Soit un vecteur quelconque

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}).$$

Considérons l'équation

$$x_{11} \cdot e_{11} + x_{12} \cdot e_{12} + x_{21} \cdot e_{21} + x_{22} \cdot e_{22} = A.$$

En calculant le membre de gauche, on trouve que

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

On obtient facilement une solution $x_{11} = a$, $x_{12} = b$, $x_{21} = c$ et $x_{22} = d$. C'est-à-dire,

$$A = a \cdot e_{11} + b \cdot e_{12} + c \cdot e_{21} + d \cdot e_{22}.$$

Ainsi, A est une combinaison linéaire de $e_{11}, e_{12}, e_{21}, e_{22}$.

Exercice. Soit $C[0, 2\pi]$ l'espace réel des fonctions continues définies sur $[0, 2\pi]$. Vérifier que la fonction $f = t^2$ 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 prenant $t = 0$ et $t = \pi$, on obtient

$$\begin{aligned} 0\alpha + \beta &= 0 \\ 0\alpha - \beta &= \pi^2. \end{aligned}$$

Ceci nous donne $\pi^2 = 0$, une contradiction. Donc la fonction t^2 n'est pas une combinaison linéaire des fonctions $\sin t$ et $\cos t$.

On introduira une notation pour les combinaisons linéaires. Soit u une combinaison linéaire de $u_1, \dots, u_n \in E$, disons

$$u = \alpha_1 \cdot u_1 + \dots + \alpha_n \cdot u_n, \text{ où } \alpha_1, \dots, \alpha_n \in K.$$

Considérons (u_1, \dots, u_n) comme une matrice-ligne formelle et mettons les coefficients en une colonne

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix},$$

Exercice. Considérons l'espace vectoriel rationnel $\mathbb{Q}_3[x]$ et ses vecteurs

$$f_1 = 1 + x, f_2 = 1 + x^2, f_3 = x^2.$$

Trouver les combinaisons linéaires g_1, g_2 de f_1, f_2, f_3 aux coefficients $\{2, 1, 3\}$ et $\{-1, 1, 0\}$ respectivement.

Solution. D'après l'hypothèse, on a

$$\begin{aligned} (g_1, g_2) &= (f_1, f_2, f_3) \begin{pmatrix} 2 & -1 \\ 1 & 1 \\ 3 & 0 \end{pmatrix} = (2 \cdot f_1 + 1 \cdot f_2 + 3 \cdot f_3, (-1) \cdot f_1 + 1 \cdot f_2 + 0 \cdot f_3) \\ &= (2(1+x) + (1+x^2) + 3x^2, -(1+x) + (1+x^2)) \\ &= (3 + 2x + 4x^2, x + x^2). \end{aligned}$$

C'est-à-dire, $g_1 = 3 + 2x + 4x^2$ et $g_2 = x + x^2$.

Le résultat suivant dit que cette multiplication formelle est aussi associativité.

4.2.2. Proposition. Soient $u_1, \dots, u_n \in E$.

(1) Si $A \in M_{n \times m}(K)$ et $B \in M_{m \times p}(K)$, alors $((u_1, \dots, u_n)A)B = (u_1, \dots, u_n)(AB)$.

(2) Si $v = \alpha_1 v_1 + \dots + \alpha_m v_m$, où $\alpha_i \in K$ et v_i est une combinaison linéaire de u_1, \dots, u_n , pour tout $1 \leq i \leq m$, alors v est aussi une combinaison linéaire de u_1, \dots, u_n .

Démonstration. La preuve de l'énoncé (1) est semblable à celle-ci de la proposition 2.1.5(2). Par l'hypothèse, $v = (v_1, \dots, v_m)B$ avec $B = (\alpha_i)_{m \times 1}$ et $(v_1, \dots, v_m) = (u_1, \dots, u_n)A$ avec $A \in M_{n \times m}(K)$. D'après l'énoncé (1), on a

$$v = (v_1, \dots, v_m)B = ((u_1, \dots, u_n)A)B = ((u_1, \dots, u_n)(AB)).$$

C'est-à-dire, v est une combinaison linéaire de u_1, \dots, u_n . La preuve de la proposition s'achève.

Exercice. Considérons l'espace vectoriel rationnel $\mathbb{Q}_3[x]$ et ses vecteurs

$$f_1 = 1 + x; f_2 = 1 + x^2; f_3 = x^2.$$

Posons $g_1 = 2f_1 + f_2 + 3f_3$; $g_2 = -f_1 + f_2$ et $h = 3g_1 - g_2$. Exprimer h comme combinaison linéaire de f_1, f_2, f_3 .

Solution. D'après l'hypothèse, on a

$$(g_1, g_2) = (f_1, f_2, f_3) \begin{pmatrix} 2 & -1 \\ 1 & 1 \\ 3 & 0 \end{pmatrix}.$$

Ainsi

$$h = (g_1, g_2) \begin{pmatrix} 3 \\ -1 \end{pmatrix} = (f_1, f_2, f_3) \begin{pmatrix} 2 & -1 \\ 1 & 1 \\ 3 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ -1 \end{pmatrix} = (f_1, f_2, f_3) \begin{pmatrix} 7 \\ 2 \\ 9 \end{pmatrix}.$$

C'est-à-dire, $h = 7 \cdot f_1 + 2 \cdot f_2 + 9 \cdot f_3$.

En général, les coefficients d'une combinaison linéaire ne sont pas uniques. Par exemple, dans l'espace vectoriel réel \mathbb{R}^3 , on a

$$(1, 5, 1) = 1 \cdot (2, 3, 2) + (-1) \cdot (1, 0, 1) + 2(0, 1, 0) = 0 \cdot (2, 3, 2) + 1 \cdot (1, 0, 1) + 5 \cdot (0, 1, 0).$$

On étudiera quand les coefficients d'une combinaison linéaire sont uniques.

4.2.3. Définition. Soient $u_1, \dots, u_n \in E$. On dit que u_1, \dots, u_n sont *linéairement dépendants* s'il existe $\alpha_1, \dots, \alpha_n \in K$, non tous nuls, tels que

$$\alpha_1 u_1 + \dots + \alpha_n u_n = 0_E;$$

et *linéairement indépendants* sinon, c'est-à-dire, si toute égalité

$$\alpha_1 u_1 + \dots + \alpha_n u_n = 0_E, \alpha_i \in K,$$

entraîne que $\alpha_1 = \dots = \alpha_n = 0_K$.

Remarque. En bref, une famille $\{u_1, \dots, u_n\}$ de vecteurs de E est dite

- (1) *liée* si u_1, \dots, u_n sont linéairement dépendants;
- (2) *libre* si u_1, \dots, u_n sont linéairement indépendants.

Exemple. (1) Dans l'espace vectoriel complexe ${}_C\mathbb{C}$, la famille $\{1, i\}$ est liée.

En effet, $1, i \in \mathbb{C}$ sont deux scalaires non nuls tels que

$$1 \cdot 1 + i \cdot i = 0.$$

(2) Dans l'espace vectoriel réel ${}_R\mathbb{C}$, la famille $\{1, i\}$ est libre.

En effet, supposons que $a, b \in \mathbb{R}$ sont tels que

$$a \cdot 1 + b \cdot i = 0.$$

En calculant le membre de gauche, on obtient $a + bi = 0$. D'après la définition de complexes, $a = b = 0$. Ceci montre que $1, i$ sont linéairement indépendants dans ${}_R\mathbb{C}$.

(3) Dans le K -espace vectoriel $K_n[x]$, la famille $\{1, x, \dots, x^{n-1}\}$ est libre. En effet, si $a_0, a_1, \dots, a_{n-1} \in K$ sont tels que

$$a_0 \cdot 1 + a_1 \cdot x + \dots + a_{n-1} \cdot x^{n-1} = 0,$$

alors $a_0 + a_1x + \dots + a_{n-1}x^{n-1} = 0$. D'après la définition, $a_0 = a_1 = \dots = a_{n-1} = 0$. Ceci montre que les monômes $1, x, \dots, x^{n-1}$ sont linéairement indépendants.

On a une autre interprétation de l'indépendance linéaire. Considérons l'équation homogène

$$x_1u_1 + \dots + x_nu_n = 0_E,$$

où $u_1, \dots, u_n \in E$. Cette équation homogène admet toujours la solution nulle

$$x_1 = 0_K, \dots, x_n = 0_K.$$

Maintenant, la famille $\{u_1, \dots, u_n\}$ est

- (1) libre s'il n'y a que la solution nulle.
- (2) liée s'il y a des solutions non nulles.

Exercice. Considérons l'espace réel $C[0, 2\pi]$ des fonctions continues $f : [0, 2\pi] \rightarrow \mathbb{R}$. Montrer que $\{f = \sin t, g = \cos t\}$ est une famille libre.

Démonstration. Rappelons que le vecteur nul de $C[0, 2\pi]$ est la fonction nulle

$$\mathbf{0} : [0, 2\pi] \rightarrow \mathbb{R} : t \mapsto 0.$$

Supposons que l'équation homogène

$$xf + yg = \mathbf{0}$$

admet une solution $x = a$ et $y = b$, où $a, b \in \mathbb{R}$. C'est-à-dire,

$$a \cdot f + b \cdot g = \mathbf{0}.$$

On veut montrer que $a = 0$ et $b = 0$. En effet, pour tout $t \in [0, 2\pi]$, on a

$$(a \cdot f + b \cdot g)(t) = \mathbf{0}(t).$$

C'est-à-dire,

$$a \cdot f(t) + b \cdot g(t) = 0.$$

Donc,

$$a \sin t + b \cos t = 0, \text{ pour tout } t \in \mathbb{R}.$$

En posant $t = \frac{\pi}{6}$ et $t = \frac{\pi}{4}$, respectivement, on obtient

$$\begin{aligned} \frac{1}{2}a + \frac{\sqrt{3}}{2}b &= 0 \\ \frac{\sqrt{2}}{2}a + \frac{\sqrt{2}}{2}b &= 0. \end{aligned}$$

En résolvant ce système homogène, on trouve $a = b = 0$. Ceci montre que $\sin t, \cos t$ sont linéairement indépendantes.

4.2.4. Proposition. Une famille $\{u_1, \dots, u_n\}$ de vecteurs de E est libre si, et seulement si, toute combinaison linéaire u de u_1, \dots, u_n s'écrit d'une façon unique

$$u = \alpha_1 u_1 + \dots + \alpha_n u_n, \alpha_1, \dots, \alpha_n \in K$$

si, et seulement si, toute équation compatible

$$x_1 u_1 + \dots + x_n u_n = u$$

admet une seule solution.

Démonstration. Supposons que $\{u_1, \dots, u_n\}$ est libre. Soit u une combinaison linéaire de u_1, \dots, u_n , disons $u = \alpha_1 u_1 + \dots + \alpha_n u_n$, $\alpha_1, \dots, \alpha_n \in K$. Si $\beta_1, \dots, \beta_n \in K$ sont tels que $u = \beta_1 u_1 + \dots + \beta_n u_n$, alors

$$(\alpha_1 - \beta_1)u_1 + \dots + (\alpha_n - \beta_n)u_n = 0.$$

Comme $\{u_1, \dots, u_n\}$ est libre, $\alpha_i - \beta_i = 0$, c'est-à-dire, $\alpha_i = \beta_i$, pour $i = 1, \dots, n$.

Réciproquement, supposons que $\{u_1, \dots, u_n\}$ satisfait à la condition énoncée dans la proposition. Supposons que

$$\alpha_1 u_1 + \dots + \alpha_n u_n = 0_E, \text{ où } \alpha_1, \dots, \alpha_n \in K.$$

Comme

$$0_E = 0_K \cdot u_1 + \dots + 0_K \cdot u_n,$$

d'après l'unicité de l'expression pour le vecteur 0_E , on a $\alpha_i = 0$, pour $i = 1, \dots, n$. Ainsi $\{u_1, \dots, u_n\}$ est libre. Ceci achève la démonstration de la proposition.

Exemple. Considérons le \mathbb{R} -espace vectoriel \mathbb{R}^3 . Comme

$$(1, 5, 1) = 1 \cdot (2, 3, 2) + (-1) \cdot (1, 0, 1) + 2(0, 1, 0) = 0 \cdot (2, 3, 2) + 1 \cdot (1, 0, 1) + 5 \cdot (0, 1, 0),$$

d'après la proposition 4.2.5, la famille $\{(2, 3, 2), (1, 0, 1), (0, 1, 0)\}$ est liée.

Le résultat suivant caractérise la dépendance linéaire.

4.2.5. Proposition. Considérons une famille $\{u_1, \dots, u_n\}$ de vecteurs de E . Les énoncés suivants sont valides.

(1) La famille $\{u_1, \dots, u_n\}$ est liée si, et seulement si, un des u_i est une combinaison linéaire des autres.

(2) La famille $\{u_1, \dots, u_n\}$ est libre si, et seulement si, aucun des u_i n'est une combinaison linéaire des autres.

Démonstration. Comme ces deux énoncés sont équivalents, il suffit de montrer le premier. Supposons que $\{u_1, \dots, u_n\}$ est liée. Alors, il existe $\alpha_1, \dots, \alpha_n \in K$, non tous nuls, tels que $\alpha_1 u_1 + \dots + \alpha_n u_n = 0_E$. Supposons que $\alpha_s \neq 0_K$. Alors

$$u_s = (-\alpha_s^{-1} \alpha_1) u_1 + \dots + (-\alpha_s^{-1} \alpha_{s-1}) u_{s-1} + (-\alpha_s^{-1} \alpha_{s+1}) u_{s+1} + \dots + (-\alpha_s^{-1} \alpha_n) u_n.$$

C'est-à-dire, u_s est une combinaison linéaire de $u_1, \dots, u_{s-1}, u_{s+1}, \dots, u_n$.

Réciproquement, on suppose que

$$u_i = \alpha_1 u_1 + \dots + \alpha_{i-1} u_{i-1} + \alpha_{i+1} u_{i+1} + \dots + \alpha_n u_n, \text{ où } \alpha_j \in K.$$

Ceci donne

$$\alpha_1 u_1 + \dots + \alpha_{i-1} u_{i-1} + (-1_K) \cdot u_i + \alpha_{i+1} u_{i+1} + \dots + \alpha_n u_n,$$

où $-1_K \neq 0_K$. Ainsi, $\{u_1, \dots, u_n\}$ est liée. Cela achève la démonstration de la proposition.

Exemple. Considérons l'espace vectoriel réel \mathbb{R}^3 . On voit que

$$2 \cdot (1, 0, 1) - 3 \cdot (-1, 2, 1) = (5, -6, -1).$$

D'après la proposition 4.2.5, la famille $\{(1, 0, 1), (5, -6, -1), (-1, 2, 1)\}$ est liée.

Le résultat suivant nous dit comment déterminer une petite famille de vecteurs est liée ou libre.

4.2.6. 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. D'abord, l'énoncé (2) est un cas particulier de la proposition 4.2.5.

Si $u = 0_E$, alors $1_K \cdot u = 0_E$ avec $1_K \neq 0_K$. Ainsi, $\{u\}$ est liée. Réciproquement, supposons que $u \neq 0_E$. Si $\alpha u = 0_E$, alors $\alpha = 0_K$. D'où, $\{u\}$ est libre. Ceci montre l'énoncé (1). La preuve du lemme s'achève.

Exemple. Considérons l'espace vectoriel réel \mathbb{R}^2 . La famille

$$\left\{ u_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, u_2 = \begin{pmatrix} 1 \\ 3 \end{pmatrix} \right\}$$

est libre. En effet, pour tout $a \in \mathbb{R}$, on voit que

$$\begin{pmatrix} a \\ 2a \end{pmatrix} \neq \begin{pmatrix} 1 \\ 3 \end{pmatrix} \text{ et } \begin{pmatrix} a \\ 3a \end{pmatrix} \neq \begin{pmatrix} 1 \\ 2 \end{pmatrix}.$$

Le résultat suivant nous dit comment agrandir des familles libres.

4.2.7. Proposition. Soient $\{u_1, \dots, u_n\}$ une famille libre de vecteurs de E . Si $u \in E$, alors $\{u_1, \dots, u_n, u\}$ est libre si, et seulement si, u n'est pas une combinaison linéaire de u_1, \dots, u_n .

Démonstration. La nécessité est une conséquence immédiate de la proposition 4.2.5. Supposons maintenant que u n'est pas une combinaison linéaire de u_1, \dots, u_n . Supposons que $\alpha_1, \dots, \alpha_n, \alpha \in K$ sont tels que

$$\alpha_1 u_1 + \dots + \alpha_n u_n + \alpha u = 0_E.$$

Si $\alpha \neq 0_K$, alors

$$u = (-\alpha_1 \alpha^{-1}) u_1 + \dots + (-\alpha_n \alpha^{-1}) u_n,$$

c'est-à-dire, u est une combinaison linéaire de u_1, \dots, u_n , une contradiction. Ainsi $\alpha = 0_K$. D'où,

$$\alpha_1 u_1 + \dots + \alpha_n u_n = 0_E.$$

Comme $\{u_1, \dots, u_n\}$ est libre, $\alpha_1 = \dots = \alpha_n = 0$. Ceci montre que $\{u_1, \dots, u_n, u\}$ est libre. La preuve du lemme s'achève.

Exercice. Considérons l'espace vectoriel réel \mathbb{R}^3 . Augmenter la famille $\{(1, 0, 0)\}$ à une famille libre de 3 vecteurs.

Solution. D'après le lemme 4.2.6(1), $\{(1, 0, 0)\}$ est libre. Comme $(1, 1, 0)$ n'est pas un multiple de $(1, 0, 0)$, d'après la proposition 4.2.7, $\{(1, 0, 0), (1, 1, 0)\}$ est libre. Comme

$(1, 1, 1)$ n'est pas une combinaison linéaire de $(1, 0, 0)$ et $(1, 1, 0)$, d'après la proposition 4.2.7, $\{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ est libre.

4.2.8. Proposition. Soit $\mathcal{U} = \{u_1, \dots, u_n\}$ 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 $1 \leq i \leq n$;
- (2) $u_i \neq u_j$, pour tous $1 \leq i, j \leq n$ avec $i \neq j$.

Démonstration. Soit \mathcal{V} une sous-famille non vide de \mathcal{U} . Sans perte de généralité, on peut supposer que $\mathcal{V} = \{u_1, \dots, u_r\}$ avec $1 \leq r \leq n$. Si $\alpha_1, \dots, \alpha_r \in K$ sont tels que $\alpha_1 u_1 + \dots + \alpha_r u_r = 0_E$, alors

$$\alpha_1 \cdot u_1 + \dots + \alpha_r \cdot u_r + 0_K \cdot u_{r+1} + \dots + 0_K \cdot u_n = 0_E.$$

Comme \mathcal{U} est libre, les coefficients dans le membre de gauche sont tous nuls. En particulier, $\alpha_i = 0$, pour $i = 1, \dots, r$. Ceci montre que \mathcal{V} est libre. La preuve de la proposition s'achève.

Exemple. Considérons le \mathbb{Q} -espace vectoriel

$$\mathbb{Q}_9[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8 \mid a_i \in \mathbb{Q}\}.$$

On a vu que $\{1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8\}$ est une famille libre. D'après la proposition 4.2.8, $\{1, x^2, x^4, x^6, x^8\}$ est aussi libre.

Jusqu'à maintenant, on ne considère que la dépendance linéaire et l'indépendance linéaire pour un nombre fini de vecteurs. La proposition 4.2.8 nous amène à définir ces notions pour un nombre infini de vecteurs comme suit.

4.2.9. Définition. Soit \mathcal{U} une famille (finie ou infinie) non vide de vecteurs de E . On dit que \mathcal{U} est *libre* si toutes ses sous-familles finies sont 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 $\mathcal{X} = \{1, x, x^2, \dots, x^i, \dots\}$ 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 entier maximal $n \geq 0$ tel que $x^n \in \mathcal{U}$. On voit maintenant que $\mathcal{U} \subseteq \{1, x, \dots, x^n\}$. Comme $\{1, x, \dots, x^n\}$ est une famille finie libre, d'après la proposition 4.2.7, \mathcal{U} est libre. Par définition, \mathcal{X} est libre.

(2) Considérons la famille infinie $\{\sin t, \sin 2t, \dots, \sin nt, \dots\}$ de vecteurs de l'espace vectoriel réel $C[0, 2\pi]$. De la même façon que ci-dessus, on peut vérifier qu'elle est libre.

4.2.10. Définition. Soit E un K -espace vectoriel. Une famille \mathcal{B} (finie ou infinie) de vecteurs de E s'appelle *base* de E si les deux conditions suivantes sont vérifiées:

- (1) \mathcal{B} est libre;
- (2) tout vecteur non nul de E est une combinaison linéaire de vecteurs de \mathcal{B} .

Remarque. (1) Si $E = \{0_E\}$, alors la famille vide \emptyset est la seule base de E .

(2) Si E est non nul 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 de vecteurs de \mathcal{B} .

Exemple. (1) L'espace vectoriel réel ${}_{\mathbb{R}}\mathbb{C}$ a pour base $\{1, i\}$, appelée *base canonique*. 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 ${}_{\mathbb{R}}\mathbb{C}$.

(2) 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 vecteurs de ${}_{\mathbb{C}}\mathbb{C}$. On verra que $\{1\}$ est une base ${}_{\mathbb{C}}\mathbb{C}$.

(3) Le K -espace vectoriel $K_n[x] = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} \mid a_i \in K\}$ a pour base $\{1, x, \dots, x^{n-1}\}$, appelée *base canonique*. En effet, on a vu que $\{1, x, \dots, x^{n-1}\}$ est libre. En outre, tout $f = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in K_n[x]$ s'écrit comme

$$f = a_0 \cdot 1 + a_1 \cdot x + \dots + a_{n-1} \cdot x^{n-1}.$$

Ainsi, $\{1, x, \dots, x^{n-1}\}$ est une base de $K_n[x]$.

4.2.11. Proposition. Le K -espace vectoriel $M_{m \times n}(K)$ avec $m, n \geq 1$ a pour base, appelée *base canonique*, la famille suivante:

$$\mathcal{E}_{m,n} = \{e_{ij} \mid i = 1, \dots, m; j = 1, \dots, n\},$$

où $e_{ij} \in M_{m \times n}(K)$ dont le (i, j) -terme est 1_K et tous les autres sont nuls.

Démonstration. Toute matrice $A = (a_{ij})_{m \times n} \in M_{m \times n}(K)$ s'écrit

$$A = \sum_{i=1}^m \sum_{j=1}^n a_{ij} e_{ij}, \quad \text{où } a_{ij} \in K.$$

C'est-à-dire, A est une combinaison linéaire de vecteurs de $\mathcal{E}_{m,n}$. En outre, supposons que $\alpha_{ij} \in K$, $i = 1, \dots, m$ et $j = 1, \dots, n$, sont tels que

$$\sum_{i=1}^m \sum_{j=1}^n \alpha_{ij} \cdot e_{ij} = 0_{m \times n}.$$

Remarquons que le membre de gauche est égal à la matrice $(\alpha_{ij})_{m \times n}$. D'où, $(\alpha_{ij})_{m \times n} = 0_{m \times n}$. Par définition, $\alpha_{ij} = 0$, pour $i = 1, \dots, m; j = 1, \dots, n$. Ainsi, la famille $\mathcal{E}_{m,n}$ est libre. Ceci montre que $\mathcal{E}_{m,n}$ est une base de $M_{m \times n}(K)$.

Exemple. (1) La base canonique du K -espace vectoriel K^n est

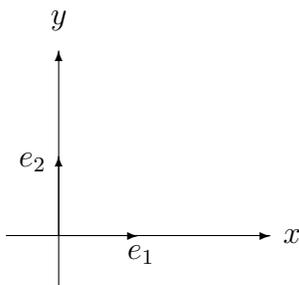
$$\{e_1 = (1_K, 0, \dots, 0), e_2 = (0, 1_K, \dots, 0), \dots, e_n = (0, \dots, 0, 1_K)\}.$$

(2) La base canonique du K -espace vectoriel $K^{(n)}$ est

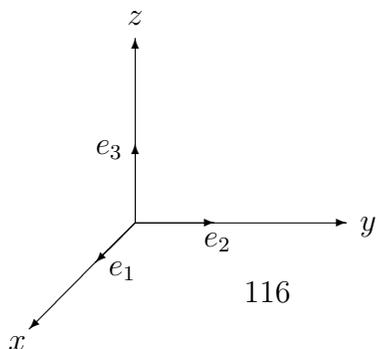
$$\left\{ e_1 = \begin{pmatrix} 1_K \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1_K \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1_K \end{pmatrix} \right\}.$$

(3) La base canonique du K -espace vectoriel K est $\{1_K\}$.

(4) La base canonique du plan \mathbb{R}^2 est $\{e_1 = (1, 0), e_2 = (0, 1)\}$, illustrée d'une façon géométrique comme suit:



(5) La base canonique de l'espace usuel \mathbb{R}^3 est $\{e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)\}$, illustrée d'une façon géométrique comme suit:



On énonce maintenant le résultat fondamental suivant, dont la démonstration est trop avancé pour ce cours.

4.2.12. Théorème. Tout espace vectoriel admet une base.

Il est à noter que, dans la plupart des 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 des matrices pour étudier les espaces vectoriels. Partout dans cette section, on se fixe E un K -espace vectoriel non nul ayant une base finie. Pour ce faire, toute base de E sera considérée comme une famille ordonnée. Par exemple, le plan \mathbb{R}^2 a deux bases distinctes $\{e_1, e_2\}$ et $\{e_2, e_1\}$, dont la première est la base canonique et la deuxième est non canonique.

4.3.1. Définition. Soit $\{u_1, \dots, u_n\}$ une base de E . D'après la proposition 4.2.5, tout vecteur u de E s'écrit d'une façon unique comme

$$u = \alpha_1 u_1 + \dots + \alpha_n u_n, \quad \alpha_1, \dots, \alpha_n \in K.$$

Dans ce cas, les coefficients $\alpha_1, \dots, \alpha_n$ s'appelle *coordonnées* de u dans la base $\{u_1, \dots, u_n\}$; et la colonne des coefficients

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

s'appelle *colonne des coordonnées* de u dans $\{u_1, \dots, u_n\}$.

Remarque. Par définition, on a

$$u = (u_1, \dots, u_n) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Ceci est illustrée par le diagramme suivant:

$$\{u_1, \dots, u_n\} \xrightarrow{\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}} u.$$

Exemple. Comme $0_E = 0_K \cdot u_1 + \cdots + 0_K \cdot u_n$, la colonne des coordonnées de 0_E dans toute base $\{u_1, \dots, u_n\}$ de E est

$$\begin{pmatrix} 0_K \\ \vdots \\ 0_K \end{pmatrix} = 0_{n \times 1}.$$

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 sa colonne des coordonnées

(1) dans la base canonique $\{e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}\}$;

(2) dans la base $\{e_{11}, e_{21}, e_{12}, e_{22}, e_{13}, e_{23}\}$.

Solution. On voit que

$$A = 2 \cdot e_{11} + 5 \cdot e_{12} + 3 \cdot e_{13} + 1 \cdot e_{21} + 0 \cdot e_{22} + 2 \cdot e_{23}.$$

Ainsi, la colonne des coordonnées de A dans $\{e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}\}$ est

$$\begin{pmatrix} 2 \\ 5 \\ 3 \\ 1 \\ 0 \\ 2 \end{pmatrix},$$

et donc,

$$A = (e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}) \begin{pmatrix} 2 \\ 1 \\ 5 \\ 0 \\ 3 \\ 2 \end{pmatrix}.$$

Par contre, comme

$$A = 2 \cdot e_{11} + 1 \cdot e_{21} + 5 \cdot e_{12} + 0 \cdot e_{22} + 3 \cdot e_{13} + 2 \cdot e_{23},$$

la colonne des coordonnées de A dans $\{e_{11}, e_{21}, e_{12}, e_{22}, e_{13}, e_{23}\}$ est

$$\begin{pmatrix} 2 \\ 1 \\ 5 \\ 0 \\ 3 \\ 2 \end{pmatrix},$$

et donc,

$$A = (e_{11}, e_{21}, e_{12}, e_{22}, e_{13}, e_{23}) \begin{pmatrix} 2 \\ 1 \\ 5 \\ 0 \\ 3 \\ 2 \end{pmatrix}.$$

Exercice. Considérer la base $\{1 + x, 2 + x, 3 + x^2\}$ de l'espace vectoriel réel $\mathbb{R}_3[x]$. Trouver $f \in \mathbb{R}_3[x]$, dont les coordonnées dans cette base sont 4, -2 , 3.

Solution. Par hypothèse, on a

$$f = (1 + x, 2 + x, 3 + x^2) \begin{pmatrix} 4 \\ -2 \\ 3 \end{pmatrix} = 4 \cdot (1 + x) + (-2)(2 + x) + 3 \cdot (3 + x^2) = 9 + 2x + 3x^2.$$

En général, trouver les coordonnées d'un vecteur u dans une base $\{u_1, \dots, u_n\}$ est équivalent à trouver la solution de l'équation

$$x_1 u_1 + \dots + x_n u_n = u.$$

Exercice. En sachant que $\{1 + i, 1 - i\}$ est une base de ${}_{\mathbb{R}}\mathbb{C}$, trouver la colonne des coordonnées de $2 + i$ dans cette base.

Solution. Considérons l'équation

$$x(1 + i) + y(1 - i) = 2 + i.$$

Ceci est équivalent au système

$$\begin{aligned} x + y &= 2 \\ x - y &= 1. \end{aligned}$$

En résolvant-le, on trouve $x = \frac{3}{2}$ et $y = \frac{1}{2}$. C'est-à-dire,

$$2 + i = \frac{3}{2}(1 + i) + \frac{1}{2}(1 - i).$$

Par conséquent, la colonne des coordonnées de $2 + i$ dans $\{1 + i, 1 - i\}$ est

$$\begin{pmatrix} \frac{3}{2} \\ \frac{1}{2} \end{pmatrix}$$

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 étudiera 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 $u = a_1e_1 + \cdots + a_ne_n$, la colonne des coordonnées de u dans $\{e_1, \dots, e_n\}$ est

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = u.$$

(2) Soit $v = (b_1, \dots, b_n) \in K^n$. Comme $v = b_1e_1 + \cdots + b_ne_n$, la colonne des coordonnées de v dans $\{e_1, \dots, e_n\}$ est

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = v^T.$$

Ceci achève la démonstration du lemme.

Exemple. (1) Considérons

$$u = \begin{pmatrix} 3 \\ 1 \\ 7 \end{pmatrix} \in \mathbb{R}^{(3)}.$$

Comme $u = 3 \cdot e_1 + 1 \cdot e_2 + 7 \cdot e_3$, la colonne des coordonnées de u dans $\{e_1, e_2, e_3\}$ est

$$\begin{pmatrix} 3 \\ 1 \\ 7 \end{pmatrix} = u.$$

(2) Considérons $v = (2, 3, 5) \in \mathbb{R}^3$. Comme $v = 2 \cdot e_1 + 3 \cdot e_2 + 5 \cdot e_3$, la colonne de v dans $\{e_1, e_2, e_3\}$ est

$$\begin{pmatrix} 2 \\ 3 \\ 5 \end{pmatrix} = v^T.$$

Le résultat suivant dit qu'un vecteur est uniquement déterminé par sa colonne des coordonnées dans une base.

4.3.3. Lemme. Soit $\{u_1, \dots, u_n\}$ une base de E . Soient $u, v \in E$ dont les colonnes de coordonnées dans $\{u_1, \dots, u_n\}$ 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

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \text{ où } a_i, b_i \in K.$$

D'après la définition, $u = a_1 u_1 + \dots + a_n u_n$ et $v = b_1 u_1 + \dots + b_n u_n$.

(1) En vue de l'unicité des coordonnées, $u = v$ si, et seulement si, $a_i = b_i$, pour $i = 1, \dots, n$, si et seulement si, $A = B$.

(2) La colonne des coordonnées de 0_E dans la base $\{u_1, \dots, u_n\}$ 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.

Plus généralement, on a la notion suivante.

4.3.4. Définition. Soit $\{u_1, \dots, u_n\}$ une base de E . Soient $v_1, \dots, v_m \in E$ dont les colonnes des coordonnées dans $\{u_1, \dots, u_n\}$ sont A_1, \dots, A_m respectivement. On appelle la matrice des coefficients

$$(A_1 \cdots A_m) \in M_{n \times m}(K)$$

matrice des coordonnées de $\{v_1, \dots, v_m\}$ dans $\{u_1, \dots, u_n\}$, notée $P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_m\}}$.

Remarque. (1) Par définition, on a

$$(v_1, \dots, v_m) = (u_1, \dots, u_n) P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_m\}},$$

ceci est illustré par le diagramme

$$\{u_1, \dots, u_n\} \xrightarrow{P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_m\}}} \{v_1, \dots, v_m\}.$$

(2) Si $m = 1$, alors $P_{\{u_1, \dots, u_n\}}^{\{v\}}$ est la colonne des coordonnées de v dans $\{u_1, \dots, u_n\}$.

Exercice. Soit $\{u_1, u_2, u_3\}$ une base de \mathbb{R}^3 . Donner $P_{\{u_1, u_2, u_3\}}^{\{u_3, u_2\}}$.

Solution. Comme

$$\begin{aligned} u_3 &= 0 \cdot u_1 + 0 \cdot u_2 + 1 \cdot u_3 \\ u_2 &= 0 \cdot u_1 + 1 \cdot u_2 + 0 \cdot u_3, \end{aligned}$$

on a

$$P_{\{u_1, u_2, u_3\}}^{\{u_3, u_2\}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

C'est-à-dire,

$$(u_3, u_2) = (u_1, u_2, u_3) \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

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

$$P_{\{e_{11}, e_{22}, e_{21}, e_{12}\}}^{\{A_1, A_2, A_3\}} = \begin{pmatrix} 1 & 5 & 7 \\ 4 & 1 & 3 \\ 3 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}.$$

Solution. Par hypothèse, on a

$$(A_1, A_2, A_3) = (e_{11}, e_{22}, e_{21}, e_{12}) \begin{pmatrix} 1 & 5 & 7 \\ 4 & 1 & 3 \\ 3 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}.$$

Ceci nous donne

$$A_1 = 1 \cdot e_{11} + 4 \cdot e_{22} + 3 \cdot e_{21} + 2 \cdot e_{12} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix};$$

$$A_2 = 5 \cdot e_{11} + 1 \cdot e_{22} + 2 \cdot e_{21} + 0 \cdot e_{12} = \begin{pmatrix} 5 & 0 \\ 2 & 1 \end{pmatrix};$$

$$A_3 = 7 \cdot e_{11} + 3 \cdot e_{22} + 0 \cdot e_{21} + 1 \cdot e_{12} = \begin{pmatrix} 7 & 1 \\ 0 & 3 \end{pmatrix}.$$

Le résultat suivant est une conséquence immédiate du lemme 4.3.2.

4.3.5. Lemme. (1) Si $v_1, \dots, v_m \in K^{(n)}$, alors la matrice des coordonnées canoniques de $\{v_1, \dots, v_m\}$ est $(v_1 \cdots v_m)$.

(2) Si $w_1, \dots, w_m \in K^n$, alors la matrice des coordonnées canoniques de $\{w_1, \dots, w_m\}$ est $(w_1^T \cdots w_m^T)$.

Exemple. (1) Considérons

$$v_1 = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}, v_3 = \begin{pmatrix} -2 \\ 3 \\ -4 \end{pmatrix}, v_4 = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} \in \mathbb{R}^{(3)}.$$

La matrice de la famille $\{v_1, v_2, v_3, v_4\}$ dans la base canonique de \mathbb{R}^3 est

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

(2) Considérons

$$w_1 = (1, 2, 0), w_2 = (2, 1, 3), w_3 = (5, 3, 4), w_4 = (1, 1, 0) \in \mathbb{Q}^3.$$

La matrice des coordonnées de $\{w_1, w_2, w_3, w_4\}$ dans la base canonique de \mathbb{Q}^3 est

$$(w_1^T w_2^T w_3^T w_4^T) = \begin{pmatrix} 1 & 2 & 5 & 1 \\ 2 & 1 & 3 & 1 \\ 0 & 3 & 4 & 0 \end{pmatrix}.$$

Le résultat suivant dit comment utiliser la matrice des coordonnées pour déterminer si l'un vecteur est une combinaison linéaire ou non d'une famille de vecteurs donnée.

4.3.6. Théorème. Soit $\{u_1, \dots, u_n\}$ une base de E . Considérons $v_1, \dots, v_m; v \in E$. Et posons $A = P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_m\}}$ et $B = P_{\{u_1, \dots, u_n\}}^{\{v\}}$. Alors

(1) $v = \alpha_1 v_1 + \dots + \alpha_m v_m$ avec $\alpha_1, \dots, \alpha_m \in K$ 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, \dots, v_m si, et seulement si, $\text{rg}(A) = \text{rg}(A|B)$.

Démonstration. (1) Par définition, $(v_1, \dots, v_m) = (u_1, \dots, u_n)A$. Pour $\alpha_1, \dots, \alpha_m \in K$, d'après la proposition 4.2.2, on voit que

$$\alpha_1 v_1 + \dots + \alpha_m v_m = (v_1, \dots, v_m) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = (u_1, \dots, u_n)A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}.$$

D'où,

$$P_{\{u_1, \dots, u_n\}}^{\{\alpha_1 v_1 + \dots + \alpha_m v_m\}} = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}.$$

D'après le lemme 4.3.3(1), $v = \alpha_1 v_1 + \dots + \alpha_m v_m$ si, et seulement si,

$$P_{\{u_1, \dots, u_n\}}^{\{\alpha_1 v_1 + \dots + \alpha_m v_m\}} = P_{\{u_1, \dots, u_n\}}^{\{v\}}$$

si, et seulement si,

$$A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = B$$

si, et seulement si,

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

est une solution du système $AX = B$.

(2) D'après l'énoncé (1), v est une combinaison linéaire de v_1, \dots, v_m si, et seulement si, $AX = B$ est compatible. D'après le théorème 3.12, cette dernière condition est équivalente à $\text{rg}(A) = \text{rg}(A|B)$. Ceci achève la démonstration du théorème.

Exercice. Considérer l'espace vectoriel rationnel $\mathbb{Q}_3[x]$ et ses vecteurs

$$f_1 = 2 - x + x^2, \quad f_2 = 1 + x - 2x^2, \quad f = 3 + x + ax^2.$$

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.

Solution. Considérons la base canonique $\{1, x, x^2\}$ de $\mathbb{Q}_3[x]$. On a

$$P_{\{1, x, x^2\}}^{\{v_1, v_2, v_3\}} = \begin{pmatrix} 2 & 1 \\ -1 & 1 \\ 1 & -2 \end{pmatrix} =: A; \quad P_{\{1, x, x^2\}}^{\{v\}} = \begin{pmatrix} 3 \\ 1 \\ a \end{pmatrix} =: B.$$

Considérons le système $AX = B$. Comme la matrice augmentée $(A \mid B)$ s'échelonne à la matrice

$$\left(\begin{array}{cc|c} -1 & 1 & 1 \\ 0 & -1 & a+1 \\ 0 & 0 & 3a+8 \end{array} \right).$$

D'après le théorème 4.3.6(2), f est une combinaison linéaire de f_1, f_2 si, et seulement si, $3a + 8 = 0$ si, et seulement si, $a = -\frac{8}{3}$. Dans ce cas, on voit que $(\frac{2}{3}, \frac{5}{3})$ est une solution du système $AX = B$. En vertu du théorème 4.3.6(1), on obtient

$$v = \frac{2}{3}u_1 + \frac{5}{3}u_2.$$

Le résultat suivant nous dit comment utiliser la matrice des coordonnées pour déterminer si une famille de vecteurs est libre ou liée.

4.3.7. Théorème. Soit $\{u_1, \dots, u_n\}$ une base de E . Considérons $v_1, \dots, v_m \in E$, et posons $A = P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_m\}}$.

- (1) Les trois conditions suivantes sont équivalentes.
 - (a) $\{v_1, \dots, v_m\}$ est libre.
 - (b) Le système homogène suivant n'a que la solution nulle

$$AX = 0.$$

- (c) $\text{rg}(A) = m$, le nombre de colonnes de A .
- (2) Si $m > n$, alors $\{v_1, \dots, v_m\}$ est toujours liée. C'est-à-dire, si $\{v_1, \dots, v_m\}$ est libre, alors $m \leq n$.

Démonstration. La famille $\{v_1, \dots, v_m\}$ est liée si, et seulement si, il existe $\alpha_1, \dots, \alpha_n \in K$, non tous nuls, tels que

$$\alpha_1 u_1 + \dots + \alpha_n u_n = 0_E.$$

Comme $P_{\{u_1, \dots, u_n\}}^{\{0_E\}} = 0_{n \times 1}$, d'après le théorème 4.3.6(1), cela est équivalent à

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

est une solution non nulle du système homogène $AX = 0_{n \times 1}$. Ceci montre l'équivalence des énoncés (a) et (b). D'après le théorème 3.14(1), les énoncés (b) et (c) sont équivalents.

(2) Supposons que $m > n$. Alors $\text{rg}(A) \leq \min\{m, n\} = n < m$. Comme les énoncés (1) et (3) sont équivalents, $\{v_1, \dots, v_m\}$ 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.

Solution. Considérant la base canonique $\{1, x, x^2\}$ de $\mathbb{Q}_3[x]$, on a

$$P_{\{1, x, x^2\}}^{\{f_1, f_2, f_3\}} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} := A,$$

qui s'échelonne à

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

Donc, $\text{rg}(A) = 2 < 3$. D'après le théorème 4.3.7, $\{f_1, f_2, f_3\}$ est liée.

Le résultat suivant est un cas particulier des théorèmes 4.3.6 et 4.3.7, qui donne une autre preuve de la première partie du théorème 3.12.

4.3.8. Théorème. Soit $A \in M_{m \times n}(K)$ de colonnes $A_1, \dots, A_n \in K^{(m)}$.

(1) La famille $\{A_1, \dots, A_n\}$ est liée si, et seulement si, $\text{rg}(A) = n$.

(2) Pour tout $B \in K^{(m)}$, les conditions suivantes sont équivalentes:

(a) B est une combinaison linéaire de A_1, \dots, A_n .

- (b) Le système $AX = B$ est compatible.
 (c) $\text{rg}(A) = \text{rg}(A | B)$.

Démonstration. Posons $A = (A_1 \cdots A_m)$, où $A_1, \dots, A_m \in K^{(m)}$. D'après le lemme 4.3.5(1), $A = P_{\{e_1, \dots, e_m\}}^{\{A_1, \dots, A_m\}}$, où $\{e_1, \dots, e_m\}$ est la base canonique de $K^{(m)}$.

(1) D'après le théorème 4.3.7(3), $\{A_1, \dots, A_m\}$ est libre si, et seulement si, $\text{rg}(A) = m$.

(2) D'après le lemme 4.3.2(1), $P_{\{e_1, \dots, e_m\}}^{\{B\}} = B$. D'après le théorème 4.3.7(2), B est une combinaison linéaire de A_1, \dots, A_m si, et seulement si, le système $AX = B$ est compatible si, et seulement si, $\text{rg}(A) = \text{rg}(A|B)$. Ceci achève la preuve du théorème.

Exercice. Considérons la matrice réelle

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

Donner les valeurs de a pour que les colonnes de A soient linéairement indépendantes.

Solution. On voit que A s'échelonne à

$$\begin{pmatrix} 1 & -2 & a \\ 0 & 1 & -2a - 8 \\ 0 & 0 & 4a + 19 \\ 0 & 0 & 0 \end{pmatrix}.$$

D'après le théorème 4.3.8(1), les colonnes de A sont linéairement indépendantes si, et seulement si, $\text{rg}(A) = 3$ si, et seulement si, $a \in \mathbb{R} \setminus \{-\frac{19}{4}\}$.

4.4. Dimension

Partout dans cette section, on se fixe E un K -espace vectoriel. D'après le théorème 4.2.12, 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 *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 $\mathcal{U} = \{u_1, \dots, u_n\}$ avec $n > 0$. Comme \mathcal{B} est libre, d'après le théorème 4.3.7(2), $|\mathcal{B}| \leq n$. En particulier, \mathcal{B} est fini. De même, $|\mathcal{U}| \leq |\mathcal{B}|$. D'où, $|\mathcal{B}| = |\mathcal{U}|$. Ceci achève la démonstration du théorème.

Remarque. On dit que E est de *dimension infinie* s'il admet une base infinie; et de *dimension finie* s'il admet une base finie.

Exemple. (1) $\dim_{\mathbb{R}} \mathbb{C} = 2$. En effet, $\mathbb{R}\mathbb{C}$ a pour base $\{1, i\}$.

(2) Par contre, $\dim_{\mathbb{C}} \mathbb{C} = 1$. En effet, $_{\mathbb{C}}\mathbb{C}$ a pour base $\{1\}$.

(3) Pour $m, n \geq 1$, $\dim M_{m \times n}(K) = mn$. En effet, $M_{m \times n}(K)$ a pour base

$$\{e_{ij} \mid i = 1, \dots, m; j = 1, \dots, n\}.$$

(4) En particulier, $\dim K^n = \dim K^{(n)} = n$, pour tout $n \geq 1$.

(5) Pour tout $n \geq 1$, $\dim K_n[x] = n$. En effet, $K_n[x]$ a pour base $\{1, x, \dots, x^{n-1}\}$.

Exercice. Considérons le K -espace vectoriel

$$K[x] = \{a_0 + a_1x + \dots + a_mx^m \mid m \geq 0; a_0, a_1, \dots, a_m \in K\}.$$

Vérifier que $K[x]$ est dimension infinie.

Preuve. D'abord, on a vu que $\mathcal{X} = \{1, x, \dots, x^i, \dots\}$ est une famille libre infinie de $K[x]$. Maintenant, tout $f(x) \in K[x]$ s'écrit

$$f(x) = a_0 + a_1x + \dots + a_mx^m = a_0 \cdot 1 + a_1 \cdot x + \dots + a_m \cdot x^m,$$

où $a_0, \dots, a_m \in K$ et $1, x, \dots, x^m \in \mathcal{X}$. Ainsi, \mathcal{X} est une base infinie de $K[x]$. Par définition, $K[x]$ est de dimension infinie.

Exercice. Montrer que $\dim(E) = 0$ si, et seulement si, $E = \{0_E\}$.

Démonstration. Si $E = \{0_E\}$, alors l'ensemble vide \emptyset est la base de E , et donc $\dim(E) = |\emptyset| = 0$. Si E est non nul, alors il a une base non vide \mathcal{B} . D'où, $\dim(E) = |\mathcal{B}| > 0$.

Le résultat suivant dit que la dimension d'un espace vectoriel de dimension finie est le plus grand nombre de vecteurs linéairement indépendants.

4.4.2. Lemme. Si E est de dimension $n(\geq 0)$, alors

(1) toute famille de plus que n vecteurs de E est liée;

(2) toute famille libre de n vecteurs de E est une base.

Démonstration. Soit $\dim(E) = n$. D'abord, 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. Donc, le lemme est valide dans ce cas.

Supposons maintenant que E admet une base $\mathcal{B} = \{u_1, \dots, u_n\}$, où $n > 0$. D'après le théorème 4.3.8, l'énoncé (1) est valide. Enfin, supposons que $\mathcal{V} = \{v_1, \dots, v_n\}$ est une famille libre. 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, \dots, v_n . D'après la proposition 4.2.7, $\{v_1, \dots, v_n, v_{n+1}\}$ est une famille libre de $n + 1$ vecteurs, une contradiction à l'énoncé (1). Ceci achève la preuve de l'énoncé (2) et celle de du lemme.

Exemple. (1) Le K -espace $K_n[x]$ est de dimension n . Ainsi, toute famille de $n + 1$ polynômes de degré $< n$ est liée.

(2) 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.

(3) Considérons l'espace réel $\mathbb{R}^{(2)}$. On a vu que

$$\left\{ u_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, u_2 = \begin{pmatrix} 1 \\ 3 \end{pmatrix} \right\}$$

est libre. Comme $\dim(\mathbb{R}^{(2)}) = 2$, il s'agit d'une base de $\mathbb{R}^{(2)}$.

Une base d'un espace vectoriel satisfait à deux conditions énoncées dans la définition 4.2.10. Maintenant, on étudiera les familles de vecteurs qui ne satisfait qu'à une de ces deux conditions.

4.4.3. Proposition. Si E est de dimension finie, alors toute famille libre de vecteurs de E est contenue dans une base de E .

Démonstration. Supposons que $\dim(E) = n$. Soit $\mathcal{U} = \{v_1, \dots, v_m\}$ une famille libre. D'après le lemme 4.4.2(1), $m \leq n$. On procède par récurrence sur $r = n - m \geq 0$.

Si $r = 0$, alors $m = n$, et d'après le lemme 4.4.2(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, E a au moins un vecteur v , qui n'est pas une combinaison linéaire de v_1, \dots, v_m . D'après la proposition 4.2.7, $\mathcal{V} = \{v_1, \dots, v_m, v\}$ est libre. Comme $n - |\mathcal{V}| = r - 1$, d'après l'hypothèse de récurrence, \mathcal{V} est contenue dans une base de E , et donc, \mathcal{U} est contenue dans cette même base de E . Ceci achève la démonstration de la proposition.

Exercice. Considérons l'espace vectoriel réel \mathbb{C} . Donner une base de ${}_{\mathbb{R}}\mathbb{C}$ contenant $2 + 3i$.

Solution. D'après le lemme 4.2.6(1), $\{2 + 3i\}$ est libre. On voit aisément que $2 - 3i$ n'est pas un multiple de $2 + 3i$. D'après la proposition 4.2.7, $\{2 + 3i, 2 - 3i\}$ est libre. Comme $\dim_{\mathbb{R}}\mathbb{C} = 2$, d'après le lemme 4.4.2(2), $\{2 + 3i, 2 - 3i\}$ est une base de $\mathbb{R}\mathbb{C}$.

4.4.4. Proposition. Soit \mathcal{U} une famille finie de vecteurs de E telle que 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 de E contenue dans \mathcal{U} .

Supposons que E est non nul. Alors \mathcal{U} contient au moins un vecteur non nul u . D'après le lemme 4.2.6(1), $\{u\}$ est une sous-famille libre de \mathcal{U} . Soit n le plus grand nombre tel que \mathcal{U} a une sous-famille libre de n vecteurs, notée $\{u_1, \dots, u_n\}$. Si \mathcal{U} contient un vecteur v qui n'est pas une combinaison linéaire de u_1, \dots, u_n , d'après la proposition 4.2.7, $\{u_1, \dots, u_n, v\}$ 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, \dots, u_n .

Soit $u \in E$. Par l'hypothèse, $u = \alpha_1 v_1 + \dots + \alpha_s v_m$, où $v_1, \dots, v_m \in \mathcal{U}$. Comme chaque v_i est une combinaison linéaire de u_1, \dots, u_n , d'après la proposition 4.2.2, u est une combinaison linéaire de u_1, \dots, u_n . D'où, $\{u_1, \dots, u_n\}$ est une base de E contenue dans \mathcal{U} . Ceci achève la démonstration de la proposition.

Le résultat suivant est très pratique pour déterminer si une famille de vecteurs est une base ou non.

4.4.5. Théorème. Soit E de dimension $n > 0$, dont $\{u_1, \dots, u_n\}$ est une base. Si $v_1, \dots, v_n \in E$, alors les conditions suivantes sont équivalentes.

- (1) $\{v_1, \dots, v_n\}$ est une base.
- (2) $\{v_1, \dots, v_n\}$ est libre.
- (3) Tout vecteur de E est une combinaison linéaire de v_1, \dots, v_n .
- (4) $P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_n\}}$ 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 $\{v_1, \dots, v_n\} \subseteq \mathcal{B}$, ou bien, $\mathcal{B} \subseteq \{v_1, \dots, v_n\}$. Comme $\dim(E) = n$, on a $|\mathcal{B}| = n$. Ainsi $\{v_1, \dots, v_n\} = \mathcal{B}$, ce qui est une base de E . Ceci montre l'équivalence des trois premiers énoncés.

Enfin, $\{v_1, \dots, v_n\}$ est une base si, et seulement si, $\{v_1, \dots, v_n\}$ est libre si, et seulement si, $P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_n\}}$ est de rang n si, et seulement si, $P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_n\}}$ 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) $\{f_1 = 1 + x, f_2 = 2 + x, f_3 = 3 + x + x^2\} \subseteq \mathbb{R}_3[x]$.

Solution. (1) Considérons la bse canonique $\{e_1, e_2, e_3\}$ de \mathbb{R}^3 . D'après le lemme 4.3.5(2), on a

$$P_{\{e_1, e_2, e_3\}}^{\{v_1, v_2, v_3\}} = (v_1^T \ v_2^T \ v_3^T) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 1 & 3 & 4 \end{pmatrix} \implies \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Ainsi $P_{\{e_1, e_2, e_3\}}^{\{v_1, v_2, v_3\}}$ n'est pas inversible. D'après le théorème 4.4.5(4), $\{v_1, v_2, v_3\}$ n'est pas une base de \mathbb{R}^3 .

(2) Considérons la base canonique $\{1, x, x^2\}$ de $\mathbb{R}_3[x]$. On voit que

$$P_{\{1, x, x^2\}}^{\{f_1, f_2, f_3\}} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \implies \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix}.$$

D'après le théorème 4.4.5(4), $\{f_1, f_2, f_3\}$ est une base de $\mathbb{R}_3[x]$.

Exercice. Augmenter la famille $\{u_1 = (1, 2, 1), u_2 = (2, 1, 1)\}$ à une base de \mathbb{R}^3 .

Solution. On veut trouver un vecteur $u_3 = (a, b, c)$, qui n'est pas une combinaison linéaire de u_1, u_2 . D'après le lemme 4.3.6(2), on a

$$P_{\{e_1, e_2, e_3\}}^{\{u_1, u_2\}} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 1 & 1 \end{pmatrix} =: A \text{ et } P_{\{e_1, e_2, e_3\}}^{\{u_3\}} = \begin{pmatrix} a \\ b \\ c \end{pmatrix} =: B.$$

Or $(A \mid B)$ s'échelonne à

$$\left(\begin{array}{cc|c} 1 & 2 & a \\ 0 & 1 & a - c \\ 0 & 0 & a + b - 3c \end{array} \right).$$

En particulier, $\text{rg}(A) = 2$, et donc $\{u_1, u_2\}$ est libre.

En outre, si l'on prend par exemple $a = 0, b = 1$ et $c = 0$, alors $a + b - 3c \neq 0$, et donc, $\text{rg}(A) < \text{rg}(A \mid B)$. D'après le théorème 4.3.7(2), u_3 n'est pas une combinaison linéaire de u_1, u_2 . En vertu de la proposition 4.2.7, $\{u_1, u_2, u_3\}$ est libre. Comme $\dim(\mathbb{R}^3) = 3$, d'après le théorème 4.4.5(2), $\{u_1, u_2, u_3\}$ est 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 positive.

4.5.1. Définition. Soient $\{u_1, \dots, u_n\}$ et $\{v_1, \dots, v_n\}$ deux bases de E . La matrice des coordonnées de la deuxième base dans la première base

$$P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_n\}}$$

s'appelle *matrice de passage* de $\{u_1, \dots, u_n\}$ vers $\{v_1, \dots, v_n\}$, illustré par

$$\{u_1, \dots, u_n\} \xrightarrow{P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_n\}}} \{v_1, \dots, v_n\}.$$

Remarque. D'après le théorème 4.4.6(4), la matrice de passage $P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_n\}}$ est toujours inversible.

Exemple. (1) La matrice de passage d'une base $\{u_1, \dots, u_n\}$ vers $\{u_1, \dots, u_n\}$ est I_n .

(2) L'espace vectoriel réel $\mathbb{R}\mathbb{C}$ a pour bases $\{1, i\}$ et $\{2 + 3i, 1 - 5i\}$. La matrice de passage de $\{1, i\}$ vers $\{2 + 3i, 1 - 5i\}$ est, par définition, la matrice des coordonnées

$$P_{\{1, i\}}^{\{2+3i, 1-5i\}} = \begin{pmatrix} 2 & 1 \\ 3 & -5 \end{pmatrix}.$$

C'est-à-dire,

$$\{1, i\} \xrightarrow{\begin{pmatrix} 2 & 1 \\ 3 & -5 \end{pmatrix}} \{2 + 3i, 1 - 5i\}.$$

Si E est l'un des espaces vectoriels de dimension finie ayant une base canonique, alors il est trivial de trouver les coordonnées d'un vecteur dans la base canonique. Le résultat suivant nous dit 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 $\{u_1, \dots, u_n\}$ et $\{v_1, \dots, v_n\}$ deux bases de E . Soit P la matrice de passage de $\{u_1, \dots, u_n\}$ vers $\{v_1, \dots, v_n\}$. Si $\{w_1, \dots, w_m\}$ est une famille ordonnée de vecteurs de E avec $P_{\{u_1, \dots, u_n\}}^{\{w_1, \dots, w_m\}} = A$, alors

$$P_{\{v_1, \dots, v_n\}}^{\{w_1, \dots, w_m\}} = P^{-1}A.$$

Ceci est illustrée par le diagramme commutatif

$$\begin{array}{ccc}
 \{u_1, \dots, u_n\} & \xrightarrow{P} & \{v_1, \dots, v_n\} \\
 & \searrow A & \downarrow P^{-1}A \\
 & & \{w_1, \dots, w_m\}.
 \end{array}$$

Démonstration. Par hypothèse, $(v_1, \dots, v_n) = (u_1, \dots, u_n)P$. D'où

$$(v_1, \dots, v_n)P^{-1} = ((u_1, \dots, u_n)P)P^{-1} = (u_1, \dots, u_n)(PP^{-1}) = (u_1, \dots, u_n)I_n = (u_1, \dots, u_n).$$

Comme $P_{\{u_1, \dots, u_n\}}^{\{w_1, \dots, w_m\}} = A$, on a

$$(w_1, \dots, w_m) = (u_1, \dots, u_n)A = ((v_1, \dots, v_n)P^{-1})A = (v_1, \dots, v_n)(P^{-1}A).$$

D'où, $P_{\{v_1, \dots, v_n\}}^{\{w_1, \dots, w_m\}} = P^{-1}A$. Ceci achève la démonstration de la proposition.

Remarque. Lorsque $m = 1$, 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 $\{1 + x, 2 + x, 3 + x + x^2\}$.

Solution. La matrice de passage de $\{1, x, x^2\}$ vers $\{1 + x, 2 + x, 3 + x + x^2\}$ est

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

Or la colonne de f dans $\{1, x, x^2\}$ est

$$B = \begin{pmatrix} 4 \\ 5 \\ 3 \end{pmatrix}.$$

Ainsi la colonne de f dans la base $\{1 + x, 2 + x, 3 + x + x^2\}$ est

$$P^{-1}B = \begin{pmatrix} -1 & 2 & 1 \\ 1 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 4 \\ 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 9 \\ -7 \\ 3 \end{pmatrix}.$$

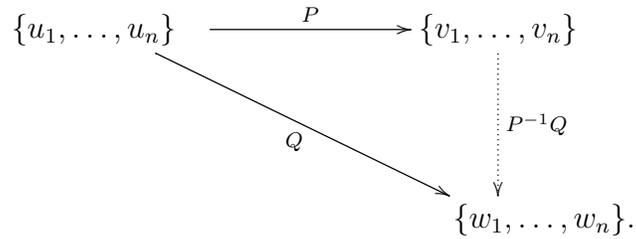
Ceci signifie que

$$f = 9(1 + x) - 7(2 + x) + 3(3 + x + x^2) = 4 + 5x - 4x^2.$$

Étant un cas particulier de la proposition 4.5.2, le résultat suivant nous permettra de trouver la matrice de passage d'une base quelconque vers une autre base quelconque.

4.5.3. Corollaire. Soient $\{u_1, \dots, u_n\}$, $\{v_1, \dots, v_n\}$ et $\{w_1, \dots, w_n\}$ trois bases de E . Si P et Q sont les matrices de passage de $\{u_1, \dots, u_n\}$ vers $\{v_1, \dots, v_n\}$ et vers $\{w_1, \dots, w_n\}$ respectivement, alors la matrice de passage

- (1) de $\{v_1, \dots, v_n\}$ vers $\{u_1, \dots, u_n\}$ est P^{-1} .
- (2) de $\{v_1, \dots, v_n\}$ vers $\{w_1, \dots, w_n\}$ est $P^{-1}Q$, ceci est illustrée par le diagram



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 $\{v_1, v_2, v_3\}$.

Solution. On voit que les matrices de passage de la base canonique $\{e_1, e_2, e_3\}$ vers $\{u_1, u_2, u_3\}$ et vers $\{v_1, v_2, v_3\}$ sont respectivement

$$P = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad Q = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

(1) D'après le corollaire 4.5.3(1), on voit la matrice de passage de la base $\{u_1, u_2, u_3\}$ vers la base $\{e_1, e_2, e_3\}$ est

$$P^{-1} = \begin{pmatrix} -1 & 2 & 1 \\ 1 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ceci signifie que

$$\begin{aligned}e_1 &= (-1) \cdot u_1 + 1 \cdot u_2 + 0 \cdot u_3 \\e_2 &= 2 \cdot u_1 + (-1) \cdot u_2 + 0 \cdot u_3 \\e_3 &= 1 \cdot u_1 + (-2) \cdot u_2 + 1 \cdot u_3.\end{aligned}$$

(2) D'après le corolaire 4.5.3(2), on voit que la matrice de passage de la base $\{u_1, u_2, u_3\}$ vers la base $\{v_1, v_2, v_3\}$ est

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

Ceci signifie que

$$\begin{aligned}v_1 &= 3 \cdot u_1 + (-3) \cdot u_2 + 1 \cdot u_3 \\v_2 &= (-1) \cdot u_2 + 1 \cdot u_3 \\v_3 &= 1 \cdot u_1\end{aligned}$$

4.6. Sous-espaces vectoriels

Partout dans cette section, on se fixe un espace vectoriel E sur K .

4.6.1. Définition. Un sous-ensemble non vide F de E s'appelle *sous-espace vectoriel* (ou simplement, *sous-espace*) si, pour tous $u, v \in F$ et $\alpha \in K$, les deux conditions suivantes sont vérifiées:

- (1) $\alpha u \in F$;
- (2) $u + v \in F$.

Remarque. Si F est un sous-espace vectoriel de E , alors

- (1) $0_E \in F$.
- (2) F est un K -espace vectoriel pour les opérations induites de celles de E comme suit:

$$\cdot : K \times F \rightarrow F : (\alpha, u) \mapsto \alpha u$$

$$+ : F \times F \rightarrow F : (u, v) \mapsto u + v.$$

En particulier, $0_F = 0_E$.

Exemple. (1) Il est évident que E est aussi un sous-espace de E . En outre, $\{0_E\}$ est un sous-espace vectoriel de E , appelé *sous-espace nul* de E . Les sous-espaces $\{0_E\}$ et E sont dits *triviaux*.

(2) $F = \{(x, y, 0) \mid x, y \in \mathbb{R}\}$ est un sous-espace de \mathbb{R}^3 .

En effet, F est non vide car $(0, 0, 0) \in F$. Si $(x, y, 0), (x', y', 0) \in F$, $\alpha \in \mathbb{R}$, alors

$$(x, y, 0) + (x', y', 0) = (x + x', y + y', 0), \quad \alpha \cdot (x, y, 0) = (\alpha x, \alpha y, 0) \in F.$$

Par définition, F est un sous-espace de \mathbb{R}^3 .

Exercice. Vérifier si les ensembles suivants sont des sous-espaces de \mathbb{R}^2 ou non.

(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) $H = \{(x, y) \in \mathbb{R}^2 \mid x = 0 \text{ ou } y = 0\}$.

Solution. (1) Comme F est vide, il n'est pas un sous-espace de \mathbb{R}^2 .

(2) On voit que $(1, 1) \in G$ et $\frac{1}{2}(1, 1) = (\frac{1}{2}, \frac{1}{2}) \notin G$. C'est-à-dire, G n'est pas stable la multiplication par un scalaire, et donc, G n'est pas un sous-espace de \mathbb{R}^2 .

(3) On voit que $(1, 0), (0, 1) \in H$ et $(1, 0) + (0, 1) = (1, 1) \notin H$. Ainsi, H n'est pas stable pour l'addition, et donc, H n'est pas un sous-espace de \mathbb{R}^2 .

4.6.2. Proposition. Soit F un sous-ensemble non vide de E . Les conditions suivantes sont équivalentes.

(1) F est un sous-espace vectoriel de E .

(2) Si $u, v \in F$ et $\alpha, \beta \in K$, alors $\alpha u + \beta v \in F$.

(3) Si $u_1, \dots, u_r \in F$ et $\alpha_1, \dots, \alpha_r \in K$, où $r \geq 1$, alors $\alpha_1 u_1 + \dots + \alpha_r u_r \in F$.

Démonstration. Supposons que l'énoncé (1) est valide. Si $u, v \in E$ et $\alpha, \beta \in K$, alors $\alpha u, \beta v \in F$, et donc, $\alpha u + \beta v \in F$. Donc, l'énoncé (2) est valide.

Supposons que l'énoncé (2) est valide. Soient $u_1, \dots, u_r \in E$ et $\alpha_1, \dots, \alpha_r \in K$ 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 valide pour $r - 1$. En particulier, $\alpha_1 u_1 + \dots + \alpha_{r-1} u_{r-1}, \alpha_r u_r \in F$. D'où

$$\alpha_1 u_1 + \dots + \alpha_{r-1} u_{r-1} + \alpha_r u_r = 1 \cdot (\alpha_1 u_1 + \dots + \alpha_{r-1} u_{r-1}) + \alpha_r u_r \in E.$$

Ceci montre que l'énoncé (3) est valide.

Enfin, supposons que l'énoncé (3) est valide. Si $u, v \in F$ et $\alpha \in K$, alors $\alpha u \in F$ et $u + v = 1_K \cdot u + 1_K \cdot v \in F$. C'est-à-dire, F est un sous-espace vectoriel de E . Ceci achève la démonstration de la proposition.

Exercice. Vérifier que \mathbb{R}^2 admet un sous-espace vectoriel

$$F = \{(x, y) \in \mathbb{R}^2 \mid 2x + 3y = 0\}.$$

Démonstration. Supposons que $u = (x, y), v = (x', y') \in F$ et $\alpha, \beta \in \mathbb{R}$. Alors $\alpha u + \beta v = (\alpha x + \beta x', \alpha y + \beta y') \in \mathbb{R}^2$ est tel que

$$2(\alpha x + \beta x') + 3(\alpha y + \beta y') = \alpha(2x + 3y) + \beta(2x' + 3y') = \alpha \cdot 0 + \beta \cdot 0 = 0.$$

Ainsi, $\alpha u + \beta v \in F$. D'après la proposition 4.6.2, F est un sous-espace vectoriel de \mathbb{R}^2 .

4.6.3. Proposition. Soit F un sous-espace de E .

(1) $\dim(F) \leq \dim(E)$.

(2) 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 $\dim(E) = n$. On prend une base \mathcal{U} de F . Alors, \mathcal{U} est une famille libre de vecteurs de E . D'après le lemme 4.4.2(1), $|\mathcal{U}| \leq n$. D'où, $\dim(F) = r \leq \dim(E)$.

Supposons que $\dim(F) = \dim(E) = n$. Alors F admet une base $\mathcal{U} = \{u_1, \dots, u_n\}$. En particulier, \mathcal{U} est une famille libre de n vecteurs de E . D'après le lemme 4.4.2(2), \mathcal{U} est une base de E . Ainsi tout $u \in E$ s'écrit $u = \alpha_1 u_1 + \dots + \alpha_n u_n$, $\alpha_i \in K$. 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 proposition 4.6.3(2) n'est pas vraie si E est de dimension infinie. Par exemple, le K -espace vectoriel de dimension infinie $K[x]$ a un sous-espace vectoriel

$$F = \{a_1 x + \dots + a_m x^m \mid m \geq 1; a_1, \dots, a_m \in K\}.$$

On voit que $\mathcal{Y} = \{x, x^2, \dots, x^m, \dots\}$ est une base de F . Ainsi, $\dim(F) = \infty = \dim(K[x])$. Mais, il est clair que $F \neq K[x]$.

Un sous-espace vectoriel F de \mathbb{R}^n avec $n \geq 1$ s'appelle *droite vectorielle* si $\dim(F) = 1$; et *plan vectoriel* si $\dim(F) = 2$.

Exemple. (1) Si F est un sous-espace non trivial du plan \mathbb{R}^2 , alors F est une droite vectorielle.

En effet, $\{(0, 0)\} \subset F \subset \mathbb{R}^2$. D'après la proposition 4.6.3(2), $\dim\{(0, 0)\} < \dim(F) < \dim(\mathbb{R}^2)$. C'est-à-dire, $0 < \dim(F) < 2$. D'où, $\dim(F) = 1$.

(2) Si F est un sous-espace non trivial de \mathbb{R}^3 , alors F est une droite vectorielle ou un plan vectoriel.

En effet, $\{(0, 0, 0)\} \subset F \subset \mathbb{R}^3$. D'après la proposition 4.6.3(2), $\dim\{(0, 0, 0)\} < \dim(F) < \dim(\mathbb{R}^3)$. C'est-à-dire, $0 < \dim(F) < 3$. D'où, $\dim(F) = 1$ ou 2 .

4.6.4. Proposition. Soit \mathcal{U} une famille non-vide de vecteurs de E . L'ensemble

$$\langle \mathcal{U} \rangle := \{ \alpha_1 + \cdots + \alpha_r u_r \mid r \geq 1; u_1, \dots, u_r \in \mathcal{U}; \alpha_1, \dots, \alpha_r \in K \}$$

est le plus petit sous-espace vectoriel de E contenant \mathcal{U} , appelé *sous-espace engendré* par \mathcal{U} .

Démonstration. Si $u \in \mathcal{U}$, alors $u = 1_K \cdot u \in \langle \mathcal{U} \rangle$. D'où, $\mathcal{U} \subseteq \langle \mathcal{U} \rangle$. Considérons $u, v \in \langle \mathcal{U} \rangle$ 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, $\alpha u + \beta v \in \langle \mathcal{U} \rangle$. D'après la proposition 4.6.2(2), $\langle \mathcal{U} \rangle$ est un sous-espace de E contenant \mathcal{U} .

Supposons que F est un sous-espace de E contenant \mathcal{U} . Pour tout $u \in \langle \mathcal{U} \rangle$, on a

$$u = \alpha_1 + \cdots + \alpha_r u_r; \alpha_1, \dots, \alpha_r \in K; u_1, \dots, u_r \in \mathcal{U}.$$

Comme $u_1, \dots, u_r \in F$, d'après la proposition 4.6.2(3), $u \in F$. Donc, $\langle \mathcal{U} \rangle \subseteq F$. C'est-à-dire, $\langle \mathcal{U} \rangle$ est le plus petit sous-espace de E contenant \mathcal{U} . La preuve de la proposition s'achève.

Remarque. (1) Le sous-espace nul $\{0_E\}$ est le plus petit sous-espace de E contenant la famille vide \emptyset . On pose, par convention, $\langle \emptyset \rangle = \{0_E\}$.

(2) Si $\mathcal{U} = \{u_1, \dots, u_n\}$, alors

$$\langle \mathcal{U} \rangle = \{ \alpha_1 u_1 + \cdots + \alpha_n u_n \mid \alpha_1, \dots, \alpha_n \in K \} =: \langle u_1, \dots, u_n \rangle.$$

(3) Une famille \mathcal{B} de vecteurs de E est une base si, et seulement si, \mathcal{B} est libre et E est engendré par \mathcal{B} .

(4) Si F est un sous-espace vectoriel de E , alors $\langle F \rangle = F$.

Exercice. Considérons l'espace vectoriel réel $C[0, 2\pi]$. Vérifier, pour tout entier $n \geq 1$, que $\sin t \notin \langle 1, t, \dots, t^{n-1} \rangle$.

Solution. Supposons au contraire que $\sin t \notin \langle 1, t, \dots, t^{n-1} \rangle$. Alors, il existe $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in \mathbb{R}$ tels que

$$\sin t = \alpha_0 + \alpha_1 t + \dots + \alpha_{n-1} t^{n-1}, \text{ pour tout } t \in [0, 2\pi].$$

En dérivant les deux côtés $2n$ fois, on obtient $(\sin t)^{(2n)} = \mathbf{0}$. C'est-à-dire, $(-1)^n \sin t = \mathbf{0}$, et donc, $\sin t = \mathbf{0}$, une contradiction. Ceci montre que $\sin t \notin \langle 1, t, \dots, t^{n-1} \rangle$.

Le résultat suivant sera pratique pour le calcul de sous-espaces d'un espace vectoriel engendrés par des familles finies de vecteurs.

4.6.5. Corollaire. Soient \mathcal{U} et \mathcal{V} des familles de vecteurs de E . Si tout vecteur de \mathcal{V} est combinaison linéaire de vecteurs de \mathcal{U} , alors $\langle \mathcal{V} \rangle \subseteq \langle \mathcal{U} \rangle$.

Démonstration. Supposons que tout vecteur de \mathcal{V} est une combinaison linéaire de vecteurs de \mathcal{U} . Alors, $\mathcal{V} \subseteq \langle \mathcal{U} \rangle$. Donc, $\langle \mathcal{U} \rangle$ est un sous-espace de E contenant \mathcal{V} . Comme $\langle \mathcal{V} \rangle$ est le plus petit sous-espace de E contenant \mathcal{V} par la proposition 4.6.4, on voit que $\langle \mathcal{V} \rangle \subseteq \langle \mathcal{U} \rangle$. Ceci achève la démonstration du corollaire.

On étudiera comment trouver une base d'un sous-espace engendré par une famille finie de vecteurs. On commence par un cas particulier, qui découle facilement de la définition d'une base.

4.6.6. Lemme. Si \mathcal{U} est une famille de vecteurs de E , alors \mathcal{U} est une base de $\langle \mathcal{U} \rangle$ si, et seulement si, \mathcal{U} est libre.

Exemple. (1) Si $u \in \mathbb{R}^3$ est non nul, alors

$$\langle u \rangle = \{\alpha u \mid \alpha \in \mathbb{R}\}$$

est la droite de \mathbb{R}^3 passant u . En effet, comme u est non nul, d'après le lemme 4.2.6(1), $\{u\}$ est libre. D'après le lemme 4.6.6, $\{u\}$ est une base de $\langle u \rangle$. D'où, $\dim \langle u \rangle = 1$.

(2) Si $u, v \in \mathbb{R}^3$ ne sont pas co-linéaires (c'est-à-dire, ils ne se trouvent dans une même droite), alors

$$\langle u, v \rangle = \{\alpha u + \beta v \mid \alpha, \beta \in \mathbb{R}\}$$

est le plan passant par u et v . En effet, comme u, v ne se trouvent dans une même droite, aucun de u, v n'est un multiple de l'autre. d'après le lemme 4.2.6(2), $\{u, v\}$ est libre. D'après le lemme 4.6.6, $\{u, v\}$ est une base de $\langle u, v \rangle$. D'où, $\dim \langle u, v \rangle = 2$.

Exemple. Considérons l'espace vectoriel réel $C[0, 2\pi]$.

(1) Soit $F = \langle \sin t, \cos t \rangle$. Comme $\{\sin t, \cos t\}$ est libre, elle est une base de F .

(2) Soit $G = \langle \sin nt \mid n \in \mathbb{Z} \rangle$. Comme $\{\sin nt \mid n \geq 1\}$ est libres, elle est une base infinie de G .

Si $F = \langle v_1, \dots, v_m \rangle$, d'après la proposition 4.4.5, $\{v_1, \dots, v_m\}$ contient une base $\{v_{j_1}, \dots, v_{j_r}\}$ de F , où $1 \leq j_1 < j_2 < \dots < j_r \leq m$. Le résultat suivant nous dit comment trouver ces indices j_1, \dots, j_r , dont la preuve est omise.

4.6.7. Théorème. Soit F un sous-espace de E engendré par des vecteurs v_1, \dots, v_m . On choisit une base $\{u_1, \dots, u_n\}$ de E , calcule $A = P_{\{u_1, \dots, u_n\}}^{\{v_1, \dots, v_m\}}$, et trouve une forme échelonnée B de A . Si les pivots de B se trouvent dans les colonnes j_1, \dots, j_r , alors $\{v_{j_1}, \dots, v_{j_r}\}$ est une base de F . En particulier, $\dim(F) = \text{rg}(A)$.

Exercice. Soit

$$F = \{(a + 2b + 2c) + (a + 2b + c)x - (2a + 4b)x^2 + (a + 2b + 2c)x^3 \mid a, b, c \in \mathbb{Q}\}.$$

Vérifier que F est un sous-espace vectoriel de $\mathbb{Q}_4[x]$, et trouver une base de F .

Solution. On voit que

$$\begin{aligned} & (a + 2b + 2c) + (a + 2b + c)x - (2a + 4b)x^2 + (a + 2b + 2c)x^3 \\ = & a(1 + x - 2x^2 + x^3) + b(2 + 2x - 4x^2 + 2x^3) + c(2 + x + 2x^3). \end{aligned}$$

Posant $f_1 = 1 + x - 2x^2 + x^3$, $f_2 = 2 + 2x - 4x^2 + 2x^3$, $f_3 = 2 + x + 2x^3$, on voit que

$$F = \{af_1 + bf_2 + cf_3 \mid a, b, c \in \mathbb{Q}\} = \langle f_1, f_2, f_3 \rangle.$$

Maintenant, la matrice des coordonnées canoniques de f_1, f_2, f_3 est la matrice

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

Ceci se réduit à la matrice échelonnée

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

Les pivots de B se trouvent dans la première et la troisième colonnes. d'après le théorème 4.6.7, $\{f_1, f_3\}$ forment une base de F .

4.6.8. Définition. Les opérations suivantes sur une famille ordonnée $\{v_1, \dots, v_m\}$ de vecteurs de E s'appelle *opérations élémentaires*.

Type 1: Permuter deux vecteurs, noté $v_i \leftrightarrow v_j$.

Type 2: Additionner à un vecteur un multiple d'un autre vecteur, noté $v_i + av_j$.

Type 3: Multiplier un vecteur par un scalaire non nul de K , noté av_i .

En outre, on dit qu'une famille ordonnée $\{v_1, \dots, v_m\}$ se réduit à une autre famille ordonnée $\{w_1, \dots, w_m\}$ si cette dernière est obtenue à partir de la première par une suite finie d'opérations élémentaires.

Remarque. (1) Les opérations élémentaires sur les familles ordonnées de vecteurs sont toutes inversibles.

(2) La notion d'opérations élémentaires sur les lignes d'une matrice est un cas particulier de la définition 4.6.8.

Exemple. Dans l'espace vectoriel réel $\mathbb{R}_3[x]$, on a

$$\begin{aligned} & \{1 + x - x^2, 2 + 3x, x + 3x^2\} \xrightarrow{v_2 - 2v_1} \{1 + x - x^2, x + 2x^2, x + 3x^2\} \\ & \xrightarrow{v_3 - v_2} \{1 + x - x^2, x + 2x^2, x^2\} \xrightarrow{v_1 + v_3, v_2 - 2v_3} \{1 + x, x, x^2\} \xrightarrow{v_1 - v_2} \{1, x, x^2\}. \end{aligned}$$

4.6.9. Théorème. Soient $\mathcal{V} = \{v_1, \dots, v_m\}$ et $\mathcal{W} = \{w_1, \dots, w_m\}$ deux familles ordonnées de vecteurs de E . Si \mathcal{V} se réduit à \mathcal{W} , alors

(1) $\langle \mathcal{V} \rangle = \langle \mathcal{W} \rangle$;

(2) \mathcal{V} est une base de E si, et seulement si, \mathcal{W} est une base de E .

Démonstration. On peut supposer que \mathcal{V} se réduit à \mathcal{W} par une seule opération élémentaire T .

(1) On voit aisément que chacun des w_i est une combinaison linéaire de v_1, \dots, v_m . D'après le corollaire 4.6.5, $\langle \mathcal{W} \rangle \subseteq \langle \mathcal{V} \rangle$. D'autre part, comme \mathcal{W} se réduit à \mathcal{V} par T^{-1} , on a aussi $\langle \mathcal{V} \rangle \subseteq \langle \mathcal{W} \rangle$. D'où, $\langle \mathcal{V} \rangle = \langle \mathcal{W} \rangle$.

(2) D'après le théorème 4.4.6(3), \mathcal{V} est une base de E si, et seulement si, $\dim(E) = m$ et $E = \langle v_1, \dots, v_m \rangle$. D'après l'énoncé (1), cette dernière condition est équivalente à $\dim(E) = m$ et $E = \langle w_1, \dots, w_m \rangle$ si, et seulement si, $\{w_1, \dots, w_m\}$ est une base de E . Ceci achève la démonstration du théorème.

Exemple. Considérons l'espace vectoriel réel $\mathbb{R}_3[x]$. Comme $\{1 + x - x^2, 2 + 3x, x + 3x^2\}$ se réduit à la base canonique $\{1, x, x^2\}$, d'après le théorème 4.6.9, elle est une base de $\mathbb{R}_3[x]$.

4.7. Sous-espaces associés à une matrice

L'objet de cette section est d'étudier trois sous-espaces associés à une matrice donnée. En particulier, on montrera que les formes échelonnées d'une matrice ont le même nombre de pivots, un résultat accepté sans démonstration dans la section 2.3.

4.7.1. Théorème. Soit un système homogène sur K à n inconnues

$$AX = 0.$$

L'ensemble $\mathcal{N}(A)$ des solutions 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 $x_{i_1}, x_{i_2}, \dots, x_{i_s}$, alors $\mathcal{N}(A)$ a une base $\{u_1, u_2, \dots, u_s\}$ trouvée de la façon suivante: on choisit s scalaires non nuls $a_1, a_2, \dots, a_s \in K$, et résout successivement le système échelonné,
 - (1) en posant $x_{i_1} = a_1, x_{i_2} = \dots = x_{i_s} = 0$, ce qui donne la solution u_1 ;
 - (2) en posant $x_{i_1} = 0, x_{i_2} = a_2, x_{i_3} = \dots = x_{i_s} = 0$, ce qui donne la solution u_2 ;
 - \vdots
 - (s) en posant $x_{i_1} = \dots = x_{i_{s-1}} = 0, x_{i_s} = a_s$, ce qui donne la solution u_s .

En tout cas, $\dim(\mathcal{N}(A)) = n - \text{rg}(A)$, le nombre d'inconnues libres du système échelonné.

Démonstration. On ne vérifie que la première partie du théorème. Soient $u, v \in \mathcal{N}(A)$ et $\alpha, \beta \in K$. Par définition, $Au = Av = 0_{n \times 1}$. Ceci nous donne

$$A(\alpha u + \beta v) = \alpha(Au) + \beta(Av) = \alpha 0_{n \times 1} + \beta 0_{n \times 1} = 0_{n \times 1}.$$

D'où, $\alpha u + \beta v \in \mathcal{N}(A)$. D'après la proposition 4.6.2(2), $\mathcal{N}(A)$ est un sous-espace de $K^{(n)}$. La preuve du théorème s'achève.

Remarque. On appelle $\mathcal{N}(A)$ *espace-solution* du système homogène $AX = 0$, ou bien, *noyau* de la matrice A .

Exemple. Trouver une base de l'espace-solution du système homogène réel suivant:

$$\begin{aligned} 2x_1 + x_2 - x_3 + 2x_4 - x_5 + 3x_6 &= 0 \\ 4x_1 + 2x_2 - x_3 + 5x_4 + 3x_5 + 5x_6 &= 0 \\ 2x_1 + x_2 - x_3 + 2x_4 + 5x_6 &= 0. \end{aligned}$$

Solution. Il suffit d'échelonner la matrice des coefficients

$$\begin{pmatrix} 2 & 1 & -1 & 2 & -1 & 3 \\ 4 & 2 & -1 & 5 & 3 & 5 \\ 2 & 1 & -1 & 2 & 0 & 1 \end{pmatrix},$$

ce qui s'échelonne à

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

Cette dernière représente le système homogène échelonné suivant:

$$\begin{aligned} 2x_1 + x_2 - x_3 + 2x_4 - x_5 + 3x_6 &= 0 \\ x_3 + x_4 + 5x_5 - x_6 &= 0 \\ x_5 + 2x_6 &= 0, \end{aligned}$$

dont les inconnues libres sont x_2, x_4 et x_6 . Ainsi l'espace-solution a une base composée de trois solutions u_1, u_2, u_3 .

(1) En posant $x_2 = 2, x_4 = x_6 = 0$, on a un système sans inconnues libres:

$$\begin{aligned} 2x_1 - x_3 - x_5 &= -2 \\ x_3 + 5x_5 &= 0 \\ x_5 &= 0. \end{aligned}$$

En résolvant par substitution, on a que $x_1 = -1, x_3 = 0$ et $x_5 = 0$. Ceci donne la première solution de la base

$$u_1 = \begin{pmatrix} -1 \\ 2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

(2) En posant $x_2 = 0, x_4 = 2$ et $x_6 = 0$, on a un système sans inconnues libres:

$$\begin{aligned} 2x_1 - x_3 - x_5 &= -4 \\ x_3 + 5x_5 &= -2 \\ x_5 &= 0. \end{aligned}$$

En résolvant par substitution, on a que $x_1 = -3, x_3 = -2$ et $x_5 = 0$. Ceci donne la deuxième solution de la base

$$u_2 = \begin{pmatrix} -3 \\ 0 \\ -2 \\ 2 \\ 0 \\ 0 \end{pmatrix}.$$

(3) Enfin en posant $x_2 = x_4 = 0$ et $x_6 = 1$, on a un système sans inconnues libres:

$$\begin{aligned} 2x_1 - x_3 - x_5 &= -3 \\ x_3 + 5x_5 &= 1 \\ x_5 &= -2. \end{aligned}$$

En résolvant par substitution, on a que $x_1 = 3, x_3 = 11$ et $x_5 = -2$. Ce qui donne la troisième solution de la base

$$u_3 = \begin{pmatrix} 3 \\ 0 \\ 11 \\ 0 \\ -2 \\ 1 \end{pmatrix}.$$

En conclusion, l'espace-solution du système original a pour base

$$\left\{ \begin{pmatrix} -1 \\ 2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \\ -2 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \\ -2 \\ 2 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

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 .

Exemple. Considérons la matrice rationnelle suivante:

$$A = \begin{pmatrix} 1 & 1 & -2 & 1 \\ 4 & 3 & -6 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

(1) D'après le corollaire 4.6.5(2), on a

$$\mathcal{L}(A) = \langle (1, 1, -2, 1), (4, 3, -6, 4), (0, 0, 0, 0) \rangle = \langle (1, 1, -2, 1), (4, 3, -6, 4) \rangle.$$

Étant libre, d'après le lemme 4.6.6, $\{(1, 1, -2, 1), (4, 3, -6, 4)\}$ est une base de $\mathcal{L}(A)$.

(2) D'après le corollaire 4.6.5(2), on a

$$\mathcal{C}(A) = \langle \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ -6 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix} \rangle = \langle \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix} \rangle.$$

Comme ces deux derniers vecteurs sont linéairement indépendants, $\mathcal{C}(A)$ a pour base

$$\left\{ \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix} \right\}.$$

Le résultat suivant dit que les opérations élémentaires sur les lignes d'une matrice ne changent l'espace-ligne.

4.7.3. Lemme. Soient A, B des matrices sur K . Si A se réduit à B , alors $\mathcal{L}(A) = \mathcal{L}(B)$.

Démonstration. Soient A_1, \dots, A_m les lignes de A , et B_1, \dots, B_m les lignes de B . Si A se réduit à B , alors la famille $\{A_1, \dots, A_m\}$ se réduit à la famille $\{B_1, \dots, B_m\}$. D'après le théorème 4.6.9, $\langle A_1, \dots, A_m \rangle = \langle B_1, \dots, B_m \rangle$. C'est-à-dire, $\mathcal{L}(A) = \mathcal{L}(B)$. Ceci achève la démonstration du lemme.

Exemple. Considérons les matrices

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

Alors A se réduit à B par une opération élémentaires sur les lignes. Donc, $\mathcal{L}(A) = \mathcal{L}(B)$. Par contre, on remarque que $\mathcal{C}(A) \neq \mathcal{C}(B)$.

4.7.4. Lemme. Soit A une matrice échelonnée sur K . Les lignes non nulles de A forment une base de $\mathcal{L}(A)$.

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, ce qui est la base de $\mathcal{L}(A)$.

Supposons que $r \geq 1$ et le résultat est vrai pour $r - 1$. Soient A_1, A_2, \dots, A_r les lignes non nulles de A . Il est évident que $\mathcal{L}(A) = \langle A_1, A_2, \dots, A_r \rangle$. 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, $\{A_2, \dots, A_r\}$ est une base de $\mathcal{L}(B)$. En particulier, $\{A_2, \dots, A_r\}$ est 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 celle-ci de A_i est nulle pour tout $i = 2, \dots, r$. Ceci implique que A_1 n'est pas une combinaison linéaire de A_2, \dots, A_r . D'après la proposition 4.2.7, $\{A_1, A_2, \dots, A_r\}$ est libre, et donc, une base de $\mathcal{L}(A)$. Ceci achève la démonstration du lemme.

Exercice. Donner une base de l'espace-ligne de la matrice

$$A = \begin{pmatrix} 1 & 3 & 2 & 3 \\ 2 & 1 & 1 & 2 \\ -1 & 3 & 1 & 3 \\ 2 & 7 & 4 & 8 \end{pmatrix}.$$

Solution. D'abord, A se réduit à la matrice échelonnée

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

D'après le lemme 4.7.3, $\mathcal{L}(A) = \mathcal{L}(B)$; et d'après le lemme 4.7.4,

$$\{(1, 3, 2, 3), (0, 1, 0, 2), (0, 0, 1, -2)\}$$

est une base de $\mathcal{L}(B)$, et donc, une base de $\mathcal{L}(A)$.

Maintenant, on est capable de donner la démonstration du théorème 2.3.6.

4.7.5. Théorème. Soit A une matrice sur K . Les formes 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, on voit que $\mathcal{L}(A) = \mathcal{L}(B)$. 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 du théorème s'achève.

4.7.6. 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 $\mathcal{C}(A) = \langle A_1, \dots, A_n \rangle$. En outre, A est la matrice des coordonnées de $\{A_1, \dots, A_n\}$ dans la base canonique. D'après le théorème 4.6.7, $\dim \mathcal{C}(A) = \text{rg}(A)$. Ceci achève la démonstration du théorème.

4.7.7. Proposition. Si A est une matrice sur K , alors $\text{rg}(A) = \text{rg}(A^T)$.

Démonstration. Soient A_1, \dots, A_m les lignes de A . Alors $\mathcal{L}(A) = \langle A_1, \dots, A_m \rangle$. D'après le lemme 4.3.6, on a

$$P_{\{e_1, \dots, e_n\}}^{\{A_1, \dots, A_m\}} = (A_1^T \cdots A_m^T) = A^T.$$

D'après le théorème 4.6.7, $\dim \mathcal{L}(A) = \text{rg}(A^T)$; et d'après le théorème 4.7.7, $\dim \mathcal{L}(A) = \text{rg}(A)$. D'où, $\text{rg}(A) = \text{rg}(A^T)$. Ceci achève la preuve de la proposition.

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

$$\text{rg}(AB) \leq \min \{ \text{rg}(A), \text{rg}(B) \}.$$

Démonstration. On partage $B = (B_1, \dots, B_p)$ en colonnes. D'après le lemme 2.2.5(1), $AB = (AB_1 \cdots AB_p)$, et donc, $\mathcal{C}(AB) = \langle AB_1, \dots, AB_p \rangle$. En vertu de la proposition 4.7.3(1), $AB_j \in \mathcal{C}(A)$, $j = 1, \dots, p$. 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(1),

$$\text{rg}(AB) = \dim \mathcal{C}(AB) \leq \dim \mathcal{C}(A) = \text{rg}(A).$$

En outre, d'après la proposition 4.7.8 et ce qu'on a montré,

$$\text{rg}(AB) = \text{rg}(AB)^T = \text{rg}(B^T A^T) \leq \text{rg}(B^T) = \text{rg}(B).$$

Ceci achève la démonstration de la proposition.

4.7.9. 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. D'après le théorèmes 4.3.9(1), les colonnes de A sont linéairement indépendantes si, et seulement si, $\text{rg}(A) = n$ si, et seulement si, A est inversible d'après le théorème 2.4.8. Ceci montre l'équivalence de (1) et (3).

En outre, $\mathcal{L}(A) = \langle A_1, \dots, A_n \rangle$, où A_1, \dots, A_n sont les lignes de A . Rappelons que $\mathcal{L}(A)$ est un sous-espace de K^n et $\dim \mathcal{L}(A) = \text{rg}(A)$. Maintenant, A est inversible si, et seulement si, $\text{rg}(A) = n$ si, et seulement si, $\dim \mathcal{L}(A) = \dim K^n$ si, et seulement si, $\langle A_1, \dots, A_n \rangle = K^n$ si, et seulement si, $\{A_1, \dots, A_n\}$ est libre d'après le théorème 4.4.6. La preuve du théorème s'achève.

4.8. Intersections et sommes de sous-espaces vectoriels

Cette section a pour but d'étudier les opérations sur les sous-espaces vectoriels d'un espace vectoriel. Partout dans cette section, on se fixe E un espace vectoriel sur K .

4.8.1. Proposition. Soient F_1, F_2, \dots, F_r des sous-espaces de E .

- (1) L'intersection $\bigcap_{i=1}^r F_i$ est un sous-espace de E .
- (2) La *somme* de F_1, \dots, F_r est définie comme étant

$$\sum_{i=1}^r F_i := \{u_1 + u_2 + \dots + u_r \mid u_i \in F_i\},$$

ce qui est un sous-espace de E .

Démonstration. (1) D'abord, $0_E \in \bigcap_{i=1}^r F_i$ car $0_E \in F_i$, pour tout $i = 1, \dots, r$. Si $u, v \in \bigcap_{i=1}^r F_i$ et $\alpha, \beta \in K$, alors $u, v \in F_i$, pour tout $i = 1, \dots, r$. Comme F_i est un sous-espace, on a $\alpha u + \beta v \in F_i$, pour tout $i = 1, \dots, r$. Par conséquent, $\alpha u + \beta v \in \bigcap_{i=1}^r F_i$. Ceci montre que $\bigcap_{i=1}^r F_i$ est un sous-espace de E .

(2) Comme $0_E = 0_E + 0_E + \dots + 0_E$, où $0_E \in F_i$, on a $0_E \in \sum_{i=1}^r F_i$ par définition. Si $u, v \in \sum_{i=1}^r F_i$ et $\alpha, \beta \in K$, alors $u = u_1 + \dots + u_r, v = v_1 + \dots + v_r$ avec $u_i, v_i \in F_i$. Donc,

$$\alpha u + \beta v = (\alpha u_1 + \beta v_1) + \dots + (\alpha u_n + \beta v_n).$$

Comme F_i est un sous-espace, $\alpha u_i + \beta v_i \in F_i$, pour tout $i = 1, \dots, r$. Par définition, on voit que $\alpha u + \beta v \in \sum_{i=1}^r F_i$. Ceci achève la démonstration de la proposition.

Remarque. Par contre, l'union de sous-espaces n'est pas nécessairement un sous-espace. En effet, la somme est le sous-espace engendré par l'union.

Exemple. Le plan réel \mathbb{R}^2 a deux sous-espaces

$$E_1 = \{(x, 0) \mid x \in \mathbb{R}\} \text{ et } E_2 = \{(0, y) \mid y \in \mathbb{R}\}.$$

On voit que

$$E_1 \cup E_2 = \{(x, y) \mid x = 0 \text{ ou } y = 0\}.$$

Or $(1, 0), (0, 1) \in E_1 \cup E_2$ sont tels que

$$(1, 0) + (0, 1) = (1, 1) \notin E_1 \cup E_2.$$

D'où, $E_1 \cup E_2$ n'est pas un sous-espace de \mathbb{R}^2 .

Exercice. Considérons les sous-espaces de \mathbb{R}^3 suivants:

$$F_1 = \{(x, x, 0) \mid x \in \mathbb{R}\}, F_2 = \{(0, y, 0) \mid y \in \mathbb{R}\}, F_3 = \{(0, 0, z) \mid z \in \mathbb{R}\}.$$

Vérifier que

- (1) $F_1 \cap F_3 = \{0\}$;
- (2) $F_1 + F_2 = P_{x,y}$, le plan des x, y de \mathbb{R}^3 ;
- (3) $F_1 + F_2 + F_3 = \mathbb{R}^3$.

Démonstration. (1) On a $\{(0, 0, 0)\} \subseteq F_1 \cap F_3$. Soit $u = (x, y, z) \in F_1 \cap F_3$. Comme $u \in F_1$, on voit que $x = y$ et $z = 0$. Et comme $u \in F_3$, $x = y = 0$. Ainsi, $u = (0, 0, 0)$. Ceci montre $F_1 \cap F_3 \subseteq \{(0, 0, 0)\}$. Donc, $F_1 \cap F_3 = \{(0, 0, 0)\}$.

(2) Pour tous $u_1 = (x, x, 0) \in F_1$ et $u_2 = (0, y, 0) \in F_2$, on a $u_1 + u_2 = (x, x + y, 0) \in P_{x,y}$. Ainsi, $F_1 + F_2 \subseteq P_{x,y}$. Réciproquement, pour tout $w = (x, y, 0) \in P_{x,y}$, on a

$$w = (x, x, 0) + (0, y - x, 0) \in F_1 + F_2.$$

D'où, $P_{x,y} \subseteq F_1 + F_2$. Par conséquent, $F_1 + F_2 = P_{x,y}$.

(3) Par définition, $F_1 + F_2 + F_3 \subseteq \mathbb{R}^3$. Or, pour tout $u = (x, y, z) \in \mathbb{R}^3$, on a

$$u = (x, x, 0) + (0, y - x, z) = (x, x, 0) + (0, y - x, 0) + (0, 0, z) \in F_1 + F_2 + F_3.$$

D'où, $\mathbb{R}^3 \subseteq F_1 + F_2 + F_3$, et donc, $\mathbb{R}^3 = F_1 + F_2 + F_3$.

Exercice. Considérons les sous-espaces de l'espace rationnel $\mathbb{Q}_4[x]$ suivants:

$$F = \langle f_1 = 1 + 2x - x^2, f_2 = 1 - x + x^2 - x^3, f_3 = 2 + x - x^2 + x^3 \rangle$$

et

$$G = \langle g_1 = 1 - x^3, g_2 = 2 + x - 2x^3, g_3 = 1 + 2x - 2x^2 + 2x^3 \rangle.$$

Trouver une base de l'intersection de F et G .

Solution. Soit $f = a + bx + cx^2 + dx^3 \in \mathbb{Q}_4[x]$. Par définition, $f \in F$ si, et seulement si, f est une combinaison linéaire de f_1, f_2, f_3 . D'après le théorème 4.3.7(2), ceci est équivalent à $\text{rg}(A) = \text{rg}(A | B)$, où

$$A = P_{\{1, x, x^2\}}^{\{f_1, f_2, f_3\}} = \begin{pmatrix} 1 & 1 & 2 \\ 2 & -1 & 1 \\ -1 & 1 & - \\ 0 & -1 & 1 \end{pmatrix}; B = P_{\{1, x, x^2\}}^{\{f\}} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}.$$

Or

$$(A | B) = \left(\begin{array}{ccc|c} 1 & 1 & 2 & a \\ 2 & -1 & 1 & b \\ -1 & 1 & -1 & c \\ 0 & -1 & 1 & d \end{array} \right) \Rightarrow \left(\begin{array}{ccc|c} 1 & 1 & 2 & a \\ 0 & 1 & -1 & -d \\ 0 & 0 & 3 & a + c + 2d \\ 0 & 0 & 0 & b + 2c + d \end{array} \right).$$

Par conséquent, $f \in F$ si, et seulement si, $b + 2c + d = 0$.

De même, considérant les coordonnées canoniques de g_1, g_2, g_3, f , on échelonne

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & a \\ 0 & 1 & 2 & b \\ 0 & 0 & -2 & c \\ -1 & -2 & 2 & d \end{array} \right) \Rightarrow \left(\begin{array}{ccc|c} 1 & 2 & 1 & a \\ 0 & 1 & 2 & b \\ 0 & 0 & 1 & a + c + d \\ 0 & 0 & 0 & 2a + 3c + 2d \end{array} \right).$$

Ainsi, $f \in G$ si, et seulement si, $2a + 3c + 2d = 0$. En conclusion, $f \in F \cap G$ si, et seulement si,

$$\begin{aligned} 2a &+ 3c + 2d = 0 \\ b &+ 2c + d = 0. \end{aligned}$$

Il s'agit d'un système échelonné, dont les inconnues libres sont c, d . Posons $c = \lambda$ et $d = \mu$, où $\lambda, \mu \in \mathbb{Q}$, on trouve $b = -(2\lambda + \mu)$ et $a = -(\frac{3}{2}\lambda + \mu)$. C'est-à-dire,

$$\begin{aligned} F \cap G &= \left\{ \left(-\frac{3}{2}\lambda - \mu \right) - (2\lambda + \mu)x + \lambda x^2 + \mu x^3 \mid \lambda, \mu \in \mathbb{Q} \right\} \\ &= \left\{ \lambda \left(-\frac{3}{2} - 2x + x^2 \right) + \mu \left(-1 - x + x^3 \right) \mid \lambda, \mu \in \mathbb{Q} \right\} \\ &= \langle -\frac{3}{2} - 2x + x^2, -1 - x + x^3 \rangle. \end{aligned}$$

Comme

$$P_{\{1,x,x^2\}}^{\{-\frac{3}{2}-2x+x^2, -1-x+x^3\}} = \begin{pmatrix} -\frac{3}{2} & -1 \\ -2 & -1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

on voit que $\{-\frac{3}{2}-2x+x^2, -1-x+x^3\}$ est libre, et donc, une base de $F \cap G$.

Le résultat suivant sera pratique pour calculer la somme de sous-espaces.

4.8.2. Lemme. Si \mathcal{U} et \mathcal{V} sont des familles de vecteurs de E , alors

$$\langle \mathcal{U} \rangle + \langle \mathcal{V} \rangle = \langle \mathcal{U} \cup \mathcal{V} \rangle.$$

Démonstration. D'abord, $\langle \mathcal{U} \rangle \subseteq \langle \mathcal{U} \cup \mathcal{V} \rangle$ et $\langle \mathcal{V} \rangle \subseteq \langle \mathcal{U} \cup \mathcal{V} \rangle$. Ainsi $\langle \mathcal{U} \rangle + \langle \mathcal{V} \rangle \subseteq \langle \mathcal{U} \cup \mathcal{V} \rangle$. Comme $\mathcal{U} \cup \mathcal{V} \subseteq \langle \mathcal{U} \rangle + \langle \mathcal{V} \rangle$, d'après la proposition 4.6.4, $\langle \mathcal{U} \cup \mathcal{V} \rangle \subseteq \langle \mathcal{U} \rangle + \langle \mathcal{V} \rangle$. Ceci montre que $\langle \mathcal{U} \cup \mathcal{V} \rangle = \langle \mathcal{U} \rangle + \langle \mathcal{V} \rangle$. La preuve du lemme 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 $\mathcal{L}(A) + \mathcal{L}(B)$.

Solution. Les matrices A et B s'échelonnent respectivement aux matrices suivantes:

$$\begin{pmatrix} 1 & 1 & -2 & 1 \\ 0 & 1 & -4 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

D'après les lemmes 4.7.4 et 4.7.5, on voit que $\{(1, 1, -2, 1), (0, 1, -4, 0)\}$ est une base de $\mathcal{L}(A)$, et $\{(1, 1, 1, 1), (0, 1, 5, 0)\}$ est une base de $\mathcal{L}(B)$. D'après le lemme 4.8.2, on a

$$\begin{aligned} \mathcal{L}(A) + \mathcal{L}(B) &= \langle (1, 1, -2, 1), (0, 1, -4, 0) \rangle + \langle (1, 1, 1, 1), (0, 1, 5, 0) \rangle \\ &= \langle (1, 1, -2, 1), (0, 1, -4, 0), (1, 1, 1, 1), (0, 1, 5, 0) \rangle. \end{aligned}$$

Ceci est l'espace-ligne de la matrice

$$\begin{pmatrix} 1 & 1 & -2 & 1 \\ 0 & 1 & -4 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 5 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 1 & -2 & 1 \\ 0 & 1 & -4 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Ainsi $\{(1, 1, -2, 1), (0, 1, -4, 0), (0, 0, 1, 0)\}$ est une base de $\mathcal{L}(A) + \mathcal{L}(B)$.

Le résultat suivant relie la dimension de la somme et celle de l'intersection de deux sous-espaces vectoriels d'un espace vectoriel.

4.8.3. La 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 $\{v_1, \dots, v_s\}$. D'après la proposition 4.4.3, $\{v_1, \dots, v_s\}$ est contenue dans une base $\{v_1, \dots, v_s, v_{s+1}, \dots, v_p\}$ de F et dans une base $\{v_1, \dots, v_s, w_{s+1}, \dots, w_q\}$ de G . On prétend que $\{v_1, \dots, v_s, v_{s+1}, \dots, v_p, w_{s+1}, \dots, w_q\}$ est une base de $F + G$. D'abord, d'après le lemme 4.8.2,

$$\begin{aligned} F + G &= \langle v_1, \dots, v_s, v_{s+1}, \dots, v_p \rangle + \langle v_1, \dots, v_s, w_{s+1}, \dots, w_q \rangle \\ &= \langle \{v_1, \dots, v_s, v_{s+1}, \dots, v_p\} \cup \{v_1, \dots, v_s, w_{s+1}, \dots, w_q\} \rangle \\ &= \langle v_1, \dots, v_s, v_{s+1}, \dots, v_p, w_{s+1}, \dots, w_q \rangle. \end{aligned}$$

Supposons ensuite que

$$\sum_{i=1}^p \alpha_i v_i + \sum_{j=s+1}^q \beta_j w_j = 0_E, \text{ où } \alpha_i, \beta_j \in K.$$

Alors

$$\sum_{i=1}^p \alpha_i v_i = -\sum_{j=s+1}^q \beta_j w_j \in F \cap G.$$

Comme $\{v_1, \dots, v_s\}$ est une base de $F \cap G$, on a

$$\sum_{i=1}^s \alpha_i v_i + \sum_{i=s+1}^p \alpha_i v_i = \sum_{i=1}^s \gamma_i v_i, \text{ où } \gamma_i \in K.$$

Donc

$$\sum_{i=1}^s (\alpha_i - \gamma_i) v_i + \sum_{i=s+1}^p \alpha_i v_i = 0_E.$$

Comme $\{v_1, \dots, v_s, \dots, v_p\}$ est libre, on voit que $\alpha_i = 0$, $i = s + 1, \dots, p$. Cela donne

$$\sum_{i=1}^s \alpha_i v_i + \sum_{j=s+1}^q \beta_j w_j = 0_E.$$

Comme $\{v_1, \dots, v_s, w_{s+1}, \dots, w_q\}$ est libre, on voit que $\alpha_i = 0$ et $\beta_j = 0$, pour $1 \leq i \leq s$ et $s + 1 \leq j \leq q$. Ainsi $\{v_1, \dots, v_s, v_{s+1}, \dots, v_p, w_{s+1}, \dots, w_q\}$ 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 du résultat.

Exemple. Si P_1, P_2 sont deux plans vectoriels de l'espace réel \mathbb{R}^3 , alors $P_1 \cap P_2$ est non nul. En effet, $\dim(P_1 + P_2) \leq \dim(\mathbb{R}^3) = 3$, et donc,

$$\dim(P_1 \cap P_2) = \dim(P_1) + \dim(P_2) - \dim(P_1 + P_2) \geq 2 + 2 - 3 = 1.$$

D'où, $P_1 \cap P_2$ est non nul.

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 $\mathcal{L}(A) \cap \mathcal{L}(B)$.

Solution. On a vu que $\dim \mathcal{L}(A) = 2$ et $\dim \mathcal{L}(B) = 2$. Posons

$$C = \begin{pmatrix} A \\ B \end{pmatrix}.$$

En vue du lemme 4.8.2, on voit aisément que $\mathcal{L}(A) + \mathcal{L}(B) = \mathcal{L}(C)$. Ainsi

$$\dim(\mathcal{L}(A) + \mathcal{L}(B)) = \dim \mathcal{L}(C) = \text{rg}(C) = 3.$$

D'après la formule de Grassmann, on a

$$\dim(\mathcal{L}(A) \cap \mathcal{L}(B)) = \dim \mathcal{L}(A) + \dim \mathcal{L}(B) - \dim(\mathcal{L}(A) + \mathcal{L}(B)) = 1.$$

En général, un vecteur $u \in \sum_{i=1}^r F_i$ s'écrit de plusieurs façons comme une somme

$$u = u_1 + \cdots + u_r, \quad \text{où } u_i \in F_i.$$

Par exemple, considérons $F_1 = \{(x, 0, z) \mid x, z \in \mathbb{R}\}$ et $F_2 = \{(0, y, z) \mid y, z \in \mathbb{R}\}$, deux sous-espaces de \mathbb{R}^3 . On voit que $(1, 2, 3) \in F_1 + F_2$, car

$$(1, 2, 3) = (1, 0, 3) + (0, 2, 0), \quad \text{où } (1, 0, 3) \in F_1 \text{ et } (0, 2, 0) \in F_2.$$

Mais, il s'écrit d'une autre façon comme suit:

$$(1, 2, 3) = (1, 0, 0) + (0, 2, 3), \quad \text{où } (1, 0, 0) \in F_1 \text{ et } (0, 2, 3) \in F_2.$$

On introduit un genre particulier de sommes de sous-espaces vectoriels suivant.

4.8.4. Théorème. Soit $F = \sum_{i=1}^r F_i$, où F_1, \dots, F_r sont des sous-espaces de E . Les conditions suivantes sont équivalentes:

- (1) Tout $u \in F$ s'écrit d'une façon unique $u = u_1 + \dots + u_r$, où $u_i \in F_i$, pour $i = 1, \dots, r$.
- (2) Toute égalité $u_1 + \dots + u_r = 0_E$ avec $u_i \in F_i$ entraîne que $u_1 = \dots = u_r = 0_E$.
- (3) $F_i \cap (\sum_{1 \leq j \leq r, j \neq i} F_j) = \{0_E\}$, pour $i = 1, \dots, r$.

Dans ce cas, on appelle F *somme directe* de F_1, \dots, F_r et on écrit $F = \oplus_{i=1}^r F_i$.

Démonstration. Supposons que l'énoncé (1) est valide avec $u_1 + \dots + u_r = 0_E$, $u_i \in F_i$. Comme $0_E = 0_E + \dots + 0_E$, $0_E \in F_i$. Par l'unicité, $u_i = 0_E$ pour $i = 1, \dots, r$. Ceci montre que l'énoncé (1) implique l'énoncé (2).

Supposons que l'énoncé (2) est valide. Soit $u \in F_i \cap (F_1 + \dots + F_{i-1} + F_{i+1} + \dots + F_r)$. Alors $u = u_1 + \dots + u_{i-1} + u_{i+1} + \dots + u_r$, $u_j \in F_j$. Donc $u_1 + \dots + u_{i-1} + (-u) + u_{i+1} + \dots + u_r = 0_E$. Ainsi, $-u = 0_E$, et donc, $u = 0_E$. Par conséquent, $F_i \cap (F_1 + \dots + F_{i-1} + F_{i+1} + \dots + F_r) = \{0_E\}$. Ceci montre que l'énoncé (2) implique l'énoncé (3).

Enfin supposons que l'énoncé (3) est valide. Supposons que $u \in \sum_{i=1}^r F_i$, qui s'écrit

$$u = \sum_{i=1}^r u_i = \sum_{i=1}^r v_i, \text{ où } u_i, v_i \in F_i.$$

Pour tout $1 \leq i \leq r$, on a

$$u_i - v_i = \sum_{1 \leq j \leq r, j \neq i} (v_j - u_j) \in F_i \cap (F_1 + \dots + F_{i-1} + F_{i+1} + \dots + F_r) = \{0_E\}.$$

Ainsi, $u_i = v_i$ pour $i = 1, \dots, r$. Ceci achève la démonstration du théorème.

Remarque. (1) Si $r = 1$, par définition, $F = F_1$ est une somme direct.

(2) Si $r = 2$, alors la somme $F_1 + F_2$ est directe si, et seulement si, $F_1 \cap F_2 = 0$.

(3) Si $r > 2$, même si $F_i \cap F_j = \{0_E\}$ pour tous $1 \leq i, j \leq r$ avec $i \neq j$, la somme $\sum_{i=1}^r F_i$ n'est pas nécessairement directe. Par exemple, considérons les sous-espaces de \mathbb{R}^3 suivants:

$$F_1 = \{(x, 0, 0) \mid x \in \mathbb{R}\}, F_2 = \{(0, y, z) \mid y, z \in \mathbb{R}\}, F_3 = \{(x, x, x) \mid x \in \mathbb{R}\}.$$

Pour tous $1 \leq i, j \leq 3$, on a $F_i \cap F_j = 0$ si $i \neq j$. Mais $F_1 + F_2 + F_3$ n'est pas une somme directe. En effet, on a

$$(1, 0, 0) + (0, 1, 1) + (-1, -1, -1) = (0, 0, 0), \text{ où } (1, 0, 0) \in F_1; (0, 1, 1) \in F_2; (-1, -1, -1) \in F_3.$$

Ainsi, la condition énoncée dans le théorème 4.8.4(3) n'est pas vérifiée.

Exemple. (1) Considérons les sous-espaces vectoriels de \mathbb{R}^3 suivants

$$F_1 = \{(x, 0, 0) \mid x \in \mathbb{R}\}, F_2 = \{(0, y, 0) \mid y \in \mathbb{R}\}, F_3 = \{(0, 0, z) \mid z \in \mathbb{R}\}.$$

On voit que $\mathbb{R}^3 = F_1 \oplus F_2 \oplus F_3$. En effet, tout $u = (x, y, z) \in \mathbb{R}^3$ s'écrit comme que $u = u_1 + u_2 + u_3$, où $u_1 = (x, 0, 0) \in F_1$, $u_2 = (0, y, 0) \in F_2$, et $u_3 = (0, 0, z) \in F_3$. En outre, si $u = v_1 + v_2 + v_3$ avec $v_i \in F_i$, alors $v_1 = (a, 0, 0)$, $v_2 = (0, b, 0)$ et $v_3 = (0, 0, c)$ avec $a, b, c \in \mathbb{R}$. Ceci donne $(x, y, z) = (a, b, c)$, et donc, $x = a$, $y = b$ et $z = c$. D'où, $v_1 = u_1$, $v_2 = u_2$ et $v_3 = u_3$. Donc, $\mathbb{R}^3 = F_1 + F_2 + F_3 = F_1 \oplus F_2 \oplus F_3$.

(2) Considérons les sous-espaces vectoriels de \mathbb{R}^3 suivants

$$E_1 = \{(x, 0, z) \mid x, z \in \mathbb{R}\}, E_2 = \{(0, y, z) \mid y, z \in \mathbb{R}\}.$$

Alors, $\mathbb{R}^3 = E_1 + E_2$, ce qui n'est pas directe. En effet, pour tout $u = (x, y, z) \in \mathbb{R}^3$, on a

$$u = (x, 0, z) + (0, y, 0), \text{ où } (x, 0, z) \in E_1, (0, y, 0) \in E_2.$$

Ainsi, $\mathbb{R}^3 = E_1 + E_2$. En outre, comme $(0, 0, 1) \in E_1 \cap E_2$, on a $E_1 \cap E_2$ est non nul. Ainsi, la somme $E_1 + E_2$ n'est pas directe.

Exercice. Considérons l'espace vectoriel réel $C[0, 2\pi] = \{f \mid f : [0, 2\pi] \rightarrow \mathbb{R} \text{ continues}\}$. Posant $F = \langle 1, t, \dots, t^n \rangle$ et $G = \langle \sin t, \sin 2t, \dots, \sin mt \rangle$, où $n, m \geq 1$, montrer que

$$F + G = F \oplus G.$$

Démonstration. Soit $f \in F \cap G$. C'est-à-dire,

$$f = a_0 + a_1 t + \dots + a_n t^n \quad (1)$$

$$f = b_1 \sin t + b_2 \sin 2t + \dots + b_m \sin mt \quad (2)$$

où $a_i, b_j \in \mathbb{R}$. Selon (1), on voit que $f^{(2n)} = 0$. Comme $(\sin kt)^{(2n)} = (-1)^n k^{2n} \sin kt$, selon (2), on a $f^{(2n)} = \sum_{k=1}^m k^{2n} (-1)^n b_k \sin kt$, et donc,

$$\sum_{k=1}^m k^{2n} (-1)^n b_k \sin kt = 0.$$

Comme $\{\sin t, \sin 2t, \dots, \sin mt\}$ est libre, $k^{2n} (-1)^n b_k = 0$, et donc, $b_k = 0$, pour tout $k = 1, \dots, m$. D'où, $f = 0$. Ceci montre que $F \cap G = 0$. D'après le théorème 4.8.4(3), on a $F + G = F \oplus G$.

4.8.5. Lemme. Une famille $\{u_1, \dots, u_r\}$ de vecteurs non nuls de E est libre si, et seulement si,

$$\langle u_1, \dots, u_r \rangle = \langle u_1 \rangle \oplus \dots \oplus \langle u_r \rangle.$$

Démonstration. D'après le lemme 4.8.2, on a

$$\langle u_1, \dots, u_r \rangle = \langle u_1 \rangle + \dots + \langle u_r \rangle .$$

Cette somme est directe si, et seulement si, toute égalité $v_1 + \dots + v_r = 0_E$, où $v_i \in \langle u_i \rangle$, entraîne que les v_i sont tous nuls. Cette condition est équivalente à dire que toute égalité $\alpha_1 u_1 + \dots + \alpha_r u_r = 0_E$ avec $\alpha_i \in K$ entraîne que les α_i sont tous nuls, c'est-à-dire, $\{u_1, \dots, u_r\}$ est libre. Ceci achève la démonstration.

Le résultat suivant nous donne un critère pour qu'une somme soit directe, en termes de dimension de sous-espaces vectoriels.

4.8.6. Théorème. Soit $F = F_1 + \dots + F_r$, où les F_i sont des sous-espaces de E . Si les F_i sont tous de dimension finie de E , alors

(1) F est de dimension;

(2) $F = F_1 \oplus \dots \oplus F_r$ si, et seulement si, $\dim(F) = \dim(F_1) + \dots + \dim(F_r)$; et dans ce cas, si \mathcal{B}_i est une base de F_i , $i = 1, \dots, r$, alors $\mathcal{B}_1 \cup \dots \cup \mathcal{B}_r$ est une base de F .

Démonstration. Supposons que F_i admet une base finie \mathcal{B}_i , pour $i = 1, \dots, r$. Alors

$$F = \langle \mathcal{B}_1 \rangle + \dots + \langle \mathcal{B}_r \rangle = \langle \mathcal{B}_1 \cup \dots \cup \mathcal{B}_r \rangle .$$

D'après la proposition 4.4.5, $\mathcal{B}_1 \cup \dots \cup \mathcal{B}_r$ contient une base \mathcal{B} de F . En particulier, F est de dimension finie.

Si $r = 1$, alors l'énoncé (2) est évidemment valide.

Si $r = 2$, alors $F = F_1 \oplus F_2$ si, et seulement si, $F_1 \cap F_2 = \{0_E\}$ si, et seulement si, $\dim(F_1 \cap F_2) = 0$ si, et seulement si, $\dim(F) = \dim(F_1) + \dim(F_2)$ d'après la formule de Grassmann.

Supposons que $r > 2$ et l'énoncé est vrai pour $r - 1$. Supposons premièrement que $F = F_1 \oplus \dots \oplus F_r$. Posant $G = F_1 + \dots + F_{r-1}$, on voit facilement que $G = \bigoplus_{i=1}^{r-1} F_i$ et $F = G \oplus F_r$. Par l'hypothèse de récurrence, $\dim(G) = \sum_{i=1}^{r-1} \dim(F_i)$. Comme l'énoncé (2) est vrai pour $r = 2$, on a $\dim(F) = \dim(G) + \dim(F_r) = \sum_{i=1}^r \dim(F_i)$.

Supposons réciproquement que $\dim(F) = \sum_{i=1}^r \dim(F_i)$. Alors

$$|\mathcal{B}| \leq |\mathcal{B}_1 \cup \dots \cup \mathcal{B}_r| \leq |\mathcal{B}_1| + \dots + |\mathcal{B}_r| = \dim(F) = |\mathcal{B}|,$$

et donc, $\mathcal{B}_1 \cup \dots \cup \mathcal{B}_r = \mathcal{B}$, une base de F . En appliquant le lemme 4.8.5, on obtient

$$F = \langle \mathcal{B}_1 \cup \dots \cup \mathcal{B}_r \rangle = \langle \mathcal{B}_1 \rangle \oplus \dots \oplus \langle \mathcal{B}_r \rangle = F_1 \oplus \dots \oplus F_r.$$

La preuve du théorème s'achève.

Exercice. Vérifier que $\mathbb{R}^3 = F_1 \oplus F_2 \oplus F_3$, où

$$F_1 = \{(x, x, 0) \mid x \in \mathbb{R}\}, F_2 = \{(0, y, y) \mid y \in \mathbb{R}\}, F_3 = \{(0, 0, z) \mid z \in \mathbb{R}\}.$$

Solution. On voit aisément que

$$F_1 = \langle (1, 1, 0) \rangle, F_2 = \langle (0, 1, 1) \rangle, F_3 = \langle (0, 0, 1) \rangle.$$

Ainsi $\dim(F_i) = 1$, $i = 1, 2, 3$. Pour tout $u = (a, b, c) \in \mathbb{R}^3$, on a

$$u = (a, a, 0) + (0, b - a, b - a) + (0, 0, c - b + a) \in F_1 + F_2 + F_3.$$

Ainsi, $\mathbb{R}^3 \subseteq F_1 + F_2 + F_3$, et par conséquent, $F_1 + F_2 + F_3 = \mathbb{R}^3$. En outre,

$$\dim(F_1) + \dim(F_2) + \dim(F_3) = 3 = \dim(\mathbb{R}^3) = \dim(F_1 + F_2 + F_3).$$

D'après le théorème 4.8.6, la somme $F_1 + F_2 + F_3$ est directe. Ainsi, $\mathbb{R}^3 = F_1 \oplus F_2 \oplus F_3$.

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.

Solution. On voit que $E_1 = \langle (1, 1, 0) \rangle$, $E_2 = \langle (2, 3, 0) \rangle$ et $E_3 = \langle (1, -1, 0) \rangle$. En conséquence, $\dim(F_i) = 1$, $i = 1, 2, 3$. Considérons le plan des x, y de \mathbb{R}^3 comme suit:

$$P_{x,y} = \{(x, y, 0) \mid x, y \in \mathbb{R}\}.$$

Comme $(1, 1, 0), (2, 3, 0), (1, -1, 0) \in P$, d'après le lemme 4.8.2, on a

$$E_1 + E_2 + E_3 = \langle (1, 1, 0), (2, 3, 0), (1, -1, 0) \rangle \subseteq P.$$

D'où, $\dim(E_1 + E_2 + E_3) \leq \dim(P) = 2$. Cela nous donne

$$\dim(E_1) + \dim(E_2) + \dim(E_3) = 3 > \dim(E_1 + E_2 + E_3).$$

D'après le théorème 4.8.8, on voit que la somme $E_1 + E_2 + E_3$ n'est pas directe.

4.9. Exercices

1. Soit K un corps et E un K -espace vectoriel non nul. Montrer premièrement 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) $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2), \quad \alpha \cdot (x, y) = (\alpha x, 0), \quad \alpha \in \mathbb{R}.$
 - (2) $(x_1, x_2) + (y_1, y_2) = (x_1 - y_1, x_2 + y_2), \quad \alpha \cdot (x, y) = (\alpha x, \alpha y), \quad \alpha \in \mathbb{R}.$

3. Considérer le K -espace vectoriel $K_5[x]$ avec $K = \mathbb{Z}_7$ et les vecteurs

$$f_2 = 2 + 3x^2 - 4x^4; f_1 = 3 + 2x + x^3 + x^4 \quad f_3 = 5x + 6x^2 - 2x^3.$$

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.

$$(1) f = 5 - 4x + 3x^2 + 4x^4; \quad (2) f = 2 + 3x^2 - x^3 + 5x^4.$$

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 $\{\cos t, \dots, \cos nt\}$ 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 avec $\{u_1, \dots, u_n\}$ une famille libre de vecteurs de E . Si $a_1, \dots, a_n \in K$ sont tous non nuls, montrer que $\{a_1u_1, \dots, a_nu_n\}$ est aussi libre.
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 $1, t, \dots, t^n$ avec $n \geq 1$ sont linéairement indépendantes.
- (3) Dédurre 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. 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.

$$(1) \left\{ \left\{ \begin{pmatrix} 1 \\ 3 \\ -1 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 8 \\ -5 \\ 7 \end{pmatrix}, \begin{pmatrix} 2 \\ 9 \\ 4 \\ 23 \end{pmatrix} \right\}; \quad (2) \left\{ \left\{ \begin{pmatrix} 1 \\ -2 \\ 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ -3 \end{pmatrix}, \begin{pmatrix} 3 \\ -6 \\ 1 \\ 4 \end{pmatrix} \right\} \right\}.$$

12. 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.
13. 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.
14. 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) $\{5 + 6x - x^2, 2 - 3x + 5x^2, 7 + 3x + 4x^2\}$.

15. 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:

$$\begin{pmatrix} 2 & -1 & \sqrt{2} & 0 & 1 \\ 2 & 1 & 5 & \sqrt{7} & 3 \\ 3 & 5 & -1 & 4 & 2 \\ 1 & 0 & 3 & 0 & 7 \end{pmatrix}.$$

16. 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) $\{1 + x + x^2 + x^3, 1 + x^2 + x^3, 1 + x + x^2, 6 + 4x + 6x^2 + 3x^3\}$.

17. 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 $\mathbb{Q}_4[x]$?

$$1 + x + x^2 + x^3, 1 + 2x + x^2 + x^3, 2x + ax^2, 1 + 3x + (a + 2)x^3.$$

18. 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 $f, f^{(1)}, f^{(2)}, \dots, f^{(n)}$, où $f^{(i)}$ est la i -ième dérivée de f , forment une base de $\mathbb{R}_{n+1}[x]$.
19. 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 .
20. Vérifier que $\{1, 1-x, (1-x)^2\}$ est une base de l'espace vectoriel $\mathbb{R}_3[x]$, et trouver les coordonnées de $6-5x+2x^2$ dans cette base.
21. 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} .
22. 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) $F_3 = \{(a, b) \in \mathbb{R}^2 \mid (a-b)^2 = 2a+b\}$.
23. 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 .
24. 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 $n > 1$.
25. 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 $1_K + 1_K \neq 0_K$.
26. Soit E un espace vectoriel sur K avec $u, v, w \in E$. Si $u + v + w = 0$, montrer que $\langle u, v \rangle = \langle u, w \rangle$.
27. Considérer l'espace vectoriel réel $C(\mathbb{R})$ des fonctions réelles continues. Soient $\lambda_1, \dots, \lambda_n$, avec $n \geq 1$, des nombres réels deux à deux distincts.
- (1) Vérifier que les fonctions $e^{\lambda_1 t}, \dots, e^{\lambda_n t}$ 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 $e^{\lambda_1 t}, \dots, e^{\lambda_n t}$.
28. Soit E un espace vectoriel. Soient $\mathcal{U} = \{u_1, \dots, u_r\}$ et $\mathcal{V} = \{v_1, \dots, v_s\}$ 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 $\langle \mathcal{U} \rangle$.
29. 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 $\{f_1, f_2, f_3\}$.
30. 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 $(3, 2, 1, 3)$.
31. 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 $1+3x+x^2+2x^3+x^4$.
32. Donner une base du sous-espace F de l'espace vectoriel réel \mathbb{R}^4 suivant:

$$F = \{(a + b, a - b, a - c, b - c) \mid a, b, c \in \mathbb{R}\}.$$

33. Donner une base du sous-espace F de l'espace vectoriel réel $M_2(\mathbb{R})$ suivant:

$$F = \left\{ \begin{pmatrix} a + 2b + c & a + 3b + 2c \\ a + b & a + 2b + c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}.$$

34. 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.

35. Trouver une base de l'espace-solution du système homogène suivant:

$$\begin{aligned} 3x_1 + 3x_2 + 5x_3 &= 0 \\ x_1 + x_2 + 3x_3 + 2x_4 &= 0 \\ 2x_1 + 2x_2 + 4x_3 + x_4 &= 0 \\ 5x_1 + 5x_2 + 9x_3 + x_4 &= 0. \end{aligned}$$

36. Dans chacun des cas suivants, montrer que $1 \leq \dim \mathcal{N}(A) \leq 2$ et trouver les valeurs de a pour que $\dim \mathcal{N}(A) = 1$.

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

37. 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

$$\mathcal{S} = \{u_0 + u \mid u \in \mathcal{N}(A)\}.$$

38. 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 $\mathcal{N}(A)$.

39. Montrer que $A \in M_n(K)$ est inversible si, et seulement si, $\text{rg}(AB) = \text{rg}(B)$ pour toute matrice B de n lignes.

40. Soient $A \in M_{m \times n}(K)$ et $B \in M_{n \times p}(K)$. Si $AB = 0$, montrer que $\text{rg}(A) + \text{rg}(B) \leq n$.

Indice: Vérifier que $\mathcal{C}(B)$ est un sous-espace vectoriel de $\mathcal{N}(A)$.

41. 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 $\text{rg}(A) = m$.

42. Soient A, B des matrices sur K . Si $B = PAQ$ avec P, Q inversibles, montrer que $\text{rg}(B) = \text{rg}(A)$. *Indice:* Utiliser la proposition 4.7.10.

43. 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, $\text{rg}(A) = \text{rg}(A|B)$.

44. Considérer deux sous-espaces de l'espace vectoriel réel $\mathbb{R}_4[x]$ suivants:

$$\langle 1 + x^3, x - x^2, 2 - x + x^2 + 2x^3 \rangle$$

et

$$\langle 1 - x + x^2 + x^3, x^2 - x^3, 1 - x + 2x^3 \rangle.$$

Trouver une base de leur somme, et calculer leur intersection.

45. Si F et G sont des sous-espaces d'un espace vectoriel E , montrer que $\langle F \cup G \rangle = F + G$.

46. Considérer les matrices réelles suivantes:

$$A = \begin{pmatrix} 1 & 2 & 0 \\ -1 & 0 & -2 \\ 2 & -1 & 5 \\ 1 & 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 4 & 3 \\ -1 & -2 & -1 \\ 2 & 0 & 2 \\ 1 & 1 & -1 \end{pmatrix}$$

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.

47. Considérer les systèmes homogènes réels suivants:

$$\begin{array}{lcl} x + y - z = 0 & & x - y + z = 0 \\ x - 3y + z = 0 & \text{et} & 3x - 3y + 3z = 0 \\ x - y = 0 & & 5x - 5y + 5z = 0. \end{array}$$

Trouver une base pour l'intersection ainsi que la somme de leur espaces-solutions, et déterminer si la somme est directe ou non.

48. 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?
49. 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.
50. Soient $S_n(K)$ et $T_n(K)$ les sous-espaces 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.
51. Considérer les matrices réelles suivantes:

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

Vérifier que la somme $\mathcal{L}(A) + \mathcal{L}(B)$ est directe.

52. Considérer l'espace vectoriel réel \mathbb{R}^3 . Montrer que $\mathbb{R}^3 = F_1 \oplus F_2 \oplus F_3$, où

$$F_1 = \{(x, x, 0) \mid x \in \mathbb{R}\}, \quad F_2 = \{(x, 0, x) \mid x \in \mathbb{R}\}, \quad F_3 = \{(0, x, x) \mid x \in \mathbb{R}\}.$$

53. Considérer l'espace vectoriel complexe $M_n(\mathbb{C})$, avec $n \geq 1$, des matrices carrées complexes d'ordre n . Montrer que $M_n(\mathbb{C}) = S_n(\mathbb{C}) \oplus A_n(\mathbb{C})$, 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.
54. 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 $M_2(\mathbb{R}) = F \oplus G$.

55. Considérer l'espace vectoriel réel $\mathbb{R}_5[x]$. Soit F le sous-espace vectoriel de $\mathbb{R}_5[x]$ engendré par les vecteurs

$$f_1 = 1 + x - x^2 - x^3 + x^4; f_2 = 2 - x + x^2 + 3x^4; f_3 = x + x^2 - x^3,$$

et

$$f_4 = 3 + 2x + 2x^2 - 2x^3 + 4x^4; f_5 = 5 + x + 3x^2 - 2x^3 + 7x^4.$$

Trouver un complément de F dans $\mathbb{R}_5[x]$.

56. 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 , $i = 1, \dots, r$. Montrer que $\mathcal{F}_1 \cup \cdots \cup \mathcal{F}_r$ est libre si, et seulement si, \mathcal{F}_i est libre pour $i = 1, \dots, r$.