ALGÈBRE LINÉAIRE 3

Licence L2
Emmanuel Hebey
Année 2024-2025

TABLE DES MATIÈRES

Licence L2 - 1er Semestre
19,5h CM

ALGÈBRE LINÉAIRE 3

EMMANUEL HEBEY

1. Introduction

L'objectif de ce cours est d'aborder les bases de la réduction des applications linéaires avec, pour point d'orgue, la théorie de la diagonalisation. L'algèbre linéaire étant très récente pour nombre d'entre vous, il n'est pas inutile de procéder à quelques rappels. Il est impossible de tout rappeler. Nous considérerons donc comme acquis les bases de l'algèbre linéaire, hors théorie des matrices. Mais, même si vous avez vu cette théorie en détails l'an passé, elle peut être perçue comme particulièrement dense par plusieurs d'entre vous. Nous en développons donc les principaux éléments au Chapitre 1 de ce polycopié.

Le cours commencera véritablement avec la théorie des matrices et sa relation plus qu'importante aux applications linéaires. Ce sera l'objet des chapitres 2 et 3. Ils sont sans doute plus complet dans ce polycopié que ce que nous pourrons réellement traiter. Mais là encore, vous aurez ainsi à disposition dans ces notes tous les éléments dont vous pourriez avoir besoin.

L'objet principal du cours est donc la diagonalisation. Elle est traitée au Chapitre 4. La question posée est de savoir s'il est possible de représenter une application linéaire par une matrice diagonale, donc très simple à manipuler. Seule la théorie réelle est développée au Chapitre 4. Des éléments de la théorie complexe sont discutés dans le chapitre suivant ainsi que la théorie compagne de la diagonalisation, à savoir la trigonalisation.

Date: 12 Février 2025.

CHAPITRE 1

ALGÈBRE LINÉAIRE NON MATRICIELLE

Dans toute la suite, on ne considère que des espaces vectoriels réels, à savoir sur le corps $\mathbb{R}$ des réels. On signale tout de même qu'il existe une théorie analogue pour les espaces vectoriels complexes.

Etant donné un ensemble E, une loi interne notée $+$ sur E est une application de $E \times E \to E$. A un couple $(x, y) \in E \times E$ elle associe un élément de E noté $x + y$.

Une loi externe sur E, construite sur $\mathbb{R}$, est une application de $\mathbb{R} \times E \to E$. A un couple $(\lambda, x) \in \mathbb{R} \times E$ elle associe un élément de E noté λx.

On adopte donc une notation additive pour la loi interne et une notation multiplicative pour la loi externe.

Définition 1.1. *Soit E un ensemble muni d'une loi interne notée $+$, agissant de $E \times E$ dans E, et d'une loi externe $\times$ sur $\mathbb{R}$, agissant de $\mathbb{R} \times E$ dans E. On dit que E muni de ces deux lois est un $\mathbb{R}$-espace vectoriel si $(E, +)$ est un groupe abélien, et si la loi externe $\times$ qui à $(t, x) \in \mathbb{R} \times E$ associe tx vérifie:*
(i) (Distributivité dans $\mathbb{R}$) $\forall t, t' \in \mathbb{R}$, $\forall x \in E$, $(t + t')x = tx + t'x$;
(ii) (Distributivité dans E) $\forall t \in \mathbb{R}$, $\forall x, x' \in E$, $t(x + x') = tx + tx'$;
(iii) (Associativité dans $\mathbb{R}$) $\forall t, t' \in \mathbb{R}$, $\forall x \in E$, $t(t'x) = (tt')x$;
(iv) (Neutralité) $\forall x \in E$, $1 \times x = x$.
Un sous ensemble F de E est dit un sous espace vectoriel de E si F muni des deux lois (internes et externes) de E est un $\mathbb{R}$-espace vectoriel.

Pour rappel, un groupe abélien $(E, +)$ est un ensemble E muni d'une loi interne $+$, i.e. agissant de $E \times E$ dans E, qui vérifie:
(i) (Associativité) $\forall x, y, z \in E$, $(x + y) + z = x + (y + z)$;
(ii) (Elément neutre) $\exists 0 \in E$ tel que $\forall x \in E$, $x + 0 = 0 + x = x$;
(iii) (Inverse) $\forall x \in E$, $\exists -x \in E$ tel que $x + (-x) = (-x) + x = 0$;
(iv) (Caractère Abélien) $\forall x, y \in E$, $x + y = y + x$.
Le 0 de (ii) est appelé élément neutre (et vecteur nul dans le cadre de la théorie des espaces vectoriels).

Des propriétés simples qui suivant de la définition d'un espace vectoriel sont les suivantes:
(P1) $\forall x \in E$, $0 \times x = 0$;
(P2) $\forall x \in E$, $(-1) \times x = -x$;
(P3) $\forall t \in \mathbb{R}$, $t \times 0 = 0$;
(P4) $\forall t \in \mathbb{R}$, $\forall x \in E$, $tx = 0 \Leftrightarrow t = 0$ ou $x = 0$.

Exercice: Démontrer les propriétés (P1)-(P4).

Solution: On vérifie (P1) en écrivant que

$$(0 + 0) \times x = 0 \times x = 0 \times x + 0 \times x$$

de sorte que, nécessairement, $0 \times x = 0$. Dans (P1), le premier 0 est le 0 de $\mathbb{R}$, le second 0 est celui de E (vecteur nul, elément neutre de $+$). Une fois (P1) démontrée, on obtient (P2):

$$0 = (1 + (-1)) \times x = x + (-1) \times x$$

de sorte que $(-1) \times x = -x$, par définition même de $-x$. Pour (P3) on écrit avec (P2) que

$$t \times 0 = t \times (x + (-x)) = t \times x + (-1) \times (t \times x) = 0 \ .$$

Pour démontrer (P4) il suffit de montrer que si $t \neq 0$ et si $tx = 0$, alors $x = 0$. Pour cela, en supposant que $t \neq 0$ et $tx = 0$, on écrit

$$0 = \frac{1}{t} \times (t \times x) = 1 \times x = x$$

D'où $tx = 0$ si et seulement si $t = 0$ ou $x = 0$, le "ou" n'étant bien sûr pas exclusif dans la mesure où $0 \times 0 = 0$. $\square$

En bref, un $\mathbb{R}$-espace vectoriel est un ensemble E muni d'une addition qui permet d'additionner ces éléments entres eux (comme on le fait dans $\mathbb{R}$), et d'une loi externe qui permet de multiplier les éléments de E par des réels…

Les éléments d'un espace vectoriel sont aussi appelés des vecteurs.

Exemple 1: $\mathbb{R}^2$ muni des lois internes et externes

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

et

$$\lambda \times (x_1, x_2) = (\lambda x_1, \lambda x_2)$$

est un $\mathbb{R}$-espace vectoriel. Le 0 ici est le couple $(0, 0)$. L'exemple s'étend facilement à $\mathbb{R}^n$, $n \geq 2$. Pour $n = 3$, on aura par exemple que $(x_1, x_2, x_3) + (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$ et $\lambda \times (x_1, x_2, x_3) = (\lambda x_1, \lambda x_2, \lambda x_3)$. Le 0 est maintenant le triplet $(0, 0, 0)$. Etc pour $n \geq 4$.

Exemple 2: L'ensemble des fonctions $f : \mathbb{R} \to \mathbb{R}$ est un $\mathbb{R}$-espace vectoriel lorsque muni des deux lois

$$\text{Addition interne: } \big(f + g\big)(x) = f(x) + g(x);$$
$$\text{Multiplication externe: } \big(t \times f\big)(x) = tf(x).$$

Là encore, les vérifications des propriétés (i)-(iv) de groupe abélien, et des propriétés (i)-(iv) pour la multiplication externe, sont très simples. Le 0 est ici l'application nulle de $\mathbb{R}$ dans $\mathbb{R}$.

Lemme 1.1. *Soient E_1 et E_2 deux espace vectoriels munis de lois internes et externes notées $+_i$ et $\times_i$, $i = 1, 2$. Soit $E = E_1 \times E_2$ le produit cartésien de E_1 et E_2 constitué des couples (x, y) où $x \in E_1$ et $y \in E_2$. On munit E des deux lois $+$ et $\times$ définies par:*

$$\textit{Addition interne: } (x, y) + (\tilde{x}, \tilde{y}) = (x +_1 \tilde{x}, y +_2 \tilde{y});$$
$$\textit{Multiplication externe: } t \times (x, y) = (t \times_1 x, t \times_2 y).$$

Alors E muni de ces deux lois est un $\mathbb{R}$-espace vectoriel.

Soit E un ensemble que l'on suppose être un $\mathbb{R}$-espace vectoriel lorsque muni de deux lois $+$ et $\times$. Soit de plus F un sous ensemble de E. Par définition, on l'a vu, F est un sous espace vectoriel de E si F muni de ces deux lois est un $\mathbb{R}$-espace vectoriel. Cela suppose déjà que les lois $+$ et $\times$ de E soient bien des lois respectivement internes et externes pour F. Et donc que:

(1) $\forall x, y \in F$, $x + y \in F$;
(2) $\forall t \in \mathbb{R}$, $\forall x \in F$, $tx \in F$.

Ce n'est pas obligatoirement le cas pour un sous ensemble quelconque de E comme on le verra dans les exercices qui suivent.

Remarques: (1) Si F est un sous espace vectoriel, alors forcément $0 \in F$.
(2) Si F est un sous espace vectoriel, alors pour tout $x \in F$ on a que $-x \in F$.

Proposition 1.1 (Caractérisation des sous espaces vectoriels). *Soit E un $\mathbb{R}$-espace vectoriel muni de deux lois $+$ et $\times$. Soit $F \neq \emptyset$ un sous ensemble de E. Alors F est un sous espace vectoriel de E si et seulement si*
(1) $\forall x, y \in F$, $x + y \in F$;
(2) $\forall t \in \mathbb{R}$, $\forall x \in F$, $tx \in F$.
Cela se caractérise encore par le fait que pour tous $t, t' \in \mathbb{R}$, et tous $x, y \in F$, $tx + t'y \in F$.

Soit E l'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni des deux lois de l'exemple 2. Le sous ensemble $C^0(\mathbb{R})$ de E constitué des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ est alors par exemple un sous espace vectoriel de E. L'ensemble $\mathbb{R}[X]$ des polynômes réels est aussi un sous espace vectoriel de E. L'ensemble $\mathbb{R}_n[X]$ des polynômes réels de degré au plus n est lui encore aussi un sous espace vectoriel de E. On a $\mathbb{R}_n[X] \subset_{sev} \mathbb{R}[X] \subset_{sev} C^0(\mathbb{R})$, l'inclusion $\subset_{sev}$ signifiant "est un sous espace vectoriel de".

Exercice: Montrer que le sous ensemble de $\mathbb{R}^3$ donné par

$$F = \left\{(x, y, z) \in \mathbb{R}^3 \ / \ x + 2y - z = 0\right\}$$

est un sous espace vectoriel de $\mathbb{R}^3$.

Solution: On vérifie que $F \neq \emptyset$, par exemple $(0, 0, 0) \in F$. On applique la proposition de caractérisation des sous espaces vectoriels. Soient $(x, y, z) \in F$ et $(x', y', z') \in F$ deux vecteurs quelconques de F et $\lambda \in \mathbb{R}$ un réel quelconque. On a que $(x, y, z) + (x', y', z') = (x + x', y + y', z + z') \in F$ car

$$x + x + 2(y + y') - (z + z') = (x + 2y - z) + (x' + 2y' - z') = 0 + 0 = 0 \ .$$

De même, $\lambda(x, y, z) = (\lambda x, \lambda y, \lambda z) \in F$ car

$$(\lambda x) + 2(\lambda y) - (\lambda z) = \lambda(x + 2y - z) = \lambda \times 0 = 0 \ .$$

Donc F est un sous espace vectoriel de $\mathbb{R}^3$. $\square$

Exercice: Montrer que le sous ensemble de $\mathbb{R}^3$ donné par

$$F = \left\{(x, y, z) \in \mathbb{R}^3 \ / \ x + 2y - z = 1\right\}$$

n'est pas un sous espace vectoriel de $\mathbb{R}^3$.

Solution: Les vecteurs $(1, 0, 0)$ et $(0, 0, -1)$ sont dans F. Pourtant, lorsque l'on additionne ces deux vecteurs, $(1, 0, 0) + (0, 0, -1) = (1, 0, -1)$ n'est pas dans F. $\square$

Exercice: Montrer que le sous ensemble de $\mathbb{R}^2$ donné par

$$F = \left\{(x, y) \in \mathbb{R}^2 \ / \ xy = 0\right\}$$

n'est pas un sous espace vectoriel de $\mathbb{R}^2$.

Solution: Les vecteurs $(1, 0)$ et $(0, 1)$ sont dans F. Pourtant $(1, 0) + (0, 1) = (1, 1)$ n'est pas dans F. $\square$

Exercice: Montrer que le sous ensemble de $\mathbb{R}^2$ donné par

$$F = \left\{(x, y) \in \mathbb{R}^2 \ / \ y = x^2\right\}$$

n'est pas un sous espace vectoriel de $\mathbb{R}^2$.

Solution: Le vecteur $(1,1)$ est dans F. Par contre $(2,2) = 2 \times (1,1)$ n'est pas dans F. $\square$

Exercice: Montrer que le sous ensemble F de $\mathbb{R}[X]$ constitué des polynômes réels P pour lesquels $P(0) = P(1)$ est un sous espace vectoriel de $\mathbb{R}[X]$.

Solution: Clairement $F \neq \emptyset$. On vérifie facilement que la somme de deux polynômes de F est encore un polynôme de F et que le produit d'un polynôme de F par un réel quelconque est encore un polynôme de F. $\square$

2. Opérations sur les sous espaces vectoriels

On discute de différentes opérations possibles sur les sous espaces vectoriels.

2.1. **Intersections de sous espaces vectoriels.** Soit E un espace vectoriel muni de deux lois $+$ et $\times$, et soient $F_1, \dots, F_k$ des sous espaces vectoriels de E. Alors $F_1 \cap \dots \cap F_k$ est encore un sous espace vectoriel de E. La propriété se démontre très facilement. Bien sûr, on peut avoir que $F_1 \cap \dots \cap F_k = \{0\}$.

2.2. **Union de sous espaces vectoriels.** Soit E un espace vectoriel muni de deux lois $+$ et $\times$, et soient F_1, F_2 deux sous espaces vectoriels de E. En général, $F_1 \cup F_2$ N'EST PAS un sous espace vectoriel de E.

Proposition 2.1. *Soit E un espace vectoriel muni de deux lois $+$ et $\times$, et soient F_1, F_2 deux sous espaces vectoriels de E. Alors $F_1 \cup F_2$ est un sous espace vectoriel de E si et seulement si $F_1 \subset F_2$ ou $F_2 \subset F_1$.*

Démonstration. Si $F_1 \subset F_2$, ou $F_2 \subset F_1$, alors $F_1 \cup F_2 = F_1$ ou F_2, et donc $F_1 \cup F_2$ est bien un sous espace vectoriel de E. A l'inverse, on raisonne par l'absurde en supposant que $F_1 \cup F_2$ est un sous espace vectoriel de E, mais que $F_1 \not\subset F_2$ et $F_2 \not\subset F_1$. Soit $x \in F_2 \backslash F_1$ et $y \in F_1 \backslash F_2$. Puisque nous avons supposé que $F_1 \cup F_2$ est un sous espace vectoriel, $x + y \in F_1 \cup F_2$, et donc, soit
 (1) $x + y \in F_1$, soit
 (2) $x + y \in F_2$.
Si (1) a lieu, alors $x \in F_1$ puisque $y \in F_1$ et F_1 est un sous espace vectoriel de E. Si (2) a lieu, alors $y \in F_2$ puisque $x \in F_2$ et F_2 est un sous espace vectoriel de E. Dans les deux cas, on aboutit à une contradiction. Donc $F_1 \cup F_2$ sous espace vectoriel $\Rightarrow F_1 \subset F_2$ ou $F_2 \subset F_1$. D'où la proposition. $\square$

2.3. **Sommes de sous espace vectoriels.** Soit E un espace vectoriel muni de deux lois $+$ et $\times$, et soient F_1, F_2 deux sous espaces vectoriels de E. On définit la somme $F_1 + F_2$ des sous espaces F_1 et F_2 par

$$F_1 + F_2 = \left\{ x + y \in E \text{ tels que } x \in F_1, y \in F_2 \right\} .$$

On vérifie alors très facilement que $F_1 + F_2$ est encore un sous espace vectoriel de E. En effet, soient z et $\tilde{z}$ deux éléments de $F_1 + F_2$. On peut écrire que $z = x + y$ et $\tilde{z} = \tilde{x} + \tilde{y}$, où $x, \tilde{x} \in F_1$ et $y, \tilde{y} \in F_2$. Dès lors, si $t, \tilde{t} \in \mathbb{R}$, alors

$$tz + \tilde{t}\tilde{z} = (tx + \tilde{t}\tilde{x}) + (ty + \tilde{t}\tilde{y})$$

et donc, puisque $tx + \tilde{t}\tilde{x} \in F_1$ et $ty + \tilde{t}\tilde{y} \in F_2$, on a que $tz + \tilde{t}\tilde{z} \in F_1 + F_2$. D'où le fait que $F_1 + F_2$ est un sous espace vectoriel de E.

Exercice: Soient A, B, C trois sous espaces vectoriels d'un espace vectoriel E. On suppose que $A \cap B = A \cap C$, $A + B = A + C$ et $B \subset C$. Montrer que $B = C$.

Solution: Il suffit de montrer que $C \subset B$. Soit $c \in C$ quelconque dans C. Comme $0 \in A$ et $c = 0 + c$ on a que $c \in A + C$. Comme $A + B = A + C$, on a que $c \in A + B$. Donc il existe $a \in A$ et $b \in B$ tels que $c = a + b$. On a $B \subset C$, donc $b \in C$. On a aussi $c - b = a$, et comme C est un sous espace vectoriel, $c - b \in C$. Comme $a \in A$, on en déduit que $c - b \in A \cap C$. Or $A \cap C = A \cap B$. Donc $c - b \in A \cap B$ et, en particulier, $c - b \in B$. Ainsi il existe $b' \in B$ tel que $c - b = b'$. Soit $c = b + b'$, et comme B est un sous espace vectoriel, $c \in B$. $\square$

Par définition, on dit que la somme $F_1 + F_2$ est directe, et on écrit $F_1 \oplus F_2$, si $\forall z \in F_1 + F_2$, $\exists! x \in F_1$, et $\exists! y \in F_2$ tels que $z = x + y$. En d'autres termes, la somme $F_1 + F_2$ est directe si les éléments de la somme $F_1 + F_2$ se décomposent de façon unique en somme d'un élément de F_1 et d'un élément de F_2.

Exemple: Soit $E = \mathbb{R}^3$ muni de ses lois usuels $+$ et $\times$. Soient de plus
$F_1 = \big\{(x, y, z) \in E \ / \ z = 0\big\}$,
$F_2 = \big\{(x, y, z) \in E \ / \ x = 0\big\}$, et
$F_3 = \big\{(x, y, z) \in E \ / \ x = y = 0\big\}$.
On vérifie facilement que F_1, F_2, et F_3 sont des sous espaces vectoriels de E, que $E = F_1 + F_2$ et que $E = F_1 + F_3$. La somme $F_1 + F_2$ n'est pas directe. En effet, on peut tout à la fois écrire que $(x, y, z) = (x, y, 0) + (0, 0, z)$ et que $(x, y, z) = (x, 0, 0) + (0, y, z)$, avec $(x, y, 0), (x, 0, 0) \in F_1$ et $(0, 0, z), (0, y, z) \in F_2$. Cela fournit deux écritures différentes pour (x, y, z) si $y \neq 0$. La somme $F_1 + F_2$ n'est donc pas directe. Par contre, la somme $F_1 + F_3$ est directe, un élément (x, y, z) se décomposant de façon unique en $(x, y, z) = (x, y, 0) + (0, 0, z)$. On écrit donc $F_1 \oplus F_3$.

Proposition 2.2. *Soit E un espace vectoriel muni de deux lois $+$ et $\times$, et soient F_1, F_2 deux sous espaces vectoriels de E. Alors la somme $F_1 + F_2$ est directe si et seulement si $F_1 \cap F_2 = \{0\}$.*

Démonstration. Supposons que la somme $F_1 + F_2$ est directe. S'il existe $x \in F_1 \cap F_2$, alors les deux écritures $x = 0 + x$ et $x = x + 0$ entraînent que nécessairement $x = 0$. Donc, $F_1 \cap F_2 = \{0\}$. Réciproquement, supposons que $F_1 \cap F_2 = \{0\}$. Soit $z \in F_1 + F_2$. Si $z = x + y$ et $z = x' + y'$ avec $x, x' \in F_1$ et $y, y' \in F_2$, alors

$$x - x' = y' - y \ .$$

Or $x - x' \in F_1$ et $y' - y \in F_2$. Comme $F_1 \cap F_2 = \{0\}$, c'est donc que $x - x' = y' - y = 0$. Donc la somme $F_1 + F_2$ est directe. $\square$

Ce qui a été dit à propos de la somme de deux sous espaces vectoriels se généralise à la somme de k sous espaces vectoriels. Si $F_1, \dots, F_k$ sont k sous espaces vectoriels de E, on définit

$$F_1 + \cdots + F_k = \big\{x_1 + \cdots + x_k \in E \text{ tels que } x_i \in F_i, i = 1, \dots, k\big\} \ .$$

Là encore, comme lorsque $k = 2$, $F_1 + \cdots + F_k$ est un sous espace vectoriel de E. Par définition, on dit que la somme $F_1 + \cdots + F_k$ est directe, et on écrit $F_1 \oplus \cdots \oplus F_k$, si la propriété suivante est vérifiée par la somme $F_1 + \cdots + F_k$: $\forall z \in F_1 + \cdots + F_k$, $\exists! x_1 \in F_1$, ..., $\exists! x_k \in F_k$ tels que $z = x_1 + \cdots + x_k$. En d'autres termes, la somme $F_1 + \cdots + F_k$ est directe si les éléments de la somme $F_1 + \cdots + F_k$ se décomposent de façon unique en somme d'un élément de F_1, ..., et d'un élément de F_k. On peut alors montrer que la somme $F_1 + \cdots + F_k$ est directe si et seulement si pour tout $i = 2, \ldots, k$, $F_i \cap (\sum_{j<i} F_j) = \{0\}$.

Théorème 2.1. *Soient k sous espaces vectoriels $F_1, \ldots, F_k$ d'un espace vectoriel E. La somme $F_1 + \cdots + F_k$ est directe, et on écrit $F_1 \oplus \cdots \oplus F_k$, si et seulement si pour tout $i = 2, \ldots, k$, $F_i \cap (\sum_{j<i} F_j) = \{0\}$.*

Démonstration. On procède par récurrence sur k. On considère la propriété $(\mathcal{P}_k)$ stipulant que pour tout $\mathbb{R}$-espace vectoriel E, et toute famille $F_1, \ldots, F_k$ de k sous espaces vectoriels de E, $F_1 \oplus \cdots \oplus F_k$ si et seulement si pour tout $i = 2, \ldots, k$, $F_i \cap (\sum_{j<i} F_j) = \{0\}$. Si $k = 2$ on a déjà vu que $(\mathcal{P}_k)$ est vraie. On suppose maintenant $(\mathcal{P}_k)$ et on montre que $(\mathcal{P}_{k+1})$ est vraie. On se donne donc E un $\mathbb{R}$-espace vectoriel et $F_1, \ldots, F_{k+1}$ des sous espaces vectoriels de E. Soit $F = F_1 + \cdots + F_k$. Clairement,

$$F_1 \oplus \cdots \oplus F_{k+1} \text{ ssi } F_1 \oplus \cdots \oplus F_k \text{ et } F \oplus F_{k+1}$$

et donc si et seulement si $F \cap F_{k+1} = \{0\}$ d'après ce qui a été dit dans le cas $k = 2$. Or $F_i \cap (\sum_{j<i} F_j) = \{0\}$ pour tout $i = 2, \ldots, k$ et $F \cap F_{k+1} = \{0\}$ équivaut à $F_i \cap (\sum_{j<i} F_j) = \{0\}$ pour tout $i = 2, \ldots, k+1$. D'où le théorème. □

Exercice: Soient A, B, C trois sous espaces vectoriels d'un espace vectoriel E. Montrer que la somme $A + B + C$ est directe si et seulement si $A \cap B = \{0\}$ et $(A + B) \cap C = \{0\}$.

Solution: Supposons $A + B + C$ directe. Soit $x \in A \cap B$. En écrivant que $x + 0 + 0 = 0 + x + 0$ on a deux écritures dans $A + B + C$ d'un même vecteur de $A + B + C$. La somme étant directe c'est que $x = 0$. Donc $A \cap B = \{0\}$. De même, soit $x \in (A + B) \cap C$. Comme $x \in A + B$ il existe $a \in A$ et $b \in B$ tels que $x = a + b$. On a $a + b + 0 = 0 + 0 + x$ qui fournit deux écritures d'un même vecteur dans $A + B + C$. La somme étant directe c'est que $a = 0$, $b = 0$ et $x = 0$. Donc $(A + B) \cap C = \{0\}$. Réciproquement, supposons que $A \cap B = \{0\}$ et que $(A+B) \cap C = \{0\}$. Soient $a, a' \in A$, $b, b' \in B$ et $c, c' \in C$ tels que $a+b+c = a'+b'+c'$. Alors $(a - a') + (b - b') = c' - c$. Or $(a - a') + (b - b') \in A + B$ et $c' - c \in C$. Comme $(A+B) \cap C = \{0\}$, c'est que $c' = c$ et $(a-a')+(b-b') = 0$. En particulier, $a - a' = b' - b$. Or $a - a' \in A$ et $b' - b \in B$. Comme $A \cap B = \{0\}$, c'est que $a' = a$ et $b' = b$. □

2.4. **Sous espace vectoriels engendrés par un sous ensemble.** Soit E un espace vectoriel muni de deux lois $+$ et $\times$, et soit A une partie (i.e. un sous ensemble) de E. Le sous espace vectoriel de E engendré par A, noté $Vect(A)$, est par définition le plus petit sous espace vectoriel de E pour l'inclusion qui contient A. Il est caractérisé par les propriétés suivantes:

(i) $Vect(A)$ est un sous espace vectoriel de E,
(ii) $A \subset Vect(A)$,
(iii) si F est un sous espace vectoriel de E et si $A \subset F$, alors $Vect(A) \subset F$.

On vérifie que $Vect(A)$ est en fait constitué des combinaisons linéaires des éléments de A. En d'autres termes:

$$Vect(A) = \left\{ t_1 x_1 + \cdots + t_k x_k, k \in \mathbb{N}, t_i \in \mathbb{R}, x_i \in A \right\} .$$

Le sous ensemble de E définit ci-dessus est bien un sous espace vectoriel de E, et il vérifie les points (i)-(iii) listés ci-dessus.

Des propriétés simples à vérifier que satisfont les espaces $Vect(A)$ sont les suivantes:
(1) Si A est un sous espace vectoriel de E, alors $Vect(A) = A$,
(2) Si A et B sont deux sous ensembles de E,

$$Vect(A \cup B) = Vect(A) + Vect(B) \ .$$

En ce qui concerne l'intersection,

$$Vect(A \cap B) \subset Vect(A) \cap Vect(B) \ .$$

Cette propriété est elle aussi facile à vérifier (par exemple à partir de la définition première). A titre de remarque, il se peut que $Vect(A \cap B) \neq Vect(A) \cap Vect(B)$. Soit par exemple, $E = \mathbb{R}^2$, $A = \{(x,y) \ / \ x^2 + y^2 \leq 1\}$, et $B = \{(1,0),(0,2)\}$. Alors $A \cap B = \{(1,0)\}$ de sorte que $Vect(A \cap B) = \{(x,y) \ / \ y = 0\}$. Par contre $Vect(A) = Vect(B) = \mathbb{R}^2$, de sorte que $Vect(A) \cap Vect(B) = \mathbb{R}^2$.

Lorsque A est fini, par exemple lorsque $A = \{a,b,c,d\}$, alors

$$Vect(A) = \{t_1a + t_2b + t_3c + t_4d, t_1, t_2, t_3, t_4 \in \mathbb{R}\} \ .$$

Exercice: Démontrer (1) et (2) ci-dessus.

Solution: Si A est un sous espace vectoriel, alors A est clairement le plus petit sous espace vectoriel qui se contient lui-même. Donc $A = Vect(A)$. On démontre maintenant (2). Soient $k \in \mathbb{N}^\star$, $x_1, \dots, x_k$ une famille de k vecteurs de $A \cup B$ et $t_1, \dots, t_k$ des réels. Par définition de $A \cup B$ il existe $k_1 \in \mathbb{N}$ (peut-être 0), il existe $k_2 \in \mathbb{N}$ (peut-être 0), il existe des $a_1, \dots, a_{k_1} \in A$ et des $b_1, \dots, b_{k_2} \in B$ tels que

$$\{x_i, i = 1, \dots, k\} = \{a_i, i = 1, \dots, k_1\} \ \cup \{b_i, i = 1, \dots, k_2\} \ .$$

Avec la même répartition on peut écrire que $\{t_i, i = 1, \dots, k\}$ comme $\{\lambda_i, i = 1, \dots, k_1\} \cup \{\mu_i, i = 1, \dots, k_2\}$. Mais alors

$$t_1x_1 + \cdots + t_kx_k = (\lambda_1a_1 + \cdots + \lambda_{k_1}a_{k_1}) + (\mu_1b_1 + \cdots + \mu_{k_2}b_{k_2})$$

et donc $Vect(A \cup B) \subset Vect(A) + Vect(B)$. L'autre sens s'obtient encore plus facilement. On a $Vect(A) \subset Vect(A \cup B)$ et $Vect(B) \subset Vect(A \cup B)$. Donc $Vect(A) + Vect(B) \subset Vect(A \cup B)$. □

Exercice: On considère dans $\mathbb{R}^3$ les vecteurs $u_1 = (1,1,3)$, $u_2 = (1,-1,-1)$, $v_1 = (1,0,1)$ et $v_2 = (2,-1,0)$. Montrer que $Vect(u_1,u_2) = Vect(v_1,v_2)$.

Solution: On va montrer que $Vect(u_1,u_2) \subset Vect(v_1,v_2)$ et que $Vect(v_1,v_2) \subset Vect(u_1,u_2)$. Pour simplifier on ne démontre que la première inclusion. L'autre se démontre de la même manière. Pour démontrer que $Vect(u_1,u_2) \subset Vect(v_1,v_2)$ il suffit de montrer que $u_1 \in Vect(v_1,v_2)$ et que $u_2 \in Vect(v_1,v_2)$. L'équation

$$(1,1,3) = \lambda(1,0,1) + \mu(2,-1,0)$$

donne $\lambda + 2\mu = 1$, $-\mu = 1$ et $\lambda = 3$, un système dont la solution est bien donnée par $\lambda = 3$ et $\mu = -1$ (les deux dernières équations entraînent la première). On a donc $u_1 = 3v_1 - v_2$ et donc $u_1 \in Vect(v_1,v_2)$. De la même façon on vérifie que $u_2 = -v_1 + v_2$. Donc $u_2 \in Vect(v_1,v_2)$. Donc $Vect(u_1,u_2) \subset Vect(v_1,v_2)$. Comme déjà dit, l'autre inclusion se démontre de la même façon. On montre que $v_1 = \frac{1}{2}u_1 + \frac{1}{2}u_2$ et que $v_2 = \frac{1}{2}u_1 + \frac{3}{2}u_2$. □

3. Applications linéaires

Soient E et F deux espaces vectoriels sur $\mathbb{R}$, et $f : E \to F$ une application. Par définition, on dit que f est linéaire si les deux propriétés suivantes sont vérifiées:
(i) $\forall x, y \in E$, $f(x+y) = f(x) + f(y)$,
(ii) $\forall t \in \mathbb{R}$, $\forall x \in E$, $f(tx) = tf(x)$.
Ces deux propriétés se regroupent en une:
(iii) $\forall t \in \mathbb{R}$, $\forall x, y \in E$, $f(x+ty) = f(x) + tf(y)$.
On a donc (i)+(ii) $\Leftrightarrow$ (iii). En particulier, si f est linéaire, alors pour tout $k \in \mathbb{N}$, tous $t_i \in \mathbb{R}$, et tous $x_i \in E$, $i = 1, \dots, k$,

$$f\left(\sum_{i=1}^k t_i x_i\right) = \sum_{i=1}^k t_i f(x_i) \ .$$

On a toujours$f(0) = 0$ car $f(0) = f(0+0) = f(0) + f(0)$. On note $L(E,F)$ l'ensemble des applications linéaires de E dans F. Lorsque $F = E$, on note aussi $End(E)$ au lieu de $L(E,E)$. Les applications de $End(E)$ sont appelées endomorphismes de E.

On vérifie facilement que si E, F, G sont trois espace vectoriels, et si $f \in L(E,F)$ et $g \in L(F,G)$, alors $g \circ f \in L(E,G)$.

Indépendamment, si E et F sont deux espaces vectoriels, on définit sur $L(E,F)$ la loi interne $+$ et la loi externe $\times$ par:
$\big(f+g\big)(x) = f(x) + g(x)$,
$\big(tf\big)(x) = tf(x)$.
Alors $L(E,F)$ muni de ces deux lois est un espace vectoriel sur $\mathbb{R}$. Lorsque $F = \mathbb{R}$ on parle de forme linéaire et on note souvent $E^\star$ au lieu de $L(E,\mathbb{R})$.

Exercice: Soient $f, g : \mathbb{R}^2 \to \mathbb{R}^3$ les applications définies par

$$f(x,y) = (x+y, x-2y, 0) \text{ et } g(x,y) = (x+y, x-2y, 1)$$

pour tous $(x,y) \in \mathbb{R}^2$. Montrer que f est linéaire mais que g ne l'est pas.

Solution: Pour montrer que f est linéaire il suffit de vérifier que pour tous $(x,y), (x',y') \in \mathbb{R}^2$ et tout $\lambda \in \mathbb{R}$,

$$f(x+\lambda x', y+\lambda y') = f(x,y) + \lambda f(x',y') \ ,$$

et donc que

$$\begin{aligned}&(x+\lambda x' + y + \lambda y', x + \lambda x' - 2(y+\lambda y'), 0)\\ &= (x+y, x-2y, 0) + \lambda\,(x'+y', x'-2y', 0) \ .\end{aligned}$$

C'est immédiat. On montre par ailleurs que g n'est pas linéaire par exemple en remarquant que $(2,2) = 2 \times (1,1)$ tandis que

$$g(2,2) = (4,-2,1) \neq 2 \times (2,-1,1) = 2g(1,1) \ .$$

□

Exercice: Soit E un $\mathbb{R}$-espace vectoriel et $f, g \in L(E,\mathbb{R})$ deux formes linéaires sur E. Montrer que $f \times g = 0$ si et seulement si $f = 0$ ou $g = 0$.

Solution: Bien évidemment, si $f = 0$, ou $g = 0$, alors $f \times g = 0$. C'est la réciproque qui va être plus difficile à montrer. On suppose donc que $f \times g = 0$. Supposons par l'absurde qu'il existe $u \in E$ tel que $f(u) \neq 0$ et qu'il existe $v \in E$ tel que $g(v) \neq 0$. Comme $f \times g = 0$ on a forcément $f(v) = 0$ et $g(u) = 0$. Mais alors

$$0 = (fg)(u+v) = f(u)g(v)$$

ce qui est impossible puisque $f(u) \neq 0$ et $g(v) \neq 0$. D'où une contradiction et donc nécessairement soit $f = 0$ (sur tout E) soit $g = 0$ (sur tout E). □

Note: Le résultat cesse bien sûr d'être vrai si on ne parle plus de formes linéaires mais de fonctions quelconques. Par exemples les fonctions $f, g : \mathbb{R} \to \mathbb{R}$ définies par $f(x) = 0$ si $x \leq 0$ et $f(x) = x$ si $x \geq 0$, et $g(x) = x$ si $x \leq 0$ et $g(x) = 0$ si $x \geq 0$ ne sont pas identiquement nulles et pourtant vérifient que $f \times g = 0$.

Par définition, une application $f : E \to F$ est injective si les éléments de F ont au plus un antécédant par f. Donc f est injective si pour tous $x, y \in E$, si $f(x) = f(y)$, alors $x = y$. Toujours par définition, f est surjective si tout élément de F a au moins un antécédant. Donc f est surjective si pour tout $y \in F$, il existe $x \in E$ tel que $f(x) = y$. Pour finir, f est bijective si tout élément de F a précisément un et un seul antécédant. Par suite f est bijective si et seulement si elle est à la fois injective et surjective. Dans ce cas, lorsque f est bijective, il existe $f^{-1} : F \to E$ une application telle que $f^{-1} \circ f = Id_E$ et $f \circ f^{-1} = Id_F$.

Définition 3.1. *Si E et F sont deux espaces vectoriels, et si $f \in L(E,F)$, on définit: le noyau de f, noté $Ker(f)$, par*

$$Ker(f) = \big\{x \in E \ / \ f(x) = 0\big\} ,$$

et l'image de f, notée $Im(f)$, par $Im(f) = \big\{f(x) \ , \ x \text{ parcourt } E\big\}$.

On vérifie que $Ker(f)$ est un sous ensemble de E, et $Im(f)$ est un sous ensemble de F. Une application linéaire bijective de $L(E,F)$ est dite un isomorphisme de E sur F.

Théorème 3.1. *Soient E et F deux espaces vectoriels sur $\mathbb{R}$, et $f \in L(E,F)$ une application linéaire de E dans F. Alors:*

(i) $Ker(f)$ est un sous espace vectoriel de E et f est injective si et seulement si $Ker(f) = \{0\}$;

(ii) $Im(f)$ est un sous espace vectoriel de F et f est surjective si et seulement si $Im(f) = F$.

Par suite, f est un isomorphisme de E sur F si et seulement si $Ker(f) = \{0\}$ et $Im(f) = F$. Dans ce cas, l'application inverse f^{-1} est elle aussi linéaire.

Démonstration. Il est clair que $Ker(f)$ est un sous espace vectoriel de E dans la mesure ou si $t, t' \in \mathbb{R}$ et $x, x' \in Kerf(f)$, alors $tx + t'x' \in Ker(f)$ puisque

$$f(tx + t'x') = tf(x) + t'f(x') .$$

En remarquant par ailleurs que

$$f(y) = f(x) \quad \Leftrightarrow \quad f(y - x) = 0 \quad \Leftrightarrow \quad y - x \in Ker(f)$$

on voit que f est injective si et seulement si $Ker(f) = \{0\}$. On vérifie tout aussi facilement que $Im(f)$ est un sous espace vectoriel de F en remarquant comme ci-dessus que

$$tf(x) + t'f(x') = f(tx + t'x') .$$

Par ailleurs, il suit de la définition même d'une application surjective que f est surjective si et seulement si $Im(f) = F$. Reste à montrer que si f est un isomorphisme, alors f^{-1} est linéaire. Soient $z, z' \in F$ et $t \in \mathbb{R}$. Soient $x, x' \in E$ tels que $f(x) = z$ et $f(x') = z'$. Alors

$$\begin{aligned} f^{-1}\big(z + tz'\big) &= f^{-1}\big(f(x) + tf(x')\big) \\ &= f^{-1}\big(f(x + tx')\big) \\ &= x + tx' \\ &= f^{-1}(z) + tf^{-1}(z') \end{aligned}$$

et ainsi f^{-1} est bien linéaire. D'où le théorème. □

Exercice: Soit $E = \mathbb{R}[X]$ l'espace vectoriel des polynômes réels. On considère $f : E \to E$ donnée par $f(P) = P'$ pour tous $P \in E$. Montrer que f est linéaire. Déterminer son image et son noyau. L'application est-elle injective ? surjective ?

Solution: L'application est clairement linéaire par règles de dérivation: $(P_1 + \lambda P_2)' = P_1' + \lambda P_2'$ pour tous $\lambda \in \mathbb{R}$ et tous $P_1, P_2 \in E$. Son noyau $Ker(f)$ est constitué des polynômes $P \in E$ pour lesquels $P'(x) = 0$ pour tous $x \in \mathbb{R}$. Il s'agit donc des seuls polynômes constants:

$$Ker(f) = \{P \in E \ / \ P \text{ est constant}\} \ .$$

Comme $Ker(f) \neq \{0\}$, f n'est pas injective. Par contre, tout polynôme réel est clairement la dérivée d'un autre polynôme réel: le polynôme $P(X) = \sum_{k=0}^n a_k X^k$ est la dérivée du polynôme $Q(X) = \sum_{k=0}^n \frac{a_k}{k+1} X^{k+1}$. Donc

$$Im(f) = E$$

et f est surjective. □

Exercice: Soient E un $\mathbb{R}$-espace vectoriel et $f, g \in End(E)$ deux endomorphismes de E. On suppose que f et g commutent, à savoir que $g \circ f = f \circ g$. Montrer que $Ker(f)$ et $Im(f)$ sont stables par g, à savoir que $g\left(Ker(f)\right) \subset Ker(f)$ et que $g\left(Im(f)\right) \subset Im(f)$.

Solution: Il faut montrer que si $x \in Ker(f)$, alors $g(x) \in Ker(f)$ et que si $x \in Im(f)$ alors $g(x) \in Im(f)$. Soit $x \in Ker(f)$. On a

$$f\left(g(x)\right) = g\left(f(x)\right) = g(0) = 0 \ .$$

Donc on a bien que $g(x) \in Ker(f)$ si $x \in Ker(f)$. De même, si $x \in Im(f)$ alors il existe $x' \in E$ tel que $x = f(x')$. Mais alors

$$g(x) = g\left(f(x')\right) = f\left(g(x')\right) = f(x'')$$

avec $x'' = g(x')$. Donc $g(x) \in Im(f)$ si $x \in Im(f)$. □

Exercice: Soient E un $\mathbb{R}$-espace vectoriel et $f \in End(E)$ un endomorphisme de E. On note $E_1 = Ker(f)$, $E_2 = Ker(f - Id_E)$ et $E_3 = Ker(f + Id_E)$, où Id_E est l'application linéaire identité de E dans E (l'endomorphisme identité de E). Montrer que E_1, E_2 et E_3 sont en somme directe.

Solution: Il faut montrer (cf. cours précédents) que $E_1 \cap E_2 = \{0\}$ et que $(E_1 + E_2) \cap E_3 = \{0\}$. Soit $x \in E_1 \cap E_2$. Alors $f(x) = 0$ et $(f - Id_E)(x) = f(x) - x = 0$ de sorte que $x = 0$. Donc $E_1 \cap E_2 = \{0\}$. Soit maintenant $x \in (E_1 + E_2) \cap E_3$. Comme $x \in E_1 + E_2$ il existe $y \in E_1$ et $z \in E_2$ tels que $x = y + z$. On a alors

$f(y) = 0$, $f(z) - z = 0$ et $f(x) + x = 0$. Comme $f(x) = f(y) + f(z) = f(z)$, on a donc

$$0 = f(z) + x = f(z) - z + y + 2z = y + 2z \ .$$

Soit $y = -2z$. Comme $f(y) = 0$ on devrait aussi avoir $f(z) = 0$ par linéarité de f. Or $f(z) - z = 0$, donc $z = 0$. Puis ensuite, puisque $y = -2z$, on récupère que $y = 0$. Au final, $x = 0$ et donc on bien aussi que $(E_1 + E_2) \cap E_3 = \{0\}$. □

4. Familles libres, génératrices, et bases

Soient E un $\mathbb{R}$-espace vectoriel et $(e_1, \ldots, e_n)$ une famille composée de n vecteurs de E. Par définition, on dit que $(e_1, \ldots, e_n)$ est une famille libre si la seule combinaison linéaire de la famille qui soit nulle est la combinaison linéaire nulle. Donc $(e_1, \ldots, e_n)$ est une famille libre si

$$\forall t_1, \ldots, t_n \in \mathbb{R}, t_1 e_1 + \cdots + t_n e_n = 0 \quad \Rightarrow \quad t_1 = \cdots = t_n = 0 \ .$$

Une famille qui n'est pas libre est dite liée.

Remarque: Une famille qui contient le vecteur nul est forcément liée.

Toujours par définition, on dit que $(e_1, \ldots, e_n)$ est une famille génératrice si tout x de E s'écrit comme combinaison linéaire des $e_1, \ldots, e_n$. Donc $(e_1, \ldots, e_n)$ est une famille génératrice si

$$\forall x \in E, \exists t_1, \ldots, t_n \in \mathbb{R} \text{ tels que } x = t_1 e_1 + \cdots + t_n e_n \ .$$

Pour finir, on dit que $(e_1, \ldots, e_n)$ est une base de E si tout x de E s'écrit de façon unique comme combinaison linéaire des $e_1, \ldots, e_n$. Donc $(e_1, \ldots, e_n)$ est une base de E si

$$\forall x \in E, \exists! t_1 \in \mathbb{R}, \ldots, \exists! t_n \in \mathbb{R} \text{ tels que } x = t_1 e_1 + \cdots + t_n e_n \ .$$

Théorème 4.1. *Une famille est une base si et seulement si elle est à la fois libre et génératrice.*

Démonstration. Supposons que $(e_1, \ldots, e_n)$ est une base de$E$. Il est évident que $(e_1, \ldots, e_n)$ est alors génératrice pour E. Soient maintenant des $t_1, \ldots, t_n \in \mathbb{R}$. Supposons que $t_1 e_1 + \cdots + t_n e_n = 0$. Comme on a aussi que

$$0 = 0 e_1 + \cdots + 0 e_n \ ,$$

l'unicité de la décomposition donne que forcèment $t_1 = 0, t_2 = 0, \ldots, t_n = 0$. Donc $(e_1, \ldots, e_n)$ est aussi une famille libre et base $\Rightarrow$ libre et génératrice. Supposons à l'inverse que $(e_1, \ldots, e_n)$ est à la fois libre et génératrice. Puisque $(e_1, \ldots, e_n)$ est génératrice, $\forall x \in E$, $\exists t_1 \in \mathbb{R}, \ldots, \exists t_n \in \mathbb{R}$ tels que $x = t_1 e_1 + \cdots + t_n e_n$. Reste à montrer l'unicité des $t_1, \ldots, t_n$. Supposons pour cela qu'on ait aussi que $x = \tilde{t}_1 e_1 + \cdots + \tilde{t}_n e_n$. Alors

$$t_1 e_1 + \cdots + t_n e_n = \tilde{t}_1 e_1 + \cdots + \tilde{t}_n e_n \ ,$$

d'où l'on déduit facilement que

$$(\tilde{t}_1 - t_1) e_1 + \cdots + (\tilde{t}_n - t_n) e_n = 0 \ .$$

Comme $(e_1, \ldots, e_n)$ est une famille libre, cela implique que $\tilde{t}_1 - t_1 = 0, \ldots, \tilde{t}_n - t_n = 0$. D'où l'unicité. □

Dire que $(e_1, \dots, e_n)$ est une base de E c'est donc dire que $\forall x \in E$, $\exists! t_1 \in \mathbb{R}, \dots, \exists! t_n \in \mathbb{R}$ tels que $x = t_1 e_1 + \cdots + t_n e_n$. Les t_i sont appelés coordonnées de x dans la base $(e_1, \dots, e_n)$. Dire qu'un vecteur x a pour coordonnées $t_1, \dots, t_n$ dans une base $(e_1, \dots, e_n)$ c'est donc précisément dire que $x = t_1 e_1 + \cdots + t_n e_n$.

Exercice: Soit $\mathbb{R}[X]$ l'espace des polynômes réels. On considère les polynômes P, Q, R de $\mathbb{R}[X]$ donnés par $P(X) = 16X^3 - 7X^2 + 21X - 4$, $Q(X) = 8X^3 - 5X^2 + 1$ et $R(X) = X^2 + 7X - 2$. Montrer que P est une combinaison linéaire de Q et R, à savoir que $P \in Vect(\{Q, R\})$.

Solution: En raison du terme en X^3, si P est une combinaison linéaire de Q et R alors forcément que $P = 2Q + \lambda R$ avec $\lambda \in \mathbb{R}$. La comparaison des termes en X^2 donne que forcément $\lambda = 3$. Donc la combinaison linéaire candidate est

$$P = 2Q + 3R \ .$$

Les deux polynômes P et $2Q + 3R$ sont tous deux de degré 3 et ont les mêmes coeeficients des termes en X^3 et X^2 en raison de ce qui a été dit jusqu'ici. Reste à vérifier qu'ils ont les mêmes coefficients des termes en X et constants. C'est bien le cas car $21 = 2 \times 0 + 3 \times 7$ tandis que $-4 = 2 \times 1 + 3 \times (-2)$. $\square$

Exercice: Soit $\mathbb{R}[X]$ l'espace des polynômes réels et $P_1, \dots, P_n \in \mathbb{R}[X]$ tels que

$$\text{degré} P_1 < \text{degré} P_2 < \cdots < \text{degré} P_n \ .$$

Montrer que $(P_1, \dots, P_n)$ est alors une famille libre de $\mathbb{R}[X]$.

Solution: Supposons que la famille soit liée. Alors il existe des $\lambda_1, \dots, \lambda_n$ non tous nuls tels que $\lambda_1 P_1 + \cdots + \lambda_n P_n = 0$ (le polynôme nul). Le terme de plus haut degré du polynôme $\lambda_1 P_1 + \cdots + \lambda_n P_n$ est donné par $\lambda_n P_n$. Comme il doit être nul c'est que $\lambda_n = 0$. Mais alors $\lambda_1 P_1 + \cdots + \lambda_{n-1} P_{n-1} = 0$ et on recommence le raisonnement. Le terme de plus haut degré du polynôme $\lambda_1 P_1 + \cdots + \lambda_{n-1} P_{n-1}$ est donné par $\lambda_{n-1} P_{n-1}$. Comme il doit être nul c'est que $\lambda_{n-1} = 0$. On recommence encore le raisonnement et ainsi de suite jusqu'à annuler tous les λ_i. La famille $(P_1, \dots, P_n)$ est bien une famille libre de $\mathbb{R}[X]$. $\square$

Remarques: (1) Toute sur famille d'une famille génératrice est génératrice.
(2) Toute sous famille d'une famille libre est libre.

Théorème 4.2 (Théorème fondamental de la théorie de la dimension.)**.** *Soit E un $\mathbb{R}$-espace vectoriel. Si E possède une famille génératrice composée de k vecteurs, $k \in \mathbb{N}$, alors toute famille libre de E a au plus k vecteurs. En d'autres termes, une famille libre a forcément moins d'éléments qu'une famille génératrice.*

Dans la suite on écrira avec un léger abus de notation $Vect(e_1, \dots, e_k)$ au lieu de $Vect(\{e_1, \dots, e_k\})$.

Démonstration. On démontre le théorème par récurrence sur k. Si $k = 1$, le résultat est immédiat. Il existe en effet un vecteur e de E qui est tel que tout vecteur de E s'écrit sous la forme te, $t \in \mathbb{R}$. On en déduit que si x et y sont deux vecteurs de E, alors il existe $t \in \mathbb{R}$ tel que soit $y = tx$, soit $x = ty$. En particulier, soit $y - tx = 0$ soit $x - ty = 0$, et donc, toute famille composée de plus de deux vecteurs est liée. On suppose maintenant le résultat vrai à l'ordre k, et on le démontre à l'ordre $k + 1$. Soit $(e_1, \dots, e_{k+1})$ une famille génératrice, et soit $(x_1, \dots, x_p)$ une famille libre. On veut montrer que nécessairement $p \leq k + 1$. Puisque la famille $(e_1, \dots, e_{k+1})$ est génératrice, les x_i, $i = 1, \dots, p$, s'écrivent comme combinaison linéaire des e_j, $j = 1, \dots, k+1$. Il existe donc des $\lambda_i^j \in \mathbb{R}$ tels que pour tout $i = 1, \dots, p$,

$$x_i = \sum_{j=1}^{k+1} \lambda_i^j e_j$$

Si $\lambda_1^1 = \cdots = \lambda_p^1 = 0$, alors les x_i sont en fait dans l'espace vectoriel $Vect(e_2, \dots, e_{k+1})$. Par définition même de cet espace, la famille $(e_2, \dots, e_{k+1})$ est génératrice pour cet espace. Cette famille comportant k vecteurs, on peut appliquer l'hypothèse de récurrence qui nous donne que nécessairement $p \leq k$. Donc, en particulier, $p \leq k+1$. Supposons maintenant que l'un des λ_i^1 est non nul, $i = 1, \dots, p$. Sans perdre en généralité, on peut supposer que $\lambda_1^1 \neq 0$. Si on pose $\lambda_i = \lambda_i^1/\lambda_1^1$, alors pour tout $i = 2, \dots, p$,

$$x_i - \lambda_i x_1 \in Vect(e_2, \dots, e_{k+1})$$

Par ailleurs, la famille $(x_2 - \lambda_2 x_1, \dots, x_p - \lambda_p x_1)$ est toujours libre. En effet, si

$$t_1(x_2 - \lambda_2 x_1) + \cdots + t_{p-1}(x_p - \lambda_p x_1) = 0$$

alors

$$(-\sum_{i=1}^{p-1} t_i \lambda_{i+1}) x_1 + t_1 x_2 + \cdots + t_{p-1} x_p = 0$$

et puisque la famille $(x_1, \dots, x_p)$ est libre, on doit avoir $t_1 = \cdots = t_{p-1} = 0$. L'espace vectoriel $Vect(e_2, \dots, e_{k+1})$ admet, par définition même, $(e_2, \dots, e_{k+1})$ comme famille génératrice. Cette famille comportant k vecteurs, on peut là encore appliquer l'hypothèse de récurrence. On trouve alors que $p - 1 \leq k$, et donc que $p \leq k+1$. D'où le fait que si la propriété est vraie à l'ordre k, alors elle l'est aussi à l'ordre $k+1$. Par récurrence on a ainsi démontré le théorème. □

Plusieurs propriétés importantes suivent de ce théorème fondamental de la théorie de la dimension. Il en va ainsi de la propriété suivante.

Théorème 4.3. *Si un espace vectoriel E possède une base composée de n vecteurs, $n \in \mathbb{N}$, alors toute autre base de E est elle aussi composée d'exactement n vecteurs.*

Démonstration. Si $(e_1, \dots, e_n)$ et si $(\tilde{e}_1, \dots, \tilde{e}_p)$ sont deux bases de E, on veut montrer que $n = p$. Une base étant à la fois libre et génératrice: (i) $(e_1, \dots, e_n)$ est libre et $(\tilde{e}_1, \dots, \tilde{e}_p)$ est génératrice, et (ii) $(e_1, \dots, e_n)$ est génératrice et $(\tilde{e}_1, \dots, \tilde{e}_p)$ est libre. Du théorème fondamental de la théorie de la dimension et de (i) on tire que $n \leq p$. Du théorème fondamental de la théorie de la dimension et de (ii) on tire que $p \leq n$. Donc $n = p$. □

Cette propriété permet de définir la notion de dimension.

Définition 4.1. *On dit d'un espace vectoriel E qu'il est de dimension finie n s'il possède une base composée de n vecteurs. Toute autre base de E est alors composée elle aussi de n vecteurs. On note parfois $dim(E)$ la dimension de E.*

Par exemple, $\mathbb{R}^2$ est de dimension 2 car $\{(1,0);(0,1)\}$ est une base de $\mathbb{R}^2$. Ou encore $\mathbb{R}^3$ est de dimension 3 car $\{(1,0,0);(0,1,0);(0,0,1)\}$ est une base de $\mathbb{R}^3$. Etc. $\mathbb{R}^n$ est de dimension n.

L'espace $\mathbb{R}_n[X]$ des polynômes de degré au plus n est de dimension $n+1$ car $\left\{1, X, X^2, \dots, X^{n-1}, X^n\right\}$ est une base de $\mathbb{R}_n[X]$. La famille est génératrice par définition des polynômes. Elle est libre car si un polynôme est nul sur $\mathbb{R}$ alors tous ses coefficients sont nuls (un polynôme de degré n a au plus n racines réelles, sauf s'il s'agit du polynôme nul).

On a vu que toute sur famille d'une famille génératrice est encore une famille génératrice et que toute sous famille d'une famille libre est encore une famille libre. Le lemme qui suit va dans "l'autre sens".

Lemme 4.1. *(1) Dans un $\mathbb{R}$-espace vectoriel E, si $(x_1,\dots,x_n)$ est une famille libre mais non génératrice, alors il existe un vecteur $x_{n+1}\in E$ pour lequel la famille $(x_1,\dots,x_n,x_{n+1})$ est encore une famille libre.*

(2)A l'inverse si $(x_1,\dots,x_n)$ est une famille génératrice mais n'est pas libre, alors il existe un $i\in\{1,\dots,n\}$ pour lequel la famille $(x_1,\dots,x_{i-1},x_{i+1},\dots,x_n)$ est encore génératrice.

En d'autres termes, si une famille libre n'est pas génératrice, alors on peut lui rajouter un vecteur convenablement choisi de sorte que la famille ainsi augmentée reste libre. Et si une famille génératrice n'est pas libre, alors on peut lui enlever un vecteur convenablement choisi de sorte que la famille ainsi diminuée reste génératrice.

Démonstration. (1) Supposons que $(x_1,\dots,x_n)$ est une famille libre mais non génératrice. Dire que $(x_1,\dots,x_n)$ n'est pas génératrice c'est dire, par définition, que $\mathrm{Vect}(x_1,\dots,x_n)\neq E$. Donc il existe $x_{n+1}\in E$ tel que $x_{n+1}\notin\mathrm{Vect}(x_1,\dots,x_n)$. Soient $\lambda_1,\dots,\lambda_n,\lambda_{n+1}\in\mathbb{R}$ des réels tels que

$$\lambda_1x_1+\cdots+\lambda_nx_n+\lambda_{n+1}x_{n+1}=0\ .$$

Forcément $\lambda_{n+1}=0$ car sinon,

$$x_{n+1}=\left(-\frac{\lambda_1}{\lambda_{n+1}}\right)x_1+\cdots+\left(-\frac{\lambda_n}{\lambda_{n+1}}\right)x_n\ ,$$

et donc on aurait que $x_{n+1}\in\mathrm{Vect}(x_1,\dots,x_n)$, ce qui est faux par construction. Comme $\lambda_{n+1}=0$ alors

$$\lambda_1x_1+\cdots+\lambda_nx_n=0\ ,$$

et comme $(x_1,\dots,x_n)$ est libre, on en déduit qu'on a aussi $\lambda_1=\cdots=\lambda_n=0$. La famille $(x_1,\dots,x_n,x_{n+1})$ est donc aussi une famille libre.

(2) Supposons que $(x_1,\dots,x_n)$ est une famille génératrice mais non libre. Dire que $(x_1,\dots,x_n)$ n'est pas libre c'est dire, par définition, qu'il existe $\lambda_1,\dots,\lambda_n\in\mathbb{R}$, non tous nuls, tels que

$$\lambda_1x_1+\cdots+\lambda_nx_n=0\ .$$

Supposons par exemple que ce soit λ_n qui est non nul. Alors

$$x_n=\left(-\frac{\lambda_1}{\lambda_n}\right)x_1+\cdots+\left(-\frac{\lambda_{n-1}}{\lambda_n}\right)x_{n-1}\ ,$$

et donc $x_n\in\mathrm{Vect}(x_1,\dots,x_{n-1})$. Par suite:

$$\mathrm{Vect}(x_1,\dots,x_n)=\mathrm{Vect}(x_1,\dots,x_{n-1})\ .$$

Dire que $(x_1,\dots,x_n)$ est génératrice c'est dire que l'on a que $\mathrm{Vect}(x_1,\dots,x_n)=E$. Donc, d'après l'équation ci-dessus, $\mathrm{Vect}(x_1,\dots,x_{n-1})=E$ et $(x_1,\dots,x_{n-1})$ est aussi génératrice. $\square$

Théorème 4.4. *Soit E un $\mathbb{R}$-espace vectoriel E de dimension n. Toute famille libre de E composée de n vecteurs est une base de E. Toute famille génératrice de E composée de n vecteurs est une base de E.*

En d'autre termes, en dimension n, pour montrer qu'une famille composée de n vecteurs est une base de E il suffit de montrer soit qu'elle est libre, soit qu'elle est génératrice (et si elle n'est pas composée d'exactement n vecteurs elle n'a aucune chance d'être une base puisque les bases ont toujours autant de vecteurs que la dimension).

Démonstration. Soit $n = \dim(E)$ et soit $(e_1, \ldots, e_n)$ une base de E. Supposons que $(x_1, \ldots, x_n)$ est une famille libre de E. Si elle n'était pas génératrice on pourrait fabriquer, en vertu du lemme précédent, une famille libre $(x_1, \ldots, x_n, x_{n+1})$ de E ayant $n+1$-vecteurs. Or, d'après le théorème fondamental de la théorie de la dimension, sachant que $(e_1, \ldots, e_n)$ est en particulier génératrice, on devrait avoir que $(x_1, \ldots, x_{n+1})$ a moins de vecteurs que $(e_1, \ldots, e_n)$, ce qui est faux. Donc $(x_1, \ldots, x_n)$ est à la fois libre et génératrice, donc une base. Si on suppose au départ que $(x_1, \ldots, x_n)$ est génératrice, on montre avec le même genre de raisonnement qu'elle est obligatoirement aussi une famille libre. $\square$

Exercice: Soit $E = \mathbb{R}_n[X]$ l'espace vectoriel des polynômes réels de degrés inférieurs ou égaux à n. Pour $k \in \{0, 1, \ldots, n\}$ on note P_k le polynôme de E donné par $P_0(X) = 1$ et $P_k(X) = X^k + Q_k[X]$ pour $k \geq 1$ où les Q_k sont des polynômes réels quelconques donnés de degrés degré$Q_k \leq k - 1$. Montrer que la famille $(P_0, P_1, \ldots, P_n)$ est une base de E.

Solution: On a $\dim(E) = n + 1$ et $\mathrm{Card}\{P_0, P_1, \ldots, P_n\} = n + 1$. Il suffit donc de montrer que $(P_0, P_1, \ldots, P_n)$ est une famille libre de E. Or degré$P_k = k$ et donc

$$\text{degré} P_0 < \text{degré} P_1 < \cdots < \text{degré} P_n \ .$$

On l'a déjà vu, une telle relation entraîne que la famille $(P_0, P_1, \ldots, P_n)$ est libre. D'où le résultat. $\square$

Théorème 4.5 (Théorème de la base incomplète)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n. Si $(x_1, \ldots, x_k)$ est une famille libre de E, donc $k \leq n$, elle peut être complétée par $n - k$ vecteurs de E pour en faire une base de E. En d'autres termes, toute famille libre dans un espace vectoriel de dimension finie peut être complétée en une base de l'espace par adjonction de vecteurs convenables.*

Démonstration. Il suffit de raisonner par induction à partir des résultats précédents. Si $k < n$ alors $(x_1, \ldots, x_k)$ ne peut être génératrice d'après le théorème fondamental de la théorie de la dimension. Le lemme précédent donne l'existence de $x_{k+1} \in E$ tel que $(x_1, \ldots, x_k, x_{k+1})$ est encore libre. Si $k + 1 = n$ le théorème précédent permet d'affirmer que $(x_1, \ldots, x_k, x_{k+1})$ est une base de E. Le théorème de la base incomplète est alors démontré. Sinon $k + 1 < n$ et $(x_1, \ldots, x_k, x_{k+1})$ ne peut de nouveau pas être génératrice d'après le théorème fondamental de la théorie de la dimension. On applique alors le lemme précédent qui donne l'existence de $x_{k+2} \in E$ tel que $(x_1, \ldots, x_{k+1}, x_{k+2})$ est encore libre. Si $k + 2 = n$, la preuve s'arrète. Sinon $k + 2 < n$ et on continue à ajouter des vecteurs jusqu'à atteindre n vecteurs et donc obtenir une base de E. $\square$

5. Sous espaces vectoriels et dimension

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie. Soit F un sous espace vectoriel de E. Alors F est aussi de dimension finie et $\dim(F) \leq \dim(E)$ avec égalité si et seulement si $F = E$. Le résultat s'obtient facilement en remarquant que toute famille libre de F est aussi une famille libre de E. Les familles libres de F ont donc au plus $\dim(E)$ vecteurs, ce qui prouve (penser au lemme précédent) que F est de dimension finie et que $\dim(F) \leq \dim(E)$. On remarque alors facilement que $\dim(F) = \dim(E)$ si et seulement si $F = E$ (base de $F \Rightarrow$ famille libre de $F \Rightarrow$ famille libre de E ayant autant de vecteurs que la dimension de $E \Rightarrow$ base de E).

Une autre affirmation simple à vérifier est que si E et F sont deux espaces vectoriels de dimensions finies, alors $E \times F$ possède une structure naturelle d'espace vectoriel de dimension finie $\dim(E \times F) = \dim(E) + \dim(F)$. La structure d'espace vectoriel est donnée par les opérations

$$(u,v) + (u',v') = (u+u', v+v') \text{ et } t \times (u,v) = (tu, tv) \ ,$$

et on remarque que si $(u_1, \ldots, u_p)$ est une base de E et $(v_1, \ldots, v_q)$ est une base de F, alors la famille composée des vecteurs $(u_1, 0), \ldots, (u_p, 0), (0, v_1), \ldots, (0, v_q)$ est une base de $E \times F$.

Théorème 5.1. *Soit E un $\mathbb{R}$-espace vectoriel et soient F_1, F_2 deux sous espaces vectoriels de E de dimensions finies. Alors $F_1 + F_2$ est encore de dimension finie, et*

$$dim(F_1 + F_2) = dim(F_1) + dim(F_2) - dim(F_1 \cap F_2) \ .$$

En particulier, F_1 et F_2 sont en somme directe, à savoir on a $F_1 \oplus F_2$, si et seulement si $dim(F_1 + F_2) = dim(F_1) + dim(F_2)$.

Démonstration. L'intersection $F_1 \cap F_2$ est un sous espace vectoriel de E de dimension finie (puisque sous espace aussi de F_1 et F_2). Soit $(x_1, \ldots, x_k)$ une base de $F_1 \cap F_2$. Du théorème de la base incomplète pour l'inclusion $F_1 \cap F_2 \subset F_1$ on tire l'existence de vecteurs $x_{k+1}, \ldots, x_m$ dans F_1 tels que $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_m)$ est une base de F_1, et du théorème de la base incomplète pour l'inclusion $F_1 \cap F_2 \subset F_2$, on tire l'existence de vecteurs $\tilde{x}_{k+1}, \ldots, \tilde{x}_n$ dans F_2 tels que $(x_1, \ldots, x_k, \tilde{x}_{k+1}, \ldots, \tilde{x}_n)$ est une base de F_2. On affirme alors que la famille

$$(x_1, \ldots, x_k, x_{k+1}, \ldots, x_m, \tilde{x}_{k+1}, \ldots, \tilde{x}_n)$$

est une base de $F_1 + F_2$. Une telle proposition suffit à démontrer le théorème puisque, dans ce cas,

$$dim(F_1 + F_2) = m + n - k \ .$$

Pour montrer que $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_m, \tilde{x}_{k+1}, \ldots, \tilde{x}_n)$ est une base de $F_1 + F_2$ on montre que la famille est à la fois libre et est génératrice pour $F_1 + F_2$. Le fait que la famille soit génératrice pour $F_1 + F_2$ est une évidence puisqu'elle contient les bases de F_1 et de F_2. Reste donc à montrer que cette famille est libre. Supposons que

$$\sum_{i=1}^m t_i x_i + \sum_{j=k+1}^n \tilde{t}_j \tilde{x}_j = 0 \ .$$

Alors

$$\sum_{i=1}^m t_i x_i = - \sum_{j=k+1}^n \tilde{t}_j \tilde{x}_j \in F_1 \cap F_2 \ .$$

On en déduit que $\tilde{t}_j = 0$ pour $j = k+1, \ldots, n$ car si $\sum_{j=k+1}^{n} \tilde{t}_j \tilde{x}_j \in F_1 \cap F_2$, et comme $(x_1, \ldots, x_k)$ est une base de $F_1 \cap F_2$, on obtient qu'il existe $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ tels que

$$\sum_{j=k+1}^{n} \tilde{t}_j \tilde{x}_j = \sum_{i=1}^{k} \lambda_i x_i \ .$$

Et comme $(x_1, \ldots, x_k, \tilde{x}_{k+1}, \ldots, \tilde{x}_n)$ est libre, c'est que $\lambda_1 = \cdots = \lambda_k = \tilde{t}_{k+1} = \cdots = \tilde{t}_n = 0$. Maintenant, si les $\tilde{t}_j = 0$ pour $j = k+1, \ldots, n$, alors $\sum_{i=1}^{m} t_i x_i = 0$. Mais comme $(x_1, \ldots, x_m)$ est aussi une famille libre, c'est que $t_i = 0$ pour tout $i = 1, \ldots, m$. En particulier, on a montré que la seule combinaison linéaire de la famille

$$(x_1, \ldots, x_k, x_{k+1}, \ldots, x_m, \tilde{x}_{k+1}, \ldots, \tilde{x}_n)$$

qui soit nulle, est la combinaison linéaire nulle. La famille

$$(x_1, \ldots, x_k, x_{k+1}, \ldots, x_m, \tilde{x}_{k+1}, \ldots, \tilde{x}_n)$$

est ainsi libre. Elle est donc à la fois génératrice pour $F_1 + F_2$ et libre, ce qui prouve qu'il s'agit bien d'une base de $F_1 + F_2$. $\square$

Exercice: Soient F_1, F_2 deux hyperplans d'un $\mathbb{R}$-espace vectoriel E de dimension n (un hyperplan d'un espace vectoriel de dimension n est un sous espace vectoriel de dimension $n-1$, soit un de moins, cf. Section 8). Montrer que $F_1 \cap F_2 \neq \{0\}$ dès que $n \geq 3$. Que se passe-t-il lorsque $n = 2$?

Solution: Supposons $n \geq 3$. On a

$$\dim(F_1 + F_2) = \dim(F_1) + \dim(F_2) - \dim(F_1 \cap F_2) \ .$$

On raisonne par contradiction et on suppose que $F_1 \cap F_2 = \{0\}$. Alors $\dim(F_1 \cap F_2) = 0$. On aurait donc

$$\dim(F_1 + F_2) = n - 1 + n - 1 = 2(n-1) \ .$$

Comme $F_1 + F_2 \subset E$ on a $\dim(F_1 + F_2) \leq n$. Or $n < 2(n-1)$ dès que $n \geq 3$. D'où une contradiction et le résultat pour $n \geq 3$. Lorsque $n = 2$ le résultat cesse d'être vrai. Par exemple dans $\mathbb{R}^2$ l'axe des x et l'axe des y sont deux hyperplans d'intersection réduite au vecteur nul. $\square$

6. Dimension finie et applications linéaires

On rappelle qu'un isomorphisme d'un espace vectoriel E sur un espace vectoriel F est une application linéaire bijective de E sur F.

Théorème 6.1. *Soient E, F deux $\mathbb{R}$-espaces vectoriels et $f \in L(E,F)$ une application linéaire de E dans F. Si f est injective et si $(x_1, \ldots, x_n)$ est une famille libre de E, alors $(f(x_1), \ldots, f(x_n))$ est une famille libre de F. Si f est surjective et si $(x_1, \ldots, x_n)$ est génératrice pour E, alors $(f(x_1), \ldots, f(x_n))$ est génératrice pour F. En particulier, si f est un isomorphisme et si $(x_1, \ldots, x_n)$ est une base de E, alors $(f(x_1), \ldots, f(x_n))$ est une base de F.*

En d'autres termes, une application linéaire injective envoie les familles libres sur des familles libres, une application linéaire surjective envoie les familles génératrices sur des familles génératrices et un isomorphisme envoie les bases sur des bases.

Démonstration. (1) Supposons que f est injective et que $(x_1, \ldots, x_n)$ est libre. Soient $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ tels que

$$\lambda_1 f(x_1) + \cdots + \lambda_n f(x_n) = 0 \ .$$

Alors $f(\sum_{i=1}^n \lambda_i x_i) = 0$ et donc $\lambda_1 x_1 + \cdots + \lambda_n x_n \in \mathrm{Ker}(f)$. Comme f est injective $Ker(f) = \{0\}$ et il s'ensuit que $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$, et comme $(x_1, \ldots, x_n)$ est libre on en déduit que $\lambda 1 = \cdots = \lambda_n = 0$. Par suite $(f(x_1), \ldots, f(x_n))$ est une famille libre de F.

(2) Supposons que f est surjective et que $(x_1, \ldots, x_n)$ est une famille génératrice de E. Comme f est surjective, tout $y \in F$ s'écrit $y = f(x)$ pour un certain $x \in E$. Comme $(x_1, \ldots, x_n)$ est génératrice pour E, il existe $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ tels que $x = \lambda_1 x_1 + \cdots + \lambda_n x_n$. Par suite

$$y = \lambda_1 f(x_1) + \cdots + \lambda_n f(x_n) \ .$$

On en déduit que $(f(x_1), \ldots, f(x_n))$ est génératrice pour F.

(3) Qu'un isomorphisme envoie les bases sur des bases est une conséquence de (1) et (2). □

Corollaire 6.1. *Si deux espaces vectoriels sont isomorphes, et l'un de ces espaces est de dimension finie, alors l'autre l'est aussi et les deux espaces ont même dimension.*

Démonstration. Supposons qu'il existe $f \in L(E, F)$ un isomorphisme de E sur F, et supposons que E est de dimension finie. Soit $(e_1, \ldots, e_n)$ une base de E. Comme f est un isomorphisme, donc injective et surjective, $(f(e_1), \ldots, f(e_n))$ est une famille libre et génératrice pour F. Donc une base de F. Donc F est aussi de dimension finie et $\dim(F) = \dim(E)$. □

Définition 6.1. *On appelle rang d'une application linéaire f, et on note $Rg(f)$, la dimension de l'espace $Im(f)$.*

Le théorème suivant est un des théorèmes importants de l'algèbre linéaire.

Théorème 6.2 (Théorème du rang)**.** *Soient E et F deux espaces vectoriels de dimensions finies, et soit $f \in L(E, F)$ une application linéaire de E dans F. Alors*

$$dim Ker(f) + Rg(f) = dim(E)$$

où $Ker(f)$ est le noyau de f, et $Rg(f) = dim(Im(f))$ son rang.

Un moyen mnémotechnique pour se souvenir qu'il s'agit bien de $\dim E$ à droite de l'équation, et non de $\dim(F)$, est qu'on peut toujours augmenter F (une application linéaire de E dans F est aussi une application linéaire de E dans F' si F' est un espace vectoriel qui contient F) alors qu'on ne peut pas a priori augmenter E.

Démonstration. Soit $(e_1, \ldots, e_k)$ une base de $Ker(f)$. On complète cette base par des vecteurs $(e_{k+1}, \ldots, e_n)$ pour obtenir une base $(e_1, \ldots, e_n)$ de E. Une telle opération est toujours possible en vertue du théorème de la base incomplète. On prétend maintenant que la famille $\big(f(e_{k+1}), \ldots, f(e_n)\big)$ est une base de $Im(f)$. Tout d'abord, on constate facilement que cette famille est génératrice pour $Im(f)$. En effet, pour tout $y \in Im(f)$, il existe $x \in E$ tel que $f(x) = y$ (par définition même de $Im(f)$). Puisque $(e_1, \ldots, e_n)$ est une base de E, il existe des t_i tels que

$$x = t_1 e_1 + \cdots + t_n e_n \ .$$

Mais alors
$$y = f(x) = t_{k+1}f(e_{k+1}) + \cdots + t_n f(e_n)$$
puisque $f(e_i) = 0$ si $i = 1, \ldots, k$. Or y est quelconque, et donc $\big(f(e_{k+1}), \ldots, f(e_n)\big)$ est une famille génératrice de $Im(f)$. On affirme par ailleurs que cette famille est libre. En effet, si
$$t_{k+1}f(e_{k+1}) + \cdots + t_n f(e_n) = 0$$
alors
$$f(t_{k+1}e_{k+1} + \cdots + t_n e_n) = 0$$
et donc $t_{k+1}e_{k+1}+\cdots+t_n e_n \in Ker(f)$. Comme $(e_1, \ldots, e_k)$ est une base de $Ker(f)$, il devrait ainsi exister des $t_1, \ldots, t_k$ tels que
$$t_{k+1}e_{k+1} + \cdots + t_n e_n = t_1 e_1 + \cdots + t_k e_k$$
soit encore tels que
$$(-t_1)e_1 + \cdots + (-t_k)e_k + t_{k+1}e_{k+1} + \cdots + t_n e_n = 0\ .$$
Une telle relation, puisque $(e_1, \ldots, e_n)$ est libre, impose $t_1 = \cdots = t_n = 0$. La famille $\big(f(e_{k+1}), \ldots, f(e_n)\big)$ est donc bien libre. On déduit de tout cela que $\big(f(e_{k+1}), \ldots, f(e_n)\big)$ est une base de $Im(F)$. Il s'ensuit que $dimIm(f) = n - k$, et on a donc bien que $dimKer(f) + Rg(f) = dimE$ (i.e. que $n = k + (n - k)$). Le théorème est démontré. □

Proposition 6.1. *On a toujours $Rg(f) \leq \min(dim(E), dim(F))$. Par ailleurs f est surjective si et seulement si $Rg(f) = dim(F)$. Enfin f est injective si et seulement si $Rg(f) = dim(E)$.*

Démonstration. Les deux premières affirmations sont évidentes. La trosième suit du théorème du rang sachant que $\mathrm{Rg}(f) = \dim(E) \Leftrightarrow \dim(\mathrm{Ker}(f)) = 0 \Leftrightarrow \mathrm{Ker}(f) = \{0\} \Leftrightarrow f$est injective. □

Corollaire 6.2. *Soit E un $\mathbb{R}$- espace vectoriel de dimension finie et $f \in End(E)$. Alors f est un isomorphisme de E sur E si et seulement si f est injective. De même, f est un isomorphisme de E sur E si et seulement si f est surjective.*

Démonstration. Lorsque $E = F$, $\mathrm{Rg}(f) = \dim(F) \Leftrightarrow \dim(\mathrm{Ker}(f)) = 0$ et donc f injective $\Leftrightarrow f$ surjective $\Leftrightarrow f$ isomorphisme. □

Exercice: Soient $n \in \mathbb{N}^\star$ et $E = \mathbb{R}_n[X]$ l'espace des polynômes réels de degrés inférieurs ou égaux à n. On considère l'endomorphisme f de E donné pour tout $P \in \mathbb{R}_n[X]$ par $f(P)(X) = P(X+1) - P(X)$. Déterminer $Ker(f)$ et $Im(f)$.

Solution: Pour tout $P \in E$, $P(X+1) - P(X)$ est encore un polynôme et son degré est inférieur ou égale à degré$P - 1$. On a donc bien que $f : E \to E$ et on vérifie facilement par ailleurs que f est linéaire. Supposons maintenant que $P \in Ker(f)$. Alors $P(x+1) = P(x)$ pour tout $x \in \mathbb{R}$. Fixons un $x_0 \in \mathbb{R}$ quelconque. Alors
$$Q(X) = P(X) - P(x_0)$$
est un polynôme qui a pour zéros: x_0, x_0+1, x_0+2, x_0+3 etc. puisque $P(x_0+1) = P(x_0)$, $P(x_0+2) = P(x_0+1) = P(x_0)$ etc. Donc Q serait un polynôme de degré inférieur ou égale à n qui aurait une infinité de zéros. C'est impossible sauf si

$Q = 0$ est le polynôme nul. Mais alors P est un polynôme constant. A l'inverse, tout polynôme constant vérifie bien que $P(X+1) = P(X)$. Donc

$$Ker(f) = \{P \in E \ / \ P \text{ est constant}\} \ .$$

On cherche maintenant à déterminer $Im(f)$. On l'a déjà dit, on a forcément $Im(f) \subset \mathbb{R}_{n-1}[X]$. En vertue du théorème du rang,

$$\dim Ker(f) + \dim Im(f) = \dim(E)$$

Comme $\dim Ker(f) = 1$, c'est que $\dim Im(f) = \dim(E) - 1$. Or $\dim \mathbb{R}_{n-1}[X] = \dim(E) - 1$. Donc

$$Im(f) = \mathbb{R}_{n-1}[X] \ .$$

□

Exercice: Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n. Montrer qu'il existe un endomorphisme $f \in End(E)$ vérifiant $Ker(f) = Im(f)$ si et seulement si n est pair.

Solution: Si f existe alors avec le théorème du rang

$$n = \dim E = \dim Ker(f) + \dim Im(f) = 2\dim Ker(f)$$

et donc n est pair. Réciproquement si $n = 2k$, on considère $(e_1, \ldots, e_{2k})$ une base de E et l'endomorphisme $f \in End(E)$ défini par $f(e_i) = e_{k+i}$ pour tout $1 \leq i \leq k$ et $f(e_i) = 0$ pour tout $i = k+1, \ldots 2k$. Alors $Ker(f) = Im(f) = Vect(e_{k+1}, \ldots, e_{2k})$.
□

7. Projecteurs

Soient E un $\mathbb{R}$-espace vectoriel et E_1, E_2 deux sous espaces vectoriels de E. On dit que E_1 et E_2 sont supplémentaires dans E si

$$E = E_1 \oplus E_2 \ .$$

On appelle alors projection (ou projecteur) sur E_1 parallèlement à E_2 l'endomorphisme $p \in End(E)$ de E donné par

$$p : \begin{cases} E = E_1 \oplus E_2 \to E \\ x = x_1 + x_2 \to x_1 \end{cases}$$

On vérifie facilement que si p est une projection alors forcément $p \circ p = p$. En fait la condition est aussi suffisante.

Théorème 7.1. *Soient E un $\mathbb{R}$-espace vectoriel et $p \in End(E)$ un endomorphisme de E. Alors p est une projection si et seulement si $p \circ p = p$. Les sous espaces $Ker(p)$ et $Im(p)$ sont alors supplémentaires et p est la projection sur $Im(p)$ parallèlement à $Ker(p)$.*

Démonstration. On a déjà dit que si p est une projection alors $p \circ p = p$. Reste donc à montrer que si $p \circ p = p$ alors $Ker(p)$ et $Im(p)$ sont supplémentaires et p est la projection sur $Im(p)$ parallèlement à $Ker(p)$. Pour tout $x \in E$ on a que

$$x = (x - p(x)) + p(x)$$

et $x - p(x) \in Ker(p)$ puisque $p \circ p = p$ tandis que $p(x) \in Im(p)$. Donc $E = Ker(p) + Im(p)$. Pour montrer que la somme est directe il suffit de montrer que $Ker(p) \cap Im(p) = \{0\}$. Si $x \in Ker(p) \cap Im(p)$ alors $p(x) = 0$ et $x = p(y)$ pour un certain $y \in E$. Comme $p \circ p = p$, $0 = p(x) = (p \circ p)(y) = p(y) = x$ et donc $Ker(p) \cap Im(p) = \{0\}$. Donc

$$E = Ker(f) \oplus Im(f)$$

avec la décomposition $x = (x - p(x)) + p(x)$. Clairement $p : x \to p(x)$ est alors la projection sur $Im(p)$ parallèlement à $Ker(p)$. $\square$

Exercice: Soient E un $\mathbb{R}$-espace vectoriel et p_1, p_2 deux projections non nulles et distinctes. Montrer que (p_1, p_2) est une famille libre de $End(E)$.

Solution: Si (p_1, p_2) n'est pas libre alors il existe $\lambda \in \mathbb{R}$ tel que $p_2 = \lambda p_1$ ou $p_1 = \lambda p_2$. Quitte à intervertir p_1 et p_2 on peut supposer $p_2 = \lambda p_1$. Mais alors $p_2 \circ p_2 = \lambda^2 p_1 \circ p_1$ et donc $p_2 = \lambda^2 p_1$ puisque $p_1 \circ p_1 = p_1$ et $p_2 \circ p_2 = p_2$. Par suite $\lambda^2 p_1 = \lambda p_1$. Comme p_1 est non nulle, il existe $x \in E$ tel que $p_1(x) \neq 0$. Mais alors $\lambda^2 p_1(x) = \lambda p_1(x)$, puis $\lambda^2 = \lambda$ et enfin $\lambda = 1$ (puisque p_2 est non nulle elle aussi on a $\lambda \neq 0$). Donc $p_2 = p_1$. Or p_1 et p_2 sont distinctes. Une contradiction. Donc, forcément, (p_1, p_2) est libre. $\square$

Exercice: Soient E un $\mathbb{R}$-espace vectoriel, $u \in End(E)$ et $p \in End(E)$ une projection. Montrer que u et p commutent si et seulement si $Ker(p)$ et $Im(p)$ sont stables par u, i.e si et seulement si $u\,(Ker(p)) \subset Ker(p)$ et $u\,(Im(p)) \subset Im(p)$.

Solution: Supposons que u et p commutent, donc que $u \circ p = p \circ u$. Soit $x \in Ker(p)$. Alors

$$p\,(u(x)) = u\,(p(x)) = u(0) = 0$$

et donc $u(x) \in Ker(p)$ pour tout $x \in Ker(p)$. En d'autres termes, $Ker(p)$ est stable par u. De même, soit $y \in Im(p)$. Alors il existe $x \in E$ tel que $y = p(x)$. Mais alors

$$u(y) = u\,(p(x)) = p\,(u(x)) = p(z)$$

avec $z = u(x)$ dans E. Donc $u(y) \in Im(p)$. En d'autres termes, $Im(p)$ est lui aussi stable par u. Réciproquement, supposons que $Ker(p)$ et $Im(p)$ sont stables par u. Comme p est une projection on a $E = Ker(p) \oplus Im(p)$ (cf. le théorème précédent) et p est la projection sur $Im(p)$ parallèlement à $Ker(p)$. Soit $x \in E$ quelconque. Il existe $y \in Ker(p)$ et $z \in Im(p)$ tels que $x = y + z$. Comme $p(y) = 0$ et $p(z) = z$ on a

$$u\,(p(x)) = u\,(p(y)) + u\,(p(z)) = u(0) + u(z) = u(z)\ .$$

Par ailleurs,

$$p\,(u(x)) = p\,(u(y)) + p\,(u(z)) = 0 + u(z) = u(z)$$

puisque p est la projection sur $Im(p)$ parallèlement à $Ker(p)$ et puisque par hypothèse de stabilité, $u(y) \in Ker(p)$ et $u(z) \in Im(p)$. Donc, au final, $u\,(p(x)) = p\,(u(x))$ pour tout $x \in E$ et ainsi p et u commutent. $\square$

Les projections ne se comportent pas très bien par combinaison linéaire. Par exemple, si p est une projection non nulle alors $-p$ ne l'est plus car $(-p) \circ (-p) = p \neq -p$. De même, le résultat suivant a lieu.

Théorème 7.2. *Soient E un $\mathbb{R}$-espace vectoriel et p, q deux projections de E. Alors $p + q$ est encore une projection de E si et seulement si $p \circ q = q \circ p = 0$.*

Démonstration. Supposons par l'absurde que $p+q$ est encore un projecteur. Alors, puisque $p^2 = p$ et $q^2 = q$,

$$\begin{aligned}(p+q)^2 &= p+q \\ &= (p+q)\circ(p+q) \\ &= p^2 + q^2 + p\circ q + q\circ p \\ &= p + q + p\circ q + q\circ p\end{aligned}$$

et donc

$$p\circ q + q\circ p = 0\ . \tag{7.1}$$

Mais alors, comme $p^2 = p$,

$$0 = p\circ(p\circ q + q\circ p) = p\circ q + p\circ q\circ p$$

et

$$0 = (p\circ q + q\circ p)\circ p = p\circ q\circ p + q\circ p$$

et donc

$$p\circ q = q\circ p\ . \tag{7.2}$$

De (7.1) et (7.2) on tire que $p\circ q = q\circ p = 0$. Réciproquement, si $p\circ q = q\circ p = 0$, il suit clairement du développement de $(p+q)^2$ que $(p+q)^2 = p+q$. $\square$

On termine cette section avec le lemme des noyaux. Soit $P \in \mathbb{R}[X]$ un polynôme réel. On écrit $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Soient E un $\mathbb{R}$-espace vectoriel et $\varphi \in \mathrm{End}(E)$ un endomorphisme de E. Alors $P(\varphi)$ est l'endomorphisme de E donné par

$$P(\varphi) = a_n\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_1\varphi + a_0\mathrm{Id}_E\ ,$$

où $\varphi^k = \varphi\circ\cdots\circ\varphi$ (k fois) et Id_E est l'endomorphisme identité de E. Indépendamment, dire que deux polynôme réels non identiquement nuls $P_1, P_2 \in \mathbb{R}[X]$ sont premiers entre eux signifie qu'ils n'ont aucun facteur commun dans leur décomposition en éléments simples (voir le cours d'intégration). Il y a alors un théorème de Bezout pour les polynômes premiers entre eux, comme pour les entiers premiers entre eux, et deux polynôme réels non identiquement nuls $P_1, P_2 \in \mathbb{R}[X]$ sont premiers entre eux si et seulement si il existe des polynômes réels $Q_1, Q_2 \in \mathbb{R}[X]$ tels que $P_1Q_1 + P_2Q_2 = 1$ (en tout point de $\mathbb{R}$).

Théorème 7.3 (Lemme des Noyaux)**.** *Soit E un $\mathbb{R}$-espace vectoriel et soit aussi $\varphi \in End(E)$ un endomorphisme de E. Soient de plus $P_1, P_2 \in \mathbb{R}[X]$ deux polynômes réels non identiquement nuls et premiers entre eux. Alors*

$$Ker\big(P_1P_2(\varphi)\big) = Ker\big(P_1(\varphi)\big) \oplus Ker\big(P_2(\varphi)\big) \tag{7.3}$$

avec $Ker\big(P_1(\varphi)\big) = Im\big(P_2(\varphi)\big)$ et $Ker\big(P_2(\varphi)\big) = Im\big(P_1(\varphi)\big)$. De plus, les restrictions à $Ker\big(P_1P_2(\varphi)\big)$ des projections sur un noyau parallélement à l'autre, projections dont l'existence découlent de (7.3)*, sont des polynômes en φ.*

Démonstration. On vérifie sans difficulté que

$$P_1P_2(\varphi) = P_1(\varphi)\circ P_2(\varphi) = P_2(\varphi)\circ P_1(\varphi)\ .$$

En particulier, $\mathrm{Ker}\big(P_1(\varphi)\big)$ et $\mathrm{Ker}\big(P_2(\varphi)\big)$ sont des sous espaces vectoriels du noyau $\mathrm{Ker}\big(P_1P_2(\varphi)\big)$. Sans perdre en généralité on peut se restreindre à $\mathrm{Ker}\big(P_1P_2(\varphi)\big)$

et donc travailler avec $E = \mathrm{Ker}\big(P_1P_2(\varphi)\big)$. Comme P_1, P_2 sont supposés premiers entre eux, il existe $Q_1, Q_2 \in \mathbb{R}[X]$ tels que $P_1Q_1 + P_2Q_2 = 1$. Par suite,

$$P_1Q_1(\varphi) + P_2Q_2(\varphi) = \mathrm{Id}_E \ . \tag{7.4}$$

On note $p = P_1Q_1(\varphi)$ et $q = P_2Q_2(\varphi)$. Comme $P_1P_2(\varphi) = 0$, puisque maintenant $E = \mathrm{Ker}\big(P_1P_2(\varphi)\big)$, on a que $Q_1Q_2P_1P_2(\varphi) = 0$, soit donc que $p \circ q = q \circ p = 0$. Avec (7.4), on calcule alors que

$$p^2 = p \circ (\mathrm{Id}_E - q) = p \text{ et } q^2 = q \circ (\mathrm{Id}_E - p) = q \ .$$

Donc, p et q sont des projecteurs. Comme (7.4) avec (7.4), on a aussi que $\mathrm{Ker}(p) = \mathrm{Im}(q)$ et $\mathrm{Ker}(q) = \mathrm{Im}(p)$. Les inclusions $\mathrm{Ker}(p) \subset \mathrm{Im}(q)$ et $\mathrm{Ker}(q) \subset \mathrm{Im}(p)$ s'obtiennent immédiatement à partir de la relation $p + q = \mathrm{Id}_E$. Par ailleurs, comme $p \circ q = q \circ p = 0$ on a aussi que $\mathrm{Im}(q) \subset \mathrm{Ker}(p)$ et $\mathrm{Im}(p) \subset \mathrm{Ker}(q)$. D'où les égalités. Toujours puisque $p + q = \mathrm{Id}_E$, et comme $\mathrm{Ker}(p) \cap \mathrm{Im}(p) = \{0\}$ (puisque $p^2 = p$), on peut alors écrire que

$$\mathrm{Im}(p) \oplus \mathrm{Im}(q) = E \ .$$

On remarque maintenant que $\mathrm{Ker}\big(P_1(\varphi)\big) = \mathrm{Im}(q)$ et que $\mathrm{Ker}\big(P_2(\varphi)\big) = \mathrm{Im}(p)$. Par exemple, si $x \in \mathrm{Im}(q)$, alors $x = q(y)$ pour un certain y, mais alors $\big(P_1(\varphi)\big)(x) = Q_2P_1P_2(y) = 0$ car $E = \mathrm{Ker}\big(P_1P_2(\varphi)\big)$. Donc $\mathrm{Im}(q) \subset \mathrm{Ker}\big(P_1(\varphi)\big)$. Pour l'inclusion inverse, si $x \in \mathrm{Ker}\big(P_1(\varphi)\big)$ alors $x \in \mathrm{Ker}(p) = \mathrm{Im}(q)$, d'où l'égalité $\mathrm{Ker}\big(P_1(\varphi)\big) = \mathrm{Im}(q)$. Par symétrie, $\mathrm{Ker}\big(P_2(\varphi)\big) = \mathrm{Im}(p)$. Reste pour définitivement conclure à remarquer que $\mathrm{Im}\big(P_1(\varphi)\big) = \mathrm{Im}(p)$ et $\mathrm{Im}\big(P_2(\varphi)\big) = \mathrm{Im}(q)$. Toujours par symétrie il suffit de démontrer que $\mathrm{Im}\big(P_1(\varphi)\big) = \mathrm{Im}(p)$. Comme $\mathrm{Im}(p) = \mathrm{Ker}\big(P_2(\varphi)\big)$, et comme $P_1P_2(\varphi) = 0$, on a que $\mathrm{Im}\big(P_1(\varphi)\big) \subset \mathrm{Im}(p)$. L'inclusion inverse $\mathrm{Im}(p) \subset \mathrm{Im}\big(P_1(\varphi)\big)$ étant immédiate puisque $\big(P_1Q_1(\varphi)\big)(x) = P_1(\varphi)\big(Q_1(\varphi)(x)\big)$, le théorème est démontré. $\square$

8. Hyperplans

On aborde ici, rapidement, la notion importante d'hyperplan.

Définition 8.1. *Soit E un $\mathbb{R}$-espace vectoriel. Un sous espace vectoriel H de E est dit un hyperplan de E s'il existe une droite vectorielle D de E (donc un sous espace vetoriel de dimension 1 de E) qui est telle que $E = H \oplus D$.*

On dit aussi que H est un hyperplan de E si et seulement si il est de codimension 1. Attention, dans la définition, E n'est pas nécessairement de dimension finie. Le résultat suivant a lieu.

Théorème 8.1. *Soient E un $\mathbb{R}$-espace vectoriel et H un hyperplan de E. Pour $x \in E$ on note $\mathbb{R}x$ la droite vectorielle de vecteur directeur x. Pour tout $x \in E \backslash H$, $E = H \oplus \mathbb{R}x$.*

Démonstration. Soit $x_0 \in E\backslash H$. Il est clair qu'alors $H \cap (\mathbb{R}x_0) = \{0\}$. Donc $H \oplus \mathbb{R}x$ et il reste à montrer que la somme donne E. Comme H est un hyperplan il existe $x_1 \in E$ tel que $E = H \oplus \mathbb{R}x_1$. Tout $y \in E$ s'écrit ainsi $y = x + \lambda x_1$ avec $x \in H$ et $\lambda \in \mathbb{R}$. Mais donc il existe $\tilde{x}_0 \in H$ et $\lambda_0 \in \mathbb{R}$ tel que $x_0 = \tilde{x}_0 + \lambda_0 x_1$. Forcément $\lambda_0 \neq 0$ car $x_0 \notin H$. Donc,

$$x_1 = \frac{1}{\lambda_0} x_0 + \hat{x_0} \ ,$$

où $\hat{x}_0 = -\tilde{x}_0 \in H$. Mais alors pour tout $y \in E$, il existe $x \in H$ et $\lambda \in \mathbb{R}$ tels que

$$\begin{aligned} y &= x + \lambda x_1 \\ &= x + \frac{\lambda}{\lambda_0} x_0 + \lambda \hat{x_0} \\ &= \tilde{x} + \mu x_0 \ , \end{aligned}$$

où $\tilde{x} = x + \lambda \hat{x_0} \in H$ et $\mu = \lambda/\lambda_0$. Tout vecteur de E s'écrit donc comme somme d'un vecteur de H et d'un vecteur de $\mathbb{R}x_0$. D'où $E = H + \mathbb{R}x_0$ et donc, au final, $E = H \oplus \mathbb{R}x_0$. □

Le résultat suivant donne plusieurs caractérisations possibles des hyperplans.

Théorème 8.2. *Soient E un $\mathbb{R}$-espace vectoriel et H un sous espace vectoriel de E. (1) H est un hyperplan de E si et seulement si il est maximal pour la relation d'inclusion au sein des sous espaces vectoriels stricts de E, donc si et seulement si pour tout sous espace vectoriel $\tilde{H}$ de E, $H \subset \tilde{H}$ implique que $\tilde{H} = H$ ou $\tilde{H} = E$.*
(2) H est un hyperplan de E si et seulement si il existe une application linéaire $f : E \to \mathbb{R}$ (don,c une forme linéaire sur E), non identiquement nulle, pour laquelle $H = Ker(f)$.

Démonstration. (1) Supposons que H est un hyperplan de E. Soit $\tilde{H}$ un sous espace vectoriel de E tel que $H \subset \tilde{H}$. Si $H \neq \tilde{H}$ alors il existe $x \in \tilde{H} \backslash H$. Mais alors, en vertue du théorème précédent, $E = H \oplus \mathbb{R}x$. Or $H \oplus \mathbb{R}x \subset \tilde{H}$ puisque $H \subset \tilde{H}$ et $x \in \tilde{H}$. Donc $\tilde{H} = E$ et, ainsi, H est maximal pour la relation d'inclusion au sein des sous espaces vectoriels stricts de E. Réciproquement, supposons que H est maximal pour la relation d'inclusion au sein des sous espaces vectoriels stricts de E. Soit $x \in E \backslash H$. Clairement $H \cap (\mathbb{R}x) = \{0\}$ (pusique $x \notin H$) et donc $H \oplus \mathbb{R}x$. Si $\tilde{H} = H \oplus \mathbb{R}x$, alors $H \subset \tilde{H}$. Donc, comme H est maximal, $\tilde{H} = E$. En particulier, H est un hyperplan.
(2) Supposons que H est un hyperplan. Alors $E = H \oplus \mathbb{R}x_0$ pour un certain $x_0 \in E$. Soit p la projection sur $\mathbb{R}x_0$ parallélement à H, et soit $f : E \to \mathbb{R}$ définie par le fait que $p(x) = f(x)x_0$. Comme p est linéaire, f l'est aussi. Et clairement f est non identiquement nulle et $H = \mathrm{Ker}(f)$. Réciproquement, soit $f : E \to \mathbb{R}$ une application linéaire non identiquement nulle, et soit $H = \mathrm{Ker}(f)$. Comme f n'est pas identiquement nulle, $H \neq E$ et il existe $x_0 \in E \backslash H$. Donc $f(x_0) \neq 0$. Soit $x \in E$ quelconque. Comme $f(x_0) \neq 0$, il existe $\lambda_x \in \mathbb{R}$ tel que $f(x) = \lambda_x f(x_0)$. Mais alors $x - \lambda_x x_0 \in H$, le noyau de f. Et en posant $y_x = x - \lambda_x x_0$ on voit que tout x de E s'écrit $x = y_x + \lambda_x x_0$, donc comme somme d'un vecteur de H et d'un vecteur de $\mathbb{R}x_0$. Ainsi $E = H + \mathbb{R}x_0$. Clairement $H \cap (\mathbb{R}x_0) = \{0\}$ puisque $f(x_0) \neq 0$. Donc $E = H \oplus \mathbb{R}x_0$ et H est un hyperplan. □

On démontre enfin le résultat suivant qui donne une caractérisation très simple des hyperplans en dimension finie.

Théorème 8.3. *Soient E un $\mathbb{R}$-espace vectoriel. Si E est de dimension finie n, les hyperplans de E sont précisément les sous espaces vectoriels de E qui sont de dimension $n - 1$.*

Démonstration. Supposons que H est un hyperplan de E. Il existe alors D de dimension 1 tel que $E = H \oplus D$. Avec le Théorème 5.1 on obtient alors que $n = \dim(H) + 1$, et donc que $\dim(H) = n - 1$. Réciproquement soit H un sous espace vectoriel de dimension $n-1$ de E. Soit $(e_1, \ldots, e_{n-1})$ une base de H. Avec le théorème de la base incomplète, il existe $e_n \in E$ pour lequel $(e_1, \ldots, e_{n-1}, e_n)$ devient une base de E. Clairement $e_n \notin H$ car sinon la famille $(e_1, \ldots, e_{n-1}, e_n)$ serait liée. De façon toute aussi claire, $E = H \oplus \mathbb{R}e_n$. Donc H est un hyperplan. $\square$

CHAPITRE 2

MATRICES ET APPLICATIONS LINÉAIRES

On continue de ne considérer que le cas d'espaces vectoriels réels. Formellement, une matrice réelle à p lignes et q colonnes est une application de $\{1,\dots,p\} \times \{1,\dots,q\}$ dans $\mathbb{R}$. Concrètement, il s'agit de la donnée de $p\times q$ réels a_{ij}, $i=1,\dots,p$, $j=1,\dots,q$, et si M est une telle matrice, on écrit $M=(a_{ij})$ ou $M=(a_{ij})_{i,j}$ ou encore

$$M = \begin{pmatrix} a_{11} & \dots & a_{1q} \\ \vdots & & \vdots \\ a_{p1} & \dots & a_{pq} \end{pmatrix}$$

Le terme à la $i$ème ligne et $j$ème colonne est a_{ij}. On dit que a_{ij} est le terme général de M. On note $\mathcal{M}_{p,q}(\mathbb{R})$ l'ensemble des matrices réelles à p lignes et q colonnes. Si $p=q$, on note aussi $\mathcal{M}_p(\mathbb{R})$ au lieu de $\mathcal{M}_{p,p}(\mathbb{R})$, et on parle de matrices carrées.

9. Opérations élémentaires sur les matrices

On définit la somme de deux matrices réelles de $\mathcal{M}_{p,q}(\mathbb{R})$ par

$$\begin{pmatrix} a_{11} & \dots & a_{1q} \\ \vdots & & \vdots \\ a_{p1} & \dots & a_{pq} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1q} \\ \vdots & & \vdots \\ b_{p1} & \dots & b_{pq} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1q}+b_{1q} \\ \vdots & & \vdots \\ a_{p1}+b_{p1} & \dots & a_{pq}+b_{pq} \end{pmatrix}$$

ce que l'on peut encore écrire sous la forme

$$(a_{ij}) + (b_{ij}) = (a_{ij}+b_{ij}) \ ,$$

et on définit la multiplication d'une matrice de $\mathcal{M}_{p,q}(\mathbb{R})$ par un réel λ en posant

$$\lambda \begin{pmatrix} a_{11} & \dots & a_{1q} \\ \vdots & & \vdots \\ a_{p1} & \dots & a_{pq} \end{pmatrix} = \begin{pmatrix} \lambda a_{11} & \dots & \lambda a_{1q} \\ \vdots & & \vdots \\ \lambda a_{p1} & \dots & \lambda a_{pq} \end{pmatrix}$$

ce que l'on peut encore écrire sous la forme

$$\lambda(a_{ij}) = (\lambda a_{ij}) \ .$$

L'espace $\mathcal{M}_{p,q}(\mathbb{R})$ muni des deux opération internes $+$ et externes $\times$ a une structure naturelle d'espace vectoriel (de dimension pq).

Définition 9.1 (Transposée)**.** *La transposée d'une matrice M de $\mathcal{M}_{p,q}(\mathbb{R})$, notée ${}^tM$, est la matrice de $\mathcal{M}_{q,p}(\mathbb{R})$ dont les coefficients b_{ij} sont donnés par $b_{ij}=a_{ji}$ pour tous $i=1,\dots,q$ et $j=1,\dots,p$.*

L'opération de transposition réalise un isomorphisme de $\mathcal{M}_{p,q}(\mathbb{R})$ sur $\mathcal{M}_{q,p}(\mathbb{R})$. Lorsque $p=q$ la transposition revient à faire une symétrie par rapport à la diagonale $\backslash$ (la diagonale existe lorsque $p=q$).

Définition 9.2 (Produit de deux matrices)**.** *Le produit d'une matrice $A=(a_{ij})$ à p lignes et q colonnes, avec une matrice $B=(b_{ij})$ à q lignes et r colonnes, est la matrice $AB=(c_{ij})$ à p lignes et r colonnes dont les coefficients sont définis par*

$$c_{ij} = \sum_{k=1}^{q} a_{ik} b_{kj}$$

pour tous $i = 1, \ldots, p$, *et* $j = 1, \ldots, r$.

Pour multiplier une matrice A par une matrice B, et donc pour pouvoir écrire le produit AB, il faut que A ait autant de colonnes que B a de lignes. A titre d'exemple:

$$\begin{aligned}&\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix} \times \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix} \\ &= \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} & a_{11}b_{13} + a_{12}b_{23} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} & a_{21}b_{13} + a_{22}b_{23} \\ a_{31}b_{11} + a_{32}b_{21} & a_{31}b_{12} + a_{32}b_{22} & a_{31}b_{13} + a_{32}b_{23} \end{pmatrix}\end{aligned}$$

On vérifie aisément que la proposition suivante a lieu.

Proposition 9.1. *Le produit de matrices est distributif par rapport à l'addition:* $A(B + C) = AB + AC$. *Il est aussi associatif:* $(AB)C = A(BC)$ *et on a enfin que* ${}^t(AB) = {}^t B\, {}^t A$.

Si A et B sont deux matrices carrées d'ordre n, on peut parler des matrices AB et BA. Attention le produit de deux matrices n'est pas commutatif au sens où on peut très bien avoir $AB \neq BA$. Par exemple

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

tandis que

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

Dans le même ordre d'idée, on peut avoir $AB = 0$ (matrice nulle) sans pour autant que soit $A = 0$ soit $B = 0$. Par exemple

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

Exercice: Pour $x \in \mathbb{R}$ on note $A(x)$ la matrice

$$A(x) = \begin{pmatrix} \cos(x) & -\sin(x) \\ \sin(x) & \cos(x) \end{pmatrix}$$

Montrer que pour tous $x, y \in \mathbb{R}$, $A(x)A(y) = A(x + y)$. En déduire $A(x)^n$ pour tout $x \in \mathbb{R}$ et tout $n \in \mathbb{N}$.

Solution: On a

$$\begin{aligned}A(x)A(y) &= \begin{pmatrix} \cos(x) & -\sin(x) \\ \sin(x) & \cos(x) \end{pmatrix} \begin{pmatrix} \cos(y) & -\sin(y) \\ \sin(y) & \cos(y) \end{pmatrix} \\ &= \begin{pmatrix} \cos(x)\cos(y) - \sin(x)\sin(y) & -\cos(x)\sin(y) - \sin(x)\cos(y) \\ \sin(x)\cos(y) + \cos(x)\sin(y) & -\sin(x)\sin(y) + \cos(x)\cos(y) \end{pmatrix}\end{aligned}$$

Les formules trigonométriques donnent

$$\cos(x + y) = \cos(x)\cos(y) - \sin(x)\sin(y)$$
$$\sin(x + y) = \cos(x)\sin(y) + \cos(y)\sin(x)$$

On trouve donc bien $A(x)A(y) = A(x+y)$. Ensuite, par récurrence, $A(x)^n = A(nx)$. $\square$

Produit AB et produit BA: Soit $A \in \mathcal{M}_{p,q}(\mathbb{R})$. Pour pouvoir effectuer à la fois le produit AB et le produit BA il faut que B ait autant de lignes que A a de colonnes et que A ait autant de lignes que B a de colonnes. En bref il faut donc que $B \in \mathcal{M}_{q,p}(A)$. On a alors $AB \in \mathcal{M}_p(\mathbb{R})$ (matrice carrée $p \times p$) et $BA \in \mathcal{M}_q(\mathbb{R})$ (matrice carrée $q \times q$). A priori AB et BA ne sont donc pas des matrices de même taille. Si l'on veut que AB et BA soient dans le même espace il faut que $p = q$, et donc travailler au sein des matrices carrées de même taille.

10. Matrices et applications linéaires

On illustre ici l'idée fondamentale suivante: étant donnés E et F deux espaces vectoriels de dimensions finies,

à une application linéaire $f \in L(E, F)$, et à deux bases $\mathcal{B}$ et $\mathcal{B}'$ respectivement de E et F correspondent une matrice ayant $dim(F)$ lignes et $dim(E)$ colonnes qui représente f dans les bases $\mathcal{B}$ et $\mathcal{B}'$.

En d'autres termes: une matrice s'intérprète comme la lecture d'une application linéaire dans deux bases, une au départ, une à l'arrivée. De façon plus précise, notons $\mathcal{B} = (e_1, \dots, e_m)$ une base de E, et $\mathcal{B}' = (\tilde{e}_1, \dots, \tilde{e}_n)$ une base de F. Soit de plus $f \in L(E, F)$ une application linéaire de E dans F. Pour tout $j = 1, \dots, m$, notons a_{ij}, $i = 1, \dots, n$, les coordonnées de $f(e_j)$ dans $\mathcal{B}'$, de sorte que

$$f(e_j) = \sum_{i=1}^{n} a_{ij} \tilde{e}_i \ .$$

La matrice de f dans les bases $\mathcal{B}$ de E et $\mathcal{B}'$ de F, notée $M_{\mathcal{B}\mathcal{B}'}(f)$, est alors la matrice à n ligne et m colonnes constituée des a_{ij}.

Définition 10.1. *La matrice de f dans les bases $\mathcal{B}$ de E et $\mathcal{B}'$ de F, notée $M_{\mathcal{B}\mathcal{B}'}(f)$ et encore appelée matrice de représentation de f dans les bases $\mathcal{B}$ et $\mathcal{B}'$, est la matrice dont les colonnes sont constituées des coordonnées dans la base d'arrivée $\mathcal{B}'$ des images par f des vecteurs de la base de départ $\mathcal{B}$.*

Avec une telle lecture de f, si $x \in E$ est un vecteur de E de coordonnées $(x_1, \dots, x_m)$ dans la base $\mathcal{B}$, alors les coordonnées $(f(x)_1, \dots, f(x)_n)$ de $f(x)$ dans la base $\mathcal{B}'$ sont données par le produit

$$\begin{pmatrix} f(x)_1 \\ \vdots \\ f(x)_n \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

où $M_{\mathcal{B}\mathcal{B}'}(f) = (a_{ij})_{i,j}$ est la matrice de f dans les bases $\mathcal{B}$ et $\mathcal{B}'$.

Démonstration. On a

$$\begin{aligned} f(x) &= f(x_1 e_1 + \cdots + x_m e_m) \\ &= \sum_{j=1}^{m} x_j f(e_j) \\ &= \sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ij} x_j) \tilde{e}_i \end{aligned}$$

puisque $f(e_j) = \sum_{i=1}^{n} a_{ij}\tilde{e}_i$. Donc,

$$f(x)_i = a_{i1}x_1 + \cdots + a_{im}x_m$$

pour tout $i = 1, \ldots, n$, ce qui correspond bien à la formule énoncée ci-dessus. □

Des propriétés élémentaires vérifiées par es matrices de représentations $M_{\mathcal{B}\mathcal{B}'}(f)$ sont les suivantes:

(i) $M_{\mathcal{B}\mathcal{B}'}(f+g) = M_{\mathcal{B}\mathcal{B}'}(f) + M_{\mathcal{B}\mathcal{B}'}(g)$, et

(ii) $M_{\mathcal{B}\mathcal{B}'}(\lambda f) = \lambda M_{\mathcal{B}\mathcal{B}'}(f)$

pour toutes applications linéaires f et g, et tout réel λ.

Exercice: Soient E un $\mathbb{R}$-espace vectoriel de dimension 3 et $\mathcal{B} = (e_1, e_2, e_3)$ une base de E. On note $f \in End(E)$ l'endomorphisme de E dont la matrice de représentation dans $\mathcal{B}$ est

$$M_{\mathcal{B}\mathcal{B}}(f) = \begin{pmatrix} 2 & 1 & 0 \\ -3 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}$$

(1) Déterminer $f(2e_1 - 3e_2 + 5e_3)$.
(2) Déterminer $Ker(f)$ et $Im(f)$.

Solution: **(1)** On a

$$\begin{pmatrix} 2 & 1 & 0 \\ -3 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 2 \\ -3 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}$$

Donc, $f(2e_1 - 3e_2 + 5e_3) = e_1 + 2e_2 - 3e_3$.

(2) On a

$$\begin{pmatrix} 2 & 1 & 0 \\ -3 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x + y \\ -3x - y + z \\ x - z \end{pmatrix}$$

Donc

$$\begin{pmatrix} 2 & 1 & 0 \\ -3 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

si et seulement si

$$\begin{cases} 2x + y = 0 \\ -3x - y + z = 0 \\ x - z = 0 \end{cases}$$

soit si et seulement si

$$\begin{cases} z = x \\ y = -2x \end{cases}$$

On trouve donc que

$$\begin{aligned} Ker(f) &= \{xe_1 + ye_2 + ze_3 \ / \ y = -2x \text{ et } z = x\} \\ &= \{x(e_1 - 2e_2 + e_3), x \in \mathbb{R}\} \end{aligned}$$

Donc $Ker(f)$ est la droite vectorielle de vecteur directeur $u = e_1 - 2e_2 + e_3$. Le théorème du rang donne maintenant que $Im(f)$ est un plan vectoriel (sous espace vectoriel de dimension 2). Il suffit alors de trouver deux vecteurs de $Im(f)$ qui forment une famille libre pour avoir une base de $Im(f)$. Par définition même de $M_{\mathcal{B}\mathcal{B}}(f)$ on a $f(e_1) = 2e_1 - 3e_2 + e_3$ tandis que $f(e_2) = e_1 - e_2$. Clairement les vecteurs $v = 2e_1 - 3e_2 + e_3$ et $w = e_1 - e_2$ forment une famille libre car $\lambda v + \mu w = (2\lambda + \mu)e_1 - (3\lambda + \mu)e_2 + \lambda e_3$ de sorte que $\lambda v + \mu w = 0$ si et seulement si $\lambda = \mu = 0$. Comme $v, w \in Im(f)$, on obtient que $Im(f)$ est le plan vectoriel de base (v, w). □

Théorème 10.1. *Soient E_1, E_2, E_3 trois espaces vectoriels de dimensions finies, et soient $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ trois bases respectivement de E_1, E_2, et E_3. Soient $f \in L(E_1, E_2)$ et $g \in L(E_2, E_3)$ deux applications linéaires. Alors $M_{\mathcal{B}_1\mathcal{B}_3}(g \circ f) = M_{\mathcal{B}_2\mathcal{B}_3}(g)M_{\mathcal{B}_1\mathcal{B}_2}(f)$.*

Démonstration. Cette propriété se vérifie assez facilement. On note $M_{\mathcal{B}_1\mathcal{B}_2}(f) = (a_{ij})_{i,j}$ et $M_{\mathcal{B}_2\mathcal{B}_3}(g) = (b_{ij})_{i,j}$, et on note $\mathcal{B}_1 = (e_1^1, \dots, e_{n_1}^1)$, $\mathcal{B}_2 = (e_1^2, \dots, e_{n_2}^2)$, et $\mathcal{B}_3 = (e_1^3, \dots, e_{n_3}^3)$. Alors pour tout $j = 1, \dots, n_1$,

$$f(e_j^1) = \sum_{k=1}^{n_2} a_{kj} e_k^2$$

tandis que pour tout $k = 1, \dots, n_2$,

$$g(e_k^2) = \sum_{i=1}^{n_3} b_{ik} e_i^3 \ .$$

On en déduit que pour tout $j = 1, \dots, n_1$,

$$\big(g \circ f\big)(e_j^1) = \sum_{i=1}^{n_3} \Big(\sum_{k=1}^{n_2} b_{ik} a_{kj}\Big) e_i^3$$

de sorte que

$$M_{\mathcal{B}_1\mathcal{B}_3}\big(g \circ f\big)_{ij} = \sum_{k=1}^{n_2} b_{ik} a_{kj}$$

ce qui correspond bien au produit des deux matrices $M_{\mathcal{B}_2\mathcal{B}_3}(g)$ et $M_{\mathcal{B}_1\mathcal{B}_2}(f)$. Cela prouve le théorème. □

11. Matrices inversibles. Première approche

On ne parle de matrice inversible que pour les matrices carrées. Soit donc A une matrice carrée de $\mathcal{M}_n(\mathbb{R})$. On dit que A est inversible s'il existe $B \in \mathcal{M}_n(\mathbb{R})$ telle que

$$AB = BA = \mathrm{Id}_n$$

où Id_n est la matrice identité de $\mathcal{M}_n(\mathbb{R})$, à savoir

$$\mathrm{Id}_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

encore définie par $\mathrm{Id}_n = (\delta_{ij})_{i,j}$ où $\delta_{ij} = 1$ si $i = j$ et $\delta_{ij} = 0$ si $i \neq j$. Les δ_{ij} sont appelés symboles de Kroenecker. On montre que l'inverse est unique. On note $B = A^{-1}$. La matrice identité Id_n a la propriété que pour toute matrice $A \in \mathcal{M}_n(\mathbb{R})$, $\mathrm{Id}_n A = A\mathrm{Id}_n = A$.

Théorème 11.1. *Soient E et F deux $\mathbb{R}$-espaces vectoriels de même dimension n, $\mathcal{B}$ et $\mathcal{B}'$ deux bases respectivement de E et F, et $f \in L(E, F)$. Alors f est un isomorphisme de E sur F si et seulement si $M_{\mathcal{B}\mathcal{B}'}(f)$ est une matrice inversible. De plus, dans ce cas, $M_{\mathcal{B}\mathcal{B}'}(f)^{-1} = M_{\mathcal{B}'\mathcal{B}}(f^{-1})$.*

Démonstration. (1) Supposons pour commencer que f est un isomorphisme de E sur F. Alors il existe $g = f^{-1} \in L(F, E)$ tel que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$, où Id_E et Id_F sont les applications linéaires identités de E et de F. De ces deux formules, et de la formule de composition des matrices de représentations on tire que

$$\mathrm{Id}_n = M_{\mathcal{B}\mathcal{B}}(\mathrm{Id}_E) = M_{\mathcal{B}'\mathcal{B}}(g)M_{\mathcal{B}\mathcal{B}'}(f),$$
$$\mathrm{Id}_n = M_{\mathcal{B}'\mathcal{B}'}(\mathrm{Id}_F) = M_{\mathcal{B}\mathcal{B}'}(f)M_{\mathcal{B}'\mathcal{B}}(g)$$

Par suite, $M_{\mathcal{B}\mathcal{B}'}(f)$ est une matrice inversible, et $M_{\mathcal{B}\mathcal{B}'}(f)^{-1} = M_{\mathcal{B}'\mathcal{B}}(f^{-1})$.

(2) A l'inverse, supposons que $M_{\mathcal{B}\mathcal{B}'}(f)$ est inversible. Notons $(b_{ij})_{i,j}$ la matrice inverse de $M_{\mathcal{B}\mathcal{B}'}(f)$, et notons e_i les vecteurs de $\mathcal{B}$ et e'_i les vecteurs de $\mathcal{B}'$. On construit une application linéaire $g \in L(F, E)$ en posant

$$g(e'_i) = \sum_{j=1}^{n} b_{ji}e_j$$

pour tout $i = 1, \ldots, n$. Alors, par construction même de g,

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

De la formule de composition des matrices de représentations on tire alors que

$$M_{\mathcal{B}\mathcal{B}}(g \circ f) = M_{\mathcal{B}'\mathcal{B}}(g)M_{\mathcal{B}\mathcal{B}'}(f) = \mathrm{Id}_n,$$
$$M_{\mathcal{B}'\mathcal{B}'}(f \circ g) = M_{\mathcal{B}\mathcal{B}'}(f)M_{\mathcal{B}'\mathcal{B}}(g) = \mathrm{Id}_n \ .$$

Donc, $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$, ce qui prouve que f est un isomorphisme. D'où le théorème. □

Avec les idées développées dans la preuve ci-dessus (à une matrice et deux bases correspondent une application linéaire ayant cette matrice pour lecture dans les bases) on peut montrer qu'il suffit de demander une seule des deux relations $AB = \mathrm{Id}_n$ ou $BA = \mathrm{Id}_n$ dans la définition de l'inversibilité d'une matrice.

Corollaire 11.1. *S'il existe $B \in \mathcal{M}_n(\mathbb{R})$ telle que $AB = Id_n$, alors $BA = Id_n$ (et vis versa). En particulier, A est inversible et $B = A^{-1}$.*

Démonstration. Posons $E = \mathbb{R}^n$. On note $\mathcal{B}$ une base de $\mathbb{R}^n$, et on considère $f \in End(\mathbb{R}^n)$ et $g \in End(\mathbb{R}^n)$ tels que $M_{\mathcal{B}\mathcal{B}}(f) = A$ et $M_{\mathcal{B}\mathcal{B}}(g) = B$. Supposons que $BA = \mathrm{Id}_n$. Alors $g \circ f = \mathrm{Id}_{\mathbb{R}^n}$, et il s'ensuit que f est nécessairement injective (on remarque que $f(x) = f(y) \Rightarrow g \circ f(x) = g \circ f(y) \Rightarrow x = y$). Donc, cf. Chapitre 1, f est un isomorphisme et (cf. théorème précédent) A est inversible. Même genre de raisonnement si on suppose que $AB = \mathrm{Id}_n$ car alors $f \circ g = \mathrm{Id}_{\mathbb{R}^n}$ et f est automatiquement surjective. Le corollaire est démontré. □

Exercice: Soit

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

Calculer $A^3 - A$. En déduire que A est inversible et déterminer A^{-1}.

Solution: On a

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

et

$$A^3 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \\ 1 & -2 & 0 \end{pmatrix} \begin{pmatrix} 3 & -4 & 2 \\ 1 & -1 & -1 \\ 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 0 & 2 \\ 0 & 3 & 1 \\ 1 & -2 & 4 \end{pmatrix}$$

On trouve alors $A^3 - A = 4Id_3$. Soit $B = \frac{1}{4}(A^2 - Id_3)$. Alors $AB = BA = Id_3$. Donc A est inversible d'inverse $A^{-1} = B$. □

Théorème 11.2. *Si $A, B \in \mathcal{M}_n(\mathbb{R})$ sont deux matrices inversibles, alors AB est inversible et $(AB)^{-1} = B^{-1}A^{-1}$.*

Démonstration. On a

$$\begin{aligned} AB \times (B^{-1}A^{-1}) &= A(BB^{-1})A^{-1} \\ &= (A\mathrm{Id}_n)A^{-1} \\ &= AA^{-1} \\ &= \mathrm{Id}_n \ , \end{aligned}$$

ce qui prouve le théorème. □

12. Changement de base

Il s'agit dans cette section importante de décrire la changement de matrice de représentation d'une application linéaire donnée par changement de bases.

Définition 12.1 (Matrice de changement de base)**.** *Soient E un espace vectoriel de dimension finie n, et $\mathcal{B} = (e_1, \dots, e_n)$, $\tilde{\mathcal{B}} = (\tilde{e}_1, \dots, \tilde{e}_n)$ deux bases de E. On note $\Phi_{\mathcal{B}\tilde{\mathcal{B}}}$ l'isomorphisme (endomorphisme bijectif) de E défini par:*

$$\Phi_{\mathcal{B}\tilde{\mathcal{B}}}(e_i) = \tilde{e}_i$$

pour tout $i = 1, \dots, n$. La matrice de passage de la base $\mathcal{B}$ à la base $\tilde{\mathcal{B}}$, notée $M_{\mathcal{B}\to\tilde{\mathcal{B}}}$, est, par définition, la matrice $M_{\mathcal{B}\mathcal{B}}(\Phi_{\mathcal{B}\tilde{\mathcal{B}}})$, représentant la lecture de $\Phi_{\mathcal{B}\tilde{\mathcal{B}}}$ dans la base $\mathcal{B}$.

En d'autres termes, la matrice de passage d'une base $\mathcal{B}$ à une base $\tilde{\mathcal{B}}$ est la matrice de lecture dans $\mathcal{B}$ de l'isomorphisme qui envoie les vecteurs de $\mathcal{B}$ sur les vecteurs de $\tilde{\mathcal{B}}$.

Les colonnes de $M_{\mathcal{B}\to\tilde{\mathcal{B}}}$ sont constituées des coordonnées des vecteurs de $\tilde{\mathcal{B}}$ dans $\mathcal{B}$. Avec les notations précédente, soit $\Phi_{\tilde{\mathcal{B}}\mathcal{B}}$ l'isomorphisme de E défini par: $\Phi_{\tilde{\mathcal{B}}\mathcal{B}}(\tilde{e}_i) = e_i$, pour tout $i = 1, \dots, n$. On a alors $\Phi_{\mathcal{B}\tilde{\mathcal{B}}} \circ \Phi_{\tilde{\mathcal{B}}\mathcal{B}} = \Phi_{\tilde{\mathcal{B}}\mathcal{B}} \circ \Phi_{\mathcal{B}\tilde{\mathcal{B}}} = \mathrm{Id}_E$. En particulier:

Lemme 12.1. *$M_{\mathcal{B}\to\tilde{\mathcal{B}}}$ est inversible et $M^{-1}_{\mathcal{B}\to\tilde{\mathcal{B}}} = M_{\mathcal{B}\mathcal{B}}(\Phi_{\tilde{\mathcal{B}}\mathcal{B}}) = M_{\tilde{\mathcal{B}}\to\mathcal{B}}$.*

Démonstration. Seule la dernière égalité est à démontrer. Posons $M_{\mathcal{B}\to\tilde{\mathcal{B}}} = (a_{ij})_{i,j}$ et $M_{\tilde{\mathcal{B}}\to\mathcal{B}} = (b_{ij})_{i,j}$. Alors $\tilde{e}_i = \sum_{j=1}^n a_{ji}e_j$ pour tout i et $e_i = \sum_{j=1}^n b_{ji}\tilde{e}_j$ pour tout i. Donc

$$\begin{aligned}\tilde{e}_i &= \sum_{j=1}^{n} a_{ji} e_j = \sum_{j=1}^{n} a_{ji} \sum_{k=1}^{n} b_{kj} \tilde{e}_k \\ &= \sum_k \left(\sum_j b_{kj} a_{ji} \right) \tilde{e}_k \ ,\end{aligned}$$

ce qui prouve que $\sum_{j=1}^{n} b_{kj} a_{ji} = \delta_{ki}$ pour tous i, k. Donc $M_{\tilde{\mathcal{B}} \to \mathcal{B}} \times M_{\mathcal{B} \to \tilde{\mathcal{B}}} = \mathrm{Id}_n$ et le lemme est démontré. □

Lemme 12.2. *La matrice de passage $M_{\mathcal{B} \to \tilde{\mathcal{B}}}$ envoie les coordonnées d'un vecteur x dans $\tilde{\mathcal{B}}$ sur les coordonnées de x dans $\mathcal{B}$.*

En d'autres termes, pour tout $x \in E$ de coordonnées x_i dans $\mathcal{B}$ et $\tilde{x}_i$ dans $\tilde{\mathcal{B}}$, on a que

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} \tilde{x}_1 \\ \vdots \\ \tilde{x}_n \end{pmatrix}$$

où, dans cette relation, la matrice des a_{ij} est la matrice de passage de $\mathcal{B}$ à $\tilde{\mathcal{B}}$, à savoir

$$M_{\mathcal{B} \to \tilde{\mathcal{B}}} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \ .$$

Attention à l'inversion (la matrice de passage de $\mathcal{B}$ à $\tilde{\mathcal{B}}$ envoie les coordonnées des vecteurs dans $\tilde{\mathcal{B}}$ sur leurs coordonnées dans $\mathcal{B}$).

Démonstration. Puisque $M_{\mathcal{B} \to \tilde{\mathcal{B}}} = M_{\mathcal{B}\mathcal{B}}(\Phi_{\mathcal{B}\tilde{\mathcal{B}}})$, on a que

$$\tilde{e}_j = \sum_{i=1}^{n} a_{ij} e_i$$

pour tout j. On écrit alors que

$$\begin{aligned} x &= \sum_{j=1}^{n} \tilde{x}_j \tilde{e}_j \\ &= \sum_{j=1}^{n} \tilde{x}_j \left(\sum_{i=1}^{n} a_{ij} e_i \right) \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} \tilde{x}_j \right) e_i \end{aligned}$$

de sorte que $x_i = \sum_{j=1}^{n} a_{ij} \tilde{x}_j$, ce qui démontre le lemme. □

Théorème 12.1 (Théorème de changement de base)**.** *Soient E, F deux $\mathbb{R}$-espaces vectoriels de dimensions finies, $\mathcal{B}_1$, $\mathcal{B}_2$ deux bases de E, et $\mathcal{B}_1'$, $\mathcal{B}_2'$ deux bases de F. Soit aussi $f \in L(E, F)$ une application linéaire de E dans F. Alors*

$$M_{\mathcal{B}_2 \mathcal{B}_2'}(f) = M_{\mathcal{B}_1' \to \mathcal{B}_2'}^{-1} M_{\mathcal{B}_1 \mathcal{B}_1'}(f) M_{\mathcal{B}_1 \to \mathcal{B}_2}$$

où $M_{\mathcal{B}_1\to\mathcal{B}_2}$ est la matrice de passage de la base $\mathcal{B}_1$ à la base $\mathcal{B}_2$, et $M_{\mathcal{B}'_1\to\mathcal{B}'_2}$ est la matrice de passage de la base $\mathcal{B}'_1$ à la base $\mathcal{B}'_2$.

On pourra se souvenir de l'ordre des matrices dans ce théorème à l'aide du diagramme commutatif suivant:

$$\begin{array}{ccccc} & \mathcal{B}_1 & \xrightarrow{M_{\mathcal{B}_1\mathcal{B}'_1}(f)} & \mathcal{B}'_1 & \\ M_{\mathcal{B}_1\to\mathcal{B}_2} & \Big\uparrow & & \Big\uparrow & M_{\mathcal{B}'_1\to\mathcal{B}'_2} \\ & \mathcal{B}_2 & \xrightarrow{M_{\mathcal{B}_2\mathcal{B}'_2}(f)} & \mathcal{B}'_2 & \end{array}$$

Démonstration. Soit x un vecteur de E. Notons V_x^1 la matrice colonne composée des coordonnées de x dans la base $\mathcal{B}_1$, et V_x^2 la matrice colonne composée des coordonnées de x dans la base $\mathcal{B}_2$. Si $y \in F$, on note de même V_y^1 la matrice colonne composée des coordonnées de y dans la base $\mathcal{B}'_1$, et V_y^2 la matrice colonne composée des coordonnées de y dans la base $\mathcal{B}'_2$. On a alors

$$V_x^1 = M_{\mathcal{B}_1\to\mathcal{B}_2}V_x^2 \quad \text{et} \quad V_y^1 = M_{\mathcal{B}'_1\to\mathcal{B}'_2}V_y^2 \ .$$

Dans le même ordre d'idées on a que

$$V_{f(x)}^1 = M_{\mathcal{B}_1\mathcal{B}'_1}(f)V_x^1 \quad \text{et} \quad V_{f(x)}^2 = M_{\mathcal{B}_2\mathcal{B}'_2}(f)V_x^2 \ .$$

On écrit alors que

$$\begin{aligned} V_{f(x)}^2 &= M^{-1}_{\mathcal{B}'_1\to\mathcal{B}'_2}V^1_{f(x)} \quad \text{puisque } V_y^1 = M_{\mathcal{B}'_1\to\mathcal{B}'_2}V_y^2 \\ &= M^{-1}_{\mathcal{B}'_1\to\mathcal{B}'_2}M_{\mathcal{B}_1\mathcal{B}'_1}(f)V_x^1 \quad \text{puisque } V^1_{f(x)} = M_{\mathcal{B}_1\mathcal{B}'_1}(f)V_x^1 \\ &= M^{-1}_{\mathcal{B}'_1\to\mathcal{B}'_2}M_{\mathcal{B}_1\mathcal{B}'_1}(f)M_{\mathcal{B}_1\to\mathcal{B}_2}V_x^2 \quad \text{puisque } V_x^1 = M_{\mathcal{B}_1\to\mathcal{B}_2}V_x^2 \end{aligned}$$

Donc, pour tout x de E,

$$M_{\mathcal{B}_2\mathcal{B}'_2}(f)V_x^2 = M^{-1}_{\mathcal{B}'_1\to\mathcal{B}'_2}M_{\mathcal{B}_1\mathcal{B}'_1}(f)M_{\mathcal{B}_1\to\mathcal{B}_2}V_x^2$$

puisque $V^2_{f(x)} = M_{\mathcal{B}_2\mathcal{B}'_2}(f)V_x^2$. En prenant successivement x tel que x a pour coordonnées $(1,0,\dots,0)$, $(0,1,\dots,0)$, $\dots$, $(0,\dots,0,1)$ dans $\mathcal{B}_2$, on en déduit que

$$M_{\mathcal{B}_2\mathcal{B}'_2}(f) = M^{-1}_{\mathcal{B}'_1\to\mathcal{B}'_2}M_{\mathcal{B}_1\mathcal{B}'_1}(f)M_{\mathcal{B}_1\to\mathcal{B}_2}$$

ce qui prouve le théorème. □

Un cas particulier du théorème est donné par le résultat suivant.

Théorème 12.2 (Théorème de changement de base dans le cas $F = E$)**.** *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie, $\mathcal{B}, \mathcal{B}'$ deux bases de E, et $f \in End(E)$ un endomorphisme de E. Alors*

$$M_{\mathcal{B}'\mathcal{B}'}(f) = M^{-1}_{\mathcal{B}\to\mathcal{B}'}M_{\mathcal{B}\mathcal{B}}(f)M_{\mathcal{B}\to\mathcal{B}'}$$

où $M_{\mathcal{B}\to\mathcal{B}'}$ est la matrice de passage de la base $\mathcal{B}$ à la base $\mathcal{B}'$.

Deux matrices carrées $M, M' \in \mathcal{M}_n(\mathbb{R})$, reliées par une relation du type

$$M' = A^{-1}MA \ ,$$

où $A \in \mathcal{M}_n(\mathbb{R})$ est inversible, sont dites semblables. On vérifie facilement qu'il s'agit là d'une relation d'équivalence. On vérifie tout aussi facilement que deux matrices sont semblables si elles représentent le même endomorphisme mais dans deux bases différentes.

Exercice: Soit $f \in L(\mathbb{R}^3, \mathbb{R}^2)$ l'application linéaire de $\mathbb{R}^3$ dans $\mathbb{R}^2$ dont la matrice A dans les bases canoniques $\mathcal{B}_1 = (u_1, u_2, u_3)$ et $\mathcal{B}_2 = (v_1, v_2)$ de $\mathbb{R}^3$ et $\mathbb{R}^2$ est donnée par

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

On note

$$\begin{cases} \tilde{u}_1 = u_2 + u_3, \tilde{u}_2 = u_1 + u_3, \tilde{u}_3 = u_1 + u_2, \\ \tilde{v}_1 = v_1 + v_2, \tilde{v}_2 = v_1 - v_2 \ . \end{cases}$$

Montrer que les familles $\tilde{\mathcal{B}}_1 = (\tilde{u}_1, \tilde{u}_2, \tilde{u}_3)$ et $\tilde{\mathcal{B}}_2 = (\tilde{v}_1, \tilde{v}_2)$ sont des bases de $\mathbb{R}^3$ et $\mathbb{R}^2$, et déterminer la matrice $\tilde{A}$ de f dans ces bases.

Solution: $\tilde{\mathcal{B}}_1$ est composée de 3 vecteurs en dimension 3. Il suffit donc de vérifier que $\tilde{\mathcal{B}}_1$ est libre. On a $\lambda\tilde{u}_1 + \mu\tilde{u}_2 + \nu\tilde{u}_3 = 0$ si et seulement si

$$(\mu + \nu)u_1 + (\lambda + \nu)u_2 + (\lambda + \mu)u_3 = 0$$

et comme (u_1, u_2, u_3) est une base, on trouve que

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

En additionnant les deux premières équations, et grâce à la dernière, on voit que forcément $\nu = 0$. On trouve ensuite facilement que nécessairement $\lambda = \mu = \nu = 0$. Donc $\tilde{\mathcal{B}}_1$ est libre et ensuite (puisqu'elle comporte autant de vecteurs que la dimension) $\tilde{\mathcal{B}}_1$ est une base de $\mathbb{R}^3$. Même raisonnement pour $\tilde{\mathcal{B}}_2$. Il y a deux vecteurs en dimension 2. Il suffit donc de vérifier que $\tilde{\mathcal{B}}_2$ est libre. On a $\lambda\tilde{v}_1 + \mu\tilde{v}_2 = 0$ si et seulement si

$$(\lambda + \mu)v_1 + (\lambda - \mu)v_2 = 0$$

et comme (v_1, v_2) est une base, on trouve que

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

En additionnant les deux équations on voit que $\lambda = 0$ puis que $\lambda = \mu = 0$. Donc $\tilde{\mathcal{B}}_2$ est libre et ensuite (puisqu'elle comporte autant de vecteurs que la dimension) $\tilde{\mathcal{B}}_2$ est une base de $\mathbb{R}^2$. Les matrices de passage de $\mathcal{B}_1$ à $\tilde{\mathcal{B}}_1$ et de $\mathcal{B}_2$ à $\tilde{\mathcal{B}}_2$ sont données par

$$M_{\mathcal{B}_1 \to \tilde{\mathcal{B}}_1} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \text{ et } M_{\mathcal{B}_2 \to \tilde{\mathcal{B}}_2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

On saura très bientôt comment procéder pour l'inverse (et le calcul est très facile en dimension 2): on a

$$M^{-1}_{\mathcal{B}_2 \to \tilde{\mathcal{B}}_2} = \frac{1}{2} \times \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Le diagramme de changement de bases s'écrit ici (avec les notations de l'exercice):

$$\begin{array}{ccccc} & \mathcal{B}_1 & \xrightarrow{M_{\mathcal{B}_1\mathcal{B}_2}(f)} & \mathcal{B}_2 & \\ M_{\mathcal{B}_1\to\tilde{\mathcal{B}}_1} & \Big\uparrow & & \Big\uparrow & M_{\mathcal{B}_2\to\tilde{\mathcal{B}}_2} \\ & \tilde{\mathcal{B}}_1 & \xrightarrow{M_{\tilde{\mathcal{B}}_1\tilde{\mathcal{B}}_2}(f)} & \tilde{\mathcal{B}}_2 & \end{array}$$

Le théorème de changement de base donne donc que

$$M_{\tilde{\mathcal{B}}_1\tilde{\mathcal{B}}_2}(f) = M^{-1}_{\mathcal{B}_2\to\tilde{\mathcal{B}}_2} M_{\mathcal{B}_1\mathcal{B}_2}(f) M_{\mathcal{B}_1\to\tilde{\mathcal{B}}_1}$$

Donc

$$\begin{aligned}\tilde{A} &= M_{\tilde{\mathcal{B}}_1\tilde{\mathcal{B}}_2}(f)\\ &= \frac{1}{2}\times\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}2 & -1 & 1\\ 3 & 2 & -3\end{pmatrix}\begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{pmatrix}\\ &= \frac{1}{2}\times\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 3 & 1\\ -1 & 0 & 5\end{pmatrix}\\ &= \frac{1}{2}\begin{pmatrix}-1 & 3 & 6\\ 1 & 3 & -4\end{pmatrix}\\ &= \begin{pmatrix}-1/2 & 3/2 & 3\\ 1/2 & 3/2 & -2\end{pmatrix}\end{aligned}$$

□

13. Matrices inversibles. Déterminants

Pour ne pas perdre trop de temps, on énonce les résultats de cette section sans preuve. On renvoie au cours de première année pour plus de détails.

Soit $n \in \mathbb{N}$ un entier naturel. Par définition, une permutation de $\{1, \dots, n\}$ est une application bijective de $\{1, \dots, n\}$ dans $\{1, \dots, n\}$. On note $\mathcal{P}_n$ l'ensemble des permutations de $\{1, \dots, n\}$. L'ensemble $\mathcal{P}_n$ a $n!$ éléments. Si $\sigma \in \mathcal{P}_n$, le signe $\varepsilon(\sigma)$ de σ est le réel valant -1 ou $+1$ défini par

$$\varepsilon(\sigma) = \frac{\prod_{1\le i<j\le n}\big(\sigma(i)-\sigma(j)\big)}{\prod_{1\le i<j\le n}(i-j)}\ .$$

Si $\varepsilon(\sigma) = -1$, on parle de permutation impaire. Si $\varepsilon(\sigma) = +1$, on parle de permutation paire. On vérifie que $\varepsilon(\tau\circ\sigma) = \varepsilon(\tau)\varepsilon(\sigma)$. Une transposition de $\mathcal{P}_n$ est une permutation qui n'échange que deux éléments. Le signe d'une transposition est toujours -1.

Lemme 13.1. *Toute permutation de $\mathcal{P}_n$ se décompose (de façon non unique) en composition de transpositions. Le signe de la permutation est alors $(-1)^k$ où k est la nombre de transpositions qui interviennent dans cette décomposition.*

On adopte alors la définition suivante du déterminant d'une matrice carrée.

Définition 13.1. *Soit $A = (a_{ij})_{i,j}$ une matrice carrée réelle d'ordre n. Par définition, le déterminant de A est le réel $det(A)$ défini par*

$$det(A) = \sum_{\sigma\in\mathcal{P}_n}\varepsilon(\sigma)a_{1\sigma(1)}\dots a_{n\sigma(n)}$$

soit encore $det(A) = \sum_{\sigma \in \mathcal{P}_n} \varepsilon(\sigma) \left(\prod_{i=1}^{n} a_{i\sigma(i)} \right)$.

A partir de cette formule on obtient par le calcul les déterminants suivants (cas $n = 2$ et $n = 3$). A savoir:

$$\det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = ad - bc$$

Pour le voir on remarque que les permutations de $\mathcal{P}_2$ sont au nombre de 2 et données par

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} .$$

Deux permutations de signes respectifs $+1$ et -1. De même

$$\begin{aligned} \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{12}a_{23}a_{31} \\ &\quad - a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33} - a_{32}a_{23}a_{11} \end{aligned}$$

Pour démontrer cette formule on remarque que les permutations de $\mathcal{P}_3$ sont au nombre de 6 et données par

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

qui sont de signes respéctifs $+1$, -1, -1, -1, $+1$, $+1$. Un moyen mnémotechnique pour ce souvenir de cette formule:

$$\begin{aligned} \det(A) \quad = & \begin{vmatrix} \bullet & \cdot & \cdot \\ \cdot & \bullet & \cdot \\ \cdot & \cdot & \bullet \end{vmatrix} + \begin{vmatrix} \cdot & \cdot & \bullet \\ \bullet & \cdot & \cdot \\ \cdot & \bullet & \cdot \end{vmatrix} + \begin{vmatrix} \cdot & \bullet & \cdot \\ \cdot & \cdot & \bullet \\ \bullet & \cdot & \cdot \end{vmatrix} \\ & - \begin{vmatrix} \cdot & \cdot & \bullet \\ \cdot & \bullet & \cdot \\ \bullet & \cdot & \cdot \end{vmatrix} - \begin{vmatrix} \cdot & \bullet & \cdot \\ \bullet & \cdot & \cdot \\ \cdot & \cdot & \bullet \end{vmatrix} - \begin{vmatrix} \bullet & \cdot & \cdot \\ \cdot & \cdot & \bullet \\ \cdot & \bullet & \cdot \end{vmatrix} \end{aligned}$$

Des propriétés élémentaires du déterminant sont les suivantes:

(i) $det(Id_n) = 1$,

(ii) $det(AB) = det(A)det(B)$,

(iii) $det({}^tA) = det(A)$.

En particulier, on déduit de (i) et (ii) que si A est inversible, alors $det(A) \neq 0$ et

(iv) $det(A^{-1}) = \frac{1}{det(A)}$.

Le théorème suivant donne toute sa puissance à la notion de déterminant.

Théorème 13.1. *Une matrice carrée A est inversible si et seulement si $det(A) \neq 0$.*

En particulier, le résultat important suivant a lieu.

Corollaire 13.1. *Soient E, F deux $\mathbb{R}$-espaces vectoriels de même dimension n, $\mathcal{B}$ une base de E, $\tilde{\mathcal{B}}$ une base de F et $f \in L(E, F)$ une application linéaire de E sur F. Alors f est un isomorphisme si et seulement si $detM_{\mathcal{B}\tilde{\mathcal{B}}}(f) \neq 0$ et dans ce cas $M_{\tilde{\mathcal{B}}\mathcal{B}}(f^{-1}) = M_{\mathcal{B}\tilde{\mathcal{B}}}(f)^{-1}$.*

Exercice: Soient $p < n$ deux entiers, $A \in \mathcal{M}_{n,p}(\mathbb{R})$ une matrice à n lignes et p colonnes et $B \in \mathcal{M}_{p,n}(\mathbb{R})$ une matrice à p lignes et n colonnes. Montrer que $\det(AB) = 0$.

Solution: Soient E, F deux $\mathbb{R}$-espaces vectoriels de dimensions respectives n et p, $\mathcal{B}$ une base de E et $\tilde{\mathcal{B}}$ une base de F. On note $f \in L(E,F)$ l'application linéaire de E dans F donnée par l'équation $M_{\mathcal{B}\tilde{\mathcal{B}}}(f) = B$ et $g \in L(F,E)$ l'application linéaire de F dans E donnée par l'équation $M_{\tilde{\mathcal{B}}\mathcal{B}}(g) = A$. Alors, par composition,

$$M_{\mathcal{B}\mathcal{B}}(g \circ f) = AB \ .$$

On a clairement que

$$Rg(g \circ f) \leq Rg(g) \ .$$

En vertue du théorème du rang, $Rg(g) \leq p$ (dimension de l'espace de départ F). Or $p < n$, donc $Rg(g \circ f) < n$. On en déduit que $g \circ f \in L(E,E)$ n'est pas surjective, puis qu'elle n'est donc pas bijective. Par suite $\det\left(M_{\mathcal{B}\mathcal{B}}(g \circ f)\right) = 0$ et donc $\det(AB) = 0$. □

D'autres propriétés des déterminants sont les suivantes. Notons $A = (a_{ij})_{i,j}$ une matrice réelle carrée d'ordre n, i.e. un élément de $\mathcal{M}_n(\mathbb{R})$. Soit de plus σ une permutation de $\mathcal{P}_n$. On note

$$A^\sigma = (a_{i\sigma(j)})_{i,j} \quad \text{et} \quad A_\sigma = (a_{\sigma(i)j})_{i,j}$$

de sorte que A^σ consiste à effectuer une permutation sur les colonnes de A suivant σ, tandis que A_σ consiste à effectuer une permutation sur les lignes de A suivant σ. Alors

$$\det(A^\sigma) = \det(A_\sigma) = \varepsilon(\sigma)\det(A) \ .$$

Indépendamment, on pourra montrer qu'on ne change pas un déterminant en ajoutant à une des lignes (resp. colonnes) de la matrice un multiple d'une autre ligne (resp. colonne). Pour finir, si λ est un réel, et si A est une matrice carrée d'ordre n, on a que $\det(\lambda A) = \lambda^n \det(A)$, tandis que si l'on se contente de ne multiplier qu'une ligne ou qu'une colonne de A par λ alors le déterminant de cette nouvelle matrice vaut $\lambda\det(A)$. Avec ces règles on peut se débrouiller pour placer des zéros sur une ligne donnée de la matrice sans changer son déterminant.

Définition 13.2. *Soit $A = (a_{ij})_{i,j}$ une matrice réelle carrée d'ordre n, i.e. un élément de $\mathcal{M}_n(\mathbb{R})$. Etant donnés $i,j \in \{1,\dots,n\}$, on appelle mineur de a_{ij}, et on note Δ_{ij}, le déterminant de la matrice carrée d'ordre $n-1$ obtenue à partir de A en supprimant la $i$ème ligne et la $j$ème colonne de A. On appelle cofacteur de a_{ij}, le réel $(-1)^{i+j}\Delta_{ij}$.*

Le théorème de développement suivant a lieu.

Théorème 13.2. *Soit $A = (a_{ij})_{i,j}$ une matrice réelle carrée d'ordre n. Etant donnés $i,j \in \{1,\dots,n\}$,*

$$det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij}\Delta_{ij} \ \textit{et}\ det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij}\Delta_{ij} \ .$$

Dans la première formule on développe le déterminant suivant la $i$ème ligne, et dans la seconde on développe le déterminant suivant la $j$ème colonne.

On aura bien sûr tout intérêt à choisir la ligne ou la colonne qui comporte le plus de zéros. A partir de ces formules, et de la formule générale donnant le déterminant d'une matrice d'ordre 3, on calculera facilement le déterminant d'une matrice d'ordre 4 (et ainsi de suite...)

Théorème 13.3. *Si $(A_{ij})_{i,j}$ est la matrice des cofacteurs, donc $A_{ij} = (-1)^{i+j}\Delta_{ij}$, et si A est inversible, donc si $det(A) \neq 0$, l'inverse de A est donnée par la formule suivante:*

$$A^{-1} = \frac{1}{det(A)}\ {}^t(A_{ij})_{i,j}$$

où ${}^t(A_{ij})_{i,j}$ est la transposée de la matrice des cofacteurs.

Une application simple de ce dernier théorème est la suivante: Une matrice 2×2 donnée par

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

est inversible si et seulement $ad - bc \neq 0$ et, dans ce cas,

$$\begin{aligned} A^{-1} &= \frac{1}{ad-bc} \times {}^t\begin{pmatrix} \Delta_{11} & -\Delta_{12} \\ -\Delta_{21} & \Delta_{22} \end{pmatrix} \\ &= \frac{1}{ad-bc} \times {}^t\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \\ &= \frac{1}{ad-bc} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} . \end{aligned}$$

14. Trace d'un endomorphisme

Si $A = (a_{ij})_{i,j}$ est une matrice carrée réelle d'ordre n, i.e. un élément de $\mathcal{M}_n(\mathbb{R})$, on définit la trace de A comme étant le réel donné par la relation

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

Le résultat suivant a lieu.

Lemme 14.1. *Pour toutes matrices $A, B \in \mathcal{M}_n(\mathbb{R})$, $tr(AB) = tr(BA)$. En particulier, deux matrices semblables $M, M' \in \mathcal{M}_n(\mathbb{R})$, c'est à dire reliées par une relation du type $M' = A^{-1}MA$, où $A \in \mathcal{M}_n(\mathbb{R})$ est inversible, ont même trace.*

Démonstration. On écrit $A = (a_{ij})_{i,j}$, $B = (b_{ij})_{i,j}$, $AB = (c_{ij})_{i,j}$ et $BA = (d_{ij})_{i,j}$. On a

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} \text{ et } d_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}$$

pour tous i, j. Donc

$$\mathrm{tr}(AB) = \sum_{i=1}^{n}\sum_{k-1}^{n} a_{ik}b_{ki} \text{ et } \mathrm{tr}(BA) = \sum_{i=1}^{n}\sum_{k=1}^{n} b_{ik}a_{ki}$$

et en inversant les rôles de i et k dans la seconde expression on obtient la première des deux affirmations du lemme. Pour ce qui est de la seconde, on écrit avec la première que

$$\mathrm{tr}(A^{-1}MA) = \mathrm{tr}(A^{-1}AM) = \mathrm{tr}(M) .$$

D'où le résultat. □

Ce lemme, et la formule de changement de base pour les endomorphismes, permet d'obtenir la définition suivante de la trace d'un endomorphisme.

Définition 14.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie. Soit $f \in End(E)$ un endomorphisme de E. On définit la trace de f par*

$$tr(f) = tr\big(M_{\mathcal{B}\mathcal{B}}(f)\big)$$

où $\mathcal{B}$ est une base quelconque de E. La définition fait sens car si $\mathcal{B}$ et $\mathcal{B}'$ sont deux bases de E, les matrices $M_{\mathcal{B}\mathcal{B}}(f)$ et $M_{\mathcal{B}'\mathcal{B}'}(f)$ sont semblables (formule de changement de bases pour les endomorphismes) et elles ont donc mêmes traces en vertue du lemme ci-dessus.

Exercice: Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ deux matrices carrées d'ordre n.
(1) On suppose que $\mathrm{tr}(A^t A) = 0$. Qu'en déduit-on sur A ?
(2) On suppose que $\mathrm{tr}(AM) = \mathrm{tr}(BM)$ pour toutes les matrices $M \in \mathcal{M}_n(\mathbb{R})$. Que peut-on dire de A et B ?

Solution: **(1)** Ecrivons $A = (a_{ij})$, ${}^tA = (b_{ij})$ et $A^tA = (c_{ij})$. On a $b_{ij} = a_{ji}$ pour tous i, j. Par multiplication des matrices,

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj} \ .$$

Par suite,

$$\mathrm{tr}(A^t A) = \sum_{i=1}^n \sum_{k=1}^n a_{ik} b_{ki} = \sum_{i=1}^n \sum_{k=1}^n a_{ik}^2 \ .$$

Donc $\mathrm{tr}(A^t A) = 0$ si et seulement si $a_{ik} = 0$ pour tout i et tout k, et donc si et seulement si $A = 0$ est la matrice nulle.

(2) Soient i_0, j_0 quelconques fixés. Ecrivons $A = (a_{ij})$, $B = (b_{ij})$ et notons $M(\delta)_{i_0 j_0}$ la matrice dont les coefficents λ_{ij} vérifient $\lambda_{i_0 j_0} = 1$ et $\lambda_{ij} = 0$ sinon. Ecrivons $AM(\delta)_{i_0 j_0} = (c_{ij})$ et $BM(\delta)_{i_0 j_0} = (d_{ij})$. Alors $c_{ij} = \sum_{k=1}^n a_{ik}\lambda_{kj}$, et donc

$$c_{ij} = \begin{cases} 0 \text{ si } j \neq j_0 \\ a_{ii_0} \text{ si } j = j_0 \ . \end{cases}$$

De même, $d_{ij} = \sum_{k=1}^n b_{ik}\lambda_{kj}$, et donc

$$d_{ij} = \begin{cases} 0 \text{ si } j \neq j_0 \\ b_{ii_0} \text{ si } j = j_0 \ . \end{cases}$$

Par suite, $\mathrm{tr}(AM(\delta)_{i_0 j_0}) = \mathrm{tr}(BM(\delta)_{i_0 j_0})$ si et seulement si $a_{j_0 i_0} = b_{j_0 i_0}$. Si $\mathrm{tr}(AM) = \mathrm{tr}(BM)$ pour toutes les matrices $M \in \mathcal{M}_n(\mathbb{R})$ alors, en particulier,

$$\mathrm{tr}(AM(\delta)_{i_0 j_0}) = \mathrm{tr}(BM(\delta)_{i_0 j_0})$$

pour tous i_0, j_0. Comme i_0 et j_0 sont quelconques, on voit que $\mathrm{tr}(AM) = \mathrm{tr}(BM)$ pour toutes les matrices $M \in \mathcal{M}_n(\mathbb{R})$ si et seulement si $A = B$. $\square$

CHAPITRE 3
RANG D'UNE MATRICE

Soient p, q deux entiers, et soit $A \in \mathcal{M}_{p,q}(\mathbb{R})$ une matrice réelle à p lignes et q colonnes. Soit aussi k un entier tel que $k \leq \min(p,q)$. On appelle sous matrice carrée d'ordre k de A toute matrice réelle carrée M d'ordre k, qui s'écrit sous la forme

$$M = \left(a_{i_s j_t}\right)$$

où s,t parcourent $\{1,\ldots,k\}$, les $i_1,\ldots,i_k$ sont une selection d'indices dans $\{1,\ldots,p\}$, et les $j_1,\ldots,j_k$ sont une selection d'indices dans $\{1,\ldots,q\}$.

En d'autres termes, une sous matrices carrée d'ordre $k \leq \min(p,q)$ d'une matrice A à p lignes et q colonnes est n'importe quelle matrice carrée d'ordre k que l'on obtient à partir de A en supprimant $p-k$ lignes et $q-k$ colonnes dans A (ou, de façon équivalente, en sélectionnant k lignes et k colonnes dans A). Si par exemple

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \end{pmatrix} \quad \text{et} \quad M = \begin{pmatrix} a_{12} & a_{13} & a_{15} \\ a_{32} & a_{33} & a_{35} \\ a_{42} & a_{43} & a_{45} \end{pmatrix}$$

alors M est la sous matrice 3×3 de A obtenue en supprimant à A la ligne 2 et les colonnes 1 et 4 (ou de façon équivalente en selectionnant dans A les lignes 1, 3, 4 et les colonnes 2, 3, 5):

$$A = \begin{pmatrix} \color{red}{a_{11}} & a_{12} & a_{13} & \color{red}{a_{14}} & a_{15} \\ \color{red}{a_{21}} & \color{red}{a_{22}} & \color{red}{a_{23}} & \color{red}{a_{24}} & \color{red}{a_{25}} \\ \color{red}{a_{31}} & a_{32} & a_{33} & \color{red}{a_{34}} & a_{35} \\ \color{red}{a_{41}} & a_{42} & a_{43} & \color{red}{a_{44}} & a_{45} \end{pmatrix},$$

en rouge ce qui est supprimé.

15. Définition du rang d'une matrice

Définition 15.1. *Soient p, q deux entiers, et soit $A \in \mathcal{M}_{p,q}(\mathbb{R})$ une matrice réelle non nulle à p lignes et q colonnes. Le rang de A, noté $Rg(A)$, est par définition le plus grand entier $r \leq \min(p,q)$ pour lequel on peut trouver une sous matrice carrée d'ordre r de A qui soit inversible.*

Par convention, on pose $\mathrm{Rg}(A) = 0$ si A est une matrice nulle. Dès que A est non nulle, $\mathrm{Rg}(A) \geq 1$ (il y a au moins une sous matrice 1×1 qui soit inversible... à savoir au moins un coefficient de A qui est non nul). Une définition équivalente du rang $\mathrm{Rg}(A)$ de A est

$$\mathrm{Rg}(A) = \max\left\{r \in \mathbb{N} \ / \ \exists M \text{ S.M.C. d'ordre } r \text{ de } A \text{ avec } \det(M) \neq 0\right\},$$

où S.M.C. signifie "Sous Matrice Carrée". Si $p = q$, on a bien sûr que A est inversible si et seulement si $\mathrm{Rg}(A) = p$.

Exercice: Soit a, b, c trois réels non tous nuls et soit la matrice

$$A = \begin{pmatrix} a^2 & ba & ca \\ ab & b^2 & cb \\ ac & bc & c^2 \end{pmatrix}.$$

Calculer le rang de A.

Solution: Le déterminant de cette matrice vaut

$$\Delta = a^2b^2c^2 + a^2b^2c^2 + a^2b^2c^2 - a^2b^2c^2 - a^2b^2c^2 - a^2b^2c^2 = 0 \ .$$

La matrice n'est donc pas de rang 3. Notons Δ_{ij} le déterminant de la matrice où l'on a supprimé la ième ligne et la jème colonne. Alors

$$\begin{aligned} &\Delta_{11} = b^2c^2 - b^2c^2 \ , \ \Delta_{12} = abc^2 - abc^2 \ , \ \Delta_{13} = ab^2c - ab^2c \\ &\Delta_{21} = bac^2 - bac^2 \ , \ \Delta_{22} = a^2c^2 - a^2c^2 \ , \ \Delta_{23} = a^2bc - a^2bc \\ &\Delta_{31} = b^2ac - b^2ac \ , \ \Delta_{32} = a^2bc - a^2bc \ , \ \Delta_{33} = a^2b^2 - a^2b^2 \ . \end{aligned}$$

Tous les sous déterminants 2×2 sont donc nuls. Donc le rang de la matrice n'est pas non plus égal à 2. Comme $(a,b,c) \neq (0,0,0)$ le rang de la matrice est au moins égal à 1 (un des coefficients de la matrice est non nul). On en déduit que $\mathrm{Rg}(A) = 1$.
□

16. Rang des matrices et des applications linéaires

Le théorème suivant est un des résultats importants de l'algèbre linéaire.

Théorème 16.1 (Théorème fondamental sur le rang des matrices et des applications linéaires)**.** *Soient E et F deux espaces vectoriels de dimensions finies, $\mathcal{B}$ une base de E, $\tilde{\mathcal{B}}$ une base de F, et $f \in L(E,F)$ une application linéaire de E dans F. Alors*

$$Rg\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) = Rg\big(f\big) \ .$$

En d'autres termes, le rang d'une application linéaire coïncide avec le rang de l'une quelconque de ses matrices de représentations.

La preuve de ce théorème est difficile. On la donne en appendice de ce chapitre.

Exercice: Soient E, F deux $\mathbb{R}$-espaces vectoriels de dimensions respectives 4 et 3, $\mathcal{B}$ une base de E, $\tilde{\mathcal{B}}$ une base de F, $f \in L(E,F)$ une application linéaire de E dans F et $A = M_{\mathcal{B}\tilde{\mathcal{B}}}$ la matrice de représentation de f dans $\mathcal{B}$ et $\tilde{\mathcal{B}}$ donnée par

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

où α, β sont deux réels. Déterminer les valeurs de α et β pour lesquelles f est surjective.

Solution: En vertue du théorème fondamental sur le rang des matrices et des applications linéaires il suffit de trouver les valeurs de α et β pour lesquelles la matrice A est de rang 3 (f est surjective si et seulement si $Rg(f) = 3$). La matrice A a quatre sous matrices 3×3 que l'on obtient en supprimant les colonnes 1, puis 2, puis 3, puis 4. Les quatre sous matrices 3×3 de A sont donc les matrices:

$$A_1 = \begin{pmatrix} 3 & \alpha & \beta \\ -1 & 2 & 1 \\ 1 & 2 & 0 \end{pmatrix} \ , \ A_2 = \begin{pmatrix} 1 & \alpha & \beta \\ 2 & 2 & 1 \\ -1 & 2 & 0 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 1 & 3 & \beta \\ 2 & -1 & 1 \\ -1 & 1 & 0 \end{pmatrix} \ , \ A_4 = \begin{pmatrix} 1 & 3 & \alpha \\ 2 & -1 & 2 \\ -1 & 1 & 2 \end{pmatrix} \ .$$

Leurs déterminants sont donnés par

$$\det A_1 = \alpha - 4\beta - 6\ ,\ \det(A_2) = 6\beta - \alpha - 2$$
$$\det(A_3) = \beta - 4\ ,\ \det(A_4) = \alpha - 22\ .$$

Il est donc déjà clair que A est de rang 3 si $\alpha \neq 22$ ou $\beta \neq 4$ puisque dans le premier cas $\det A_4 \neq 0$ tandis que $\det A_3 \neq 0$ dans le second. Reste à remarquer que si $\alpha = 22$ et $\beta = 4$ alors $\det(A_1) = \det(A_2) = \det(A_3) = \det(A_4) = 0$. Donc f est surjective si et seulement si $\alpha \neq 22$ ou $\beta \neq 4$. □

17. Matrices équivalentes

On commence par donner la définition de deux matrices équivalentes.

Définition 17.1. *Soient p, q deux entiers, et soient $A, B \in \mathcal{M}_{p,q}(\mathbb{R})$ deux matrices réelles à p lignes et q colonnes. On dit que les matrices A et B sont équivalentes s'il existe une matrice $P \in \mathcal{M}_p(\mathbb{R})$ carrée inversible d'ordre p, et une matrice $Q \in \mathcal{M}_q(\mathbb{R})$ carrée inversible d'ordre q, telles que $B = PAQ$.*

On vérifie que cette relation est bien une relation d'équivalence: à savoir refléxive, symétrique et transitive. En posant $P = \mathrm{Id}_p$ et $Q = \mathrm{Id}_q$, on voit qu'une matrice A est bien équivalente à elle-même. Par ailleurs, si $B = PAQ$, et si P et Q sont inversibles, alors $A = (P^{-1})B(Q^{-1})$ de sorte que si A est équivalente à B, alors B est équivalente à A. Pour finir, si $B = PAQ$, et si $C = \hat{P}B\hat{Q}$, alors

$$C = (\hat{P}P)A(Q\hat{Q})\ .$$

Le produit de deux matrices inversibles étant encore une matrice inversible, $\hat{P}P$ et $Q\hat{Q}$ sont des matrices inversibles. Il suit que si B est équivalente à A, et si C est équivalente à B, alors C est équivalente à A. La relation d'équivalence de matrices est bien une relation d'équivalence.

A titre de remarque, considérons E, F deux espaces vectoriels de dimensions finies, considérons $\mathcal{B}_1$, $\mathcal{B}_2$ deux bases de E, et considérons $\tilde{\mathcal{B}}_1$, $\tilde{\mathcal{B}}_2$ deux bases de F. Considérons de plus $f \in L(E, F)$ une application linéaire de E dans F. Les matrices de représentations $M_{\mathcal{B}_1\tilde{\mathcal{B}}_1}(f)$ et $M_{\mathcal{B}_2\tilde{\mathcal{B}}_2}(f)$ sont alors équivalentes. Cette propriété suit du théorème de changement de bases pour les matrices de représentations. Donc:

Proposition 17.1. *Etant données deux matrices de représentations d'une même application linéaire, elles sont toujours équivalentes.*

Une autre remarque élémentaire est la suivante. Etant donnés s et t deux entiers, notons $\mathrm{O}_{s,t}$ la matrice nulle à s lignes et t colonnes. Notons de même Id_r la matrice identité $r \times r$. Pour p et q deux entiers, et $r \leq \min(p, q)$, on construit la matrice A_r de $\mathcal{M}_{pq}(\mathbb{R})$ en posant

$$A_r = \begin{pmatrix} \mathrm{Id}_r & \mathrm{O}_{r,q-r} \\ \mathrm{O}_{p-r,r} & \mathrm{O}_{p-r,q-r} \end{pmatrix}\ .$$

Alors, clairement, A_r est de rang r. C'est même la plus simple des matrices de rang r que l'on puisse imaginer... Le théorème qui suit est une réciproque à cette remarque: puisqu'il affirme que toute matrice de $\mathcal{M}_{pq}(\mathbb{R})$ qui est de rang r est équivalente à A_r.

Théorème 17.1. *Si une matrice $A \in \mathcal{M}_{pq}(\mathbb{R})$ est de rang r, alors elle est équivalente à la matrice*
$$A_r = \begin{pmatrix} Id_r & O_{r,q-r} \\ O_{p-r,r} & O_{p-r,q-r} \end{pmatrix}$$
où Id_r est la matrice identité $r \times r$, et $O_{s,t}$ est la matrice nulle à s lignes et t colonnes.

Démonstration. On considère E et F deux $\mathbb{R}$-espaces vectoriels de dimensions respectives q et p, $\mathcal{B}_1$ une base de E, et $\tilde{\mathcal{B}}_1$ une base de F. On considère de plus $f \in L(E,F)$ définie par la propriété que $M_{\mathcal{B}_1\tilde{\mathcal{B}}_1}(f) = A$. Le théorème du rang nous dit que
$$\text{dimKer}(f) + \text{Rg}(f) = \text{dim}E \ ,$$
tandis qu'il suit du théorème précédent que $\text{Rg}(f) = r$, où $r = \text{Rg}(A)$. Ainsi, $\text{dimKer}(f) = q - r$. En utilisant le théorème de la base incomplète, en considérant une base de $\text{Ker}(f)$ puis en la complétant, on construit facilement une base $\mathcal{B}_2 = (e_1^2, \dots, e_q^2)$ de E pour laquelle $(e_{r+1}^2, \dots, e_q^2)$ est une base de $Ker(f)$. Il suit que la famille $\big(f(e_1^2), \dots, f(e_r^2)\big)$ est une base de $\text{Im}(f)$. Elle est en effet clairement génératrice pour $\text{Im}(f)$, et elle a autant d'éléments que la dimension de $\text{Im}(f)$ (qui vaut, par définition, $\text{Rg}(f)$). On applique de nouveau le théorème de la base incomplète pour fabriquer une base $\tilde{\mathcal{B}}_2$ de F dont les r premiers vecteurs sont les $f(e_i^2)$, $i = 1, \dots, r$. Alors, par construction même,
$$M_{\mathcal{B}_2\tilde{\mathcal{B}}_2}(f) = \begin{pmatrix} \text{Id}_r & \text{O}_{r,q-r} \\ \text{O}_{p-r,r} & \text{O}_{p-r,q-r} \end{pmatrix}$$
Les matrices $M_{\mathcal{B}_1\tilde{\mathcal{B}}_1}(f)$ et $M_{\mathcal{B}_2\tilde{\mathcal{B}}_2}(f)$ étant équivalentes d'après le théorème de changement de base (cf. remarque ci-dessus), il suit que A est bien équivalente à A_r. Le théorème est démontré. □

Le corollaire suivant a lieu.

Corollaire 17.1. *Si $A, B \in \mathcal{M}_{pq}(\mathbb{R})$ ont même rang, alors elles sont équivalentes. Inversement, deux matrices équivalentes ont même rang.*

Démonstration. Si A et B ont même rang, disons r, elles sont toutes deux équivalentes à la matrice A_r du théorème précédent. La relation d'équivalence de matrices étant une relation d'équivalence, elles sont équivalentes entres elles. Inversement, supposons que les matrices A et B sont équivalentes, et donc supposons qu'il existe des matrices inversibles P et Q telles que $B = PAQ$. On considère E un $\mathbb{R}$-espace vectoriel de dimension q, F un $\mathbb{R}$-espace vectoriel de dimension p, $\mathcal{B}$ une base de E, $\tilde{\mathcal{B}}$ une base de F, $f \in L(E,F)$ telle que $M_{\mathcal{B}\tilde{\mathcal{B}}}(f) = A$, $g \in L(E,F)$ telle que $M_{\mathcal{B}\tilde{\mathcal{B}}}(g) = B$, $\varphi \in End(E)$ telle que $M_{\mathcal{B}\mathcal{B}}(\varphi) = Q$, et $\psi \in End(F)$ telle que $M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(\psi) = P$. Alors, en vertue du théorème de composition des matrices de représentations, et comme $B = PAQ$,
$$\begin{aligned} M_{\mathcal{B}\tilde{\mathcal{B}}}(g) &= M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(\psi) M_{\mathcal{B}\tilde{\mathcal{B}}}(f) M_{\mathcal{B}\mathcal{B}}(\varphi) \\ &= M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(\psi) M_{\mathcal{B}\tilde{\mathcal{B}}}(f \circ \varphi) \\ &= M_{\mathcal{B}\tilde{\mathcal{B}}}(\psi \circ f \circ \varphi) \end{aligned}$$
de sorte que $g = \psi \circ f \circ \varphi$. Or φ et ψ sont des isomorphismes puisque P et Q sont des matrices inversibles. Cela entraîne que $\text{Rg}(g) = \text{Rg}(f)$, puis que $\text{Rg}(A) = \text{Rg}(B)$ en vertue de ce qui a été dit plus haut. Pour voir que $\text{Rg}(g) = \text{Rg}(f)$, on applique tout

simplement la définition du rang, et on remarque qu'un isomorphisme ne change pas la dimension d'un sous espace vectoriel (si X est un sous espace vectoriel d'un espace vectoriel Y, et si Φ est un isomorphisme de Y sur Z, alors Φ réalise un isomorphisme de X sur $\Phi(X)$ de sorte que $\Phi(X)$ a même dimension que X). En particulier, le corollaire est démontré. □

Exercice: Montrer qu'une matrice $A \in \mathcal{M}_{pq}(\mathbb{R})$ qui est de rang r s'écrit comme somme de r matrices de rang 1.

Solution: On a vu que A est équivalente à la matrice

$$A_r = \begin{pmatrix} \mathrm{Id}_r & \mathrm{O}_{r,q-r} \\ \mathrm{O}_{p-r,r} & \mathrm{O}_{p-r,q-r} \end{pmatrix}$$

où Id_r est la matrice identité $r \times r$, et $\mathrm{O}_{s,t}$ est la matrice nulle à s lignes et t colonnes. Donc il existe P et Q inversibles telles que

$$A = PA_rQ \ .$$

Pour $i = 1, \ldots, r$ notons $A_r(i)$ la matrice dont tous les coefficients sont nuls sauf le coefficient à la $i$ème ligne et $i$ème colonne qui vaut 1. Clairement $Rg(A_r(i)) = 1$, et de façon toute aussi claire, $A_r = \sum_{i=1}^r A_r(i)$. On peut écrire que

$$A = \sum_{i=1}^r PA_r(i)Q$$

et les matrices $PA_r(i)Q$ sont de rang 1 puisqu'elles sont équivalentes aux matrices $A_r(i)$ qui sont de rang 1. □

18. Rang des matrices, lignes et colonnes indépendantes

Dans la pratique calculer le rang d'une matrice revient souvent à compter le nombre maximal de lignes et de colonnes qui forment des vecteurs indépendants.

Théorème 18.1. *Soit $A \in \mathcal{M}_{pq}(\mathbb{R})$ une matrice réelle. Le rang de A est égal au nombre maximal de colonnes formant une famille libre de vecteurs dans $\mathbb{R}^p$.*

Démonstration. Notons $\mathcal{B}, \tilde{\mathcal{B}}$ les bases canoniques de $\mathbb{R}^q$ et $\mathbb{R}^p$. Soit aussi $f \in L(\mathbb{R}^q, \mathbb{R}^p)$ l'application linéaire donnée par $M_{\mathcal{B}\tilde{\mathcal{B}}}(f) = A$. Notons e_i les vecteurs de $\mathcal{B}$ et $\tilde{e}_i$ les vecteurs de $\tilde{\mathcal{B}}$. Supposons qu'il y ait k colonnes de A formant une famille libre de vecteurs dans $\mathbb{R}^p$. On note $j_1, \ldots, j_k$ les numéros de ces colonnes, qui correspondent donc, par définition des matrices de représentation, aux coordonnées dans $\tilde{\mathcal{B}}$ des vecteurs $f(e_{j_1}), \ldots, f(e_{j_k})$. On a donc une famille libre $(f(e_{j_1}), \ldots, f(e_{j_k}))$ dans $\mathrm{Im}(f)$. Donc $\mathrm{Rg}(f) \geq k$. Ce qui implique que $\mathrm{Rg}(A) \geq k$ en vertue du theórème 16.1. On a donc montré que

$$\mathrm{Rg}(A) \geq \text{nombre maximal de colonnes formant une famille libre} \qquad (18.1)$$

(de vecteurs dans $\mathbb{R}^p$). Supposons maintenant que l'on ait une sous matrice carrée de A de taille $k \times k$ qui soit inversible. Cette sous matrice correspond à une sélection des lignes $i_1, \ldots, i_k$ et des colonnes $j_1, \ldots, j_k$. On considère les vecteurs U_m de $\mathbb{R}^p$ dont les coordonnées dans la base canonique de $\mathbb{R}^p$ sont les éléments de la $j_m$ème colonne de A. On prétend que la famille $(U_1, \ldots, U_k)$ est libre, ce qui suffit à montrer le théorème puisqu'alors

$$k \leq \text{nombre maximal de colonnes formant une famille libre}$$

(de vecteurs dans $\mathbb{R}^p$) et cette propriété entraîne donc l'inégalité inverse de (18.1). Supposons que $\sum_{m=1}^k \lambda_m U_m = 0$ dans $\mathbb{R}^p$. Alors, en particulier,

$$\sum_{m=1}^k \lambda_m a_{ij_m} = 0$$

pour tout $i = i_1, \dots, i_k$. D'un point de vue matriciel cela revient à écrire que

$$\begin{pmatrix} a_{i_1j_1} & \dots & a_{i_1j_k} \\ \vdots & & \vdots \\ a_{i_kj_1} & \dots & a_{i_kj_k} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} .$$

Or, par hypothèse, la matrice carrée

$$A_k = \begin{pmatrix} a_{i_1j_1} & \dots & a_{i_1j_k} \\ \vdots & & \vdots \\ a_{i_kj_1} & \dots & a_{i_kj_k} \end{pmatrix}$$

est inversible. On en déduit donc que $\lambda_i = 0$ pour tout $i = 1, \dots, k$. Ce qui termine la démonstration du théorème. □

Pour passer des colonnes aux lignes, il suffit de démontrer le théorème suivant.

Théorème 18.2. *Soit $A \in \mathcal{M}_{pq}(\mathbb{R})$ une matrice réelle. Le rang de A est égal au rang de la transposée ${}^tA$ de A.*

Démonstration. Si A est de rang r alors, en vertue du théorème 17.1, A est équivalente à

$$A_r = \begin{pmatrix} \mathrm{Id}_r & \mathrm{O}_{r,q-r} \\ \mathrm{O}_{p-r,r} & \mathrm{O}_{p-r,q-r} \end{pmatrix}$$

Mais si $A = PA_rQ$ avec P et Q inversibles, alors ${}^tA = {}^tQ{}^tA_r{}^tP$ et, comme ${}^tP$ et ${}^tQ$ sont encore inversibles, ${}^tA$ est équivalente à ${}^tA_r$. Or

$${}^tA_r = \begin{pmatrix} \mathrm{Id}_r & \mathrm{O}_{r,p-r} \\ \mathrm{O}_{q-r,r} & \mathrm{O}_{q-r,p-r} \end{pmatrix}$$

est toujours de rang r. En vertue du corollaire 17.1 cela entraîne que $\mathrm{Rg}({}^tA) = r$. D'où le théorème. □

De ces deux théorèmes on déduit immédiatement le théorème suivant.

Théorème 18.3. *Soit $A \in \mathcal{M}_{pq}(\mathbb{R})$ une matrice réelle. Le rang de A est égal au nombre maximal de lignes formant une famille libre de vecteurs dans $\mathbb{R}^q$.*

Démonstration. La transposition transforme les lignes en colonnes et ne change pas le rang en vertue de ce que l'on vient de démontrer. Reste à appliquer le premier théorème de cette section. □

19. Rang des matrices échelonnées

Une matrice A est dite échelonnée (en lignes) si les deux points suivants sont vérifiés:

(i) toute ligne non nulle de A commence avec strictement plus de zéros que la ligne précédente,

(ii) en-dessous d'une ligne nulle, toutes les lignes sont nulles.

Les matrices A et B ci-dessous

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

sont par exemple échelonnées. Leurs rangs est égal respectivement à 3 et 2 qui correspond au nombre de ses lignes non nulles. On démontre le résultat suivant.

Théorème 19.1. *Le rang d'une matrice échelonnée est égal au nombre de ses lignes non nulles.*

Démonstration. Notons $A = (a_{ij})$. Soit k le nombre de lignes non nulles de A. Alors

(i) $\forall i \geq k+1, \forall j, a_{ij} = 0$.

Clairement on en déduit que $\mathrm{Rg}(A) \leq k$ puisqu'une sous matrice carrée qui contiendrait plus de $k+1$ lignes aurait forcément une ligne nulle et serait donc de déterminant nul. Supposons que l'on trouve k colonnes de A formant une famille de k vecteurs linéairement indépendants. Alors, en regardant A comme la matrice de représentation d'une application linéaire entre espaces $\mathbb{R}^p$ et $\mathbb{R}^q$ (matrice de représentation que l'on prendra par exemple dans les bases canoniques de ses espaces), alors $\mathrm{Im}(f)$ contiendrait une famille libre de k vecteurs. On aurait donc $\mathrm{Rg}(f) \geq k$, et donc en particulier $\mathrm{Rg}(A) \geq k$. Soit en conclusion $\mathrm{Rg}(A) = k$, et pour résumer il suffit de trouver k colonnes de A formant une famille de vecteurs libres. Pour $1 \leq i \leq k$, on note j_i l'ordre du premier élément non nul sur la ième ligne:

(ii) $a_{ij_i} \neq 0$ et $a_{ij} = 0$ pour tout $j < j_i$.

On a alors aussi que

(iii) $a_{mj_i} = 0$ pour tout $m > i$.

On montre que les colonnes $j_1, j_2, \ldots, j_k$ sont les colonnes que nous recherchons. En considérant que la matrice A était à p lignes et q colonnes, on considère donc les vecteurs U_m, $m = 1, \ldots, k$, formés par les colonnes

$$U_j = \begin{pmatrix} a_{1j_m} \\ \vdots \\ a_{pj_m} \end{pmatrix} \ .$$

Supposons que

$$\sum_{m=1}^{k} \lambda_m U_m = 0 \ .$$

Alors

$$\sum_{m=1}^{k} \lambda_m a_{ij_m} = 0$$

pour tout $i = 1, \ldots, p$, et en fait pour tout $i = 1, \ldots, k$. D'un point de vue matriciel on a alors écrit que

$$\begin{pmatrix} a_{1j_1} & \ldots & a_{1j_k} \\ \vdots & & \vdots \\ a_{kj_1} & \ldots & a_{kj_k} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \ .$$

La matrice carrée qui intervient dans cette équation est diagonale supérieure en raison de (iii) et sa diagonale est constituée des $a_{ij_i} \neq 0$ par (ii). Le déterminant d'une telle matrice est égal au produit des termes diagonaux (on le voit en développant suivant colonnes) et donc non nul. La matrice est ainsi inversible ce qui implique que tous les λ_m sont nuls. On a bien trouvé nos k colonnes formant une famille libre de vecteurs. $\square$

20. Preuve du Théorème 16.1

On découpe la preuve en deux étapes. On montre en première étape que

(1) $\mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \leq \mathrm{Rg}\big(f\big)$

On montre en seconde étape que

(2) $\mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \geq \mathrm{Rg}\big(f\big)$.

On commence par montrer la première étape. C'est la plus simple des deux. On procède là comme dans la preuve du Théorème 18.1.

(1) On montre que $\mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \leq \mathrm{Rg}\big(f\big)$. Notons $k = \mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big)$, $(e_1, \ldots, e_m)$ les vecteurs de $\mathcal{B}$, et $(\tilde{e}_1, \ldots, \tilde{e}_n)$ les vecteurs de $\tilde{\mathcal{B}}$. Dire que $k = \mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big)$, c'est dire que $M_{\mathcal{B}\tilde{\mathcal{B}}}(f)$ possède une sous matrice carrée d'ordre k qui est inversible. Si $M_{\mathcal{B}\tilde{\mathcal{B}}}(f) = (a_{ij})_{i,j}$, notons $M = (a_{i_s j_t})_{s,t}$ la (une des) sous matrice(s) d'ordre k de $M_{\mathcal{B}\tilde{\mathcal{B}}}(f)$ qui est inversible. Pour montrer que $\mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \leq \mathrm{Rg}\big(f\big)$, il suffit de montrer que la famille $\big(f(e_{j_1}), \ldots, f(e_{j_k})\big)$ est libre. En effet, si cette famille est libre, on devra avoir $k \leq \mathrm{dimIm}(f)$, et donc $k \leq \mathrm{Rg}(f)$. Pour montrer que cette famille est libre, supposons que pour des réels $\lambda_1, \ldots, \lambda_k$,

$$\lambda_1 f(e_{j_1}) + \cdots + \lambda_k f(e_{j_k}) = 0 \ .$$

Alors

$$\sum_{i=1}^{n}\Big(\sum_{t=1}^{k}\lambda_t a_{ij_t}\Big)\tilde{e}_i = 0 \ .$$

Puisque les $\tilde{e}_i$ forment une base de F, on récupère que

$$\sum_{t=1}^{k}\lambda_t a_{ij_t} = 0$$

pour tout $i = 1, \ldots, n$. En particulier, pour tout $s = 1, \ldots, k$, $\sum_{t=1}^{k}\lambda_t a_{i_s j_t} = 0$, ce qui s'écrit encore $M\Lambda = 0$, où Λ est la matrice à k lignes et une colonne composée des λ_t, et 0 est la matrice nulle à une colonne et k lignes. Comme M est inversible, $M\Lambda = 0$ entraîne que $\Lambda = 0$, ce qui prouve que la famille $\big(f(e_{j_1}), \ldots, f(e_{j_k})\big)$ est libre. Comme déjà dit, cela entraîne à son tour que $\mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \leq \mathrm{Rg}\big(f\big)$.

(2) Plus difficile, on montre que $\mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \geq \mathrm{Rg}\big(f\big)$. On note $(e_1, \ldots, e_m)$ les vecteurs de $\mathcal{B}$, et $(\tilde{e}_1, \ldots, \tilde{e}_n)$ les vecteurs de $\tilde{\mathcal{B}}$. Une remarque déjà utilisée dans les cours précédents est la suivante: si on note $k = \mathrm{Rg}(f)$, le rang de f, alors il existe $j_1, \ldots, j_k \in \{1, \ldots, m\}$ pour lesquels la famille $\big(f(e_{j_1}), \ldots, f(e_{j_k})\big)$ est une base de $\mathrm{Im}(f)$. Pour le voir, on sait que la famille $\big(f(e_1), \ldots, f(e_n)\big)$ est une famille génératrice de $\mathrm{Im}(f)$. Si elle est libre, c'est une base de $Im(f)$ et la propriété est vraie. Si elle n'est pas libre, un des vecteurs de la famille s'exprime comme combinaison linéaire des autres. On peut alors le retirer à la famille sans changer sons caractère de famille génératrice. Et ainsi de suite jusqu'à obtenir une

famille génératrice de $\text{Im}(f)$ ayant autant de vecteurs que la dimension de $\text{Im}(f)$, ce qui en fait une base de $\text{Im}(f)$. A partir de cette propriété, on montre que $\text{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \geq \text{Rg}\big(f\big)$ en raisonnant par récurrence sur l'entier

$$r = \text{dim}F - \text{Rg}(f)$$

et donc sur $r = n - k$. Etant donné r un entier, la propriété à démontrer au rang r s'énonce: si E, F sont deux espaces vectoriels de dimensions finies, si $\mathcal{B}$ est une base de E, si $\tilde{\mathcal{B}}$ est une base de F, si $f \in L(E, F)$ est une application linéaire de E dans F, et si $\text{dim}F - \text{Rg}(f) = r$, alors $\text{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \geq \text{Rg}\big(f\big)$. On démontre tout d'abord que la propriété est vraie au rang $r = 0$. Puis on démontre que si la propriété est vraie aux rangs $0, 1, \dots, r-1, r$, alors elle est aussi vraie au rang $r+1$. Supposons tout d'abord que $r = 0$. Soit $(e_{j_1}, \dots, e_{j_k})$ la sous famille de $\mathcal{B}$ donnée par la propriété ci-dessus, donc qui est telle que la famille $\big(f(e_{j_1}), \dots, f(e_{j_k})\big)$ est une base de $\text{Im}(f)$. Si E_k est le sous espace vectoriel de E de base $\mathcal{B}_k = (e_{j_1}, \dots, e_{j_k})$, et si f_k est la restriction de f à E_k, la matrice de représentation $M_{\mathcal{B}_k\tilde{\mathcal{B}}}(f_k)$ de f_k dans les bases $\mathcal{B}_k$ et $\tilde{\mathcal{B}}$ est une sous matrice carrée d'ordre k de la matrice $M_{\mathcal{B}\tilde{\mathcal{B}}}(f)$. Elle s'obtient en selectionnant les colonnes $j_1, \dots, j_k$ de cette matrice. Or $f_k : E_k \to F$ est surjective (par construction), et $\text{dim}E_k = \text{dim}F$ (par hypothèse, puisque $r = 0$). Donc f_k est un isomorphisme de E_k sur F. Donc $M_{\mathcal{B}_k\tilde{\mathcal{B}}}(f_k)$ est inversible. Donc, en particulier, puisque cette matrice est d'ordre k, $\text{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \geq k = \text{Rg}(f)$. Si $r = 0$, on a donc bien que $\text{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \geq \text{Rg}\big(f\big)$.

Supposons maintenant la propriété à démontrer vraie aux ordres $0, 1, \dots, r-1, r$. On veut montrer que la propriété est alors aussi vraie à l'ordre $r + 1$. On suppose donc que $r+1 = n-k$. On note là encore $(e_{j_1}, \dots, e_{j_k})$ la sous famille de $\mathcal{B}$ donnée par la propriété ci-dessus, donc qui est telle que la famille $\big(f(e_{j_1}), \dots, f(e_{j_k})\big)$ est une base de $\text{Im}(f)$. Comme $k < n$, il existe forcément un vecteur $\tilde{e}_{i_0}$ de $\tilde{\mathcal{B}}$ qui est tel que

$$\tilde{e}_{i_0} \notin \text{Vect}\big(f(e_{j_1}), \dots, f(e_{j_k})\big) \tag{1}$$

Pour $j = 1, \dots, m$, soit λ_j la $i_0$ème coordonnée de $f(e_j)$ dans $\tilde{\mathcal{B}}$. On définit l'application linéaire $g : E \to F$ en posant

$$g(e_j) = f(e_j) - \lambda_j \tilde{e}_{i_0}$$

pour tout $j = 1, \dots, m$. Soit de plus F_{n-1} le sous espace vectoriel de F de base la famille $\tilde{\mathcal{B}}_{n-1}$ composée des $\tilde{e}_i$, $i \neq i_0$. Alors $g \in L(E, F_{n-1})$. Une première propriété évidente est la suivante:

(i) $M_{\mathcal{B}\tilde{\mathcal{B}}_{n-1}}(g)$ est une sous matrice de $M_{\mathcal{B}\tilde{\mathcal{B}}}(f)$

au sens où la matrice $M_{\mathcal{B}\tilde{\mathcal{B}}_{n-1}}(g)$ s'obtient à partir de $M_{\mathcal{B}\tilde{\mathcal{B}}}(f)$ en supprimant à cette matrice sa $i_0$ème ligne. Une autre propriété de g est la suivante:

(ii) $\text{Rg}(g) \geq \text{Rg}(f)$.

Cette propriété suit de la relation (1). Avec cette relation on vérifie en effet facilement que le famille $\big(g(e_{j_1}), \dots, g(e_{j_k})\big)$ est libre. Pour le voir, on remarque que si

$$\lambda_1 g(e_{j_1}) + \cdots + \lambda_k g(e_{j_k}) = 0$$

alors

$$\sum_{t=1}^{k} \lambda_t f(e_{j_t}) = \lambda e_{i_0} \ ,$$

où $\lambda = \sum_{t=1}^{k} \lambda_t \lambda_{j_t}$. Du coup (1), entraîne que $\lambda = 0$, puis on obtient que les λ_t doivent tous être nuls puisque les $f(e_{j_t})$, $t = 1, \dots, k$, forment une famille libre. Il suit que $\mathrm{Rg}(g) \geq k$, et donc que $\mathrm{Rg}(g) \geq \mathrm{Rg}(f)$, ce qui démontre (ii).

On avait $r+1 = \mathrm{dim}F - \mathrm{Rg}(f)$. Puisque $\mathrm{dim}F_{n-1} = dimF - 1$, et $\mathrm{Rg}(g) \geq \mathrm{Rg}(f)$, on en déduit que

$$\mathrm{dim}F_{n-1} - \mathrm{Rg}(g) \in \{1, \dots, r\} \ .$$

Par hypothèse de récurrence, il existe ainsi une sous matrice carrée d'ordre $\mathrm{Rg}(g)$ de la matrice $M_{\mathcal{B}\tilde{\mathcal{B}}_{n-1}}(g)$ qui est inversible. Avec (i), on en déduit qu'il existe une sous matrice carrée d'ordre $\mathrm{Rg}(g)$ de la matrice $M_{\mathcal{B}\tilde{\mathcal{B}}}(f)$ qui est inversible. Donc,

$$\mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \geq \mathrm{Rg}\big(g\big) \geq \mathrm{Rg}\big(f\big)$$

et on a montré que si la propriété à démontrer était vraie aux ordres $0, \dots, r$, alors elle l'était aussi à l'ordre $r+1$.

Par récurrence, sachant que la propriété à démontrer est vraie à l'ordre 0, et sachant que si la propriété est vraie aux ordres $0, \dots, r$, alors elle est vraie à l'ordre $r+1$, on obtient que la propriété est toujours vraie. On a donc montré que à la fois $\mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \leq \mathrm{Rg}\big(f\big)$ et $\mathrm{Rg}\big(M_{\mathcal{B}\tilde{\mathcal{B}}}(f)\big) \geq \mathrm{Rg}\big(f\big)$, ce qui démontre le théorème.

CHAPITRE 4

DIAGONALISATION

On continue de ne considérer que le cas d'espaces vectoriels réels. Une théorie analogue (importante) existe pour les espaces vectoriels complexes. Une différence essentielle entre $\mathbb{R}$ et $\mathbb{C}$ étant que $\mathbb{C}$ est algébriquement clos: les polynômes complexes se factorisent sur $\mathbb{C}$ en produits de polynômes de degré 1 (avec racines donc). Dans $\mathbb{R}$ ce n'est plus vrai. Exemple: x^2+1 ne se factorise pas dans $\mathbb{R}$ (alors que regardé dans $\mathbb{C}$, $x^2+1=(x-i)(x+i)$ et il se factorise). On commence par traiter du point de vue des endomorphismes, pour traiter ensuite du point de vue des matrices. La question générale qui est posée est la suivante:

Etant donné un endomorphisme f d'un $\mathbb{R}$-espace vectoriel E de dimension finie, parmi toutes les représentations possibles $M_{\mathcal{BB}}(f)$ de f, où $\mathcal{B}$ est une base de E, y en a-t-il une qui soit plus pertinente, plus esthétique, plus facile à manier que les autres ?

Dans une théorie de diagonalisation, la représentation plus pertinente que l'on cherche est une représentation diagonale. La question devient donc: “ *parmi toutes les représentations possibles $M_{\mathcal{BB}}(f)$ de f, y en a-t-il une qui soit diagonale ?* ”

21. Analyse de la problématique

On montre dans cette courte section comment plusieurs notions introduites de façon un peu arbitraire dans la suite apparaissent en fait naturellement. Soit E un $\mathbb{R}$-espace vectoriel de dimension finie, et $f\in\mathrm{End}(E)$ un endomorphisme de E. Supposons qu'il existe une base $\mathcal{B}$ de E pour laquelle $M_{\mathcal{BB}}(f)$ est diagonale. Ecrivons que $\mathcal{B}=(e_1,\dots,e_n)$ et que

$$M_{\mathcal{BB}}(f)=\begin{pmatrix}\lambda_1 & 0 & \dots & 0\\ 0 & \lambda_2 & \dots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \dots & \lambda_n\end{pmatrix} \tag{21.1}$$

où les $\lambda_i\in\mathbb{R}$. Par définition des matrices de représentation on a alors que:

$$\forall i=1,\dots,n,\ f(e_i)=\lambda_i e_i\ .$$

La question étant peut-on trouver une base $(e_1,\dots,e_n)$ et des λ_i tels que (21.1) ait lieu, et si oui, comment les trouver, on a donc tout intérêt à s'intéresser à l'équation en λ et u,

$$f(u)=\lambda u\ .$$

C'est là l'équation des valeurs et vecteurs propres (cf. Section 22). Dans cette équation on veut $\lambda\in\mathbb{R}$ et $u\in E\backslash\{0\}$. On peut récrire l'équation sous la forme $(f-\lambda\mathrm{Id}_E)(u)=0$ et on voit alors que u résoud l'équation pour un λ donné si $u\in\mathrm{Ker}(f-\lambda\mathrm{Id}_E)$. Plus précisément, résoudre l'équation revient à trouver les λ (s'il en existe) pour lesquels $\mathrm{Ker}(f-\lambda\mathrm{Id}_E)\neq\{0\}$, et ensuite on a tous les u associés dans $\mathrm{Ker}(f-\lambda\mathrm{Id}_E)\backslash\{0\}$. Dire que $\mathrm{Ker}(f-\lambda\mathrm{Id}_E)\neq\{0\}$ c'est dire que $f-\lambda\mathrm{Id}_E$ n'est pas injective, et ensuite, puisque l'on parle d'endomorphismes en dimension finie, c'est dire que $f-\lambda\mathrm{Id}_E$ n'est pas inversible. Et cela c'est une problématique qui s'étudie facilement avec les déterminants. On fixe une base $\mathcal{B}_0$ quelconque de E. On pose

$$P(X) = \det\left(M_{\mathcal{B}_0\mathcal{B}_0}(f - X\mathrm{Id}_E)\right)$$

et on remarque que, d'une part P est un polynôme de degré n (définition du déterminant), et que d'autre part $f - \lambda\mathrm{Id}_E$ n'est pas inversible si et seulement $P(\lambda) = 0$ (puisque une application linéaire est inversible si et seulement l'une quelconque de ses matrices de représentations l'est). Avec cette simple analyse on est déjà arrivé à la notion de polynôme caractéristique dont les racines sont précisément les λ que l'on cherche. Un première application: un polynôme de degré impair change forcément de signe. En dimension impaire il y a donc forcément au moins un $\lambda \in \mathbb{R}$ pour lequel l'équation $f(u) = \lambda u$ va avoir des solutions.

22. Premiers éléments

On commence avec les notions fondamentales de valeurs et vecteurs propres.

Définition 22.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie, et $f \in End(E)$ un endomorphisme de E. On dit que $\lambda \in \mathbb{R}$ est une valeur propre de f s'il existe un vecteur $u \in E$, $u \neq 0$, tel que*

$$f(u) = \lambda u \ .$$

Dans ce cas, u est dit vecteur propre de f associé à la valeur propre λ. Si λ est une valeur propre de f, on note E_λ l'espace propre de f associé à λ, défini par $E_\lambda = \left\{u \in E \ / \ f(u) = \lambda u\right\}$.

La proposition suivante a lieu.

Proposition 22.1. *E_λ est un sous espace vectoriel de E.*

Démonstration. Soient $x, y \in E_\lambda$ et $t \in \mathbb{R}$ quelconques, alors $f(x + ty) = f(x) + tf(y) = \lambda x + t\lambda y = \lambda(x + ty)$ et donc $x + ty \in E_\lambda$. La proposition est démontrée. $\square$

Le théorème suivant a lieu.

Théorème 22.1. *Un réel λ est valeur propre d'un endomorphisme f si et seulement si l'endomorphisme $f - \lambda Id_E$ n'est pas inversible. Dans ce cas,*

$$E_\lambda = Ker\big(f - \lambda Id_E\big) \ ,$$

où $f - \lambda Id_E$ est l'endomorphisme de E défini pour tout $x \in E$ par $\big(f - \lambda Id_E\big)(x) = f(x) - \lambda x$.

Démonstration. Il suffit de se souvenir qu'un endomorphisme $g \in \mathrm{End}(E)$ (ici $g = f - \lambda\mathrm{Id}_E$) est inversible si et seulement si il est injectif, et donc si et seulement si $\mathrm{Ker}(g) = \{0\}$. Et bien évidemment dire qu'il existe $u \neq 0$ tel que $f(u) = \lambda u$ équivaut à dire que $\mathrm{Ker}\big(f - \lambda\mathrm{Id}_E\big) \neq \{0\}$. Il est ensuite facile de voir que $E_\lambda = \mathrm{Ker}(f - \lambda\mathrm{Id}_E)$. Le théorème est démontré. $\square$

Le théorème donne naturellement lieu à la définition suivante.

Définition 22.2. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie n et $f \in End(E)$ un endomorphisme de E. Soit $\mathcal{B}$ une base de E. On appelle polynôme caractéristique de f le polynôme*

$$P(X) = det\big(M_{\mathcal{B}\mathcal{B}}(f) - XId_n\big)$$

pour tout $X \in \mathbb{R}$.

Le théorème suivant a lieu.

Théorème 22.2. *Le polynôme caractéristique de f ne dépend pas du choix de la base $\mathcal{B}$. C'est un polynôme de degré n dont le terme dominant est $(-1)^n X^n$. Il est suivi du terme $(-1)^{n-1} tr(f) X^{n-1}$, où $tr(f)$ est la trace de l'endomorphisme f, et son terme constant vaut $det\big(M_{\mathcal{B}\mathcal{B}}(f)\big)$, une quantité qui ne dépend pas de $\mathcal{B}$.*

Puisque la quantité ne dépend pas du choix de $\mathcal{B}$, notons $\det(f)$ pour $\det\big(M_{\mathcal{B}\mathcal{B}}(f)\big)$. On a alors

$$P(X) = (-1)^n X^n + (-1)^{n-1}\mathrm{tr}(f) X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1 X + \det(f)$$

pour tout $X \in \mathbb{R}$, où les $a_1, a_2, \ldots, a_{n-2}$ sont des réels qui ne dépendent que de f.

Démonstration. (1) On montre que P ne dépend pas de $\mathcal{B}$ et donc que $\det\big(M_{\mathcal{B}\mathcal{B}}(f)\big) = P(0)$ ne dépend pas non plus de $\mathcal{B}$. Si $\mathcal{B}, \mathcal{B}'$ sont deux bases de E, et $\lambda \in \mathbb{R}$, alors

$$\begin{aligned}\det\big(M_{\mathcal{B}\mathcal{B}}(f) - \lambda \mathrm{Id}_n\big) &= \det\big(M_{\mathcal{B}\mathcal{B}}(f - \lambda \mathrm{Id}_E)\big) ,\\ \det\big(M_{\mathcal{B}'\mathcal{B}'}(f) - \lambda \mathrm{Id}_n\big) &= \det\big(M_{\mathcal{B}'\mathcal{B}'}(f - \lambda \mathrm{Id}_E)\big) .\end{aligned}$$

On remarquera ici que $M_{\mathcal{B}\mathcal{B}}(\mathrm{Id}_E) = \mathrm{Id}_n$ pour toute base $\mathcal{B}$. Si $g \in \mathrm{End}(E)$ est un endomorphisme de E on a, cf. Chapitre 1, que

$$M_{\mathcal{B}'\mathcal{B}'}(g) = M_{\mathcal{B}\to\mathcal{B}'}^{-1} M_{\mathcal{B}\mathcal{B}}(g) M_{\mathcal{B}\to\mathcal{B}'} .$$

On en déduit que

$$\begin{aligned}\det\left(M_{\mathcal{B}'\mathcal{B}'}(g)\right) &= \det\left(M_{\mathcal{B}\to\mathcal{B}'}^{-1}\right)\det\left(M_{\mathcal{B}\mathcal{B}}(g)\right)\det\left(M_{\mathcal{B}\to\mathcal{B}'}\right)\\ &= \frac{1}{\det\left(M_{\mathcal{B}\to\mathcal{B}'}\right)}\det\left(M_{\mathcal{B}\mathcal{B}}(g)\right)\det\left(M_{\mathcal{B}\to\mathcal{B}'}\right)\\ &= \det\left(M_{\mathcal{B}\mathcal{B}}(g)\right) .\end{aligned}$$

D'où l'affirmation que ni P ni $\det\big(M_{\mathcal{B}\mathcal{B}}(f)\big)$ ne dépendent de $\mathcal{B}$.

(2) On montre que P est bien un polynôme de degré n et on calcule les coefficients a_n, a_{n-1} et a_0 de P. On a

$$P(X) = \sum_{\sigma\in\mathcal{P}_n} \varepsilon(\sigma)\big(a_{1\sigma(1)} - X\delta_{1\sigma(1)}\big)\ldots\big(a_{n\sigma(n)} - X\delta_{n\sigma(n)}\big) ,$$

où les a_{ij} sont les coefficients de $M_{\mathcal{B}\mathcal{B}}(f)$. Donc P est bien un polynôme de degré n. Le terme en X^n et aussi le terme en X^{n-1} sont forcément donnés par la permutation $\sigma =$ identité. En effet, sinon (si $\sigma \neq$ identité) alors au moins deux éléments bougent, donc il existe $i \neq j$ tels que $\sigma(i) \neq i$ et $\sigma(j) \neq j$, donc $\delta_{i\sigma(i)} = \delta_{j\sigma(j)} = 0$ pour ces deux i et j, et alors le produit correspondant $\big(a_{1\sigma(1)} - X\delta_{1\sigma(1)}\big)\ldots\big(a_{n\sigma(n)} - X\delta_{n\sigma(n)}\big)$ est au plus de degré $n-2$. Une fois identifié que les termes d'ordres n et $n-1$ proviennent de $\sigma =$ identité on a que

$$\big(a_{1\sigma(1)} - X\delta_{1\sigma(1)}\big)\ldots\big(a_{n\sigma(n)} - X\delta_{n\sigma(n)}\big) = \big(a_{11} - X\big)\ldots\big(a_{nn} - X\big)$$

et on voit que le terme d'ordre n est $(-1)^n X^n$ tandis que le terme d'ordre $n-1$ est $(-1)^{n-1}\big(\sum_{i=1}^n a_{ii}\big)X^{n-1}$. Il est enfin facile de voir que le terme constant a_0 dans P est $P(0)$, qui vaut $\det\big(M_{\mathcal{B}\mathcal{B}}(f)\big)$. D'où le théorème. $\square$

Le théorème qui suit est une conséquence naturelle de ce qui a été dit plus haut.

Théorème 22.3. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie n, $f \in End(E)$ un endomorphisme de E et P son polynôme caractéristique. Alors $\lambda \in \mathbb{R}$ est valeur propre de f si et seulement si λ est racine de P (donc si et seulement si $P(\lambda) = 0$). En particulier, f a au plus n valeurs propres distinctes.*

Démonstration. On sait que λ est valeur propre de f si et seulement si $f - \lambda \mathrm{Id}_E$ n'est pas inversible. Etant donné $\mathcal{B}$ une base de E, un endomorphisme $g \in \mathrm{End}(E)$ est inversible si et seulement si $\det(M_{\mathcal{BB}}(g)) \neq 0$. Donc $\lambda \in \mathbb{R}$ est valeur propre de f si et seulement si $\det(M_{\mathcal{BB}}(f) - \lambda \mathrm{Id}_n) = 0$, ce qui revient à dire que λ est une racine de P. Un polynôme de degré n ayant au plus n racines distinctes, le théorème est démontré. $\square$

Remarque: une grosse différence avec la théorie complexe est que $\mathbb{C}$ est un corps algébriquement clos. En d'autre termes, un polynôme se factorise toujours dans $\mathbb{C}$ en produits de polynômes de degré 1 et a donc toujours n racines (distinctes ou pas) dans $\mathbb{C}$, alors qu'un polynôme peut très bien n'avoir aucune racine dans $\mathbb{R}$ (c'est la cas de $P(X) = X^2 + 1$ qui ne sa factorise pas dans $\mathbb{R}$ en produits de polynômes de degré 1, alors qu'il le fait dans $\mathbb{C}$ puisque $X^2 + 1 = (X - i)(X + i)$ dans $\mathbb{C}$). Un endomorphisme peut du coup ne pas avoir de valeurs propres dans $\mathbb{R}$. Soit f l'endomorphisme de $\mathbb{R}^2$ dont la matrice de représentation $M_{\mathcal{BB}}(f)$ dans la base canonique de $\mathbb{R}^2$ vaut

$$M_{\mathcal{BB}}(f) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} .$$

Donc $f(e_1) = -e_2$ et $f(e_2) = e_1$ si (e_1, e_2) est la base canonique de $\mathbb{R}^2$. Cet endomorphisme a pour polynôme caractéristique $P(X) = X^2 + 1$, et il n'a donc pas de valeurs propres dans $\mathbb{R}$. Si on se reporte à la discussion en début de chapitre, ou voir aussi la remarque ci-dessous, il n'a donc aucune chance d'avoir une matrice de représentation diagonale (et donc d'être diagonalisable en anticipant sur la définition qui suit).

Soit $A = (a_{ij})$ une matrice. On dit que A est diagonale si $a_{ij} = 0$ dès que $i \neq j$. Donc A est une matrice diagonale si A ne comporte que des termes diagonaux... La terminologie est bien choisie.

Définition 22.3. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie, et soit $f \in End(E)$ un endomorphisme de E. L'endomorphisme f est dit diagonalisable s'il existe une base $\mathcal{B}$ de E pour laquelle $M_{\mathcal{BB}}(f)$ est une matrice diagonale.*

Remarque: Si f est diagonalisable, alors le polynôme caractéristique P de f a toutes ses racines dans $\mathbb{R}$. En effet, en travaillant dans la base $\mathcal{B}$ qui diagonalise f, et si on note $\lambda_1, \dots, \lambda_n$ les termes diagonaux de $M_{\mathcal{BB}}(f)$, alors

$$M_{\mathcal{BB}}(f) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

et on récupère que

$$P(X) = (\lambda_1 - X) \dots (\lambda_n - X) .$$

Donc P a bien toutes ses racines dans $\mathbb{R}$ et ces racines sont les termes diagonaux λ_i de f (qui peuvent très bien être égaux entre eux pour certains d'entre eux).

23. Le théorème fondamental

On aborde dans cette section LE théorème fondamental de la théorie de la diagonalisation.

Théorème 23.1 (Théorème fondamental de la théorie de la diagonalisation)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie, et soit $f \in End(E)$ un endomorphisme de E. Soit de plus $\lambda_1, \ldots, \lambda_k$ les valeurs propres distinctes de f (donc les racines distinctes dans $\mathbb{R}$ du polynôme caractéristique de f), et soit E_{λ_i}, $i = 1, \ldots, k$, les espaces propres correspondant. La somme $E_{\lambda_1} + \cdots + E_{\lambda_k}$ est toujours directe, donc on a toujours*

$$E_{\lambda_1} + \cdots + E_{\lambda_k} = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k} \ ,$$

et f est diagonalisable si et seulement si E est somme (directe) des E_{λ_i}, $i = 1, \ldots, k$, donc si et seulement si $E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$.

On démontre un petit résultat préliminaire sur les sommes directes avant de démontrer le théorème.

Lemme 23.1. *Une somme de sous espaces vectoriels $E_1, \ldots E_k$ est directe si et seulement si $dim(E_1 + \cdots + E_k) = \sum_{i=1}^k dim(E_i)$.*

Démonstration. Supposons tout d'abord que la somme est directe. Si $k = 2$ le résultat suit de ce qui a été dit dans le chapitre 1 puisque

$$\dim(E_1 + E_2) = \dim(E_1) + \dim(E_2) - \dim(E_1 \cap E_2) \ ,$$

et puisque la somme de E_1 et E_2 est directe si et seulement si $E_1 \cap E_2 = \{0\}$. On peut alors établir une preuve par récurrence en remarquant que si la somme des $E_1, \ldots E_k$ est directe alors, en particulier, $E_k \cap (E_1 + \cdots + E_{k-1}) = \{0\}$ et donc la somme de $E_1 + \cdots + E_{k-1}$ et de E_k est directe. Par suite,

$$\dim(E_1 + \cdots + E_k) = \dim(E_1 + \cdots + E_{k-1}) + \dim(E_k) \ .$$

La récurrence sur k se met facilement en place à partir de cette relation. A l'inverse supposons que

$$\dim(E_1 + \cdots + E_k) = \sum_{i=1}^k \dim(E_i) \ .$$

Soit $\mathcal{B}_i$ une base de E_i et soit (avec abus de notation) la famille

$$\mathcal{B} = (\mathcal{B}_1, \ldots, \mathcal{B}_k) \ .$$

Cette famille est clairement génératrice pour $E_1 + \cdots + E_k$ (tout vecteur de $E_1 + \cdots + E_k$ se décompose en somme de vecteurs des E_i, qui eux-mêmes se décomposent dans les $\mathcal{B}_i$). Or, d'après la relation de départ, $\mathcal{B}$ a autant de vecteurs que la dimension de $E_1 + \cdots + E_k$. C'est donc une base de $E_1 + \cdots + E_k$. On en déduit facilement que tout vecteur de $E_1 + \cdots + E_k$ se décompose de façon unique en somme de vecteurs des E_i car sinon on aurait des décompositions différentes dans $\mathcal{B}$, ce qui est impossible par définition d'une base. Le lemme est démontré. □

On aborde maintenant la preuve du théorème fondamental de la théorie de la diagonalisation.

Preuve du théorème. (1) On commence par montrer que la somme des E_{λ_i} est directe. On présente deux preuves distinctes de ce fait. La première est somme toute assez naturelle du point de vue de l'analyse, mais elle est un peu pénible à mettre en place. La seconde est plus algébrique et beaucoup plus élégante.

(1a) Preuve 1: Sans perdre en généralité, on peut supposer que $k \geq 2$. On doit alors montrer que pour tout $i = 2, \ldots, k$,

$$E_{\lambda_i} \cap \Big(\sum_{j<i} E_{\lambda_j}\Big) = \{0\} \ .$$

On vérifie facilement que $E_{\lambda_1} \cap E_{\lambda_2} = \{0\}$. Si ce n'était pas le cas, il existerait $u \neq 0$ tel que $u \in E_{\lambda_1} \cap E_{\lambda_2}$. Or $u \in E_{\lambda_1}$ entraîne que $f(u) = \lambda_1 u$, tandis que $u \in E_{\lambda_2}$ entraîne que $f(u) = \lambda_2 u$. Comme $\lambda_1 \neq \lambda_2$, ces deux relations ne peuvent avoir lieu simultanément. La somme $E_{\lambda_1} \oplus E_{\lambda_2}$ est donc directe. On montre maintenant que la somme $E_{\lambda_1} \oplus E_{\lambda_2} \oplus E_{\lambda_3}$ est directe. Sans perdre en généralité on pourra supposer que

(i) soit $|\lambda_1| \leq |\lambda_2| < |\lambda_3|$,

(ii) soit $|\lambda_1| < |\lambda_2| = |\lambda_3|$.

On veut montrer que

$$E_{\lambda_3} \cap (E_{\lambda_1} + E_{\lambda_2}) = \{0\} \ .$$

Soit u un vecteur dans l'intersection, donc $u \in E_{\lambda_3}$, et il existe $u_1 \in E_{\lambda_1}$ et $u_2 \in E_{\lambda_2}$ tels que $u = u_1 + u_2$. Alors $f(u) = f(u_1) + f(u_2)$, et donc $\lambda_3 u = \lambda_1 u_1 + \lambda_2 u_2$. En appliquant de nouveau f à cette égalité, et ainsi de suite, on arrive à $\lambda_3^k u = \lambda_1^k u_1 + \lambda_2^k u_2$ pour tout k entier. En particulier,

$$u = \left(\frac{\lambda_1}{\lambda_3}\right)^k u_1 + \left(\frac{\lambda_2}{\lambda_3}\right)^k u_2 \ .$$

Dans le cas (i), en faisant $k \to +\infty$ on obtient que $u = 0$. D'ou $E_{\lambda_3} \cap (E_{\lambda_1} + E_{\lambda_2}) = \{0\}$. Dans le cas (ii), en prenant $k = 2p$ et en faisant tendre $k \to +\infty$ on obtient que $u = u_2$. Or $E_{\lambda_2} \cap E_{\lambda_3} = \{0\}$ pour les mêmes raisons que $E_{\lambda_1} \cap E_{\lambda_2} = \{0\}$. Dans les deux cas on en déduit que $u = 0$. Donc

$$E_{\lambda_1} + E_{\lambda_2} + E_{\lambda_3} \ = E_{\lambda_1} \oplus E_{\lambda_2} \oplus E_{\lambda_3} \ .$$

La relation générale s'obtient de la même façon.

(1b) Preuve 2: Pour $k \geq 2$, on considère la propriété $(\mathcal{P}_k)$: pour toute famille $\lambda_1, \ldots, \lambda_k$ de k valeurs propres distinctes de f, la somme des espaces propres E_{λ_i} est directe. On démontre cette propriété par récurrence finie sur k. Si $k = 2$ on procède comme ci-dessus. Si λ_1, λ_2 sont deux valeurs propres distinctes de f, alors $E_{\lambda_1} \cap E_{\lambda_2} = \{0\}$. En effet si $u \in E_{\lambda_1} \cap E_{\lambda_2}$ alors $f(u) = \lambda_1 u$ et $f(u) = \lambda_2 u$. Comme $\lambda_1 \neq \lambda_2$, ces deux relations entraînent que $u = 0$. La somme $E_{\lambda_1} \oplus E_{\lambda_2}$ est donc directe. On suppose maintenant $\mathcal{P}_k$ pour un k et on considère $(k+1)$ valeurs propres distinctes $\lambda_1, \ldots, \lambda_{k+1}$ de f. On veut montrer que la somme des E_{λ_i} est directe. En raison du Théorème 2.1, et puisque par hypothèse $E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$, il suffit de montrer que

$$E_{\lambda_{k+1}} \bigcap \big(E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}\big) = \{0\} \ . \tag{23.1}$$

Soit u dans l'intersection. Alors il existe (des uniques) $u_i \in E_{\lambda_i}$ pour $i \in \{1, \ldots, k\}$ tels que $u = \sum_{i=1}^k u_i$. En appliquant f à cette égalité on obtient que

$$\begin{aligned} f(u) &= \lambda_{k+1} u \\ &= \sum_{i=1}^k \lambda_{k+1} u_i \\ &= \sum_{i=1}^k f(u_i) \\ &= \sum_{i=1}^k \lambda_i u_i \ . \end{aligned}$$

Par suite

$$\sum_{i=1}^k (\lambda_{k+1} - \lambda_i) u_i = 0$$

et puisque $E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$, on obtient (par unicité de la décomposition de 0 en $0 + \cdots + 0$ dans la somme) que $(\lambda_{k+1} - \lambda_i)u_i = 0$ pour tout $i \in \{1, \ldots, k\}$. Or $\lambda_i \neq \lambda_{k+1}$ pour tout $i \in \{1, \ldots, k\}$, et donc $u_i = 0$ pour tout $i \in \{1, \ldots, k\}$, puis $u = 0$, ce qui est ce que nous voulions démontrer.

(2) On montre que f est diagonalisable ssi

$$E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$$

est somme directe des sous espaces propres de f. Cette condition est nécessaire dans la mesure où si f est diagonalisable, alors il existe une base $\mathcal{B}$ de E formée de vecteurs propres, donc de vecteurs dans la somme des E_{λ_i}. En effet, si on note $\mathcal{B} = (e_1, \ldots, e_n)$, et si on note λ'_i les valeurs propres de f pour $i = 1, \ldots, n$ (avec répetition des valeurs propres égales puisque $\{\lambda'_1, \ldots, \lambda'_n\} = \{\lambda_1, \ldots, \lambda_k\}$) alors la relation

$$M_{\mathcal{B}\mathcal{B}}(f) = \begin{pmatrix} \lambda'_1 & 0 & \ldots & 0 \\ 0 & \lambda'_2 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & \lambda'_n \end{pmatrix}$$

entraîne que $f(e_i) = \lambda'_i e_i$ pour tout i, et donc que les e_i sont tous des vecteurs propres de f. Donc ils sont tous dans la somme $E_{\lambda_1} + \cdots + E_{\lambda_k}$. D'où $E = E_{\lambda_1} + \cdots + E_{\lambda_k}$ (et on sait que la somme est directe d'après ce qui a été dit plus haut). On montre qu'à l'inverse, la condition est suffisante. Pour le voir, on considère $\mathcal{B}_i = (e^i_1, \ldots, e^i_{m_i})$ une base de E_{λ_i}, $i = 1, \ldots, k$, et on pose

$$\mathcal{B} = (\mathcal{B}_1, \ldots, \mathcal{B}_k)$$

la famille constitué des vecteurs de $\mathcal{B}_1$ suivis des vecteurs de $\mathcal{B}_2$, etc., suivis des vecteurs de $\mathcal{B}_k$. Puisque

$$E = E_{\lambda_1} + \cdots + E_{\lambda_k} \ ,$$

la famille $\mathcal{B}$ est une famille génératrice de E (tout vecteur de E s'écrit comme somme de vecteurs des E_{λ_i} qui eux-mêmes sécrivent comme combinaison linéaire de vecteurs de $\mathcal{B}$… de sorte que tout vecteur de E s'écrit comme combinaison linéaire de vecteurs de $\mathcal{B}$). Par ailleurs, puisque la somme est directe, $dimE = \sum_{i=1}^k dimE_{\lambda_i}$ de sorte que $\mathcal{B}$ a exactement $dimE$ vecteurs. Donc $\mathcal{B}$ est une base de E. Comme elle est constituée uniquement de vecteurs propres, f est de ce fait diagonalisable. D'où le théorème. $\square$

Un corollaire pratique important au théorème fondamental de la théorie de la diagonalisation est le suivant.

Corollaire 23.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n, et soit $f \in End(E)$ un endomorphisme de E. Soit de plus $\lambda_1, \dots, \lambda_k$ les racines distinctes dans $\mathbb{R}$ du polynôme caractéristique P de f, et soit E_{λ_i}, $i = 1, \dots, k$, les espaces propres correspondant. Alors f est diagonalisable si et seulement si*

$$dimE = \sum_{i=1}^{k} dimE_{\lambda_i} \ .$$

En particulier, si P a n racines distinctes dans $\mathbb{R}$, avec $n = dimE$, alors f est diagonalisable.

Démonstration. Puisque la somme est directe, cf le lemme précédent,

$$\dim\big(E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}\big) = \sum_{i=1}^{k} \dim E_{\lambda_i} \ .$$

Si f est diagonalisable alors l'égalité des dimensions est vraie. Réciproquement si $\dim E = \sum_{i=1}^{k} \dim E_{\lambda_i}$, on en déduit que $E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$. Donc f est diagonalisble d'après le théorème précédent. Si maintenant $k = n$, sachant que $\dim E_{\lambda_i} \geq 1$ pour tout i, on trouve que $\sum_{i=1}^{n} \dim E_{\lambda_i} \geq n$. Comme on a aussi que

$$\sum_{i=1}^{n} \dim E_{\lambda_i} = \dim\big(E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_n}\big) \leq dimE$$

il suit que $\dim E = \sum_{i=1}^{n} \dim E_{\lambda_i}$, ce qui démontre le corollaire. En particulier, on a aussi dans ce cas que $\dim E_{\lambda_i} = 1$ pour tout $i = 1, \dots, n$. Le corollaire est démontré. $\square$

Un autre résultat est le suivant.

Lemme 23.2. *Soit f un endomorphisme de E et $E_1, \dots, E_k$ ses espaces propres. Alors f est diagonalisable si et seulement si pour toutes bases $\mathcal{B}_i$ de E_i, la famille $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_k)$ constituée des vecteurs de $\mathcal{B}_1$ suivis des vecteurs de $\mathcal{B}_2$ etc. est une base de E.*

Démonstration. Soient $\mathcal{B}_1, \dots, \mathcal{B}_k$ des bases quelconques des $E_1, \dots, E_k$. Si $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_k)$ est une base de E alors la matrice $M_{\mathcal{B}\mathcal{B}}(f)$ de f dans $\mathcal{B}$ est forcément diagonale. Les λ_i (valeurs propres des E_i) sont répétées autant de fois qu'il y a de vecteurs dans les $\mathcal{B}_i$, et donc autant de fois que la dimension des E_i. Si f est diagonalisable alors

$$E = E_1 \oplus \cdots \oplus E_k \ .$$

La famille $\mathcal{B}$ est clairement génératrice pour $E_1 \oplus \cdots \oplus E_k$. Elle est donc aussi génératrice pour E. Elle a autant de vecteurs que $\sum_{i=1}^{k} \dim(E_i)$ et donc (cf. le lemme précédent) autant de vecteurs que $\dim(E_1 \oplus \cdots \oplus E_k) = \dim(E)$. C'est donc une base de E. Le lemme est démontré. $\square$

Exercice: Soient E un $\mathbb{R}$-espace vectoriel de dimensions finie n et $f, g \in End(E)$ deux endomorphismes de E. On suppose que f est diagonalisable. Montrer que f et g commutent, à savoir $f \circ g = g \circ f$, si et seulement si les espaces propres de f sont stables par g, à savoir si et seulement si pour tout espace propre E_i de f on a $g(E_i) \subset E_i$.

Solution: Supposons que f et g commutent. Soit E_i un espace propre de f associé à une valeur propre λ_i. Soit $u \in E_i$. On a

$$g\left(f(u)\right) = \lambda_i g(u) = f\left(g(u)\right) \ .$$

Donc $v = g(u)$ appartient à E_i. Soit $g(E_i) \subset E_i$ puisque u est quelconque dans E_i. Si f et g commutent les espaces propres de f sont donc stables par g. Réciproquement supposons que les espaces propres de f sont stables par g. Puisque f est diagonalisable il existe une base $\mathcal{B}$ de E constituée de vecteurs propres. Disons que f a pour espaces propres $E_1, \ldots, E_p$ et écrivons (avec abus de langage) que $\mathcal{B} = (\mathcal{B}_1, \ldots, \mathcal{B}_p)$ où les $\mathcal{B}_i$ sont des bases des E_i. Fixons i quelconque, notons λ_i la valeur propre pour E_i et notons $\mathcal{B}_i = (e_1^i, \ldots, e_k^i)$. Comme $g(E_i) \subset E_i$, il existe des α_{jm}, $j, m = 1, \ldots, k$, tels que pour tout $j = 1, \ldots, k$,

$$g(e_j^i) = \sum_{m=1}^{k} \alpha_{jm} e_m^i \ .$$

Par suite, pour tout $j = 1, \ldots, k$,

$$f\left(g(e_j^i)\right) = \sum_{m=1}^{k} \alpha_{jm} f(e_m^i) = \lambda_i \sum_{m=1}^{k} \alpha_{jm} e_m^i$$

tandis que

$$g\left(f(e_j^i)\right) = \lambda_i g(e_j^i) = \lambda_i \sum_{m=1}^{k} \alpha_{jm} e_m^i \ .$$

On voit donc que pour tout $i = 1, \ldots, p$ et tout $j = 1, \ldots, k$,

$$f\left(g(e_j^i)\right) = g\left(f(e_j^i)\right) \ .$$

En d'autres termes, il existe une base $\mathcal{B} = (e_1, \ldots, e_n)$ de E ayant la propriété que pour tout $i = 1, \ldots, n$,

$$g \circ f(e_i) = f \circ g(e_i) \ .$$

Deux applications linéaires qui sont égales sur une base le sont sur tout l'espace. Donc $g \circ f = f \circ g$. □

24. Tout le monde doit être là

Supposons que f est diagonalisable. Il est clair que toute base qui diagonalise f est forcément constituée de vecteurs propres. Mais peut-on imaginer avoir une base de E qui diagonalise f mais dont la matrice de représentation de f associée ne reprenne pas toutes les valeurs propres de f ? Et, question subsidiaire, si f est diagonalisable et si une base de E diagonalise f, les valeurs propres de f doivent-elles intervenir précisemment avec leur multiplicité algébrique (à savoir en étant répétées autant de fois que la dimension de l'espace propre correspondant) ?

La réponse à la première question est non et à la seconde est oui. En d'autres termes, si une base de E diagonalise f alors elle comporte forcément des vecteurs propres de tous les espaces propres, et autant de vecteurs propres d'un espace propre que la dimension de cet espace propre. La matrice de représentation de f associée est alors diagonale, elle comporte toutes les valeurs propres de f, chacune étant répétée autant de fois que la dimension de l'espace propre correspondant.

Pour le voir, considérons une base $\mathcal{B} = (e_1, \dots, e_n)$ de E qui diagonalise f. Les e_i sont des vecteurs propres de f, et le terme correspondant sur la diagonale de la matrice de représentation dans $\mathcal{B}$ est la valeur propre correspondante. Notons $E_1, \dots, E_p$ les espaces propres de f, $1 \leq p \leq n$. Comme f est diagonalisable,

$$n = \sum_{i=1}^{p} \dim(E_i) \ .$$

Si l'un des E_i n'est pas représenté dans $\mathcal{B}$, où s'il y a moins de vecteurs de l'un des E_i dans $\mathcal{B}$ que la dimension de E_i, alors il faudra forcement, pour compenser, qu'il y ait plus de vecteurs dans $\mathcal{B}$ d'un autre E_j, $j \neq i$, que la dimension de E_j. Toute sous famille libre d'une famille libre (et donc a fortiori d'une base) étant libre on aurait donc une famille libre de vecteurs de E_j qui a plus de vecteurs que la dimension de E_j, ce qui est impossible en vertu du théorème fondamental de la théorie de la dimension.

On vient de dire pourquoi, il ne peut pas non plus avoir plus de vecteurs dans $\mathcal{B}$ d'un espace propre que la dimension de cet espace propre. Si une base $\mathcal{B}$ diagonalise f il faut donc que $\mathcal{B}$ comporte des vecteurs de tous les espaces propres et, de plus, qu'il y ait à chaque fois autant de vecteurs que leur dimension.

25. Multiplicité des racines et dimensions des espaces propres

On démontre ici le théorème suivant.

Théorème 25.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie, et soit $f \in End(E)$ un endomorphisme de E. Soit P le polynôme caractéristique de f et $\lambda \in \mathbb{R}$ une valeur propre de f. On suppose que l'ordre de multiplicité de λ en tant que racine de P est k, et donc que*

$$P(X) = (X - \lambda)^k Q(X)$$

où Q est un polynôme de degré $n-k$ avec $Q(\lambda) \neq 0$. Soit E_λ l'espace propre associé à la valeur propre λ. Alors forcément $dim E_\lambda \leq k$.

On dit encore que la multiplicité algébrique d'une valeur propre λ (au sens de dimension de l'espace propre correspondant) est toujours plus petite que la multiplicité polynomiale de λ. On démontre ce résultat en montrant tout d'abord que le lemme suivant a lieu.

Lemme 25.1. *Soit M une matrice carrée d'ordre n. On suppose que M est du type*

$$M = \left(\begin{array}{c|c} Id_p & A \\ \hline 0 & B \end{array} \right)$$

où $p < n$, $\lambda \in \mathbb{R}$, Id_p est la matrice identité d'ordre p, A est une matrice $p \times (n-p)$, B est une matrice $(n-p) \times (n-p)$ et 0 est la matrice nulle $(n-p) \times p$. Alors $det(M) = \lambda^p det(B)$.

Démonstration. Pour “coder” la matrice M facilement fixons n et p (on sort donc d'un raisonnement mathématique général) et supposons par exemple que $n = 8$ et $p = 4$. Alors M est du type:

$$M = \begin{pmatrix} \lambda & 0 & 0 & 0 & a_{11} & a_{12} & a_{13} & a_{14} \\ 0 & \lambda & 0 & 0 & a_{21} & a_{22} & a_{23} & a_{24} \\ 0 & 0 & \lambda & 0 & a_{31} & a_{32} & a_{33} & a_{34} \\ 0 & 0 & 0 & \lambda & a_{41} & a_{42} & a_{43} & a_{44} \\ 0 & 0 & 0 & 0 & b_{11} & b_{12} & b_{13} & b_{14} \\ 0 & 0 & 0 & 0 & b_{21} & b_{22} & b_{23} & b_{24} \\ 0 & 0 & 0 & 0 & b_{31} & b_{32} & b_{33} & b_{34} \\ 0 & 0 & 0 & 0 & b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

En développant le déterminant cette matrice suivant la première colonne on voit que

$$\det M = \lambda \det \begin{pmatrix} \lambda & 0 & 0 & a_{21} & a_{22} & a_{23} & a_{24} \\ 0 & \lambda & 0 & a_{31} & a_{32} & a_{33} & a_{34} \\ 0 & 0 & \lambda & a_{41} & a_{42} & a_{43} & a_{44} \\ 0 & 0 & 0 & b_{11} & b_{12} & b_{13} & b_{14} \\ 0 & 0 & 0 & b_{21} & b_{22} & b_{23} & b_{24} \\ 0 & 0 & 0 & b_{31} & b_{32} & b_{33} & b_{34} \\ 0 & 0 & 0 & b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

On redéveloppe suivant la première colonne et on obtient que

$$\det M = \lambda^2 \det \begin{pmatrix} \lambda & 0 & a_{31} & a_{32} & a_{33} & a_{34} \\ 0 & \lambda & a_{41} & a_{42} & a_{43} & a_{44} \\ 0 & 0 & b_{11} & b_{12} & b_{13} & b_{14} \\ 0 & 0 & b_{21} & b_{22} & b_{23} & b_{24} \\ 0 & 0 & b_{31} & b_{32} & b_{33} & b_{34} \\ 0 & 0 & b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

Encore deux développements suivant la première colonne et on obtient que

$$\det M = \lambda^4 \det \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

Soit

$$\det(M) = \lambda^4 \det(B)$$

La preuve générale fonctionne de la même façon. On développe p fois suivant la première colonne pour obtenir que

$$\det(M) = \lambda^p \det(B) \ .$$

Une preuve mathématique rigoureuse par récurrence est facilement mise en place. D'où le lemme. □

On revient maintenant à la preuve du théorème. On suppose que λ est une racine d'ordre k du polynôme caractéristique. On veut montrer que $\dim E_\lambda \leq k$. On peut définir cet ordre de deux façons différentes: soit comme l'entier k pour lequel on peut écrire que

$$P(X) = (X - \lambda)^k Q(X)$$

avec Q un polynôme réel de degré $n-k$ vérifiant que $Q(\lambda) \neq 0$, ou alors comme le plus grand entier p pour lequel on puisse écrire que $P(X) = (X-\lambda)^p Q(X)$ avec Q un polynôme réel de degré $n-p$. L'équivalence de ces deux définitions suit de la remarque que λ est racine d'un polynôme Q si et seulement si il existe un polynôme $\tilde{Q}$ avec $Q(X) = (X-\lambda)\tilde{Q}(X)$. Il s'agit aussi du plus grand entier $p \geq 1$ pour lequel $P^{(s)}(\lambda) = 0$ pour tout $0 \leq s \leq p-1$. L'ordre 1 correspond alors à $P(\lambda) = 0$ et $P'(\lambda) \neq 0$. L'ordre 2 correspond à $P(\lambda) = P'(\lambda) = 0$ et $P''(\lambda) \neq 0$, etc.

Preuve du théorème. Notons $p = \dim E_\lambda$. Si $p = n$ alors $E_\lambda = E$ et donc $f = \lambda \mathrm{Id}_E$ (i.e $f(x) = \lambda x$ pour tout $x \in E$). Mais alors $P(X) = (\lambda - X)^n$, donc $k = n$ et on a bien que $p \leq k$ (en fait $n = n$). On suppose maintenant que $p < n$. Soit $(e_1, \ldots, e_p)$ une base de E_λ. On la complète par des vecteurs $e_{p+1}, \ldots, e_n$ pour obtenir une base $\mathcal{B} = (e_1, \ldots, e_p, e_{p+1}, \ldots, e_n)$ de E. On a alors

$$M_{\mathcal{B}\mathcal{B}}(f) = \begin{pmatrix} \lambda \mathrm{Id}_p & A \\ 0 & B \end{pmatrix}$$

où Id_p est la matrice identité d'ordre p, A est une matrice $p \times (n-p)$ et B est une matrice $(n-p) \times (n-p)$. La matrice $M_{\mathcal{B}\mathcal{B}}(f) - X\mathrm{Id}_n$ s'écrit alors

$$M_{\mathcal{B}\mathcal{B}}(f) - X\mathrm{Id}_n = \begin{pmatrix} (\lambda - X)\mathrm{Id}_p & A \\ 0 & B - X\mathrm{Id}_{n-p} \end{pmatrix}$$

Avec le lemme précédent:

$$P(X) = (\lambda - X)^p Q(X) ,$$

où Q est le polynôme caractéristique de B. Donc $p \leq k$ puisqu'on peut voir k comme le plus grand de tels p. D'où le théorème. $\square$

Notons $m_{al}(\lambda)$ la multiplicité algébrique d'une valeur propre λ, à savoir la dimension de l'espace propre associé E_λ, et $m_{po}(\lambda)$ la multiplicité polynomiale de λ, à savoir l'ordre de la racine λ dans le polynôme caractéristique. Ce que dit le Théorème 25.1 c'est que $m_{al}(\lambda) \leq m_{po}(\lambda)$. Un polynôme réel P est dit scindé si toutes ses racines (entendues dans $\mathbb{C}$ qui est algébriquement clos) sont en fait dans $\mathbb{R}$ et donc si P s'écrit sous la forme

$$P(X) = a \prod_{i=1}^{k} (X - \lambda_i)^{n_i} ,$$

avec $a, \lambda_1, \ldots, \lambda_n \in \mathbb{R}$ et $n_i \in \mathbb{N}^\star$ pour tout i. On démontre le résultat suivant.

Théorème 25.2. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie, $f \in End(E)$ un endomorphisme de E et P le polynôme caractéristique de f. L'endomorphisme f est diagonalisable si et seulement si P est scindé et pour toute valeur propre λ de f, $m_{al}(f) = m_{po}(f)$.*

Démonstration. Notons n la dimension de E. Si f est diagonalisable, en calculant le polynôme caractéristique P de f dans une base qui diagonalise f, on voit que nécessairement P est scindé. Soient $\lambda_1, \ldots, \lambda_p$ les valeurs propres réelles distinctes de f. On a alors

$$P(X) = (-1)^n (X - \lambda_1)^{n_1} \ldots (X - \lambda_p)^{n_p} , \tag{25.1}$$

puisque le terme de plus haut degré de P est $(-1)^n X^n$, et $n_i = m_{po}(\lambda_i)$, $i = 1, \ldots, p$. Comme f est diagonalisable, $n = \sum_{i=1}^p \dim(E_i)$. Par ailleurs, $m_{al}(\lambda_i) = \dim(E_{\lambda_i})$ pour tout i. Par comptage des degrés dans l'expression de P, $n = \sum_{i=1}^p n_i$.

Le Théorème 25.1 donne que $m_{al}(\lambda_i) \leq m_{po}(\lambda_i)$ pour tout i. Donc forcément $m_{al}(\lambda_i) = m_{po}(\lambda_i)$ pour tout i. Réciproquement, si P est scindé alors il va s'écrire sous la forme (25.1). Si $m_{al}(\lambda_i) = m_{po}(\lambda_i)$ pour tout i, comme $n = \sum_{i=1}^{p} n_i$, on obtient que $n = \sum_{i=1}^{p} m_{al}(\lambda_i) = \sum_{i=1}^{p} \dim(E_i)$. Donc f est diagonalisable. Le théorème est démontré. □

En particulier, il suit de ce théorème que si pour un i, $n_{al}(\lambda_i) < n_{po}(\lambda_i)$, alors f n'est pas diagonalisable. Si un tel i existe, et dès qu'il est trouvé, la question de la diagonalisation de f se clôt. On a là un critère d'arrêt possible dans l'étude de la diagonalisation de f.

26. Dans la pratique

On décrit sous forme de diagramme simple le processus de diagonalisation discuté jusqu'à maintenant.

On part avec les données suivantes:
E un $\mathbb{R}$-espace vectoriel de dimension n,
$\mathcal{B}$ une base de E, $f \in \mathrm{End}(E)$ et $A = M_{\mathcal{B}\mathcal{B}}(f)$.

↓

Calcul du polynôme caractéristique
$P(X) = det\big(A - X\mathrm{Id}_n\big)$
de f où Id_n est la matrice identité $n \times n$

↓

Recherche des racines de P dans $\mathbb{R}$

↓	↓
Il y a des racines de P qui sont dans $\mathbb{C}$ mais pas dans $\mathbb{R}$. Alors f n'est pas diagonalisable.	P a n racines distinctes dans $\mathbb{R}$. Alors f est diagonalisable.

↓

Sinon soient $\lambda_1, \ldots, \lambda_k$ les racines distinctes
de P dans $\mathbb{R}$. On détermine les bases $\mathcal{B}_i$ des sous
espaces propres définis pour $i = 1, \ldots, k$ par
$E_{\lambda_i} = \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$
La famille $\tilde{\mathcal{B}} = (\mathcal{B}_1, \ldots, \mathcal{B}_k)$ est une famille
libre de E puisque la somme des E_{λ_i} est directe.

↓	↓
Si $\mathrm{Card}\tilde{\mathcal{B}} = n$, donc si $\tilde{\mathcal{B}}$ est une base de E, alors f est diagonalisable et $M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f)$ est une matrice diagonale dont la diagonale est constituée des λ_i.	Si $Card\tilde{\mathcal{B}} < n$, donc si $\tilde{\mathcal{B}}$ n'est pas une base de E, alors f n'est pas diagonalisable. En fait ce cas ne se produit que si $n_{al}(\lambda_i) < n_{op}(\lambda_i)$ pour au moins un i, et cela fournit un critère d'arrêt possible à l'étape précédente.

27. Un exemple

Soient E un $\mathbb{R}$-espace vectoriel de dimension 3, $\mathcal{B} = (e_1, e_2, e_3)$ une base de E, et $f \in \mathrm{End}(E)$ l'endomorphisme de E défini par

$$\begin{aligned} f\left(x_1e_1 + x_2e_2 + x_3e_3\right) = &\left(2x_1 - 2x_2 + x_3\right)e_1 \\ &+ \left(2x_1 - 3x_2 + 2x_3\right)e_2 - \left(x_1 - 2x_2\right)e_3 \end{aligned}$$

pour tous $x_1, x_2, x_3 \in \mathbb{R}$. Sa matrice de représentation dans $\mathcal{B}$ est donnée par

$$M_{\mathcal{B}\mathcal{B}}(f) = \begin{pmatrix} 2 & -2 & 1 \\ 2 & -3 & 2 \\ -1 & 2 & 0 \end{pmatrix} .$$

Son polynôme caractéristique est alors donné par

$$\begin{aligned} P(X) &= \det \begin{pmatrix} 2-X & -2 & 1 \\ 2 & -3-X & 2 \\ -1 & 2 & -X \end{pmatrix} \\ &= (2-X) \times (3+X) \times X + 2 \times 2 \times 1 + (-2) \times 2 \times (-1) \\ &- 1 \times (3+X) \times 1 - 2 \times 2 \times (2-X) - 2 \times (-2) \times (-X) \\ &= -X(X-2)(X+3) - (X+3) \\ &= -(X+3) \times \left(X^2 - 2X + 1\right) \\ &= -(X-1)^2(X+3) . \end{aligned}$$

L'endomorphisme f a donc deux valeurs propres qui sont -3 et 1. Soient E_{-3} et E_1 les espaces propres de f associés à ces valeurs propres. On a

$$E_{-3} = \left\{ x = x_1e_1 + x_2e_2 + x_3e_3 \ / \ f(x) = -3x \right\}$$

et on écrit que $f(x) = -3x$ si et seulement si

$$\begin{pmatrix} 2 & -2 & 1 \\ 2 & -3 & 2 \\ -1 & 2 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = -3 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} .$$

On trouve pour système d'équations

$$\begin{cases} 2x_1 - 2x_2 + x_3 = -3x_1 \\ 2x_1 - 3x_2 + 2x_3 = -3x_2 \\ -x_1 + 2x_2 = -3x_3 \end{cases}$$

On a les équivalences suivantes

$$\begin{cases} 2x_1 - 2x_2 + x_3 = -3x_1 \\ 2x_1 - 3x_2 + 2x_3 = -3x_2 \\ -x_1 + 2x_2 = -3x_3 \end{cases} \Leftrightarrow \begin{cases} 5x_1 - 2x_2 + x_3 = 0 \\ 2x_1 + 2x_3 = 0 \\ -x_1 + 2x_2 + 3x_3 = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} 4x_1 - 2x_2 = 0 \\ x_3 = -x_1 \\ -4x_1 + 2x_2 = 0 \end{cases} \Leftrightarrow \begin{cases} x_2 = 2x_1 \\ x_3 = -x_1 \end{cases} .$$

Donc

$$\begin{aligned}
E_{-3} &= \left\{x = x_1e_1 + x_2e_2 + x_3e_3 \ / \ x_2 = 2x_1 \text{ et } x_3 = -x_1\right\} \\
&= \left\{x_1e_1 + 2x_1e_2 - x_1e_3 \ / \ x_1 \in \mathbb{R}\right\} \\
&= \left\{x_1\left(e_1 + 2e_2 - e_3\right) \ / \ x_1 \in \mathbb{R}\right\}
\end{aligned}$$

et si on pose

$$\tilde{e}_1 = e_1 + 2e_2 - e_3$$

alors E_{-3} est la droite vectorielle de base $(\tilde{e}_1)$. On a de même que

$$E_1 = \left\{x = x_1e_1 + x_2e_2 + x_3e_3 \ / \ f(x) = x\right\}$$

et on écrit que $f(x) = x$ si et seulement si

$$\begin{pmatrix} 2 & -2 & 1 \\ 2 & -3 & 2 \\ -1 & 2 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} .$$

On trouve pour système d'équations

$$\begin{cases} 2x_1 - 2x_2 + x_3 = x_1 \\ 2x_1 - 3x_2 + 2x_3 = x_2 \\ -x_1 + 2x_2 = x_3 \end{cases}$$

On a les équivalences suivantes

$$\begin{aligned}
\begin{cases} 2x_1 - 2x_2 + x_3 = x_1 \\ 2x_1 - 3x_2 + 2x_3 = x_2 \\ -x_1 + 2x_2 = x_3 \end{cases} &\Leftrightarrow \begin{cases} x_1 - 2x_2 + x_3 = 0 \\ 2x_1 - 4x_2 + 2x_3 = 0 \\ -x_1 + 2x_2 - x_3 = 0 \end{cases} \\
&\Leftrightarrow \ x_1 - 2x_2 + x_3 = 0 \ .
\end{aligned}$$

Donc

$$\begin{aligned}
E_1 &= \left\{x = x_1e_1 + x_2e_2 + x_3e_3 \ / \ x_1 - 2x_2 + x_3 = 0\right\} \\
&= \left\{x_1e_1 + x_2e_2 - x_1e_3 + 2x_2e_3 \ / \ x_1, x_2 \in \mathbb{R}\right\} \\
&= \left\{x_1\left(e_1 - e_3\right) + x_2\left(e_2 + 2e_3\right) \ / \ x_1, x_2 \in \mathbb{R}\right\}
\end{aligned}$$

et si on pose

$$\tilde{e}_2 = e_1 - e_3 \text{ et } \tilde{e}_3 = e_2 + 2e_3$$

alors $(\tilde{e}_2, \tilde{e}_3)$ est une famille génératrice de E_1. Il est facile de vérifier que cette famille est aussi libre car

$$\begin{aligned}
\lambda\tilde{e}_2 + \mu\tilde{e}_3 = 0 &\Rightarrow \ \lambda e_1 + \mu e_2 + (2\mu - \lambda)e_3 = 0 \\
&\Rightarrow \ \lambda = \mu = 0
\end{aligned}$$

puisque (e_1, e_2, e_3) est une base. Donc $(\tilde{e}_2, \tilde{e}_3)$ est une base de E_1 On en déduit que f a deux valeurs propres -3 et 1, que $\dim E_{-3} = 1$ et que $\dim E_1 = 2$. Comme

$1+2=3$, on a que $E = E_{-3}+E_1$ et f est diagonalisable. Si on note $\tilde{\mathcal{B}} = (\tilde{e}_1, \tilde{e}_2, \tilde{e}_3)$, alors $\tilde{\mathcal{B}}$ est une base de E et on a que

$$M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f) = \begin{pmatrix} -3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

De plus

$$M_{\mathcal{B}\to\tilde{\mathcal{B}}} = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \\ -1 & -1 & 2 \end{pmatrix} .$$

Pour inverser $M_{\mathcal{B}\to\tilde{\mathcal{B}}}$ on peut remarquer que

$$\begin{cases} x+y = X \\ 2x+z = Y \\ -x-y+2z = Z \end{cases} \Leftrightarrow \begin{cases} x+y = X \\ 2x+z = Y \\ 2z = X+Z \end{cases}$$

$$\Leftrightarrow \begin{cases} z = \frac{1}{2}X + \frac{1}{2}Z \\ x = -\frac{1}{4}X + \frac{1}{2}Y - \frac{1}{4}Z \\ y = \frac{5}{4}X - \frac{1}{2}Y + \frac{1}{4}Z \end{cases}$$

Donc:

$$M_{\mathcal{B}\to\tilde{\mathcal{B}}}^{-1} = \begin{pmatrix} -\frac{1}{4} & \frac{1}{2} & -\frac{1}{4} \\ \frac{5}{4} & -\frac{1}{2} & \frac{1}{4} \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} ,$$

et on a que

$$M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f) = M_{\mathcal{B}\to\tilde{\mathcal{B}}}^{-1} M_{\mathcal{B}\mathcal{B}}(f) M_{\mathcal{B}\to\tilde{\mathcal{B}}} ,$$

soit encore

$$M_{\mathcal{B}\mathcal{B}}(f) = M_{\mathcal{B}\to\tilde{\mathcal{B}}} M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f) M_{\mathcal{B}\to\tilde{\mathcal{B}}}^{-1} .$$

Remarque: Il s'ensuit que pour n'importe quel entier k,

$$M_{\mathcal{B}\mathcal{B}}(f)^k = M_{\mathcal{B}\to\tilde{\mathcal{B}}} M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f)^k M_{\mathcal{B}\to\tilde{\mathcal{B}}}^{-1} , \tag{1}$$

et comme

$$M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f)^k = \begin{pmatrix} (-3)^k & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} ,$$

on va pouvoir facilement calculer $M_{\mathcal{B}\mathcal{B}}(f)^3$, $M_{\mathcal{B}\mathcal{B}}(f)^4$, $M_{\mathcal{B}\mathcal{B}}(f)^5$ etc. à partir de la formule (1).

28. Le théorème de Cayley-Hamilton

On démontre ici le théorème suivant.

Théorème 28.1 (Théorème de Cayley-Hamilton pour les endomorphismes)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie, et soit $f \in End(E)$ un endomorphisme de E. Soit P le polynôme caractéristique de f. On a $P(f) = 0$ au sens des endomorphismes et donc aussi, pour toute base $\mathcal{B}$ de E,*

$$P\big(M_{\mathcal{B}\mathcal{B}}(f)\big) = 0 .$$

Autrement dit, le polynôme caractéristique annule f et les matrices de représentations $M_{\mathcal{B}\mathcal{B}}(f)$ de f.

Le terme a_0 de P est ici à comprendre comme $a_0\mathrm{Id}_E$ pour les endomorphismes et $a_0\mathrm{Id}_n$ pour les matrices. Si par exemple $n = 3$, et si $P(X) = -X^3+2X^2+X-4$, alors d'après Cayley-Hamilton,

$$-f^3 + 2f^2 + f - 4\mathrm{Id}_E = 0$$

au sens des endomorphismes, et si $A = M_{\mathcal{B}\mathcal{B}}(f)$, alors

$$-A^3 + 2A^2 + A - 4\mathrm{Id}_3 = 0$$

où 0 est la matrice nulle 3×3. En particulier, A^3 s'exprime en fonction de A^2, A et Id_3. Il existe une preuve très simple du théorème de Cayley-Hamilton dans le cas $n = 2$, où $n = \dim(E)$. On la donne ici avant de traiter du cas général.

Démonstration lorsque $n = 2$. En dimension 2 le polynôme caractéristique P d'un endomorphisme f s'écrit toujours $X^2 - \mathrm{tr}(f)X + \det(f)$ et donc, en termes de matrices, si $A = M_{\mathcal{B}\mathcal{B}}(f)$, on obtient que

$$P(A) = A^2 - \mathrm{tr}(A)A + \det(A)I_2 \ .$$

On vérifie que $P(A) = 0$. On écrit

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

On a

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

puis $\mathrm{tr}(A) = a + d$ et $\det(A) = ad - bc$. Donc

$$\begin{aligned}
&A^2 - \mathrm{tr}(A)A + \det(A)I_2 \\
&= \begin{pmatrix} a^2+bc & ab+bd \\ ac+dc & bc+d^2 \end{pmatrix} - (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a^2+bc & ab+bd \\ ac+dc & bc+d^2 \end{pmatrix} - \begin{pmatrix} a^2+ad & ab+bd \\ ac+cd & ad+d^2 \end{pmatrix} + \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\
&= \begin{pmatrix} a^2+bc & ab+bd \\ ac+dc & bc+d^2 \end{pmatrix} - \begin{pmatrix} a^2+bc & ab+bd \\ ac+dc & bc+d^2 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \ .
\end{aligned}$$

D'où le résultat. □

Dans le cas général, avec donc $n = \dim(E)$ quelconque, un résultat technique dont nous aurons besoin est la formule du développement d'un déterminant par blocs.

Lemme 28.1. *Soit $n \geq 2$ et $1 \leq p < n$. On considère A une matrice $p \times p$, C une matrice $p \times (n-p)$, 0 la matrice nulle $(n-p) \times p$ et B une matrice $(n-p) \times (n-p)$. Alors*

$$det\left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right) = det(A)det(B)$$

Démonstration. On se ramène au Lemme 25.1 en remarquant que

$$\left(\begin{array}{c|c} I_p & C \\ \hline 0 & B \end{array}\right) \times \left(\begin{array}{c|c} A & 0 \\ \hline 0 & I_{n-p} \end{array}\right) = \left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right) \ , \tag{28.1}$$

où I_p est la matrice identité $p \times p$ et I_{n-p} est la matrice identité $(n-p) \times (n-p)$ et les 0 dans la membre de gauche de l'égalité sont les matrices nulles $(n-p) \times p$ et $p \times (n-p)$. Avec le Lemme 25.1,

$$\det \left(\begin{array}{c|c} I_p & C \\ \hline 0 & B \end{array} \right) = \det(B)$$

et après manipulations élémentaires sur les lignes et le colonnes (permutation sur les lignes $(1, \dots, p, p+1, \dots, n) \to (p+1, \dots, n, 1, \dots, p)$ et même chose sur les colonnes ensuite pour placer l'identité en bloc en haut à gauche, le signe de la permutation est alors élevé au carré et donne $+1$) on obtient que

$$\det \left(\begin{array}{c|c} A & 0 \\ \hline 0 & I_{n-p} \end{array} \right) = \det(A) \ .$$

Le lemme suit en revenant à (28.1) et en passant aux déterminants. □

Démonstration du théorème de Cayley-Hamilton. Soit $n = \dim(E)$. On note P le polynôme caractéristique de f. On suppose $n \geq 1$ (sinon $E = \{0\}$ et le résultat est trivial). Soit $x \in E \backslash \{0\}$. On distingue deux cas. (1) On suppose que $\left(x, f(x), f^2(x), \dots, f^{n-1}(x)\right)$ est libre. Alors

$$\mathcal{B} = \left(x, f(x), f^2(x), \dots, f^{n-1}(x)\right)$$

est une base de E et il existe $a_0, \dots, a_{n-1} \in \mathbb{R}$ tels que

$$f^n(x) = a_0 x + a_1 f(x) + a_2 f^2(x) + \dots + a_{n-1} f^{n-1}(x) \ .$$

On note Q le polynôme

$$Q(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_{n-1} X^{n-1} - X^n \ .$$

On a alors $Q(f)(x) = 0$ par construction. La matrice de représentation de f dans $\mathcal{B}$ est la matrice

$$M_{\mathcal{B}\mathcal{B}}(f) = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & a_0 \\ 1 & 0 & \dots & 0 & 0 & a_1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & a_{n-2} \\ 0 & 0 & \dots & 0 & 1 & a_{n-1} \end{pmatrix}$$

puisque si on note e_i les vecteurs de $\mathcal{B}$, alors $f(e_i) = e_{i+1}$ pour $i = 1, \dots, n-1$ et $f(e_n) = a_0 e_1 + \dots + a_{n-1} e_n$. Par suite,

$$P(X) = \det \begin{pmatrix} -X & 0 & \dots & 0 & 0 & a_0 \\ 1 & -X & \dots & 0 & 0 & a_1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -X & a_{n-2} \\ 0 & 0 & \dots & 0 & 1 & a_{n-1} - X \end{pmatrix}$$

Notons L_i les lignes de cette matrice. Alors

$$L_1 + \sum_{i=2}^{n} X^{i-1} L_i = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & Q(X) \end{pmatrix}$$

On effectue cette opération et on développe suivant la première ligne. Alors

$$P(X) = Q(X) R(X)$$

où R est un polynôme. Pour des raisons de degrés, R est forcément un polynôme constant. Et en comparant les termes de plus haut degré on voit que $R = \pm 1$. On en déduit que $P(f)(x) = 0$.

(2) On suppose que $\big(x, f(x), f^2(x), \dots, f^{n-1}(x)\big)$ est liée. On note k le plus grand entier pour lequel la famille $\big(x, f(x), f^2(x), \dots, f^{k-1}(x)\big)$ est libre. Forcément $k \geq 1$ puisque $x \neq 0$. Notons F le sous espaces vectoriel de E de base

$$\mathcal{B}_1 = \big(x, f(x), f^2(x), \dots, f^{k-1}(x)\big)$$

Alors f induit un endomorphisme $f_{|F} : F \to F$. On complète $\mathcal{B}_1$ par des vecteurs pour obtenir une base $\mathcal{B}$ de E. Alors

$$M_{\mathcal{B}\mathcal{B}}(f - X\mathrm{Id}_E) = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} \ ,$$

où $A = M_{\mathcal{B}_1\mathcal{B}_1}(f_{|F} - X\mathrm{Id}_F)$. Avec le Lemme 28.1 on voit que

$$P(X) = P_1(X)\tilde{Q}(X) \ ,$$

où P_1 est le polynôme caractéristique de $f_{|F}$, et $\tilde{Q}$ est un polynôme de degré $n-k$. D'après la première partie de la preuve, $P_1(f)(x) = 0$. On a $f^{p+q} = f^p \circ f^q$. Donc $(P_1Q)(f) = Q(f) \circ P_1(f)$, et on obtient que $P(f)(x) = 0$.

On a ainsi montré que $P(f)(x) = 0$ pour tout $x \neq 0$. Par linéarité l'égalité est vraie pour $x = 0$. Donc $P(f) = 0$ au sens des endomorphismes. On passe facilement à la partie matricielle de Cayley-Hamilton en remarquant que $M_{\mathcal{B}\mathcal{B}}(P(f)) = P(M_{\mathcal{B}\mathcal{B}}(f))$ de sorte que $P(M_{\mathcal{B}\mathcal{B}}(f)) = 0$ au sens des matrices. Le théorème est démontré. □

29. Le cas des matrices

On traite maintenant de la diagonalisation des matrices. La théorie est parallèle à celle de la diagonalisation des endomorphismes.

Définition 29.1. *Soit A une matrice $n \times n$, $n \in \mathbb{N}$. On dit que A est une matrice diagonalisable s'il existe M une matrice inversible $n \times n$ avec la propriété que $M^{-1}AM$ est une matrice diagonale.*

On se donne E un $\mathbb{R}$-espace vectoriel de dimension n, et $\mathcal{B}$ une base de E. Par exemple $E = \mathbb{R}^n$ et $\mathcal{B}$ la base canonique de $\mathbb{R}^n$ constituée des vecteurs $(1, 0, \dots, 0)$, $(0, 1, \dots, 0)$,..., et $(0, \dots, 0, 1)$. Il existe (on l'a déjà vu) un unique endomorphisme f de E qui est tel que

$$M_{\mathcal{B}\mathcal{B}}(f) = A \ .$$

Si $(e_1, \dots, e_n)$ sont les vecteurs de $\mathcal{B}$, f est caractérisé par le fait que les coordonnées de $f(e_i)$ dans la base $\mathcal{B}$ sont les composantes de la $i$ème colonne de A. On suppose que A est diagonalisable. On note $\tilde{\mathcal{B}}$ la famille de vecteurs de E qui est telle que

$$M_{\mathcal{B}\to\tilde{\mathcal{B}}} = M \ .$$

Si φ est l'endomorphisme de E défini par le fait que

$$M_{\mathcal{B}\mathcal{B}}(\varphi) = M \ ,$$

les vecteurs $\tilde{e}_i$ de $\tilde{\mathcal{B}}$ sont données par les relations $\varphi(e_i) = \tilde{e}_i$, et φ est un isomorphisme puisque M est inversible, de sorte que $\tilde{\mathcal{B}}$ est une base. On a alors que

$$\begin{aligned} M^{-1}AM &= M^{-1}_{\mathcal{B}\to\tilde{\mathcal{B}}} M_{\mathcal{B}\mathcal{B}}(f) M_{\mathcal{B}\to\tilde{\mathcal{B}}} \\ &= M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f) \ . \end{aligned}$$

Par suite, dire que A est diagonalisable entraîne que f est diagonalisable. La réciproque est vraie, et A est diagonalisable si et seulement si f l'est. On a $M^{-1}AM = D$ avec $A = M_{\mathcal{B}\mathcal{B}}(f)$ qui équivaut alors à $M = M_{\mathcal{B}\to\tilde{\mathcal{B}}}$ et $D = M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f)$. En particulier on a le théorème suivant.

Théorème 29.1. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie et $\mathcal{B}$ une base de E. Soit aussi $A = M_{\mathcal{B}\mathcal{B}}(f)$ où $f \in End(E)$. Alors A est diagonalisable si et seulement si f est diagonalisable et on a que $M^{-1}AM$ est une matrice diagonale si et seulement si $M_{\mathcal{B}\to\tilde{\mathcal{B}}} = M$ où $\tilde{\mathcal{B}}$ est une base qui diagonalise f.*

Dans la pratique, nul n'est besoin de déterminer f. On calcule le polynôme caractéristique $P(X) = det(A - X\mathrm{Id}_n)$, où Id_n est la matrice identité $n \times n$. On calcule les racines réelles de P, et on récupère ce qui a été dit dans la section précédente.

Términologie: Si A est une matrice $n \times n$ on appelle valeur propre de A, vecteur propre de A, espace propre de A et polynôme caractéristique de A les données correspondantes pour l'endomorphisme $f : \mathbb{R}^n \to \mathbb{R}^n$ donné par $A = M_{\mathcal{B}\mathcal{B}}(f)$ dans la base canonique $\mathcal{B}$ de $\mathbb{R}^n$.

Du théorème de Cayley-Hamilton pour les endomorphismes on tire très facilement le théorème de Cayley-Hamilton pour les matrices.

Théorème 29.2 (Théorème de Cayley-Hamilton pour les matrices)**.** *Soit A est une matrice $n \times n$. Soit P le polynôme caractéristique de A. On a alors $P(A) = 0$.*

Le terme a_0 de P est ici à comprendre comme $a_0\mathrm{Id}_n$. Si par exemple $n = 3$, et si $P(X) = -X^3 + 2X^2 + X - 4$, alors $-A^3 + 2A^2 + A - 4\mathrm{Id}_3 = 0$.

Exercice: Soit $\alpha, a, b, c \in \mathbb{R}$ des nombres réels. On considère la matrice

$$A = \begin{pmatrix} \alpha & a & b \\ 0 & \alpha & c \\ 0 & 0 & \alpha \end{pmatrix} \ .$$

Montrer que A est diagonalisable si et seulement si $a = b = c = 0$.

Solution: Si $a = b = c = 0$ alors $A = \alpha\mathrm{Id}_3$ et A est clairement diagonalisable (puisque diagonale). A l'inverse, supposons que A est diagonalisable. Son polynôme caractéristique est

$$P(X) = \det \begin{pmatrix} \alpha - X & a & b \\ 0 & \alpha - X & c \\ 0 & 0 & \alpha - X \end{pmatrix} = -(X - \alpha)^3$$

(le déterminant d'une matrice triangulaire est égal au produit de ses termes diagonaux). Donc A a une seule valeur propre qui est α. On a supposé que A était diagonalisable et donc il existe P une matrice inversible 3×3 telle que

$$P^{-1}AP = \alpha\mathrm{Id}_3 \ .$$

Soit encore, en multipliant à -gauche par P et à droite par P^{-1},

$$A = \alpha P \mathrm{Id}_3 P^{-1} = \alpha P P^{-1} = \alpha \mathrm{Id}_3$$

ce qui n'est possible que si $a = b = c = 0$. $\square$

La rang d'une matrice diagonalisable est le nombre de valeurs propres non nulles (compté avec multiplicité) ou, ce qui revient au même, la somme des dimensions des espaces propres associés à une valeur propre non nulle.

30. Diagonalisation et projecteurs

On démontre ici le résultat suivant.

Théorème 30.1. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie et $u \in End(E)$ un endomorphisme de E. Alors u est diagonalisable si et seulement si u est combinaison linéaire de projecteurs $p_1, \dots, p_k$ vérifiant que $p_i \circ p_j = 0$ pour tous $i \neq j$ dans $\{1, \dots, k\}$.*

Démonstration. **(i)** On suppose que u est diagonalisable. Soient $\lambda_1, \dots, \lambda_k$ les valeurs propres distinctes de u et $E_1, \dots, E_k$ les espaces propres associés. On a

$$E = E_1 \oplus \cdots \oplus E_k \ .$$

Soit p_i la projection sur E_i parallèlement à la somme $\bigoplus_{j \neq i} E_j$ des E_j pour $j \neq i$. Pour tout $x \in E$, $\exists! x_1 \in E_1, \dots, \exists! x_k \in E_k$ tels que $x = x_1 + \cdots + x_k$. Par suite

$$u(x) = \sum_{i=1}^{k} \lambda_i x_i$$

tandis que $\left(\sum_{i=1}^{k} \lambda_i p_i\right)(x_j) = \lambda_j x_j$ pour tout j puisque $p_i \circ p_j = 0$ si $i \neq j$ et puisque $x_j \in E_j \Rightarrow p_j(x_j) = x_j$. On en déduit que

$$\left(\sum_{i=1}^{k} \lambda_i p_i\right)(x) = \sum_{i=1}^{k} \lambda_i x_i = u(x)$$

pour tout x. Donc u s'écrit comme une combinaison linéaire de projecteurs $p_1, \dots, p_k$. De plus $\mathrm{Im}(p_j) \subset \mathrm{Ker}(p_i)$ si $i \neq j$ et ainsi $p_i \circ p_j = 0$ pour tout $i \neq j$.

(ii) Réciproquement on suppose que u s'écrit comme une combinaison linéaire de projecteurs $p_1, \dots, p_k$ vérifiant que $p_i \circ p_j = 0$ pour tous $i \neq j$ dans $\{1, \dots, k\}$. On écrit

$$u = \sum_{i=1}^{k} \lambda_i p_i \ .$$

Pour un projecteur p, $E = \mathrm{Ker}(p) \oplus \mathrm{Im}(p)$. Un projecteur est donc diagonalisable avec pour valeurs propres 0 et 1 (d'espaces propres correspondant $\mathrm{Ker}(p)$ et $\mathrm{Im}(p)$ puisque $p^2 = p$). Ici les p_i commutent deux à deux (puisque $p_j \circ p_i = 0$ si $i \neq j$) et donc, avec le Théorème 31.5 de diagonalisation multiple, on obtient que u est diagonalisable. $\square$

31. Diagonalisation simultanée

On cherche à savoir sous quelles conditions deux endomorphismes vont être diagonalisables simultanément. Un premier résultat dont nous aurons besoin est le résultat suivant. Il s'agit d'une petite variation autour du théorème de la base incomplète.

Lemme 31.1. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie n, $(u_1, \dots, u_p)$ une famille libre de E, avec $p < n$, et $\mathcal{B}$ une base de E. On peut compléter $(u_1, \dots, u_p)$ par des vecteurs $e_{p+1}, \dots, e_n$ de $\mathcal{B}$ pour obtenir une base de E.*

Démonstration. Notons $F_0 = \mathrm{Vect}(u_1, \dots, u_p)$. Clairement il existe $e_{p+1} \in \mathcal{B}$ qui est tel que $e_{p+1} \notin F_0$ car sinon on aurait $F_0 = E$ ce qui est impossible (puisque F_0 est générée par p vecteurs, $p < n$). La famille $(u_1, \dots, u_p, e_{p+1})$ est alors encore une famille libre puisque si

$$\lambda_1 u_1 + \cdots + \lambda_p u_p + \lambda_{p+1} e_{p+1} = 0 ,$$

alors soit $\lambda_{p+1} \neq 0$, et en divisant par λ_{p+1} l'égalité ci-dessus, et en passant les termes en $u_1, \dots, u_p$ de l'autre côté de l'égalité, on vient d'écrire que e_{p+1} s'écrit comme combinaison linéaire des $u_1, \dots, u_p$, donc que $e_{p+1} \in F_0$, ce qui est impossible, soit $\lambda_{p+1} = 0$, mais alors, comme $(u_1, \dots, u_p)$ est libre, on a aussi $\lambda_1 = \cdots = \lambda_p = 0$. Si $p+1 = n$, alors $(u_1, \dots, u_p, e_{p+1})$ est libre à n éléments dans E qui est de dimension n, donc c'est une base de E et on a obtenu ce que l'on voulait. Sinon $p + 1 < n$. On pose $F_1 = \mathrm{Vect}(u_1, \dots, u_p, e_{p+1})$, et on recommence. Le processus s'arrête au bout d'un nombre fini $n - p$ d'étapes. □

Un résultat clef est ensuite donné par le résultat suivant.

Théorème 31.1. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie, $F \subset E$ un sous espace vectoriel de E et $f \in End(E)$ un endomorphisme de E. On suppose que F est stable par f, à savoir que $f(F) \subset F$. On note $f_{|F}$ la restriction de f à F qui devient donc un endomorphisme de F. Si f est diagonalisable sur E alors $f_{|F}$ est diagonalisable sur F.*

Démonstration. Soit $\mathcal{B}_1$ une base de F. Comme f est diagonalisable, il existe $\tilde{\mathcal{B}}$ une base de E qui diagonalise f. On complete $\mathcal{B}_1$ par des vecteurs de $\tilde{\mathcal{B}}$ en utilisant le lemme précédent. Soit $\mathcal{B}_2$ la famille des vecteurs rajoutés. Soit H l'espace vectoriel de base $\mathcal{B}_2$. On a $E = F \oplus H$ et $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ (avec abus de notation) est une base de E. De plus, comme les vecteurs de $\mathcal{B}_2$ sont des vecteurs propres de f, on a facilement que H est lui aussi stable par f au sens où $f(H) \subset H$. On note g la restriction de f à F et h la restriction de f à H. La matrice de représentation de f dans $\mathcal{B}$ est du type

$$M_{\mathcal{B}\mathcal{B}}(f) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right) ,$$

où $A = M_{\mathcal{B}_1\mathcal{B}_1}(g)$ est $p \times p$, avec $p = \dim(F)$, et $B = M_{\mathcal{B}_2\mathcal{B}_2}(h)$ est $q \times q$, avec $q = n - p = \dim(H)$. Par suite

$$M_{\mathcal{B}\mathcal{B}}(f) - X\mathrm{Id}_n = \left(\begin{array}{c|c} A - X\mathrm{Id}_p & 0 \\ \hline 0 & B - X\mathrm{Id}_q \end{array}\right) .$$

En remarquant que

$$\left(\begin{array}{c|c} A - X\mathrm{Id}_p & 0 \\ \hline 0 & B - X\mathrm{Id}_q \end{array}\right) = \left(\begin{array}{c|c} \mathrm{Id}_p & 0 \\ \hline 0 & B - X\mathrm{Id}_q \end{array}\right) \times \left(\begin{array}{c|c} A - X\mathrm{Id}_p & 0 \\ \hline 0 & \mathrm{Id}_q \end{array}\right)$$

et puisque $\det(MN) = \det(M)\det(N)$, on obtient facilement que si $\hat{P}$ est le polynôme caractéristique de f dans E, P est le polynôme caractéristique de g dans F et Q est le polynôme caractéristique de h dans H, alors

$$\hat{P}(X) = P(X)Q(X) \ .$$

Comme f est diagonalisable dans E elle a toutes ses valeurs propres dans $\mathbb{R}$. Sachant qu'une racine de P est forcément une racine de $\hat{P}$ en raison de ce que l'on vient d'écrire, on voit que g a toutes ses valeurs propres dans $\mathbb{R}$ et que les valeurs propres de g sont des valeurs propres de f. De même pour h. Soit λ une valeur propre de f, donc une racine de $\hat{P}$. Trois cas de figures se présentent:

(1) λ est racine de P mais pas de Q

(2) λ est racine de Q mais pas de P

(3) λ est racine de P et de Q.

Dans le cas (1), λ est valeur propre de g mais pas de h. Si $\hat{E}_\lambda$ est l'espace propre de f associé à λ et E_λ est l'espace propre de g associé à λ, on a alors que $\hat{E}_\lambda = E_\lambda$. En effet, $E_\lambda \subset \hat{E}_\lambda$. Réciproquement, si $x \in \hat{E}_\lambda$, en décomposant suivant $F \oplus H$ on écrit que $x = u + v$ avec $u \in F$ et $v \in H$. On a alors que

$$\begin{aligned} f(x) &= \lambda x \\ &= \lambda u + \lambda v \\ &= f(u) + f(v) \end{aligned}$$

et donc

$$f(u) - \lambda u = -\left(f(v) - \lambda v\right) \ .$$

Or $f(u) - \lambda u \in F$, $f(v) - \lambda v \in H$ (puisque F et H sont stables par f) et $F \cap H = \{0\}$ (puisque F et H sont en somme directe). Comme λ n'est pas valeur propre de h, forcément $v = 0$. Donc $x \in F$ et ainsi $x \in E_\lambda$. D'où l'egalité. Même chose pour (2) mais avec h au lieu de g. Si $\tilde{E}_\lambda$ est l'espace propre de h associé à λ alors $E_\lambda = \tilde{E}_\lambda$. Supposons maintenant (3), donc que λ est à la fois racine de P et de Q. Dans ce cas le petit calcul ci-dessus donne que

$$\hat{E}_\lambda = E_\lambda \oplus \tilde{E}_\lambda \ .$$

En effet on a toujours $E_\lambda \cap \tilde{E}_\lambda = \{0\}$, donc $E_\lambda \oplus \tilde{E}_\lambda$, et $E_\lambda \oplus \tilde{E}_\lambda \subset \hat{E}_\lambda$ de façon évidente. Le petit calcul ci-dessus, lui, montre que $\hat{E}_\lambda \subset E_\lambda \oplus \tilde{E}_\lambda$. Comme f est diagonalisable, E est somme (directe) des espaces propres $\hat{E}_\lambda$ de f et, en vertue de ce que l'on vient de dire, on peut écrire que

$$E = \Big(\sum_{\lambda/P(\lambda)=0} E_\lambda\Big) \oplus \Big(\sum_{\lambda/Q(\lambda)=0} \tilde{E}_\lambda\Big) \ .$$

Clairement on a alors que $F = \sum_{\lambda/P(\lambda)=0} E_\lambda$ car si $E = F \oplus H = \tilde{F} \oplus \tilde{H}$ avec $\tilde{F} \subset F$ et $\tilde{H} \subset H$, alors forcément $F = \tilde{F}$ et $H = \tilde{H}$. Donc F est somme des espaces propres de g, et donc g est diagonalisable. C'est ce qu'il fallait démontrer. $\square$

Le fait que P divise $\hat{P}$, obtenu dans la preuve du Théorème 31.1 sous l'hypothèse que f est diagonalisable reste vrai sans cette hypothèse.

Théorème 31.2. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie, $F \subset E$ un sous espace vectoriel de E et $f \in End(E)$ un endomorphisme de E. On suppose que F est stable par f, à savoir donc que $f(F) \subset F$. On note $f_{|F}$ la restriction de f à F qui devient donc un endomorphisme de F. Si P est le polynôme caractéristique de $f_{|F}$ et $\hat{P}$ est le polynôme caractéristique de f, alors P divise $\hat{P}$ au sens où il existe un polynôme Q qui est tel que $\hat{P} = PQ$.*

Démonstration. Soit $\mathcal{B}$ une base de F que l'on complète en une base $\mathcal{B}'$ de E. La matrice de représentation de f dans $\mathcal{B}'$ s'écrit

$$M_{\mathcal{B}\mathcal{B}'} = \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array}\right)$$

où si $p = \dim(F)$ et $n = \dim(E)$, alors A est $p \times p$, B est $p \times (n-p)$, C est $(n-p) \times (n-p)$ et le 0 est la matrice nulle $(n-p) \times p$. On vérifie alors facilement avec le Lemme 28.1 que $\hat{P} = PQ$ où Q est le polynôme caractéristique de C. D'où le résultat. ☐

La clef dans la diagonalisation simultanée est la remarque que si deux endomorphismes f et g commutent, alors les espaces propres de l'un sont stables par l'autre. C'est l'objet de l'exercice de la Section 23. Par exemple si λ est valeur propre de f et E_λ est l'espace propre associé, alors E_λ est stable par g. En effet, pour tout $u \in E_\lambda$, $f(u) = \lambda u$. Donc $g(f(u)) = g(\lambda u) = \lambda g(u)$. Et puisque f et g commutent,

$$f(g(u)) = \lambda g(u)$$

de sorte que $g(u) \in E_\lambda$. On a donc bien montré que $g(E_\lambda) \subset E_\lambda$. Le théorème qui suit répond à la question de la diagonalisation simultanée.

Théorème 31.3. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie et soient $f, g \in End(E)$ deux endomorphismes de E. On suppose que f et g sont diagonalisables et que f et g commutent (à savoir que $f \circ g = g \circ f$). Il existe alors $\tilde{\mathcal{B}}$ une base de E pour laquelle les matrices $M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f)$ et $M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(g)$ sont toutes deux diagonales. On dit que f et g ont été diagonalisées simultanément.*

Démonstration. On raisonne par récurrence sur la dimension. Si $n = 1$ le résultat est trivialement vrai. Supposons qu'il soit vrai pour tout espace vectoriel de dimension inférieure ou égale à n (récurrence totale). Soit E un espace vectoriel de dimension $n+1$ et soient f, g deux endomorphismes diagonalisables de E tels que $g \circ f = f \circ g$. On note $\lambda_1, \ldots, \lambda_k$ les valeurs propres distinctes de f. Si $k = 1$, alors $f = \lambda_1 \mathrm{Id}_E$ et toute base qui diagonalise g diagonalise f. Le fait que f et g soient diagonalisables dans une base commune est donc vrai. Sinon $k \geq 2$. Notons E_i les sous espaces propres de f. Les E_i sont stables par g (cf. ci-dessus). En considérant les restrictions de f et g aux E_i, comme $\dim(E_i) \leq n$ puisque $k \geq 2$, et en raison du théorème 31.1, on peut appliquer l'hypothèse de récurence et on obtient qu'il existe une base $\tilde{\mathcal{B}}_i$ qui diagonalise f et g dans E_i. En posant $\tilde{\mathcal{B}} = (\tilde{\mathcal{B}}_1, \ldots, \tilde{\mathcal{B}}_n)$ on obtient que $\tilde{\mathcal{B}}$ est une base de E et que $\tilde{\mathcal{B}}$ diagonalise à la fois f et g. La récurrence est achevée. Le théorème est démontré. ☐

Un autre résultat (important) dans le cas de n valeurs propres distinctes est le suivant.

Théorème 31.4. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie n et soient $f, g \in End(E)$ deux endomorphismes de E. On suppose que f a n valeurs propres* *distinctes et que f et g commutent (à savoir que $f \circ g = g \circ f$). Alors toute base de E qui diagonalise f diagonalise aussi g. Autrement dit, pour toute base $\mathcal{B}$ de E, si $M_{\mathcal{B}\mathcal{B}}(f)$ est diagonale alors $M_{\mathcal{B}\mathcal{B}}(g)$ est aussi diagonale.*

Démonstration. Notons $\lambda_1, \ldots, \lambda_n$ est les valeurs propres de f et $E_1, \ldots, E_n$ les espaces propres associés. Comme $\dim(E_i) \geq 1$ pour tout i, et comme $\sum_{i=1}^{n} \dim(E_i) \leq n$ puisque la somme des E_i est directe, on obtient que $\dim(E_i) = 1$ pour tout i. Une base qui diagonalise f va être du type $\tilde{\mathcal{B}} = (\tilde{e}_1, \ldots, \tilde{e}_n)$, où les $\tilde{e}_i$ sont des vecteurs directeurs de E_i. Comme f et g commutent, g laisse stable E_i (cf. ci-dessus). Donc $g(\tilde{e}_i) \in E_i$ et donc il existe $\mu_i \in \mathbb{R}$ tel que $g(\tilde{e}_i) = \mu_i \tilde{e}_i$. On en déduit que $\tilde{B}$ diagonalise aussi g. □

Le cas de deux endomorphismes diagonalisables qui commutent s'étend à toute famille d'endomorphismes diagonalisables commutants.

Théorème 31.5. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie n et soit $(u_i)_{i \in I}$ une famille (peut-être même infinie) d'endomorphismes diagonalisables de E qui commutent deux à deux. Il existe alors une base $\mathcal{B}$ de E pour laquelle les matrices $M_{\mathcal{B}\mathcal{B}}(u_i)$ pour $i \in I$ sont toutes diagonales.*

Démonstration. **(i)** On montre pour commencer que pour toute famille finie $u_1, \ldots, u_p$ d'endomorphismes diagonalisables de E qui commutent deux à deux, il existe une base $\mathcal{B}$ de E pour laquelle les matrices $M_{\mathcal{B}\mathcal{B}}(u_i)$ pour $i = 1, \ldots, p$ sont toutes diagonales. On procède par récurrence sur p. Si $p = 2$ il s'agit de ce qui a été dit plus haut. On suppose maintenant que la propriété est vraie à l'ordre p. Soient alors $u_1, \ldots, u_{p+1}$ une famille de $p + 1$ endomorphismes diagonalisables de E qui commutent deux à deux. Soit $\lambda \in \mathbb{R}$ une valeur propre de u_{p+1} et soit E_λ l'espace propre correspondant. L'espace E_λ est stable par les endomorphismes $u_1, \ldots, u_p$ puisque les u_i commutent entre eux. Les $u_1, \ldots, u_p$ induisent donc des endomorphismes $v_i = u_{i|E_\lambda}$ de E_λ, $i = 1, \ldots, p$. Ces endomorphismes v_i commutent deux à deux puisque les u_i commutent deux à deux et il sont diagonalisables en vertue du Théorème 31.1. Par hypothèse de récurrence il existe ainsi une base $\mathcal{B}_\lambda$ de E_λ qui diagonalise les $v_1, \ldots, v_p$. Les vecteurs de $\mathcal{B}_\lambda$ étant des vecteurs propres des v_i ce sont aussi des vecteurs propres des u_i. Ce sont encore des vecteurs propres de u_{n+1} puisque les vecteurs de $\mathcal{B}_\lambda$ sont dans E_λ. On a

$$E = \bigoplus_{\lambda} E_\lambda \ ,$$

où la somme a lieu sur les valeurs propres distinctes de u_{p+1}, puisque u_{p+1} est diagonalisable. La réunion des bases $\mathcal{B}_\lambda$ devient ainsi une base de E constituée de vecteurs propres des $u_1, \ldots, u_{p+1}$. La propriété est donc vraie à l'ordre $p + 1$ et la récurrence est achevée.

(ii) On traite maintenant le cas où I est infini. En vertue de ce qui vient d'être démontré, toute combinaison linéaire finie des u_i est diagonalisable. Donc toute élément de $\mathrm{Vect}(\{u_i, i \in I\})$ est diagonalisable. Or $\mathrm{Vect}(\{u_i, i \in I\}) \subset \mathrm{End}(E)$ qui est de dimension finie. Ainsi $\mathrm{Vect}(\{u_i, i \in I\})$ est de dimension finie. Soit $(w_1, \ldots, w_m)$ une base de $\mathrm{Vect}(\{u_i, i \in I\})$. Clairement les w_i commutent deux à deux (en tant que combinaisons linéaires des u_i qui commutent deux à deux) et, comme on vient de le voir, ils sont diagonalisables. Il existe donc une base $\mathcal{B}$ de E qui diagonalise les w_i, $i = 1, \ldots, m$. Dès lors $\mathcal{B}$ diagonalise tous les éléments de $\mathrm{Vect}(\{u_i, i \in I\})$, et donc tous les u_i, $i \in I$. Le théorème est démontré. □

32. Racines de matrices

Soient A et B sont deux matrices $n\times n$. On note $\mathcal{B}$ la base canonique de $\mathbb{R}^n$ et on introduit les endomorphismes f et g de $\mathbb{R}^n$ définis par $M_{\mathcal{B}\mathcal{B}}(f)=A$ et $M_{\mathcal{B}\mathcal{B}}(g)=B$. Comme $AB=M_{\mathcal{B}\mathcal{B}}(f\circ g)$ et $BA=M_{\mathcal{B}\mathcal{B}}(g\circ f)$, on voit que

$$f \text{ et } g \text{ commutent si et seulement si } A \text{ et } B \text{ commutent.}$$

De plus, dire que M inversible est telle que $M^{-1}AM$ est diagonale (resp. $M^{-1}BM$ est diagonale) c'est dire que $M=M_{\mathcal{B}\to\tilde{\mathcal{B}}}$ où $\tilde{\mathcal{B}}$ est une base pour laquelle $M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f)$ est diagonale (resp. $M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(g)$ est diagonale). Des deux théorèmes de diagonalisation simultanée démontrés ci-dessus, et de la théorie de la diagonalisation des matrices, on tire ainsi le résultat suivant.

Théorème 32.1. *Soient A et B deux matrices $n\times n$. On suppose que A et B commutent, donc que $AB=BA$.*

(1) *Si A et B sont toutes deux diagonalisables, alors il existe une matrice $n\times n$ inversible M pour laquelle $M^{-1}AM$ et $M^{-1}BM$ sont toutes deux diagonales.*

(2) *Si A a n valeurs propres distinctes, alors A et B sont diagonalisables et pour toute matrice $n\times n$ inversible M qui est telle que $M^{-1}AM$ est diagonale on a que $M^{-1}BM$ est aussi diagonale.*

Soit A une matrice $n\times n$ donnée et soit $p\in\mathbb{N}^\star$ donné. On cherche à résoudre l'équation matricielle

$$X^p=A\ , \tag{32.1}$$

où X est une matrice $n\times n$. La première remarque, fondamentale, est que les solutions X de (32.1) sont à rechercher parmi les matrices qui commutent avec A. En effet, si X est solution de (32.1), alors clairement $AX=XA$ puisque dans les deux cas on trouve $AX=X^{p+1}$ et $XA=X^{p+1}$. Donc si X est solution de l'équation alors A et X commutent. On suppose maintenant que A est diagonalisable et on se place dans les deux cas du théorème ci-dessus.

Cas 1: On ne cherche pas vraiment toutes les solutions de (32.1), mais les solutions de (32.1) qui sont diagonalisables. On note

$$S=\{X \text{ solutions de (32.1) qui sont diagonalisables}\}\ .$$

Pour tout $X\in S$, il existe M une matrice $n\times n$ inversible et D une matrice diagonale $n\times n$ constituée des valeurs propres de A telles que $M^{-1}AM=D$ et $M^{-1}XM$ est diagonale. On note $\tilde{D}=\mathrm{Diag}(x_1,\dots,x_n)$ la matrice $n\times n$ diagonale de diagonale $x_1,\dots,x_n$ qui est reliée à X par $M^{-1}XM=\tilde{D}$. Alors

$$\begin{aligned} X^p=A &\Leftrightarrow (M\tilde{D}M^{-1})^p=A\\ &\Leftrightarrow M\tilde{D}^pM^{-1}=(MDM^{-1})\\ &\Leftrightarrow \tilde{D}^p=D\ . \end{aligned}$$

On est donc ramené à l'étude de l'équation

$$\tilde{D}^p=D \tag{32.2}$$

avec D matrice diagonale donnée et $\tilde{D}$ matrice diagonale inconnue. Notons $D=\mathrm{Diag}(\lambda_1,\dots,\lambda_n)$. On se ramène donc aux équations dans $\mathbb{R}$ qui s'écrivent $x^p=\lambda_i$, $i=1,\dots,n$. Si elles ont toutes des solutions on récupère les solutions de $X^p=A$ à partir de $\tilde{D}$ et de la formule $X=M\tilde{D}M^{-1}$. Attention il y a toutes les combinaisons possibles des solutions des équations réelles qui interviennent. Par contre si l'une des ces équations n'a pas de solution (parce qu'on est dans $\mathbb{R}$ et parce que p est pair et $\lambda_i < 0$ pour un i) alors il n'y a pas de solution à l'équation matricielle $X^p = A$. A priori nous n'avons pas de contrôle sur M qui diagonalise à la fois A et B, mais toute matrice $M\tilde{D}M^{-1}$ est solution. Donc

$$S = \left\{ M\tilde{D}M^{-1},\ M \in \mathcal{D}_A,\ \tilde{D} \text{ solution de } (32.2) \right\}\ , \tag{32.3}$$

où $\mathcal{D}_A$ est l'ensemble des matrices inversibles M qui sont telles que $M^{-1}AM = D$. En particulier, en fixant un $M \in \mathcal{D}_A$, on fabrique facilement une racine $p$ième de A lorsque les équations $x^p = \lambda_i$, $i = 1, \dots, n$, ont une solution. Soit $M_0 \in \mathcal{D}_A$ quelconque fixée. A titre de dernière remarque, on montre sans trop de difficulté que

$$S = \left\{ M_0\tilde{D}M_0^{-1},\ \tilde{D} \text{ solution de } (32.2) \right\}\ , \tag{32.4}$$

à savoir que l'on obtient toutes les solutions sans avoir besoin de faire varier M dans $\mathcal{D}_A$. Soit en effet $M\hat{D}M^{-1}$ quelconque dans le S de (32.3). Donc $M \in \mathcal{D}_A$ et $\hat{D}$ est solution de (32.2). On pose

$$\tilde{D} = (M^{-1}M_0)^{-1}\hat{D}(M^{-1}M_0)\ .$$

On a alors $M_0\tilde{D}M_0^{-1} = M\hat{D}M^{-1}$ tandis que

$$\begin{aligned} \tilde{D}^p &= (M^{-1}M_0)^{-1}\hat{D}^p(M^{-1}M_0) \\ &= (M^{-1}M_0)^{-1}D(M^{-1}M_0) \\ &= M_0^{-1}\big[MDM^{-1}\big]M_0 \\ &= M_0^{-1}AM_0 = D \end{aligned}$$

et ainsi $\tilde{D}$ est solution de (32.2). Donc $M\hat{D}M^{-1}$ est dans le S de (32.4) et puisque $M\hat{D}M^{-1}$ est quelconque dans le S de (32.3), on a montré que pour $M_0 \in \mathcal{D}_A$ quelconque fixé,

$$\begin{aligned} &\left\{ M\tilde{D}M^{-1},\ M \in \mathcal{D}_A,\ \tilde{D} \text{ solution de } (32.2) \right\} \\ &\subset \left\{ M_0\tilde{D}M_0^{-1},\ \tilde{D} \text{ solution de } (32.2) \right\} \end{aligned}$$

L'inclusion réciproque étant immédiate on a bien l'égalité souhaitée entre les deux S de (32.3) et (32.4).

Cas 2: C'est un cas plus simple et plus souvent rencontré. On suppose que A a n valeurs propres distinctes. Donc A est diagonalisable. Comme X commute avec A et comme A a n valeurs propres distinctes, X est automatiquement diagonalisable et toute matrice inversible M pour laquelle $M^{-1}AM$ est diagonale est aussi telle que $M^{-1}XM$ est diagonale. Là on va obtenir toutes les matrices X solutions de (32.1) sans avoir à imposer que X est diagonalisable (puisque le fait que X est diagonalisable est ici donné gratuitement). On fixe M inversible $n \times n$ et D diagonale qui sont données par $M^{-1}AM = D$, et donc qui sont données par la diagonalisation de A. Si S est l'ensemble des solutions de (32.1), alors

$$S = \left\{ M\tilde{D}M^{-1},\ \tilde{D} \text{ solution de } (32.2) \right\}\ .$$

Cette fois-ci on a un contrôle sur M puisque M est donné par la seule diagonalisation de A. Là encore, si p est pair, il se peut que $S = \emptyset$ si, dans D, il y a un terme strictement négatif sur la diagonale.

Les équations $x^p = a$ avec p pair ont, dans $\mathbb{R}$, soit 0 solution (si $a < 0$), soit 1 solution (si $a = 0$), soit 2 solutions si $a > 0$. Avec p impair elles ont toujours une et une seule solution. Donc, sous les conditions des cas 1 et 2 ci-dessus (donc en particulier on parle de solution diagonalisable dans le cas 1), l'équation (32.1) a entre 0 et 2^n solutions si p est pair, et a une unique solution si p est impair.

Exercice: Soient A et B les matrices réelles 3×3 données par

$$A = \begin{pmatrix} 1 & 7 & -7 \\ 4 & 22 & -23 \\ 4 & 14 & -15 \end{pmatrix} \text{ et } B = \begin{pmatrix} 5 & -3 & 2 \\ 6 & -4 & 4 \\ 4 & -4 & 5 \end{pmatrix} .$$

Combien y a-t-il de matrices X qui satisfont l'équation $X^2 = A$? Même question pour l'équation $X^3 = A$? Même question pour l'équation $X^2 = B$.

Solution: Soit P le polynôme caractéristique de A. Par le calcul on trouve que $P(X) = -(X-1)(X+1)(X-8)$. Donc A est diagonalisable puisqu'il y a 3 valeurs propres distinctes (qui sont ici -1, 1 et 8) et il existe M inversible telle que

$$M^{-1}AM = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 8 \end{pmatrix}$$

Clairement $AX = XA$ si $X^2 = A$ ou si $X^3 = A$ (car $X^p = A$ implique que $AX = X^{p+1}$ et $XA = X^{p+1}$) et donc, $M^{-1}XM$ est aussi une matrice diagonale (Théorème 32.1, cas 2). On cherche alors X sous la forme $X = M\tilde{D}M^{-1}$ avec $\tilde{D}$ matrice diagonale. Dès lors, les équations $X^2 = A$ et $X^3 = A$ se ramènent aux équations diagonales $\tilde{D}^2 = D$ et $\tilde{D}^3 = D$, où D est la matrice diagonale ci-dessus. En effet

$$(M\tilde{D}M^{-1})^p = A \ \Leftrightarrow \ M\tilde{D}^pM^{-1} = MDM^{-1} \ \Leftrightarrow \ \tilde{D}^p = D .$$

Si la diagonale de $\tilde{D}$ est constituée des a, b, c on veut donc $a^2 = -1$, $b^2 = 1$ et $c^2 = 8$ pour l'équation $X^2 = A$ et $a^3 = -1$, $b^3 = 1$ et $c^3 = 8$ pour l'équation $X^3 = A$. L'équation $a^2 = -1$ est impossible dans $\mathbb{R}$. Il n'y a donc aucune solution à l'équation $X^2 = A$. Toujours dans $\mathbb{R}$ il y a par contre une seule solution $(a, b, c) \in \mathbb{R}^3$ aux équations $a^3 = -1$, $b^3 = 1$ et $c^3 = 8$ (la fonction $x \to x^3$ est strictement croissante de $\mathbb{R}$ dans $\mathbb{R}$). Elle est donnée par $a = -1$, $b = 1$ et $c = 2$. Donc il y a une seule matrice réelle X qui vérifie $X^3 = A$, et elle est donnée par

$$X = M \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} M^{-1}$$

Si on veut une forme explicite il faut calculer M et M^{-1}, la matrice M étant donnée par la diagonalisation de A. On passe maintenant au cas de B. Si P est le polynôme caractéristique de B, on trouve après calculs que $P(X) = -(X-1)(X-2)(X-3)$. Donc B est diagonalisable puisqu'il y a 3 valeurs propres distinctes (qui sont ici 1, 2 et 3) et il existe M inversible telle que

$$M^{-1}BM = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

Clairement $BX = XB$ si $X^2 = B$ (car $X^2 = B$ implique que $BX = X^3$ et $XB = X^3$) et donc, $M^{-1}XM$ est aussi une matrice diagonale (Théorème 32.1, cas 2). On cherche alors X sous la forme $X = M\tilde{D}M^{-1}$ avec $\tilde{D}$ matrice diagonale. Dès lors, l'équation $X^2 = B$ se ramène à l'équation diagonale $\tilde{D}^2 = D$, où D est la matrice diagonale ci-dessus. En effet

$$(M\tilde{D}M^{-1})^2 = B \;\Leftrightarrow\; M\tilde{D}^2M^{-1} = MDM^{-1} \;\Leftrightarrow\; \tilde{D}^p = D \; .$$

Si la diagonale de $\tilde{D}$ est constituée des a, b, c on veut donc $a^2 = 1$, $b^2 = 2$ et $c^2 = 3$. On trouve donc $a = \pm 1$, $b = \pm\sqrt{2}$ et $c = \pm\sqrt{3}$. Il y a alors 8 solutions en tout qui sont données par

$$X = M \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \pm\sqrt{2} & 0 \\ 0 & 0 & \pm\sqrt{3} \end{pmatrix} M^{-1} \; .$$

Là encore, si on veut une forme explicite, il faut calculer M et M^{-1}, la matrice M étant donnée par la diagonalisation de B. □

33. Polynôme minimal et diagonalisation

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie. Soit $f \in \mathrm{End}(E)$ un endomorphisme de E. Un polynôme réel P est dit un polynôme annulateur pour f si $P(f) = 0$ au sens du théorème de Cayley-Hamilton. D'après ce même théorème, le polynôme caractéristique de f est un polynôme annulateur pour f. Le polynôme minimal défini ci-dessous est en fait le polynôme unitaire de plus bas degré qui annule f. Unitaire signifie ici que le coefficient du terme de plus haut degré vaut 1.

Théorème 33.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie. Soit $f \in$ End(E) un endomorphisme de E. Il existe un et un seul polynôme unitaire P_m qui annule f et qui vérifie que tout polynôme annulateur P de f est multiple de P_m au sens où si P annule f alors nécessairement $P = P_mQ$ où Q est un polynôme. On dit que P_m est le polynôme minimal de f.*

Démonstration. Soit $\mathcal{A}$ l'ensemble des polynômes anhulateurs de f. Cet ensemble est non vide puisque, d'après Cayley-Hamilton, le polynôme cractéristique de f est un polynôme annulateur de f. On note

$$p = \inf\{d \in \mathbb{N}^\star \; , \; d \text{ degré des polynômes annulateurs de } f\} \; .$$

Les degrés sont des entiers et donc il existe $P_m \in \mathcal{A}$ un polynôme annulateur de f de degré p. Soit $P \in \mathcal{A}$ un (autre) polynôme annulateur de f. Par division polynomiale de P par P_m il existe un couple (Q, R) de polynômes tels que $P = QP_m + R$ avec $d^0R < d^0P_m$ (où d^0R et d^0P_m représentent le degrés de R et P_m). On a $P(f) = 0$ et $P_m(f) = 0$. On en déduit que $R(f) = 0$. Or P_m est de degré $p \geq 1$ minimal. Donc forcément R est le polynôme nul et ainsi, P_m divise P. Comme $P \in \mathcal{A}$ est quelconque, le théorème est démontré. □

Le théorème de Cayley-Hamilton nous dit que le polynôme caractéristique est un polynôme annulateur. En dimension n on a donc au moins un polynôme annulateur de degré n. On peut aussi produire des polynômes annulateurs en fonction du rang de f.

Théorème 33.2. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie. Soit $f \in End(E)$ un endomorphisme de E de rang r. Il existe un polynôme annulateur de f qui est de degré $r+1$.*

Démonstration. Le rang est la dimension de l'espace image. On note $e_1, \dots, e_r$ des vecteurs de E choisis de sorte que $\big(f(e_1), \dots, f(e_r)\big)$ soit une base de $\mathrm{Im}(f)$. La famille $(e_1, \dots, e_r)$ est nécessairement libre (car toute combinaison linéaire des e_i qui s'annule induit, en prenant le f de cette combinaison, une combinaison linéaire des $f(e_i)$ qui s'annule). Avec le théorème de la base incomplète on complète les e_i en une base $\mathcal{B} = (e_1, \dots, e_n)$ de E. La matrice de représentation de f dans $\mathcal{B}$ est alors une matrice du type

$$M = \left(\begin{array}{c|c} A & B \\ \hline 0 & 0 \end{array}\right)$$

où A est une matrice $r \times r$ et B est une matrice $r \times (n-r)$ (le 0 en bas à gauche est le 0 des matrices $(n-r) \times r$ et le 0 en bas à droite est le zéro des matrices $(n-r) \times (n-r)$). Pour tout $k \in \mathbb{N}^\star$,

$$M^k = \left(\begin{array}{c|c} A^k & A^{k-1}B \\ \hline 0 & 0 \end{array}\right) .$$

Soit $P_A = \sum_{k=0}^r a_k X^k$ le polynôme caractéristique de A. On note $P = XP_A$ de sorte que

$$P = \sum_{k=0}^r a_k X^{k+1} .$$

Alors P est de degré $r+1$ et

$$\begin{aligned} P(M) &= \sum_{k=0}^r a_k \left(\begin{array}{c|c} A^{k+1} & A^k B \\ \hline 0 & 0 \end{array}\right) \\ &= \left(\begin{array}{c|c} AP_A(A) & P_A(A)B \\ \hline 0 & 0 \end{array}\right) = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & 0 \end{array}\right) \end{aligned}$$

puisque $P_A(A) = 0$ par Cayley-Hamilton. D'où le résultat. $\square$

On dira d'un polynôme unitaire qu'il est *scindé à racines simples* s'il s'écrit sous la forme de produit de termes du type $X - \lambda_i$ avec les λ_i tous distincts entre eux.

Théorème 33.3. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et soit $f \in End(E)$ un endomorphisme de E. Les racines du polynôme minimal P_m de f sont précisément les valeurs propres de f, et f est diagonalisable si et seulement si P_m est scindé à racines simples.*

Démonstration. On montre pour commencer que si λ est valeur propre de f, alors $P_m(\lambda) = 0$. Si λ est valeur propre, il existe $x \in E \backslash \{0\}$ tel que $f(x) = \lambda x$. Mais alors $f^k(x) = \lambda^k x$ pour tout k. On a $P_m(f) = 0$. Or $P_m(f)(x) = P_m(\lambda)x$. On en déduit que $P_m(\lambda) = 0$. Réciproquement, supposons que $P_m(\lambda) = 0$. Alors $P_m(X) = (X - \lambda)Q(X)$ où Q est un polynôme de degré un de moins que le degré de P_m.

On vérifie facilement que si AB sont des polynômes, alors $(AB)(f) = A(f) \circ B(f)$ (puisque $f^{p+q} = f^p \circ f^q$). Par suite, puisque $P_m(f) = 0$,

$$(f - \lambda \mathrm{Id}_E) \circ Q(f) = 0$$

au sens des endomorphismes. On a $Q(f) \neq 0$ (au sens des endomorphismes) puisque le degré de Q est strictement inférieur au degré de P_m. Donc il existe $x \in E$ tel que $Q(f)(x) \neq 0$. Mais alors, si $u = Q(f)(x)$, $(f - \lambda \mathrm{Id}_E)(u) = 0$. En particulier, λ est valeur propre de f. On a ainsi montré que les racines du polynôme minimal P_m de f sont précisément les valeurs propres de f.

Montrons maintenant que f est diagonalisable si et seulement si P_m est scindé à racines simples. Supposons que f est diagonalisable. Soient $\lambda_1, \dots, \lambda_p$ les valeurs propres distinctes de f. En vertue de ce qui a été dit ci-dessus,

$$P_m(X) = (X - \lambda_1) \dots (X - \lambda_p) Q(X)$$

avec Q unitaire de degré $d \geq 0$. On veut montrer que Q est en fait de degré zéro, à savoir que $Q = 1$. Comme f est diagonalisable, $E = E_1 \oplus \dots \oplus E_p$ où l'on a noté E_i l'espace propre associé à λ_i. Donc tout $x \in E$ se décompose (de façon unique) en $x = x_1 + \dots + x_p$ avec $x_i \in E_i$, et ainsi, clairement,

$$(u - \lambda_1 \mathrm{Id}_E) \circ \dots \circ (u - \lambda_p \mathrm{Id}_E)(x) = 0$$

puisque les $u - \lambda_i \mathrm{Id}_E$ commutent et annulent x_i. Supposons par exemple que $p = 2$. Le mécanisme ici en place est

$$\begin{aligned}
(u - \lambda_1 \mathrm{Id}_E) \circ (u - \lambda_2 \mathrm{Id}_E)(x_1 + x_2) &= (u - \lambda_1 \mathrm{Id}_E) \circ (u - \lambda_2 \mathrm{Id}_E)(x_1) \\
&= (u - \lambda_2 \mathrm{Id}_E) \circ (u - \lambda_1 \mathrm{Id}_E)(x_1) \\
&= 0 \ .
\end{aligned}$$

On en déduit donc que $(X - \lambda_1) \times \dots \times (X - \lambda_p)$ est un polynôme annulateur pour f. Donc forcément $Q = 1$ et P_m est scindé à racines simples. Réciproquement, supposons que P_m soit scindé à racines simples. Alors P_m s'écrit sous la forme $P_m(X) = (X - \lambda_1) \dots (X - \lambda_p)$ et, en vertue de ce qui a été dit plus haut, les λ_i sont précisément les valeurs propres de f. Soit encore E_i l'espace propre associé à λ_i. On a $E_i = \mathrm{Ker}(u - \lambda_i \mathrm{Id}_E)$. Le lemme des noyaux (cf. ci-dessous ou le Théorème 7.3) permet alors d'écrire que $\mathrm{Ker}(P_m(f)) = E_1 \oplus \dots \oplus E_p$. Or $P_m(f) = 0$ et donc $E = E_1 \oplus \dots \oplus E_p$. En particulier, f est diagonalisable. Le théorème est démontré. $\square$

Le lemme des noyaux ci-dessous a été utilisé dans la preuve du théorème précédent. Des polynômes $P_1, \dots, P_p$ sont dit premiers entre eux deux à deux si pour tous $i \neq j$, les relations $P_i = QR_i$ et $P_j = QR_j$, avec Q, R_i, R_j des polynômes, entraînent que Q est en fait une constante.

Lemme 33.1 (Lemme des noyaux). *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et soit $f \in End(E)$ un endomorphisme de E. Soient $P_1, \dots, P_p$ des polynômes premiers entre eux deux à deux. On note $P = P_1 \times \dots \times P_p$. Alors $Ker(P(f))$ est la somme directe des $Ker(P_i(f))$.*

Démonstration. Soit $N = \mathrm{Ker}(P(f))$ et soient $N_i = \mathrm{Ker}(P_i(f))$. Soit Q_i le produit des P_j pour $j \neq i$. On a $P = P_i Q_i$ pour tout i, et $P(f) = Q_i(f) \circ P_i(f)$ de sorte que $N_i \subset N$ pour tout i. Par récurrence il suffit de savoir traiter le cas $p = 2$. C'est ce qui a été fait au Théorème 7.3, mais pour plus de clarté on répète la preuve ici. Soient donc P_1, P_2 premiers entre eux et $P = P_1P_2$. Comme pour les entiers naturels, il y a un théorème de Bezout pour les polynômes. Puisque P_1 et P_2 sont premiers entre eux, il existe ainsi des polynômes Q_1 et Q_2 tels que

$$P_1Q_1 + P_2Q_2 = 1 \ .$$

Posons $f_1 = (P_1Q_1)(f)$ et $f_2 = (P_2Q_2)(f)$. Alors $f_1 + f_2 = \mathrm{Id}_E$. Pour tout $x \in N$ on peut alors écrire que

$$x = f_1(x) + f_2(x)$$

et que $P_2(f) \circ f_1(x) = 0$ et $P_1(f) \circ f_2(x) = 0$ puisque $P_2(f) \circ f_1 = Q_1(f) \circ (P_1P_2)(f)$ et $P_1(f) \circ f_2 = Q_2(f) \circ (P_1P_2)(f)$. Donc $f_1(x) \in N_2$ et $f_2(x) \in N_1$ de sorte que $x \in N_1 + N_2$. En particulier $N = N_1 + N_2$ (puisque $N_i \subset N$). Reste à montrer que $N_1 \cap N_2 = \{0\}$. Mais si $x \in N_1 \cap N_2$ alors $f_1(x) = 0$ puisque $f_1 = Q_1(f) \circ P_1(f)$, et de la même façon, $f_2(x) = 0$. Or $x = f_1(x) + f_2(x)$. Donc $x = 0$ et $N_1 \cap N_2 = \{0\}$. Ainsi $N = N_1 \oplus N_2$. Le lemme suit par récurrence. □

On a vu que le polynôme minimal P_m divise tout polynôme annulateur P (division polynômiale, $P = QP_m$). On en déduit le résultat suivant.

Corollaire 33.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et soit $f \in End(E)$ un endomorphisme de E. Alors f est diagonalisable si et seulement si il existe un polynôme annulateur de f qui est scindé à racines simples.*

Tous ces résultats passent évidemment aux matrices toujours en exploitant que A est diagonalisable si et seulement si f est diagonalisable lorsque $f \in \mathrm{End}(\mathbb{R}^n)$ est donné par $A = M_{\mathcal{B}\mathcal{B}}(f)$, $\mathcal{B}$ la base canonique de $\mathbb{R}^n$.

CHAPITRE 5
TRIGONALISATION

On aborde dans ce chapitre la théorie de la trigonalisation et certaines de ses conséquences. Dans ce qui suit un polynôme est dit scindé s'il s'écrit comme produit d'un réel et de polynômes de degré un du type $X - \lambda_i$, les λ_i pouvant être égaux entre eux. Un polynôme sur $\mathbb{R}$ n'est pas forcément scindé (exemple $X^2 + 1$). Par contre, comme $\mathbb{C}$ est algébriquement clos, tout polynôme sur $\mathbb{C}$ est scindé.

34. Le théorème fondamental

On commence avec la définition de la trigonalisation. Soit $A = (a_{ij})_{i,j}$ une matrice. On dit que A est triangulaire supérieure si $a_{ij} = 0$ pour pour tous $i > j$ et triangulaire inférieure si $a_{ij} = 0$ pour tous $j > i$.

Définition 34.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et soit $f \in End(E)$ un endomorphisme de E. On dit que f est trigonalisable s'il existe une base $\mathcal{B}$ de E pour laquelle $M_{\mathcal{B}\mathcal{B}}(f)$ est triangulaire supérieure.*

On a ici fait le choix de se rapporter aux matrices triangulaires supérieures, mais nous aurions tout aussi bien pu choisir les triangulaires inférieures. Si $M_{\mathcal{B}\mathcal{B}}(f)$ est triangulaire supérieure et si $\mathcal{B} = (e_1, \dots, e_n)$, alors $M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(f)$ est triangulaire inférieure lorsque l'on pose $\tilde{\mathcal{B}} = (e_n, \dots, e_1)$. Une matrice qui est à la fois triangulaire supérieure et inférieure est une matrice diagonale. Le théorème central de la trigonalisation est le suivant. Comme on s'y attend, il va être plus général que celui de la diagonalisation.

Théorème 34.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et soit $f \in End(E)$ un endomorphisme de E. Alors f est trigonalisable si et seulement si le polynôme caractéristique de f est scindé.*

En théorie de la diagonalisation, cf. Section 25, f est diagonalisable ssi P est scindé ET l'ordre des multiplicité des racines est précisément égal à la dimension des espaces propres correspondant (la somme des multiplicité des racines vaut toujours la dimension). Le seconde condition saute donc pour la trigonalisation.

Démonstration. Si f est trigonalisable, il existe une base $\mathcal{B}$ de E pour laquelle $M_{\mathcal{B}\mathcal{B}}(f)$ est triangulaire supérieure. Disons

$$M_{\mathcal{B}\mathcal{B}}(f) = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

Mais alors

$$M_{\mathcal{B}\mathcal{B}}(f - X\mathrm{Id}_E) = \begin{pmatrix} a_{11} - X & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} - X & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} - X & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_{nn} - X \end{pmatrix}$$

et en développant suivant la première colonne, puis la seconde etc. on voit que $P(X) = \prod_{i=1}^n (a_{ii} - X)$. En particulier, P est scindé.

Réciproquement on veut montrer que si P est scindé, alors f est trigonalisable. On va raisonner par récurrence sur la dimension n. Si $n = 1$ tout est trigonalisable et l'amorce à la récurrence est vérifiée. On suppose maintenant que tout endomorphisme d'un espace de dimension n dont le polynôme caractéristique est scindé est trigonalisable. Soit E un espace de dimension $n+1$ et f un endomorphisme de E dont le polynôme caractéristique P est scindé. Alors le polynôme caractéristique P de f possède au moins une racine λ_1. Soit e_1 un vecteur propre associé à λ_1. On complète e_1 par des vecteurs $e_2, \dots, e_n$ pour obtenir une base $\mathcal{B} = (e_1, e_2, \dots, e_n)$ de E. Alors $M_{\mathcal{B}\mathcal{B}}(f)$ s'écrit

$$M_{\mathcal{B}\mathcal{B}}(f) = \begin{pmatrix} \lambda_1 & a_2 & \dots & a_n \\ 0 & & & \\ \vdots & & M & \\ 0 & & & \\ 0 & & & \end{pmatrix} \tag{34.1}$$

où M est une matrice $n \times n$. Soit $F = \mathrm{Vect}(e_2, \dots, e_n)$. On note $p : E \to F$ la projection parallèlement à e_1, à savoir l'application linéaire définie par

$$p(\sum_{i=1}^n x_i e_i) = \sum_{i=2}^n x_i e_i$$

et on note $g \in \mathrm{End}(F)$ l'endomorphisme de F défini par $g(u) = p(f(u))$ pour tout $u \in F$. Si $\tilde{\mathcal{B}} = (e_2, \dots, e_n)$, alors $M = M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(g)$. Si Q est le polynôme caractéristique de g, on a alors que

$$P(X) = (\lambda_1 - X)Q(X)$$

et donc Q est aussi scindé (puisque P l'est). Par hypothèse de récurrence, puisque $\mathrm{dim} F = n$, il existe donc une base $\hat{\mathcal{B}} = (\hat{e}_2, \dots, \hat{e}_n)$ de F pour laquelle $M_{\hat{\mathcal{B}}\hat{\mathcal{B}}}(g)$ est diagonale supérieure. Posons $\hat{e}_1 = e_1$ pour homogénéiser les notations. La famille $(\hat{e}_1, \hat{e}_2, \dots, \hat{e}_n)$ est une base de E. On vérifie que $f(\hat{e}_i) \in \mathrm{Vect}(\hat{e}_1, \dots, \hat{e}_i)$ pour tout i puisque $f(\hat{e}_1) = \lambda_1 \hat{e}_1$ tandis que $g(\hat{e}_i) \in \mathrm{Vect}(\hat{e}_2, \dots, \hat{e}_i)$ pour tout $i \geq 2$ et, par définition de g, si $g(u) = v$, alors $f(u) = \lambda \hat{e}_1 + v$ pour un certain $\lambda \in \mathbb{R}$. Ainsi $M_{\hat{\mathcal{B}}\hat{\mathcal{B}}}(f)$ est diagonale supérieure. Ceci achève la récurrence. Le théorème est démontré. □

Si f est trigonalisable, les valeurs sur la diagonales d'une matrice de représentation $M_{\mathcal{B}\mathcal{B}}(f)$ de f qui est triangulaire sont les racines du polynôme caractéristique de f, donc les valeurs propres de f.

Théorème 34.2. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et soit $f \in End(E)$ un endomorphisme de E. S'il existe un polynôme scindé Q qui annule f, alors f est trigonalisable.*

Démonstration. On procède comme ci-dessus avec une preuve par récurrence sur la dimension n de E. Si $n = 1$ le résultat est vrai (tout est trigonalisable). On suppose maintenant que tout endomorphisme d'un espace de dimension n qui possède un polynôme annulateur scindé est trigonalisable. On considère E de dimension $n+1$ et f un endomorphisme de E qui possède un polynôme annulateur scindé, disons

Q. On écrit que $Q(X) = (X-\lambda_1)^{n_1}\dots(X-\lambda_p)^{n_p}$. Comme $Q(f)=0$ on peut écrire que

$$(f-\lambda_1\mathrm{Id}_E)^{n_1}\circ\cdots\circ(f-\lambda_p\mathrm{Id}_E)^{n_p}=0\ .$$

Les $f-\lambda_i\mathrm{Id}_E$ ne peuvent donc pas tous être injectifs (car sinon ils seraient bijectifs et leur composée aussi). Donc il existe i tel que $f-\lambda_i\mathrm{Id}_E$ a un noyau non trivial. Donc, pour au moins un i, λ_i est valeur propre de f. Disons $i=1$ (quitte à permuter les λ_i). Comme ci- dessus on va pouvoir écrire une équation comme (34.1) avec $M = M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(g)$. Pour pouvoir conclure il reste à montrer que g possède un polynôme annulateur scindé. Or

$$M_{\mathcal{B}\mathcal{B}}(P(f)) = \begin{pmatrix} P(\lambda_1) & a'_2 & \dots & a'_n \\ 0 & & & \\ \vdots & & M_{\tilde{\mathcal{B}}\tilde{\mathcal{B}}}(P(g)) & \\ 0 & & & \\ 0 & & & \end{pmatrix}$$

pour tout polynôme P, où les $a'_2,\dots,a'_n\in\mathbb{R}$ (tout simplement parce que la relation est vraie pour les puissances $f^p = f\circ\cdots\circ f$, p fois). En prenant $P=Q$ on voit que $Q(g)=0$. Donc g possède un polynôme annulateur scindé. Par hypothèse de récurrence g est trigonalisable. On conclue comme ci-dessus. Le théorème est démontré. $\square$

Une conséquence simple de ce théorème est qu'un endomorphisme f (en dimension finie) est trigonalisable si et seulement si son polynôme minimal est scindé (et non plus scindé à racines simples comme il fallait l'exiger pour la diagonalisation). En effet le polynôme minmal annule f. S'il est scindé f est donc trigonalisable. A l'inverse, si f est trigonalisable, alors le polynôme caractéristique de f est scindé. Or le polynôme minimal divise le polynôme caractéristique. Il est donc lui aussi scindé.

35. Espaces caractéristiques

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n et soit $f\in\mathrm{End}(E)$ un endomorphisme de E. On suppose que le polynôme caractéristique P de f est scindé. Donc

$$P(X) = (-1)^n(X-\lambda_1)^{n_1}\times\cdots\times(X-\lambda_p)^{n_p}$$

où les λ_i sont deux à deux distincts (et $n=n_1+\cdots+n_p$). On appelle alors sous espace caractéristique de f associé à la valeur propre λ_i l'espace

$$E_c^{\lambda_i} = \mathrm{Ker}(f-\lambda_i\mathrm{Id}_E)^{n_i} \tag{35.1}$$

Bien sûr, si E_{λ_i} est l'espace propre associé à la valeur propre λ_i alors $E_{\lambda_i}\subset E_c^{\lambda_i}$. Mais il n'y a pas forcément égalité. Une remarque simple est que les espaces caractéristiques $E_c^{\lambda_i}$ sont forcément stables par f car si $x\in E_c^{\lambda_i}$ alors

$$\begin{aligned}(f-\lambda_i\mathrm{Id}_E)^{n_i}(f(x)) &= (f-\lambda_i\mathrm{Id}_E)^{n_i}\left((f-\lambda_i\mathrm{Id}_E)(x)+\lambda_i x\right)\\ &= (f-\lambda_i\mathrm{Id}_E)^{n_i+1}(x)+\lambda_i(f-\lambda_i\mathrm{Id}_E)^{n_i}(x)\\ &= 0+0=0\ .\end{aligned}$$

On commence par démontrer le théorème suivant.

Théorème 35.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n et soit $f \in End(E)$ un endomorphisme de E. On suppose que le polynôme caractéristique P de f est scindé. On note $\lambda_1, \dots, \lambda_p$ les valeurs propres distinctes de f et n_i leur multiplicité. Alors pour tout $i = 1, \dots, p$, $E_c^{\lambda_i}$ est de dimension n_i et, de plus, E est toujours somme directe des $E_c^{\lambda_i}$.*

Du coup, avec ce théorème, on voit qu'un endomorphisme est diagonalisable si et seulement si son polynôme caractéristique est scindé et les espaces propres sont précisément les espaces caractéristiques.

Démonstration. Les polynômes $(X - \lambda_i)^{n_i}$ sont premiers deux à deux. Le produit de ces polynômes vaut, à $(-1)^n$ près, le polynôme caractéristique P de f. On sait avec Cayley-Hamilton que $P(f) = 0$. Donc $E = \mathrm{Ker}(P(f))$. Le lemme des noyaux, cf. Théorème 33.1, nous dit alors que

$$E = E_c^{\lambda_1} \oplus \cdots \oplus E_c^{\lambda_p} \ . \tag{35.2}$$

La seconde affirmation du théorème est démontrée. Pour ce qui est de la première on note f_i la restriction de u à $E_c^{\lambda_i}$. Clairement f_i n'a qu'une seule valeur propre λ_i car si $x \in E_c^{\lambda_i} \backslash \{0\}$ est tel que $f(x) = \lambda x$ alors

$$0 = (f - \lambda_i \mathrm{Id}_E)^{n_i}(x) = (\lambda - \lambda_i)^{n_i} x$$

de sorte que forcément $\lambda = \lambda_i$. Le polynôme $(X - \lambda_i)^{n_i}$ est scindé et il annule f_i. Donc, cf. Théorème 34.2, f_i est trigonalisable et les termes sur la diagonale de ses matrices de représentations triangulaires sont tous égaux à λ_i. Le polynôme caractéristique de f_i est donc du type $P_i(X) = (-1)^{d_i}(X - \lambda_i)^{d_i}$ où d_i est la dimension de $E_c^{\lambda_i}$. La décomposition (35.2) permet d'écrire que le polynôme caractéristique P de f est le produit des P_i car si $\mathcal{B}$ est une base de E constituée de bases $\mathcal{B}_i$ des $E_c^{\lambda_i}$ alors pour tout endomorphisme g qui laisse stable les $E_c^{\lambda_i}$, $M_{\mathcal{B}\mathcal{B}}(g)$ est diagonale par blocs en les $M_{\mathcal{B}_i\mathcal{B}_i}(g)$ (cf. Lemme 28.1). En comparant,

$$\begin{aligned} P(X) &= (-1)^n (X - \lambda_1)^{n_1} \dots (X - \lambda_p)^{n_p} \\ &= (-1)^{d_1 + \cdots + d_p} (X - \lambda_1)^{d_1} \dots (X - \lambda_p)^{d_p} \ . \end{aligned}$$

On en déduit que nécessairement $d_i = n_i$ (si $d_i < n_i$ on simplifie par $(X - \lambda_i)^{d_i}$ et on aboutit à une contradiction car deux polynômes ne peuvent être égaux si l'un s'annule en λ_i et l'autre pas). Donc, par définition de d_i, la dimension de $E_c^{\lambda_i}$ est n_i pour tout i. Le théorème est démontré. □

36. La décomposition de Dunford

La décomposition de Dunford s'applique aux endomorphismes trigonalisables. On commence avec la définition des notions jumelles d'endomorphisme nilpotent et de matrice nilpotente.

Définition 36.1. *(i) Soit E un $\mathbb{R}$-espace vectoriel et soit $f \in End(E)$ un endomorphisme de E. On dit que f est nilpotent s'il existe $k \in \mathbb{N}^\star$ pour lequel $f^k = 0$.*
(ii) Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice réelle carrée $n \times n$. On dit que A est nilpotente s'il existe $k \in \mathbb{N}^\star$ tel que $A^k = 0$.

Bien sûr, si f est nilpotent avec E de dimension finie, alors pour toute base $\mathcal{B}$ de E, la matrice de représentation $M_{\mathcal{B}\mathcal{B}}(f)$ de f dans $\mathcal{B}$ est nilpotente puisque

$$M_{\mathcal{B}\mathcal{B}}(f^k) = M_{\mathcal{B}\mathcal{B}}(f)^k \ .$$

Réciproquement, si pour une base $\mathcal{B}$ on a que $M_{\mathcal{B}\mathcal{B}}(f)$ est nilpotente, alors f est aussi nilpotent. On montre maintenant que les endomorphismes nilpotents ont 0 pour seule valeur propre et donc aussi, en particulier, que le seul endomorphisme nilpotent qui soit diagonalisable est l'endomorphisme nul.

Lemme 36.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n. Si $f \in End(E)$ est nilpotent alors 0 est l'unique valeur propre de f et, en particulier, le seul endomorphisme nilpotent de E qui soit diagonalisable est l'endomorphisme nul.*

Démonstration. Soit $\mathcal{B}$ une base de E et $A = M_{\mathcal{B}\mathcal{B}}(f)$. Si $f^k = 0$ alors $A^k = 0$ (voir ci-dessus) et donc $\det(A^k) = 0$. Or $\det(A^k) = \det(A)^k$ et donc, $\det(A) = 0$. En particulier, 0 est valeur propre de f. Par ailleurs, si λ est valeur propre de f, il existe alors $u \in E\backslash\{0\}$ tel que $f(u) = \lambda u$. Mais alors $f^k(u) = \lambda^k u$ et donc, si $f^k = 0$, alors forcément $\lambda^k = 0$, soit $\lambda = 0$. Ainsi f a pour seule valeur propre la valeur propre 0. Si f était diagonalisable alors on pourrait choisir $\mathcal{B}$ dans la preuve comme étant formée de vecteurs propres de f. Mais alors $A = 0$, donc $f = 0$, ce qui démontre le lemme. □

En regardant A dans la preuve du Lemme 36.1 comme une matrice complexe, et le polynôme caractéristique comme un polynôme complexe, en passant au cas complexe comme dans la Section 38, on montre sans difficulté que le polynôme caractéristique d'un endomorphisme nilpotent en dimension n s'écrit toujours sous la forme $(-1)^n X^n$.

Théorème 36.1 (Décomposition de Dunford)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et $f \in End(E)$ un endomorphisme trigonalisable de E. Il existe alors un unique endomorphisme nilpotent $u \in End(E)$, et un unique endomorphisme diagonalisable $g \in End(E)$ tels que $f = u + g$ et $u \circ g = g \circ u$. De la même façon, pour toute matrice carrée $A \in \mathcal{M}_n(\mathbb{R})$ dont le polynôme caractéristique est scindé, il existe une unique matrice nilpotente $N \in \mathcal{M}_n(\mathbb{R})$ et une unique matrice diagonalisable $\Delta \in \mathcal{M}_n(\mathbb{R})$ telles que $A = N + \Delta$ et $N\Delta = \Delta N$.*

Les deux énoncés sont bien sûr équivalents, ce que l'on montre facilement en fixant une base de E et en passant aux matrices de représentations. On démontre la version "endomorphisme" de la décomposition de Dunford.

Démonstration. (i) Existence. Soit donc $f \in \mathrm{End}(E)$ un endomorphisme trigonalisable de E. Le polynôme caractéristique P de f est alors scindé. On note $\lambda_1, \ldots, \lambda_p$ les valeurs propres distinctes de f et n_i leur multiplicité. On a d'après le Théorème 35.1 que pour tout $i = 1, \ldots, p$, l'espace caractéristique $E_c^{\lambda_i}$ est de dimension n_i et, de plus, que E est toujours somme directe des $E_c^{\lambda_i}$. On définit $g \in \mathrm{End}(E)$ en posant que

$$g(x) = \lambda_i x$$

pour tout $x \in E_c^{\lambda_i}$ et pour tout $i = 1, \ldots, p$. Comme $E = E_c^{\lambda_1} \oplus \cdots \oplus E_c^{\lambda_p}$, cela définit bien un endomorphisme de E. De plus g est clairement diagonalisable puisque si $\mathcal{B}_1, \ldots, \mathcal{B}_p$ sont des bases de $E_c^{\lambda_1}, \ldots, E_c^{\lambda_p}$, et si $\mathcal{B} = (\mathcal{B}_1, \ldots, \mathcal{B}_p)$, alors $M_{\mathcal{B}\mathcal{B}}(g)$ est diagonale de diagonale les λ_i (répétés n_i-fois chacun). On pose alors

$$u = f - g$$

qui est bien un endomorphisme de E. Par définition de $E_c^{\lambda_i}$, et construction de g, $E_c^{\lambda_i} \subset \mathrm{Ker}(u^{n_i})$ pour tout i. Soit $m = \max_i n_i$. Comme $\mathrm{Ker}(u^\alpha) \subset \mathrm{Ker}(u^\beta)$

pour tous entiers $\alpha \leq \beta$, on obtient que $u^m(x) = 0$ pour tout $x \in E_c^{\lambda_i}$. Et comme E est somme directe des $E_c^{\lambda_i}$, $u^m(x) = 0$ pour tout $x \in E$. En particulier, u est nilpotent. Comme $f = u + g$ il reste à montrer que u et g commutent. Les espaces caractéristiques $E_c^{\lambda_i}$ sont stables par f comme on l'a vu à la Section 35. Ils sont aussi clairement stables par g (par construction de g). Ils sont donc stables par u. Pour tout i et tout $x \in E_c^{\lambda_i}$, on a alors que $g \circ u(x) = \lambda_i u(x)$ tandis que $u \circ g(x) = u(\lambda_i x) = \lambda_i u(x)$. Donc $g \circ u = u \circ g$ sur $E_c^{\lambda_i}$ pour tout i. Là encore, comme E est somme directe des $E_c^{\lambda_i}$, on obtient que $g \circ u = u \circ g$ sur E, et donc que g et u commutent. La partie existence de la décomposition de Dunford est démontrée.

(ii) Unicité. Soit (u, g) le couple d'endomorphismes construit ci-dessus. Soient $(\tilde{u}, \tilde{g})$ un couple constitué d'un endomorphisme nilpotent et d'un endomorphisme diagonalisable, avec les deux qui commutent et qui sont de somme f. On montre dans ce qui suit que u et $\tilde{u}$ commutent alors forcément, ainsi que g et $\tilde{g}$. En tout premier lieu on remarque que f et g commutent et que f et $\tilde{g}$ commutent aussi. En effet $f = u + g$ et donc, puisque u et g commutent,

$$\begin{aligned} g \circ f &= g \circ u + g^2 \\ &= u \circ g + g^2 \\ &= (u + g) \circ g \\ &= f \circ g \end{aligned}$$

et même chose si l'on part de $f = \tilde{u} + \tilde{g}$. On remarque maintenant que les espaces propres $E_c^{\lambda_i}$ sont forcément stables par $\tilde{g}$ puisque si $x \in E_c^{\lambda_i}$, et comme f et $\tilde{g}$ commutent,

$$\begin{aligned} \left(f - \lambda_i \mathrm{Id}_E\right)^{n_i} (\tilde{g}(x)) &= \tilde{g}\big(\left(f - \lambda_i \mathrm{Id}_E\right)^{n_i} (x)\big) \\ &= \tilde{g}(0) = 0 \ . \end{aligned}$$

Comme $g(x) = \lambda_i x$ pour $x \in E_c^{\lambda_i}$, on en déduit que g et $\tilde{g}$ commutent sur $E_c^{\lambda_i}$ pour tout i. Et comme E est somme directe des $E_c^{\lambda_i}$, g et $\tilde{g}$ commutent sur E. On a $u = f - g$ et $\tilde{u} = f - \tilde{g}$. Or f et g commutent, f et $\tilde{g}$ commutent et g et $\tilde{g}$ commutent. On en déduit que u et $\tilde{u}$ commutent puisqu'alors

$$\begin{aligned} u \circ \tilde{u} &= f^2 - f \circ \tilde{g} - g \circ f + g \circ \tilde{g} \\ &= f^2 - \tilde{g} \circ f - f \circ g + \tilde{g} \circ g \\ &= \tilde{u} \circ u \ . \end{aligned}$$

D'où ce qui a été annoncé plus haut. Comme g et $\tilde{g}$ commutent, et puisqu'ils sont tous deux diagonalisables, il existe d'après le Théoreme 31.3 une base $\mathcal{B}$ de E qui diagonalise à la fois g et $\tilde{g}$. Donc $\tilde{g} - g$ est diagonalisable. Par ailleurs, avec la formule du binôme de Newton, et puisque u et $\tilde{u}$ commutent, on voit que si $u^m = 0$ et $\tilde{u}^{\tilde{m}} = 0$, alors

$$\begin{aligned} (u - \tilde{u})^{m+\tilde{m}} &= \sum_{k=0}^{m+\tilde{m}} (-1)^{m+\tilde{m}-k} u^k \circ \tilde{u}^{m+\tilde{m}-k} \\ &= 0 \end{aligned}$$

puisque pour tout $k = 0, \dots, m+\tilde{m}$, on a soit $k \geq m$, soit $m+\tilde{m}-k \geq \tilde{m}$ (on pourra préférer écrire la formule du binôme de Newton pour les matrices de représentations de u et $\tilde{u}$ en fixant une base de E, mais cela revient en fait exactement à ce que l'on vient d'écrire). Or

$$\tilde{g} - g = u - \tilde{u} \ .$$

Donc $\tilde{g} - g$ est à la fois diagonalisable et nilpotent. Avec le Lemme 36.1 on en déduit que $\tilde{g} - g = 0$ et donc que $\tilde{g} = g$. Il suit qu'on a aussi que $\tilde{u} = u$. D'où l'unicité. Le Théorème est démontré. □

37. La réduction de Jordan

On aborde ici la réduction de Jordan des matrices trigonalisables, à savoir dont le polynôme caractéristique est scindé. Il convient en premier lieu de définir ce que l'on entend par bloc de Jordan et par matrice de Jordan..

Définition 37.1. *Un bloc de Jordan est une matrice carrée $B_\lambda \in \mathcal{M}_p(\mathbb{R})$, avec $p \in \mathbb{N}^\star$, qui s'écrit sous la forme*

$$B_\lambda = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & \ddots & 0 \\ \vdots & \ddots & \ddots & 1 \\ 0 & \dots & 0 & \lambda \end{pmatrix}$$

où $\lambda \in \mathbb{R}$, autrement dit qui s'écrit sous la forme d'une diagonale constituée d'une même valeur λ et d'une "petite diagonale" juste au dessus constituée uniquement de 1, toutes les autres entrées étant des 0.

Lorsque $p = 2$, les blocs de Jordan sont du type

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

Lorsque $p = 3$ les blocs de Jordans sont du type

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

Lorsque $p = 4$ les blocs de Jordans sont du type

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

et on peut continuer avec $p = 5$, $p = 6$ etc. Une matrice de Jordan est alors une matrice diagonale par blocs, les blocs étant des blocs de Jordan de tailles possiblement différentes.

Définition 37.2. *Une matrice de Jordan est une matrice diagonale par blocs de la forme*

$$J = \begin{pmatrix} B_{\lambda_1} & 0 & 0 & 0 \\ 0 & B_{\lambda_2} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & B_{\lambda_p} \end{pmatrix}$$

les B_{λ_i} étant des blocs de Jordan, possiblement de tailles différentes.

Par exemple,

$$J = \begin{pmatrix} \lambda & 1 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & \mu & 1 & 0 \\ 0 & 0 & 0 & 0 & \mu & 1 \\ 0 & 0 & 0 & 0 & 0 & \mu \end{pmatrix}$$

est une matrice de Jordan 6×6 avec deux blocs de Jordan 3×3 donnés par

$$B_\lambda = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix} \quad \text{et} \quad B_\mu = \begin{pmatrix} \mu & 1 & 0 \\ 0 & \mu & 1 \\ 0 & 0 & \mu \end{pmatrix} .$$

La réduction de Jordan des matrices trigonalisables (à savoir dont le polynôme caractéristique est scindé) est donnée par le théorème suivant.

Théorème 37.1 (Réduction de Jordan)**.** *Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice réelle carrée $n \times n$. Il existe alors $P \in \mathcal{M}_n(\mathbb{R})$ inversible pour laquelle $P^{-1}AP$ est une matrice de Jordan. De façon équivalente, si E est un $\mathbb{R}$-espace vectoriel de dimension finie, et $f \in End(E)$ est un endomorphisme trigonalisable, alors il existe une base $\mathcal{B}$ de E pour laquelle $M_{\mathcal{B}\mathcal{B}}(f)$ est de Jordan.*

Les deux énoncés sont équivalents comme on le voit en passant aux matrices de représentations et en utilisant bien sûr la formule de changement de bases pour les matrices de représentations dans le cas des endomorphismes (avec une même base répétée au départ et à l'arrivée). La première étape dans la preuve du théorème est constituée du lemme suivant.

Lemme 37.1. *Etant donnés E un $\mathbb{R}$-espace vectoriel et $f \in End(E)$ un endomrophisme nilpotent de E, on définit l'indice de nilpotence de f comme étant le plus petit entier $k \geq 1$ pour lequel $f^k = 0$. Si k est l'indice de nilpotence d'un endomorphisme nilpotent f, et si $x \in E$ est tel que $f^{k-1}(x) \neq 0$, alors le sous espace vectoriel*

$$E_x(f) = Vect\big(x, f(x), \ldots, f^{k-1}(x)\big)$$

est stable par f et de dimension k. En particulier, si f est nilpotent, et si E est de dimension finie, alors automatiquement $f^n = 0$ où n est la dimension de E.

Démonstration. Clairement la famille $\big(x, f(x), \ldots, f^{k-1}(x)\big)$ est libre car si

$$\sum_{i=0}^{k-1} \lambda_i f^i(x) = 0$$

alors en appliquant f^p au membre de gauche de cette identité on récupère encore le vecteur nul, et puisque $f^j = 0$ pour $j \geq k$,

$$\sum_{i=0}^{k-p-1} \lambda_i f^{i+p}(x) = 0$$

pour tout p. En prenant $p = k-1$, et puisque $f^{k-1}(x) \neq 0$, on trouve que $\lambda_0 = 0$. En prenant ensuite $p = k-2$ on trouve que $\lambda_1 = 0$ et ainsi de suite jusqu'à annuler tous les λ_i, ce qui prouve bien que la famille est libre. Donc $E_x(f)$ est de dimension k. Clairement $E_x(f)$ est stable par f car pour tous $\lambda_1, \ldots, \lambda_{k-1} \in \mathbb{R}$

$$f\left(\sum_{i=0}^{k-1} \lambda_i f^i(x)\right) = \sum_{i=0}^{k-1} \lambda_i f^{i+1}(x) = \sum_{i=0}^{k-2} \lambda_{i-1} f^i(x)$$

de sorte que pour tout $y \in E_x(f)$, $f(y) \in E_x(f)$. La première partie du lemme est démontrée. Si maintenant E est de dimension finie n, alors clairement $k \leq n$. Donc $f^n = 0$. La seconde partie du lemme est démontrée. □

La seconde étape est donnée par le lemme suivant.

Lemme 37.2. *Le théorème de réduction de Jordan et vrai dans le cas nilpotent, donc si A ou f sont trigonalisables et nilpotents.*

Démonstration. On se place dans le cas des endomorphismes et on effectue une récurrence forte sur la dimension de E. L'hypothèse de récurrence considérée à l'ordre n est alors que pour tout $1 \leq p \leq n$, tout $\mathbb{R}$-espace vectoriel de dimension p et tout endomorphisme trigonalisable nilpotent de E, il existe une base $\mathcal{B}$ de E pour laquelle $M_{\mathcal{B}\mathcal{B}}(f)$ est de Jordan. Si $n = 1$ le résultat est évident. On suppose donc notre hypothèse de récurrence totale vraie à l'ordre n et on veut la montrer à l'ordre $n+1$. Soient alors $1 \leq p \leq n+1$, E un $\mathbb{R}$-espace vectoriel de dimension p et f un endomorphisme trigonalisable nilpotent de E. On peut supposer que $p = n+1$ car sinon on tombe dans notre hypothèse à l'ordre n. Soit k l'indice de nilpotence de f. En vertue du Lemme 37.1, $k \leq n+1$. Soit $x \in E$ tel que $f^{k-1}(x) \neq 0$ qui existe car par définition de l'indice de nilpotence f^{k-1} ne peut être l'endomorphisme nul. Toujours en vertue du Lemme 37.1, la famille $\mathcal{B}' = (e_1, \ldots, e_k)$ est libre, où $e_i = f^{k-i}(x)$ pour tout $i = 1, \ldots, k$. Attention, pour obtenir des 1 au dessus de la diagonal principale, et non pas en dessous, on inverse ici l'ordre des e_i:

$$e_1 = f^{k-1}(x), \ldots, e_{k-1} = f(x), e_k = x \ .$$

En notant $E_f(x)$ l'espace engendré par $(e_1, \ldots, e_k)$, et $\tilde{f}$ la restriction de f à cet espace, la matrice de représentation de $\tilde{f}$ dans la base $(e_1, \ldots, e_k)$ est le bloc de Jordan B_0 (avec $\lambda = 0$) de taille k de la Définition 37.1. On prétend ici qu'il existe F un sous espace vectoriel de E, de dimension $n+1-k$ et stable par f, qui est tel que

$$E = E_f(x) \oplus F \ .$$

On démontre l'existence d'un tel F plus bas (la question ne se pose que si $k \leq n$). Si $\hat{f}$ est la restriction de f à F, alors, par hypothèse de récurrence, il existe une base $\mathcal{B}''$ de F pour laquelle la matrice de représentation de $\hat{f}$ dans cette base est une matrice de Jordan. En posant $\mathcal{B} = (\mathcal{B}', \mathcal{B}'')$, on obtient une base $\mathcal{B}$ de E et la matrice de représentation de f dans $\mathcal{B}$ est elle aussi clairement une matrice de Jordan, le premier bloc étant le B_0 de taille k obtenu ci-dessus, suivi des blocs associés à la réduction de $\hat{f}$. Le lemme est démontré. □

Pour être complet, on démontre ici l'existence du supplémentaire stable F qui a été utilisé dans la preuve du Lemme 37.2 ci-dessus.

Démonstration de l'existence de F. On complète la famille $(e_1, \ldots, e_k)$ en une base $(e_1, \ldots, e_k, e_{k+1}, \ldots, e_{n+1})$ de E. Soit $e_1^\star$ la forme linéaire duale de e_1, que l'on définit comme étant la forme linéaire sur E qui vérifie que $e_1^\star(e_j) = 0$ pour tout $j \geq 2$ tandis que $e_1^\star(e_1) = 1$. On pose alors

$$\begin{aligned} F &= \left\{ y \in E \ / \ e_1^\star \circ f^j(y) = 0, \forall j \geq 0 \right\} \\ &= \bigcap_{j=0}^{k-1} \mathrm{Ker}(e_1^\star \circ f^j) \ . \end{aligned}$$

La première remarque est que F est bien un sous espace vectoriel de E. Soit maintenant φ l'application linéaire de E dans $\mathbb{R}^q$ donnée par

$$\varphi(y) = \left(e_1^\star(y), e_1^\star \circ f(y), \dots, e_1^\star \circ f^{k-1}(y) \right)$$

pour tout $y \in E$. Alors $F = \mathrm{Ker}(\varphi)$ et donc, avec le théorème du rang, puisque $\mathrm{Rg}(\varphi) \leq p$, on obtient que $\dim(F) \geq n - p$. Clairement F est stable par f par définition même de F. On affirme maintenant que

$$E_f(x) \cap F = \{0\} \ .$$

En effet si $y \in E_f(x)$, alors $y = \sum_{j=0}^{k-1} \lambda_j f^j(x)$. Si on a aussi que $y \in F$ alors $e_1^\star(y) = 0$, $e_1^\star \circ f(y) = 0, \dots, e_1^\star \circ f^{k-1}(y) = 0$ et donc $\lambda_{k-1} = 0$, $\lambda_{k-2} = 0, \dots, \lambda_0 = 0$, soit encore $y = 0$. D'où l'affirmation. Comme $\dim(E_f(x)) = k$ et puisque $E_f(x) \oplus F$ en raison de ce que l'on vient de dire,

$$k + \dim(F) \leq n$$

de sorte que $\dim(F) \leq n - k$. On en déduit que $\dim(F) = n - k$ puis, par argument de dimension, que $E = E_f(x) \oplus F$, ce que l'on voulait démontrer. □

On démontre maintenant le Théorème 37.1. On le démontre dans sa version "endomorphisme".

Démonstration du Théorème 37.1. Soit donc E est un $\mathbb{R}$-espace vectoriel de dimension finie et $f \in \mathrm{End}(E)$ un endomorphisme trigonalisable de E. On note $\lambda_1, \dots, \lambda_p$ les valeurs propres distinctes de f et n_i leur multiplicité. On a d'après le Théorème 35.1 que pour tout $i = 1, \dots, p$, l'espace caractéristique $E_c^{\lambda_i}$ est de dimension n_i et, de plus, que E est toujours somme directe des $E_c^{\lambda_i}$. Les espaces $E_c^{\lambda_i}$ sont stables par f comme on l'a vu à la Section 35. Si f_i est la restriction de f à $E_c^{\lambda_i}$,

$$g_i = f_i - \lambda_i \mathrm{Id}_{E_c^{\lambda_i}}$$

est nilpotent par définition de $E_c^{\lambda_i}$. Il est aussi trigonalisable comme vu dans la preuve du Théorème 35.1. Avec le lemme 37.2 on obtient donc l'existence d'une base $\mathcal{B}_i$ pour laquelle $M_{\mathcal{B}_i\mathcal{B}_i}(f - \lambda_i \mathrm{Id}_{E_c^{\lambda_i}})$ est une matrice de Jordan, ce qui implique que $M_{\mathcal{B}_i\mathcal{B}_i}(f)$ est aussi une matrice de Jordan. Si on pose $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_p)$ alors $\mathcal{B}$ est une base de E et $M_{\mathcal{B}\mathcal{B}}(f)$ est encore de Jordan, les blocs de Jordan de cette matrice étant constitués de la succession des blocs de Jordan associés aux $M_{\mathcal{B}_i\mathcal{B}_i}(f)$. Le théorème est démontré. □

38. Le cas complexe

Une théorie analogue existe lorsque le corps de base est $\mathbb{C}$ et non plus $\mathbb{R}$ (et on peut même généraliser à des corps plus généraux). Dit autrement, il existe une théorie analogue des espaces vectoriels complexes. Rien ne change, si ce n'est que $\mathbb{C}$ est un corps algébriquement clos ce qui, comme vous pouvez vous en douter, induit quelques petits changements notables sur la réduction des endomorphismes qui est très liée aux racines du polynômes caractéristiques. La propriété essentielle de $\mathbb{C}$ est donc que "*tout polynôme complexe P de degré $n \geq 1$ s'écrit sous la forme*

$$P(X) = a \prod_{i=1}^{n} (X - \lambda_i) \ ,$$

où $a, \lambda_1, \ldots, \lambda_n \in \mathbb{C}$ et peuvent être égaux". En d'autres termes, un polynôme sur $\mathbb{C}$ est toujours scindé. La théorie de la diagonalisation reste essentiellement inchangée.

Théorème 38.1. *Soit E un $\mathbb{C}$-espace vectoriel de dimension finie et soit $f \in End(E)$ un endomorphisme de E. On note $\lambda_1, \ldots, \lambda_p$ les valeurs propres distinctes de f et $E_{\lambda_1}, \ldots, E_{\lambda_p}$ les espaces propres correspondants. Alors f est diagonalisable si et seulement si $E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_p}$.*

Pour la trigonalisation par contre cela change tout puisque la seule condition est que le polynôme caractéristique soit scindé et puisque tout polynôme sur $\mathbb{C}$ est scindé.

Théorème 38.2. *Soit E un $\mathbb{C}$-espace vectoriel de dimension finie. Tout endomorphisme $f \in End(E)$ est trigonalisable.*

On a bien sûr les analogues matriciels de ces deux théorèmes. En particulier, pour tout matrice carrée complexe A, il existe P complexe inversible et T complexe triangulaire supérieure telles que $A = PTP^{-1}$. Une conséquence "amusante" de ce changement porte sur la densité des matrices diagonalisables dans l'espace de toutes les matrices. Cette densité a lieu dans $\mathbb{C}$ mais pas dans $\mathbb{R}$.

Théorème 38.3. *Soit $A = (a_{ij})_{i,j}$ une matrice carrée $n \times n$ à coefficients complexes. Il existe alors une suite $A_k = (a_{ij}^k)_{i,j}$ de matrices carrées diagonalisables à coefficients complexes telle que pour tous $i, j = 1, \ldots, n$,*

$$a_{ij} = \lim_{k \to +\infty} a_{ij}^k \ .$$

Cette propriété générale de densité cesse par contre d'être vraie lorsque l'on remplace $\mathbb{C}$ par $\mathbb{R}$.

Dit autrement, si $\mathcal{M}_n(\mathbb{C})$ désigne l'espaces des matrices carrées $n \times n$ à coefficients complexes, si $D_{\mathbb{R}}^n$ désigne l'espace des matrices réelles $n \times n$ diagonalisables et si $D_{\mathbb{C}}^n$ désigne l'espace des matrices complexes $n \times n$ diagonalisables, alors $D_{\mathbb{C}}^n$ est dense dans $\mathcal{M}_n(\mathbb{C})$ tandis que $D_{\mathbb{R}}^n$, lui, n'est pas dense dans $\mathcal{M}_n(\mathbb{R})$.

Démonstration. La matrice A est trigonalisable. Quitte à la trigonaliser on peut donc supposer que

$$A = \begin{pmatrix} \lambda_1 & b_{12} & b_{13} & \ldots & b_{1n} \\ 0 & \lambda_2 & b_{23} & \ldots & b_{2n} \\ 0 & 0 & \lambda_3 & \ldots & b_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

Si les λ_i sont tous distincts, A est diagonalisable et on pose $A_k = A$ pour tout k. Sinon il est clair que l'on va toujours pouvoir trouver des suites $(\varepsilon_k^{(1)})_k, \ldots, (\varepsilon_k^{(n)})_k$

de réels strictement positifs par exemple, qui convergent vers zéro, et qui sont telles que: pour tout k et tous $i, j = 1, \ldots, n$,

$$\lambda_i + \varepsilon_k^{(i)} \neq \lambda_j + \varepsilon_k^{(j)}$$

dès que $i \neq j$. On pose

$$A_k = \begin{pmatrix} \lambda_1 + \varepsilon_k^{(1)} & b_{12} & b_{13} & \ldots & b_{1n} \\ 0 & \lambda_2 + \varepsilon_k^{(2)} & b_{23} & \ldots & b_{2n} \\ 0 & 0 & \lambda_3 + \varepsilon_k^{(3)} & \ldots & b_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_n + \varepsilon_k^{(n)} \end{pmatrix}$$

Alors toutes les valeurs propres de A_k (les termes sur la diagonale) sont distinctes. Donc A_k est diagonalisable. Et clairement les coefficients de A_k tendent vers ceux de a lorsque $k \to +\infty$. La densité de $D^n_{\mathbb{C}}$ dans $\mathcal{M}_n(\mathbb{C})$ est démontrée. Le problème dans $\mathbb{R}$ est bien sûr qu'une matrice réelle n'est pas forcément trigonalisable. Soit par exemple $n = 2$ et

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

Le polynôme caractéristique de A est $P(X) = X^2 + 1$ qui n'est pas scindé. Supposons qu'il existe une suite $(A_k)_k$ de matrices diagonalisables dont les coefficients convergent vers ceux de A. Le polynôme caractéristique d'une matrice diagonalisable est scindé. On aurait donc une ou deux suite réelles $(a_k)_k$, $(b_k)_k$, convergentes (par construction du polynôme caractéristique et convergence des coefficients de A_k) telles que, pour tout $x \in \mathbb{R}$,

$$x^2 + 1 = \lim_{k \to +\infty} (x - a_k)(x - b_k) .$$

Si a et b sont les limites de $(a_k)_k$ et $(b_k)_k$ on aurait ainsi $x^2 + 1 = (x - a)(x - b)$, ce qui est impossible dans $\mathbb{R}$. Donc $D^n_{\mathbb{R}}$ n'est pas dense dans $\mathcal{M}_n(\mathbb{R})$. $\square$

Ce théorème fournit une preuve simple de Cayley-Hamilton (dans le cas complexe donc). Si $A = \lim_{k \to +\infty} A_k$, si P est le polynôme caractéristique de A et les P_k sont les polynômes caractéristiques des A_k, alors clairement $P(A) = \lim_{k \to +\infty} P_k(A_k)$. Pour une matrice diagonalisable B il est simple de vérifier que $P(B) = 0$ puisqu'il suffit de le vérifier sur les matrices diagonales elles-mêmes, sachant que les termes diagonaux sont précisément les racines de leur polynôme caractéristique. On a donc $P_k(A_k) = 0$ pour tout k. D'où $P(A) = 0$.

Emmanuel Hebey, Université de Cergy-Pontoise, Département de Mathématiques, Site de Saint-Martin, 2 avenue Adolphe Chauvin, 95302 Cergy-Pontoise cedex, France

Email address: `Emmanuel.Hebey@cyu.fr`