Algèbre Linéaire

Hammadi Rafik Ouariachi.

Table des matières

Chapitre 1

Les Espaces Vectoriels

1.1 Introduction

Un espace vectoriel est une structure algébrique stable par addition interne (de vecteurs) et par multiplication externe (par un scalaire).

1.1.1 Définitions :

Définition

Soit E un ensemble non vide, et $(K, +, x)$ un corps dont le neutre pour la loi "+" est noté, et pour la loi "x" est noté .
On note l'ensemble E muni d'une loi interne " + " et d'une loi externe ".".
On dit que est un K-espace vectoriel lorsque :

i) $(E, +)$ forme un groupe abélien, dont l'élément neutre, noté 0_E , est appelé le vecteur nul.

ii) La loi est distributive par rapport à la loi + :
$\forall \lambda \in K, \forall (x, y) \in E^2, \lambda.(x + y) = (\lambda.x) + (\lambda.y)$

iii) $\forall (\lambda, \mu) \in K^2, \forall x \in E, (\lambda + \mu).x = (\lambda.x) + (\mu.x) et (\lambda * \mu).x = \lambda.(\mu.x)$

iv) $\forall x \in E, 1_K.x = x$

Les éléments de E s'appellent des **vecteurs** et les éléments de K des **scalaires**.

1.1.2 Exemples :

$(R^2, +, *)$ est un R-espace vectoriel , en effet :

— (i) : $(R^2, +)$ est un groupe abélien de neutre (0,0).

— (ii) : Soient $\lambda \in R, (x, y) \in R^2 * R^2$ tel que $x = (x_1, x_2)$ et $y = (y_1, y_2)$, on a :

$$\begin{aligned}
\lambda(x + y) &= \lambda(x_1 + y_1, x_2 + y_2) \\
\Leftrightarrow \quad &= (\lambda x_1 + \lambda y_1, \lambda x_2 + \lambda y_2) \\
\Leftrightarrow \quad &= ((\lambda x_1, \lambda x_2) + (\lambda y_1, \lambda y_2)) \\
\Leftrightarrow \quad &= \lambda(x_1, x_2) + \lambda(y_1, y_2) \\
\Leftrightarrow \quad &= (\lambda.x) + (\lambda.y)
\end{aligned}$$

— (iii) : Soient $(\lambda, \mu) \in R^2, x \in R^2$ tel que $x = (x_1, x_2)$ on a :

$$\begin{aligned}
(\lambda + \mu).x &= (\lambda + \mu).(x_1, x_2) \\
&\Leftrightarrow = (\lambda.x_1 + \mu.x_1, \lambda.x_2 + \mu.x_2) \\
&\Leftrightarrow = (\lambda.x_1, \lambda.x_2) + (\mu.x_1, \mu.x_2) \\
&\Leftrightarrow = (\lambda.x) + (\mu.x) \\
(\lambda * \mu).x &= (\lambda * \mu.x_1, \lambda * \mu.x_2) \\
&\Leftrightarrow = \lambda.(\mu.x_1, \mu.x2)
\end{aligned}$$

(Car la multiplication est associative dans R.)
(iv) Soit $x \in R^2$ tel que $x = (x_1, x_2)$ on a :
$1_R.x = 1.x = (1.x_1, 1.x_2) = (x_1, x_2) = x$. (Car x_1, x_2 sont dans R.)

Donc $(R^2, +, .)$ est un R-espace vectoriel, on peut visualiser cet espace et illustrer les proposition et les theorèmes qu'on va étudier sur cet espace , on peut également les illustrer à travers le R-espace vectoriel $(R^3, +, .)$ pour lequel la démonstration est similaire à ce qu'on a déja fait.

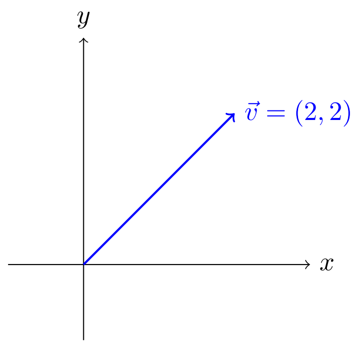
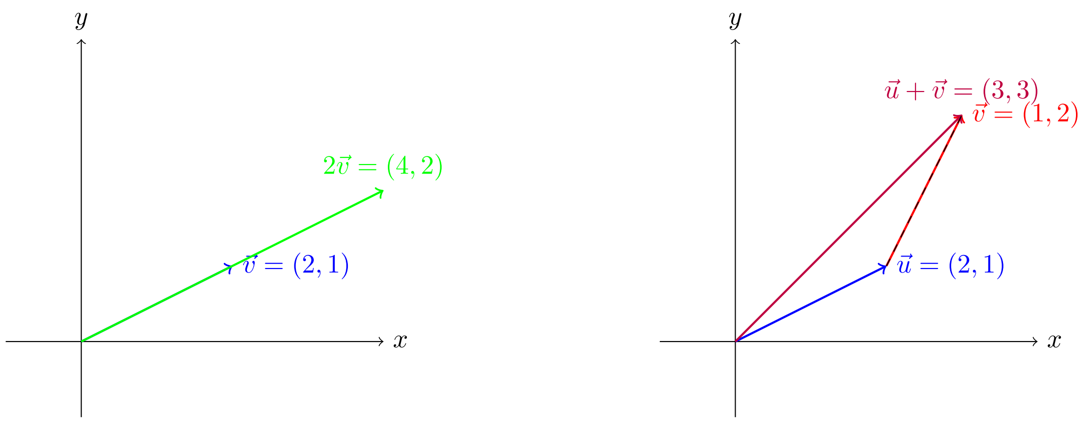


FIGURE 1.1 – Un vecteur dans $\mathbb{R}^2$



(a) Multiplication scalaire d'un vecteur ($\lambda = 2$) (b) Addition de deux vecteurs

FIGURE 1.2 – Exemples d'opérations dans $\mathbb{R}^2$

Exemples illustrés :

1.1.3 Propriétés :

Propriétés

— $\forall \lambda \in K, \forall x \in E, \lambda.x = 0 \Leftrightarrow \lambda = 0_K$ ou $x = 0_E$.
— $\forall x \in E, (-1_K).x = -x$. ($-1_K$ est l'opposé de 1_K dans $\mathbb{K}$ et -x est l'opposé de x dans E.)

Remarque : On verra lors de l'étude de l'algèbre linéaire plusieurs exemples d'espaces vectoriels dont on va détaillera l'étude et les propriétés prochainement.

1.2 Sous-espace vectoriel

1.2.1 Définition :

Définition

Soit E un K-espace vectoriel et F une partie de E, F est un sous-espace vectoriel si la restriction des lois "+", "." sur F lui confère la structure d'un espace vectoriel , c'est à dire , si F est aussi un K-espace vectoriel.

Exemples : Si E est un K-espace vectoriel alors E et $\{0_E\}$ sont les deux des sous espaces vectoriels de E.

1.2.2 Caractérisation :

Caractérisation : S

oit F une partie de E. On peut montrer que F est un sous-espace vectoriel de E si les conditions suivantes sont réalisées :
i)$F \neq \varnothing$.
ii)$\forall (x, y) \in E, \forall (\lambda, \mu) \in K, \lambda.x + \mu.y \in F$.

Remarque : 0_E est dans F et $0_F = 0_E$, généralement , on montre qu'un ensemble est un sous-espace vectoriel d'un$\mathbb{K}$espace vectoriel en utilisant cette caractérisation en commençant par montrer que 0_E est dans F, souvent on montre aussi qu'un ensemble est un$\mathbb{K}$espace vectoriel en montrant qu'il est en effet un sous-espace vectoriel d'un$\mathbb{K}$espace vectoriel usuel.

1.2.3 Sous-espace vectoriel engendré

Combinaison linéaire

Soit I un ensemble éventuellement infini.

Définition

On appelle combinaison linéaire d'éléments de la famille de vecteurs $(x_i)_{i\in I}$ tout vecteur v de E tel qu'il existe une famille de scalaires $(\lambda_i)_{i\in I} \in K$ tel que les $(\lambda_i)_{i\in I}$ sont nuls sauf un nombre fini d'entre eux et qu'elle vérifie $v = \sum_{i\in I} \lambda_i x_i$.

Exemple illustré : Soient $(0, 1), (3, 2), (5, 1)$ trois vecteurs du $\mathbb{R}$-espace vectoriel R^2, alors (-1,-3/5) est une combinaison linéaire de ces vecteur, en effet on a :
$(1, -1, 2/5) \in R$ tels que $(-1, -3/5) = 1 * (0, 1) - 1 * (3, 2) + 2/5 * (5, 1)$

S-ev engendré par une famille de vecteurs

Définition

On appelle sous-espace vectoriel de E engendré par la famille $(x_i)_{i\in I}$, qu'on note $\operatorname{Vect}((x_i)_{i\in I})$: l'ensemble des combinaisons linéaires d'éléments de $(x_i)_{i\in I}(x_i)_{i\in I}$:

$$\boxed{\operatorname{Vect}((x_i)_{i\in I}) = \left\{ \sum_{i\in I} \lambda_i x_i \;\middle|\; (\forall i \in I), \lambda_i \in K \right\}.}$$

L'ensemble $\operatorname{Vect}((x_i)_{i\in I})$ est, au sens de l'inclusion, le plus petit sous-espace vectoriel de E contenant tous les x_i.

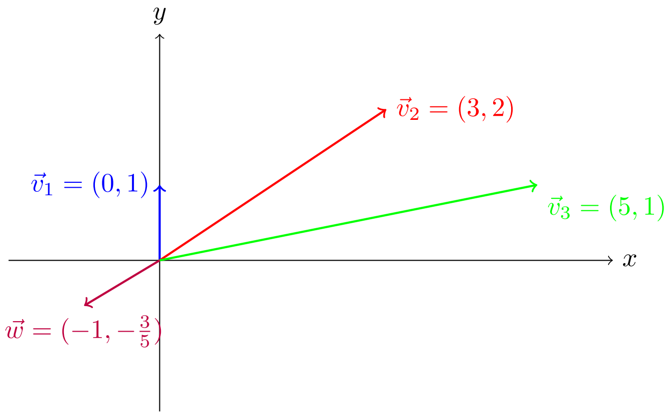


FIGURE 1.3 – Combinaison linéaire des vecteurs $\vec{v}_1, \vec{v}_2, \vec{v}_3$

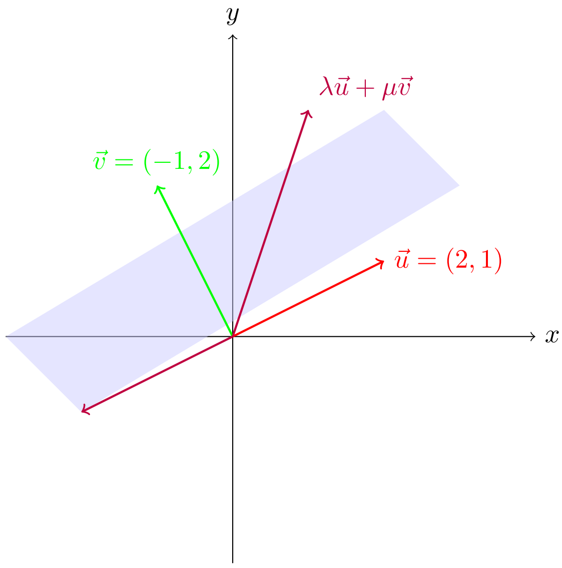


FIGURE 1.4 – Sous-espace engendré par $\vec{u}$ et $\vec{v}$

Exemple illustré : Soient deux vecteurs $\vec{u}$ et $\vec{v}$ dans $\mathbb{R}^2$. L'ensemble des combinaisons linéaires de ces vecteurs est donné par :

$$\text{Vect}(\vec{u}, \vec{v}) = \{\lambda\vec{u} + \mu\vec{v} \mid \lambda, \mu \in \mathbb{R}\}.$$

Interprétation géométrique :

— Si $\vec{u}$ et $\vec{v}$ sont **colinéaires**, alors leur espace engendré est une **droite** passant par l'origine.
— Si $\vec{u}$ et $\vec{v}$ sont **linéairement indépendants**, alors leur espace engendré est **tout le plan** $\mathbb{R}^2$.

Dans la figure ci-dessous :

— Les vecteurs $\vec{u} = (2, 1)$ et $\vec{v} = (-1, 2)$ sont représentés en rouge et vert.
— Le **sous-espace vectoriel engendré** est la **région bleue** qui contient toutes les combinaisons linéaires possibles de ces vecteurs.
— Les vecteurs en violet sont des exemples de combinaisons linéaires de $\vec{u}$ et $\vec{v}$.

Ainsi, dans cet exemple, les vecteurs $\vec{u}$ et $\vec{v}$ étant non colinéaires, leur espace engendré est bien $\mathbb{R}^2$.

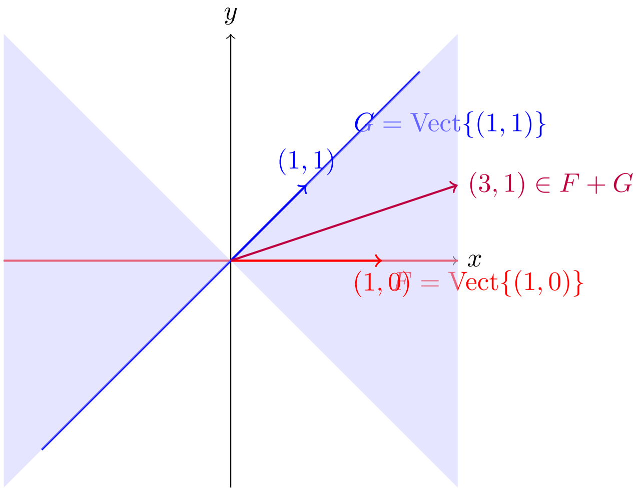


FIGURE 1.5 – Exemple de somme de sous-espaces $F + G = \mathbb{R}^2$

S-ev engendré par une partie

Définition

Soient E un espace vectoriel sur K et $A \subset E$.
On appelle sous-espace vectoriel engendré par A, et l'on note Vect(A)l'ensemble de toutes les combinaisons linéaires d'éléments de A :

$$\mathrm{Vect}(A) = \left\{ \sum_{i=1}^{n} \lambda_i . a_i \;\middle|\; n \in \mathbb{N}, (\lambda_1, \cdots, \lambda_n) \in K^n, (a_1, \cdots, a_n) \in A^n \right\}.$$

Il s'agit, au sens de l'inclusion, du plus petit espace vectoriel contenant A.

1.2.4 Somme de Sous-espaces vectoriels

Définition

Soient $FetG$ deux sous-espaces vectoriels de E. On définit la somme de Fet G comme l'ensemble :

$$F + G = \{u + v \mid (u, v) \in F \times G\}.$$

Remarque : $F + G = \mathrm{Vect}\,(F \cup G)$.

Exemples-illus Soient deux sous-espaces vectoriels de $\mathbb{R}^2$:
- $F = \mathrm{Vect}\{(1, 0)\}$: l'axe des abscisses.
- $G = \mathrm{Vect}\{(1, 1)\}$: la droite $y = x$.

Leur somme est :

$$F + G = \mathrm{Vect}\{(1, 0), (1, 1)\} = \mathbb{R}^2.$$

1.2.5 Intersection de Sous-espaces vectoriels

Proposition

Toute intersection de sous-espaces vectoriels de E est un sous-espace vectoriel de E.

Démonstration : Soients E un K-espace vectoriel, F et G deux sous espaces vectoriel de E,

i) puisque F et G sont deux sous espaces vectoriel de E , $0_E \in F$ et $0_E \in G$ donc $0_E \in F \cap G$ donc $F \cap G \neq \varnothing$.
ii) Soient $(x, y, \lambda) \in F \cap G * F \cap G * K$, on a $(x, y, \lambda) \in F * F * K$ donc $x + \lambda y \in F$ car F est un sous espace vectoriel de E,
De même $(x, y, \lambda) \in G * G * K$ donc $x + \lambda y \in G$ car G est un sous espace vectoriel de E,
donc $x + \lambda y \in F \cap G$.

Donc d'après la caractérisation des sous espaces vectoriel on déduit que $F \cap G$ est un sous espace vectoriel de E.

Pour une intersection de plus de deux sous espaces vectoriel , on montre la proposition en utilisant la récurrence sur le nombre des sous espaces vectoriel, en fait l'hérédite se montre exactement comme on a fait ci-dessus.

Remarque : Cette dernière n'est pas toujours vraie pour la réunion.

Proposition-HP

Si$\mathbb{K}$est un corps commutatif et E un K-espace vectoriel et F et G deux sous espaces vectoriel de E tel que $F \cup G$ est un sous espace vectoriel de E, alors $F \subset G$ ou $G \subset F$.

Démonstration : Raisonnement par absurde :

Soient$\mathbb{K}$est un corps commutatif et E un K-espace vectoriel et F et G deux sous espaces vectoriel de E tel que $F \cup G$ est un sous espace vectoriel de E,

Supposons le contraire de " $F \subset G$ ou $G \subset F$ ", c'est à dire "$F \not\subset G$ et $G \not\subset F$" alors il existe $x \in F, x \notin G$ et $y \in G, y \notin F$.
On a $x + y \in F \cup G$ donc $x + y \in F$ ou $x + y \in G$ Si $x + y \in F$, puisque $x \in F, -x \in F$, donc $x + y + (-x) = x + y - x = y \in F$, ce qui est absurde. De même si $x + y \in G$, on obtient $x \in G$, ce qui est aussi absurde.

Donc dans tous les cas , par raisonemment par absurde on obtient $F \subset G$ ou $G \subset F$.

Proposition-HP

Soit $k \geq 2$ et $(V_i)_{1 \leq i \leq k}$ une famille finie de k sous-espaces vectoriels stricts de E (c'est-à-dire que pour tout i, $V_i \neq \{0\}$ et $V_i \neq E$). Si l'on a :

$$E = V_1 \cup V_2 \cup \cdots \cup V_k,$$

alors le corps $\mathbb{K}$ est fini et on a :

$$k \geq \mathrm{Card}(\mathbb{K}) + 1.$$

Démonstration : On suppose que $V_1 \not\subset (V_2 \cup \cdots \cup V_k)$. Il existe donc $x \in V_1$ tel que $x \notin V_2 \cup \cdots \cup V_k$. Or $(V_2 \cup \cdots \cup V_k) \not\subset V_1$ (sinon $V_1 = E$), donc il existe $y \in V_2 \cup \cdots \cup V_k$ tel que $y \notin V_1$.

Si $\lambda \in \mathbb{K}$, alors $y + \lambda x \in E$. Or, $y + \lambda x \notin V_1$ (sinon $y \in V_1$ car $x \in V_1$), donc pour tout $\lambda \in \mathbb{K}$, il existe $i_\lambda \in \{2, \ldots, k\}$ tel que $y + \lambda x \in V_{i_\lambda}$. L'application

$$\mathbb{K} \to \{2, \ldots, k\}, \quad \lambda \mapsto i_\lambda$$

est injective (en effet, si $\lambda = \mu$, alors $y + \lambda x$ et $y + \mu x$ sont dans le même V_{i_λ}, donc $(\lambda - \mu)x \in V_{i_\lambda}$, et comme $x \notin V_{i_\lambda}$, on doit avoir $\lambda = \mu$). De cette injectivité, on déduit que

$$\mathrm{Card}(\mathbb{K}) \leq \mathrm{Card}\{2, \dots, k\} = k - 1,$$

d'où l'inégalité souhaitée.

1.2.6 Supplémentaire de Sous-espaces vectoriels

Définition

Deux sous-espaces vectoriels F et G de E sont dits supplémentaires si $F + G = E$ et $F \cap G = \{0\}$ autrement dit : si
$E \subset F + G \quad \text{et} \quad F \cap G \subset \{0\}$
On note alors $E = F \oplus G$.

Proposition-HP

Soit E un K-espace vectoriel de dimension finie, si A et B sont deux sous-espaces vectoriels de E de même dimension r, alors A et B admettent un supplémentaire commun (i.e. il existe un sous-espace vectoriel S de E tel que $A \oplus S = B \oplus S = E$).

Démonstration : On raisonne par récurrence descendante sur r :

— Initialisation :
  Si $r = \dim E$, c'est évident car $\{0\}$ est un supplémentaire commun à A et à B.
  L'initialisation est établie.

— Hérédité :
  Supposons le résultat vérifié au rang $r + 1 < \dim E$ et démontrons-le au rang r.
  On a $A \cup B \neq E$. En effet, supposons $A \cup B = E$. Comme $A \neq B$ (sinon $E = A \cup B = B$), il existe $x \in A$ tel que $x \notin B$. De même, il existe $y \in B$, $y \notin A$. Or $x + y \in E = A \cup B$, donc $x + y \in A$ ou $x + y \in B$, par exemple $x + y \in A$. Alors $y = (x + y) - x \in A$, ce qui est absurde. On a donc bien $A \cup B \neq E$.
  Donc il existe $x \in B$, $x \notin A \cup B$. Soit $A' = A + \mathrm{Vect}(x)$, $B' = B + \mathrm{Vect}(x)$. On a $\dim A' = \dim B' = r + 1$, donc d'après l'hypothèse de récurrence, il existe un s.e.v S' de E tel que $A' \oplus S' = B' \oplus S' = E$. Si $S' = S' + \mathrm{Vect}(x)$, on a donc $E = A' \oplus S' = A \oplus \mathrm{Vect}(x) \oplus S' = A \oplus S$ et $E = B' \oplus S' = B \oplus \mathrm{Vect}(x) \oplus S' = B \oplus S$, d'où le résultat.

1.2.7 Produit Cartésien de Sous-espaces vectoriels

Définition

Soient E et F deux K-espaces vectoriels.
On définit l'espace produit de E et F comme l'ensemble produit $E \times F$, muni des deux lois suivantes, qui en font un $\mathbb{K}$-espace vectoriel :

$$(x, y) +_{E \times F} (x', y') = (x +_E x', y +_F y') \text{ et } \lambda \cdot_{E \times F} (x, y) = (\lambda \cdot_E x, \lambda \cdot_F y)$$

1.3 Famille de Vecteurs

1.3.1 Famille génératrice

Définition

La famille $(x_i)_{i \in I}$est dite génératrice de E si $E = \mathrm{Vect}\left((x_i)_{i \in I}\right)$. Cela équivaut à dire que tout vecteur de E s'exprime comme combinaison linéaire de la famille $(x_i)_{i \in I}$:

$$\boxed{\forall v \in E \quad \exists (\lambda_i)_I \in K^{Card(I)} \quad v = \sum \lambda_i x_i}$$

Remarque : Si A est une partie de E et $E = \text{Vect}\,(A)$, on dit que A est une partie génératrice de E.

Exemples :

— **Famille des Monômes :**
$\{1, x, x^2, \ldots, x^n\}$

Démonstration L'ensemble des polynômes de degré inférieur ou égal à n, noté $\mathbb{R}_n[X]$, est un espace vectoriel de dimension $n+1$. Un polynôme quelconque de degré inférieur ou égal à n s'écrit :

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

avec $a_i \in \mathbb{R}$. Tout polynôme peut donc être exprimé comme une combinaison linéaire des éléments de la famille donnée, ce qui prouve qu'elle est génératrice.

— **Famille des Fonctions Exponentielles** $\{e^{\lambda x} \mid \lambda \in \mathbb{R}\}$

Démonstration : La solution générale de l'équation différentielle homogène :

$$y'' - \lambda y = 0$$

peut s'écrire comme une combinaison linéaire de $e^{\sqrt{\lambda}x}$ et $e^{-\sqrt{\lambda}x}$. Ces fonctions forment donc une famille génératrice des solutions de cette équation.

— **Famille des Fonctions Trigonométriques** $\{\cos(nx), \sin(nx)\}$

Démonstration : Si $f(x)$ est une fonction définie sur $[-\pi, \pi]$, elle peut s'écrire sous la forme :

$$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos(nx) + b_n \sin(nx)\right).$$

Les fonctions $\{\cos(nx), \sin(nx)\}$ forment donc une famille génératrice des fonctions périodiques dans $L^2([-\pi, \pi])$.

— **Famille des Polynômes de Legendre** $\{P_n(x)\}$

Démonstration : Les polynômes de Legendre sont solutions de l'équation :

$$(1 - x^2)P_n''(x) - 2xP_n'(x) + n(n+1)P_n(x) = 0.$$

Ils forment une base orthogonale des fonctions définies sur $[-1, 1]$, et toute fonction définie sur cet intervalle peut être approchée par une combinaison de ces polynômes.

— **Famille des Fonctions de Bessel** $\{J_n(x)\}$
Les fonctions de Bessel apparaissent comme solutions de l'équation :

$$x^2 y'' + x y' + (x^2 - n^2) y = 0.$$

Elles interviennent en physique pour les problèmes de symétrie cylindrique et permettent de générer des solutions adaptées aux systèmes circulaires.

— **Famille des Fonctions de Hermite** $\{H_n(x)e^{-x^2/2}\}$
Les polynômes de Hermite, définis par :

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2},$$

apparaissent naturellement en mécanique quantique, notamment dans la résolution de l'équation de Schrödinger pour l'oscillateur harmonique.

1.3.2 Famille libre, liée

Définitions :

Définitions

On dit que la famille $(x_i)_{i\in I}$ est libre, ou que les vecteurs x_i sont linéairement indépendants, si aucun vecteur n'est combinaison linéaire des autres vecteurs.
Cela équivaut à dire que :

$$\forall(\lambda_i)_{i\in I} \in K^{Card(I)} \quad \sum \lambda_i x_i = 0 \Rightarrow \forall i \in I \quad \lambda_i = 0_E.$$

Une famille qui n'est pas libre est dite liée. Elle est donc liée si un vecteur est une combinaison linéaire des autres dans , c'est-à-dire :

$$\exists(\lambda_i)_{i\in I} \in K^{Card(I)} \quad \sum \lambda_i x_i = 0 \text{ et } (\lambda_i)_{i\in I} \neq (0_E).$$

Exemples : Dans le $\mathbb{R}$-espace vectoriel des fonctions continues de$\mathbb{R}$ dans $\mathbb{R}$, les familles suivantes sont des familles libres :

i) $(f_\lambda)_{\lambda\in R}$ où

$$f_\lambda : \mathbb{R} \to \mathbb{R}\ x \mapsto \exp \lambda x$$

ii) $(f_\lambda)_{\lambda\in R}$ où

$$f_\lambda : \mathbb{R} \to \mathbb{R}\ x \mapsto \cos(\lambda x)$$

iii) $(f_\lambda)_{\lambda\in R}$ où

$$f_\lambda : \mathbb{R} \to \mathbb{R}\ x \mapsto |x-\lambda|$$

iv) $(f_k)_{k\in\mathbb{N}}$ où

$$f_n : \mathbb{R} \to \mathbb{R}\ x \mapsto \cos(x^n)$$

.

v) Soit $\mathbb{K}$ un sous corps de $\mathbb{C}$, dans le $\mathbb{K}$-espace vectoriel $K[X]$,
la famille $(1, X, ..., X^{n-p-1}, P(X), P(X+1), ..., P(X+p))$ avec $P \in K[X]$ de degré $n \geq 1$ et $p \in [|0,n|]$, est libre quelque soit $p \in [|0,n|]$.

Démonstration :

i) On note le $\mathbb{R}$-espace vectoriel par E et on montre par absurde que la famille est libre.
On suppose que la famille $(f_\lambda)_{\lambda\in R}$ où $f_\lambda : \mathbb{R} \to \mathbb{R}\ x \mapsto \exp(\lambda x)$ est liée.
On aura donc :
$\exists(\lambda_i)_{1\leq i\leq n} \in \mathbb{R}^n, \exists(\mu_i)_{1\leq i\leq n} \in \mathbb{R}^n$, avec les μ_i sont non tous nuls telles que

$$\sum_{1\leq i\leq n} \mu_i\lambda_i = 0_E$$

On indexe les λ_i de sorte que $\lambda_i \leq \lambda_j$ si $j \leq i$, c'est à dire : $\lambda_n \leq ... \leq \lambda_1$.
Soit $k \in [|1,n|]$ tel que $k = min\{\{1,..,n\}|\mu_i \neq 0_{\mathbb{R}}\}$
$Lim_{x\to+\infty} exp(-\lambda_1 x)\sum_{i=k}^{n} \mu_i exp(\lambda_i x) = \sum_{i=k}^{n} \mu_i exp(\lambda i - \lambda_1) = \mu_1$.
car pour tout $i \geq 2, \lambda_i - \lambda_1 \leq 0$..

Or $\sum_{i=k}^{n} \mu i f_{\lambda_i} = 0$,, donc $u_1 = 0$, ce qui est absurde.

> On conclut par raisonnement par absurde que la famille $(f_\lambda)_{\lambda\in R}$ où $f_\lambda : \mathbb{R} \to \mathbb{R}\ x \mapsto \exp(\lambda x)$ est libre.

ii) La famille $(f_\lambda)_{\lambda\in R}$ où $f_\lambda : \mathbb{R} \to \mathbb{R}\ x \mapsto \cos(\lambda x)$ étant libre est équivalent à

$$\forall(\mu_i) \in K^{Card(I)} \sum_{i\in I} \mu_i x_i = 0 \Rightarrow \forall \in I, \mu_i = 0.$$

l'ensemble I qui indexe les μ_i contient qu'un nombre fini d'éléments non nuls qu'on note $n \in \mathbb{N}^*$ donc $(\mu_i)_{i\in I} = (\mu_i)_{i\in[|1,n|]}$,
On conclut donc qu montrer que la liberté de la famille est équivalent à montrer que :

$$P : \forall n \in \mathbb{N}^*, \forall (\lambda_i)_{i\in[|1,n|]} \in \mathbb{R}^n \ \forall (\mu_i)_{i\in[|1,n|]} \in \mathbb{R}^n \sum_{i=1}^n \mu_i f_{\lambda_i} = 0_E \Rightarrow \forall i \in [|1,n|], \mu_i = 0_\mathbb{R}$$

Or le *cos* étant paire on va prendre (les λ_i distincts dans $\mathbb{R}^+$).
On montrera alors cette proposition par récurrence simple sur $n \in \mathbb{N}^*$
Initialisation : P(1)
Pour n=1, soient $(\lambda_1, \mu_1) \in \mathbb{R}^2$ telles que $\mu_1 f_{\lambda_1} = 0_E$, on a donc $\forall x \in R, \mu_1. \cos \lambda_1 x = 0_R$, pour $x = 0, cos(0) = 1$ donc $\mu_1 = 0_R$).
On a montré donc

$$\forall \mu_1 \in \mathbb{R}, \forall \lambda_1 \in \mathbb{R}^+, (\mu_1 f_{\lambda_1} = 0_E) \Rightarrow (\mu_1 = 0_R).$$

Hérédité : $P(n) \Rightarrow P(n+1)$
Soit $n \geq 1$, supposant la proposition vraie au rang n, et montrons la au rang n+1 :
Soient $(\mu_i)_{i\in[|1,n+1|]}$ et $(\lambda_i)_{i\in[|1,n+1|]}$ telles que
$\sum_{i\in[|1,n+1|]} \mu_i f_{\lambda_i} = 0_E$
Par double dérivation et puisque (les λ_i distincts dans $\mathbb{R}^+$) on a :
$\sum_{i=1}^{n+1} \mu_i(-\lambda_i^2) f_{\lambda_i} = 0_E$ (1)
et par multiplication par λ_n^2 : $\sum_{i=1}^{n+1} \mu_i(\lambda_n^2) f_{\lambda_i} = 0_E$ (2)
On ajoute (1) et (2) et on obtient λ_{n+1}^2 : $\sum_{i=1}^{n} \mu_i(\lambda_{n+1}^2 - \lambda_i^2) f_{\lambda_i} = 0_E$
D'après l'hypothèse de la récurrence "P(n)", on a :
$\forall i \in [|1,n|], \mu_i(\lambda_{n+1}^2 - \lambda i^2) = 0_R$
Et puisque les λ_i distincts dans $\mathbb{R}^+$ on déduit que :
$\forall i \in [|1,n|], \mu_i = 0_R$
Donc $\sum_{i\in[|1,n+1|]} \mu_i f_{\lambda_i} = 0_E$ devient $\mu_{n+1} f_{\lambda_{n+1}} = 0_E$
ce qui veut dire $\forall x \in R, \mu_{n+1} f_{\lambda_{n+1}}(x) = 0_R$ donc $\mu_{n+1} = 0_R$.
Donc $\forall i \in [|1,n+1|], \mu_i = 0_R$
On a montré que , en supposant que P(n) est vraie on déduit que : $\sum_{i\in[|1,n+1|]} \mu_i f_{\lambda_i} = 0_E \Rightarrow \forall i \in [|1,n+1|], \mu_i = 0_R$
Finalement par raisonnement par récurrence :

La famille $(f_\lambda)_{\lambda\in R}$ où $f_\lambda : \mathbb{R} \to \mathbb{R}\ x \mapsto \cos(\lambda x)$ est libre.

iii) On montre par absurde que la famille $(f_\lambda)_{\lambda\in R}$ où $f_\lambda : \mathbb{R} \to \mathbb{R} x \mapsto |x - \lambda|$ est libre.
Supposant que la famille $(f_\lambda)_{\lambda\in R}$ est liée, alors comme précédemment la libérté de la famille étant équivalent à
$P : \forall n \in \mathbb{N}^*, \forall (\lambda_i)_{i\in[|1,n|]} \in \mathbb{R}^n \ \forall (\mu_i)_{i\in[|1,n|]} \in \mathbb{R}^n \sum_{i=1}^n \mu_i f_{\lambda_i} = 0_E \Rightarrow \forall i \in [|1,n|], \mu_i = 0_\mathbb{R}$
On supposera :
$\bar{P} : \exists n \in \mathbb{N}^*, \exists (\lambda_i)_{i\in[|1,n|]} \in \mathbb{R}^n, \exists (\mu_i)_{i\in[|1,n|]} \in \mathbb{R}^n \sum_{i=1}^n \mu_i f_{\lambda_i} = 0_E$ et les μ_i non tous nuls.
D'après la proposition il existe $\lambda_0 \in \mathbb{R}$ tel que f_{λ_0} est combinaison linéaire des $(f_\lambda)_{\lambda\in\mathbb{R}} - \{\lambda_0\}$ ce qui est équivalent à :
$\exists n \in \mathbb{N}^*, \exists (\lambda_i)_{i\in[|1,n|]} \in \mathbb{R}^n - \{\lambda_0\}, \exists (\mu_i)_{i\in[|1,n|]} \in \mathbb{R}^n f_{\lambda_0} = \sum_{i=1}^n \mu_i f_{\lambda_i}$
Pour tout $\lambda \in \mathbb{R}$ la fonction de $\mathbb{R}$ dans $\mathbb{R}$ $x \mapsto |x - \lambda|$ est dérivable en tout $x \neq \lambda$ donc $\forall i \in [|1,n|], f_{\lambda_i}$ est dérivable sur λ_0 car $\forall i \in [|1,n|], \lambda_0 \neq \lambda_i$
Cependant, par addition de fonction dérivable au même point et multiplication par scalaires $\sum_{i=1}^n \mu_i f_{\lambda_i}$ est dérivable en λ_0 or $f_{\lambda_0} = \sum_{i=1}^n \mu_i f_{\lambda_i}$ donc f_{λ_0} est dérivable en λ_0 ce qui est absurde.
Finalement on a montré que la proposition $P : \forall n \in \mathbb{N}^*, \forall (\lambda_i)_{i\in[|1,n|]} \in \mathbb{R}^n \ \forall (\mu_i)_{i\in[|1,n|]} \in \mathbb{R}^n \sum_{i=1}^n \mu_i f_{\lambda_i} = 0_E \Rightarrow \forall i \in [|1,n|], \mu_i = 0_\mathbb{R}$ est vraie, donc

La famille $(f_\lambda)_{\lambda\in R}$ où $f_\lambda : \mathbb{R} \to \mathbb{R}\ x \mapsto |x - \lambda|$ est libre.

iv) Supposons qu'il existe une combinaison linéaire nulle de ces fonctions, c'est-à-dire qu'il existe des coefficients $\lambda_n \in \mathbb{R}$, dont un au moins est non nul, tels que :

$$\sum_{n=1}^{N} \lambda_n \cos(x^n) = 0, \quad \forall x \in \mathbb{R}.$$

Nous allons prouver que cela implique nécessairement que tous les λ_n sont nuls.
Pour $x = 0$, on obtient :

$$\sum_{n=1}^{N} \lambda_n \cos(0) = \sum_{n=1}^{N} \lambda_n = 0.$$

Cela donne une première équation, mais ne suffit pas encore pour conclure.
Développons $\cos(x^n)$ en série de Taylor autour de $x = 0$:

$$\cos(x^n) = 1 - \frac{x^{2n}}{2} + O(x^{4n}).$$

Ainsi, la combinaison linéaire s'écrit :

$$\sum_{n=1}^{N} \lambda_n \left(1 - \frac{x^{2n}}{2} + O(x^{4n})\right) = 0.$$

Décomposons cette somme en termes de puissances de x :

$$\left(\sum_{n=1}^{N} \lambda_n\right) - \frac{1}{2}\sum_{n=1}^{N} \lambda_n x^{2n} + O(x^4) = 0.$$

Par unicité du développement en série de Taylor, chaque coefficient doit être nul.
Nous avons déjà vu que $\sum \lambda_n = 0$. Maintenant, en identifiant les termes de plus petit degré en x, on obtient :

$$\sum_{n=1}^{N} \lambda_n x^{2n} = 0 \quad \forall x.$$

Puisque les puissances x^{2n} sont linéairement indépendantes dans l'espace des fonctions analytiques, cela implique que chaque coefficient doit être nul :

$$\lambda_n = 0 \quad \forall n.$$

Nous avons démontré que la seule combinaison linéaire de $\cos(x^n)$ qui donne la fonction nulle est celle où tous les coefficients sont nuls.

Ainsi, la famille $\{x \mapsto \cos(x^n)\}_{n\in\mathbb{N}^*}$ est **libre** dans $\mathcal{C}(\mathbb{R}, \mathbb{R})$.

v) Supposons qu'il existe une combinaison linéaire nulle de ces éléments, c'est-à-dire qu'il existe des coefficients $\lambda_0, \lambda_1, \ldots, \lambda_{n-p-1}, \mu_0, \ldots, \mu_p \in K$ tels que :

$$\lambda_0 + \lambda_1 X + \cdots + \lambda_{n-p-1} X^{n-p-1} + \sum_{k=0}^{p} \mu_k P(X + k) = 0, \quad \forall X \in K.$$

Nous devons prouver que tous ces coefficients sont nuls.
- Le polynôme $P(X)$ est de degré n, donc chaque $P(X + k)$ est également un polynôme de degré n. - Le seul terme dans l'expression ci-dessus qui peut contenir X^n provient de la somme $\sum \mu_k P(X + k)$. - Si cette somme est nulle, alors son coefficient dominant doit s'annuler. Comme les transformations de $P(X)$ sont linéairement indépendantes, il en résulte que $\mu_k = 0$ pour tout k.
Après annulation des coefficients de degré n, il ne reste que l'expression :

$$\lambda_0 + \lambda_1 X + \cdots + \lambda_{n-p-1} X^{n-p-1} = 0, \quad \forall X \in K.$$

Puisque les monômes $1, X, \ldots, X^{n-p-1}$ sont linéairement indépendants dans $K[X]$, il en résulte que :

$$\lambda_0 = \lambda_1 = \cdots = \lambda_{n-p-1} = 0.$$

Nous avons montré que tous les coefficients λ_i et μ_k sont nuls, ce qui implique que la famille donnée est linéairement indépendante.

Par conséquent, elle est **libre** dans $K[X]$, quel que soit $p \in \{0, 1, \dots, n\}$

1.3.3 Base d'un espace vectoriel

Définition

Une famille $(e_i)_{i\in I}$ de vecteurs de E est une base de E si et seulement si elle est libre et génératrice de E.
Ce qui est équivalent à :
Tout vecteur de E s'écrit comme une combinaison linéaire unique des e_i :

$$\forall v \in E \quad \exists! (\lambda_i)_{i\in I} \in K^{Card(I)} \quad v = \sum \lambda_i e_i$$

Les $(\lambda_i)_{i\in I}$ sont tous nuls sauf un nombre fini, et sont alors appelées les coordonnées de v dans la base $(e_i)_{i\in I}$.

Exemple :
- (1,i) est une base du R-espace vectoriel $(C, +, .)$.
- il existe une certaine type de base dit priviligée qui s'appele base canonique, elle apparait comme la base la plus simple pour un espace vectoriel : Soit $n \in \mathbb{N}^*$, la base canonique du $\mathbb{R}$-espace vectoriel $\mathbb{R}^n$ est $B_c = (e_1, e_2, \dots, e_n$ avec $\forall i \in [|1, n|], e_i = (0, \dots, 1, \dots, 0)$, le 1 étant le i-ème coefficient du vecteur e_i, tout simplement e_i est le vecteur dont tous ces coefficients sont nuls sauf le i-ème qui égale à 1.
  Cette base parait celle la plus naturelle à considérer, en fait prenant l'exemple de $(R^3, +, .)$ un vecteur de ce dernier s'écrit sous la forme : (a, b, c) avec $a, b, c \in R$ donc :
  $(a, b, c) = a * (1, 0, 0) + b * (0, 1, 0) + c * (0, 0, 1)$
  du coup la base canonique de $(R^2, +, .)$ est $((1, 0, 0), (0, 1, 0), (0, 0, 1)), e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)$, il faut bien retenir et comprendre la base canonique car elle est utilisée extensivement en algèbre linéaire.

Théorème

Si E est un espace vectoriel engendré par une famille de vecteurs finie $(x_i)_{i\in[|1,n|]}, n \in N^*$, alors :
i) Toute famille libre a au plus n vecteurs.
ii) Toute famille génératrice a au moins n vecteurs.

Démonstration Soit E Si E est un espace vectoriel engendré par une famille de vecteurs finie $(x_i)_{i\in[|1,n|]}, n \in N^*$,
i) Soit L une famille libre de E, raisonnant par absurde et supposant qu'elle a n+1 vecteurs, choisissant un vecteur v dans L, v est combinaison linéaire des $(x_i)_{i\in[|1,n|]}, n \in N^*$, or chaque vecteur de L s'écrit sous forme de combinaison linéaire des $(x_i)_{i\in[|1,n|]}, n \in N^*$ puisque on a n vecteurs restant dans L, on peut écrire chaque $(x_i)_{i\in[|1,n|]}, n \in N^*$ sous forme de combinaison linéaire des vecteurs de L et puisque v est combinaison linéaire des $(x_i)_{i\in[|1,n|]}, n \in N^*$, il sera aussi combinaison linéaire des vecteurs de L, or L est libre d'où la contradiction.
ii) Soit G une famille génératrice de E, donc E= Vect(G)=Vect($(x_i)_{i\in[|1,n|]}$), $n \in N^*$, donc nécessairement G a au moins n vecteurs.

1.4 Dimension

Définition

Un espace vectoriel est dit de dimension finie s'il existe un famille génératrice finie de celui ci, dans le cas contraire , on parle d'espace vectoriel de dimension infinie.

Remarque : Il faut faire attention au corps de base de l'espace vectoriel car il agit sur la dimension , par exemple $(\mathbb{C}, ., +)$ est un espace vectoriel de dimension 2 si on le voit en tant que R-espace vectoriel, en fait sa base est $(1, i)$, cependant en tant qu'un $\mathbb{C}$-espace vectoriel , il est de dimension 1.

On aborde cette remarque avec plus de détail dans les subsections concernant la notion hors programme d'extension de corps.

Exemples :

— Soit $n \in N^*$ alors $(R^n, +, *)$ est de dimension n.

1.4.1 Théorème de la base incomplète :

Théorème de la base incomplète :

Soit E un espace de dimension finie, si $G = (x_i)_{i\in I}$ est une famille génératrice de E et il existe $J \in I$pour laquelle la famille $L = (x_i)_{i\in J}$ est libre, alors il existe une base B de E tq $L \subset B \subset G$

Démonstration : On considère l'ensemble de toutes les sous-familles libres d'éléments de G. Cet ensemble est non vide puisqu'il contient L. Il existe un nombre finie de telles familles car G est un ensemble fini. On en choisit une de cardinal maximum. Notons la B, et montrons que B est une base de E. Déjà B est libre par construction. Soit $g \in G \backslash B$. Alors la famille $B \cup \{g\}$ est de cardinal plus grand que celui de B, donc est liée. Comme B est libre, c'est que le vecteur ajouté g est combinaison linéaire des éléments de B. Ceci étant vrai pour tous les éléments de G B, on en déduit $Vect(B) = Vect(G) = E$, et donc B est aussi génératrice de E. C'est donc une base de E.

Corollaire

Soit E un K-espace vectoriel de dimension finie,
De toute famille génératrice de E, on peut en extraire une base en prenant les vecteurs linéairement indépendants.
Toute famille libre de E peut être complétée en une base, en ajoutant des vecteurs qui ne sont pas une combinaison linéaire des vecteurs de la famille libre.

Définition

Soit E un K-espace vectoriel de dimension finie, toutes les bases de E ont le même cardinal qu'on note $dim_K E$.
Par convention : $\dim_K E = 0$ pour $E = \{0\}$.

1.4.2 Proposition :

Proposition

Soit E un K-espace vectoriel de dimension $n \in N^*$:

i) Toute famille de n vecteurs libre de est une base de E.

ii) Toute famille de n vecteurs génératrice est une base de E.

Démonstration : Soit E un K-espace vectoriel de dimension $n \in N^*$:

i) Par hypothèse, E possède une base B avec n éléments. Soit une famille libre L avec n éléments. Supposons L non génératrice, c'est-à-dire qu'il existe un vecteur $v \in E$ qui n'est pas combinaison linéaire des vecteurs de L, dans ce cas, $\{L_0\}$ est aussi libre or elle a plus d'éléments qu'une famille génératrice B, ce qui est contradictoire.

ii) Soit une famille génératrice G avec n éléments. Supposons G non libre, donc elle contient un élément v qui est combinaison linéaire des autres, la famille $G\{v\}$ est encore génératrice or elle a moins d'éléments qu'une famille libre B, ce qui est contradictoire.

1.4.3 Proposition :

Proposition

Soit E un K-espace vectoriel de dimension finie et F un sous espace vectoriel de E alors :
$dim_K E \leq dim_K F$.
Cas d'égalité : Si $dim_K E = dim_K F$, on a $E = F$.

1.4.4 Formule de Grassman :

Formule de Grassman

Soit E un K-espace vectoriel et E_1 et E_2 deux sous espace vectoriels de E alors $E_1 + E_2$ est aussi un sous espace vectoriel de E et on a la formule suivante :

$$dim_K E_1 dim_K E_2 = dim_K(E_1 + E_2) - dim_K(E_1 \cap E_2)$$

$dim_K E = dim_K E_1 + dim_K E_2$ et $E_1 \cap E_2 = \{0\}$.
$\iff dim_K E = dim_K E_1 + dim_K E_2$ et $E = E_1 + E_2 \iff E = E_1 \oplus E_2$

Chapitre 2

Les Applications Linéaires

2.1 Definitions

Soient E et F deux $\mathbb{K}$-espaces vectoriels :

2.1.1 Application Linéaire :

Définition

Une application $u : E \to F$ est dite linéaire si elle vérifie :

i) L'additivité : $\forall (x,y) \in E^2, u(x+y) = u(x) + u(y)$
ii) L'homogéniété : $\forall x \in E, \forall \lambda \in K, u(\lambda x) = \lambda u(x)$

ou encore, si elle vérifie :

$$\forall (x,y) \in E^2, \forall \lambda \in K, u(\lambda x + y) = \lambda u(x) + u(y).$$

Elles s'appellent donc des homomorphismes (ou tout simplement morphismes) et leur ensemble est un $\mathbb{K}$-espace vectoriel noté $L(E,F)$

Exemples :

— **Application d'évaluation**
Soit f une fonction polynomiale dans l'espace $K[X]$, on définit l'application :

$$\varphi_a : K[X] \to K, \quad P(X) \mapsto P(a).$$

C'est l'application qui associe à tout polynôme sa valeur en a.

— **Dérivation**
L'opérateur de dérivation est défini sur l'espace des polynômes $K[X]$ par :

$$D : K[X] \to K[X], \quad P(X) \mapsto P'(X).$$

— **Intégration**
L'opérateur d'intégration est défini sur $\mathcal{C}^1(\mathbb{R}, \mathbb{R})$ par :

$$I : f \mapsto \int f(x)dx.$$

C'est une application qui associe à chaque fonction sa primitive.

— **Matrice associée à une application linéaire**
Soit A une matrice $m \times n$, on définit l'application :

$$\varphi_A : \mathbb{R}^n \to \mathbb{R}^m, \quad X \mapsto AX.$$

C'est l'application qui associe à tout vecteur X son image par la matrice A.

— **Projection sur un sous-espace**
Soit $E = \mathbb{R}^3$ et F le plan d'équation $ax + by + cz = 0$. On définit l'application de projection sur F par :

$$\pi : \mathbb{R}^3 \to F, \quad v \mapsto v - \mathrm{proj}_F(v).$$

— **Rotation dans $\mathbb{R}^2$**
L'application qui effectue une rotation d'angle θ autour de l'origine est définie par :

$$R_\theta : \mathbb{R}^2 \to \mathbb{R}^2, \quad (x, y) \mapsto (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta).$$

— **Homothétie**
L'application d'homothétie de rapport k dans $\mathbb{R}^n$ est définie par :

$$H_k : \mathbb{R}^n \to \mathbb{R}^n, \quad v \mapsto kv.$$

— **Transformation de Fourier**
L'application qui associe à une fonction f sa transformée de Fourier est donnée par :

$$\mathcal{F}(f)(\xi) = \int_{-\infty}^{+\infty} f(x)e^{-2i\pi x\xi}dx.$$

— **Produit scalaire dans un espace de fonctions**
L'application définie par :

$$\langle f, g\rangle = \int_a^b f(x)g(x)dx$$

associe à deux fonctions leur produit scalaire dans $L^2([a, b])$.

Propriétés

— L'addition, composée, de deux applications linéaires est une application linéaire.
— Une application linéaire reste linéaire si elle est multipliée par un scalaire.
— La réciproque d'une bijection linéaire est encore linéaire.

Termes

On appelle :
— Endomorphisme de E : toute application linéaire de E dans E.
— Isomorphisme de E vers F : toute bijection linéaire de E dans F ;
— Automorphisme de E : tout endomorphisme bijectif de E, ou encore, tout isomorphisme de E dans E.
— Forme linéaire sur E : toute application linéaire de E dans $\mathbb{K}$.

Remarque :
— L'ensemble $\mathcal{L}(E, E)$ des endomorphismes de E se note plus simplement $L(E)$.
— L'ensemble des automorphismes de E s'appelle le groupe linéaire de E et se note $\mathcal{GL}(E)$.
— L'ensemble $\mathcal{L}(E, K)$ des formes linéaires sur E se note plus simplement E* et porte le nom de dual de E. (On va voir plus tard).

2.1.2 Noyau, Image :

Définitions

Soit $u \in \mathrm{L}(E, F)$. On appelle :
— L'ensemble $f(E) = \{u(x) \mid x \in E\}$, s'appelle l'image de u et est noté $Im(u)$.
— L'ensemble $f^{-1}(\{0_F\}) = \{x \in E \mid u(x) = 0_F\}$, s'appelle le noyau de u et est noté $\ker(u)$.

Remarque : La notation "ker" vient du mot allemand "kern" qui signifie noyau.

Théorème

Soit $u \in \mathrm{L}(E, F)$.
L'image réciproque par u d'un sous-espace vectoriel de F est un sous-espace vectoriel de E ; L'image directe par u d'un sous-espace vectoriel de E est un sous-espace vectoriel de F.

Corollaire

- $\ker(u)$ est un sous-espace vectoriel de E.
- $Im(u)$ est un sous-espace vectoriel de F.

Théorème

Soit $u \in \mathrm{L}(E, F)$.

i) u est injective si et seulement si $\ker(u) = \{0_E\}$.

ii) u est surjective si et seulement si $Im(u) = F$.

Demonstration :

i) Supposons f injective. Soit $x \in \ker(u)$, alors $u(x) = 0_F = u(0_E)$donc$x = 0_E$ par définition de l'injectivité. On a donc $\ker(u) = \{0_E\}$. Réciproquement, supposons que $\ker(u) = \{0_E\}$. Soient x et y deux éléments de E tels que $u(x) = u(y)$. Par linéarité de f, on en déduit que $u(xy) = 0$ donc $xy \in \ker(u)$. Or $\ker(u) = \{0_E\}$, d'où $x = y$ et f est injective.

ii) On a $Im(u) = u(E)$, et on sait que u est surjective si et seulement si $u(E) = F$ d'où le résultat.

2.2 Caracterisation par les bases :

Théorème

Pour toute base $(e_i)_{i \in I} de E$, l'application :

$$\begin{aligned} \mathrm{L}(E, F) &\to F^{\mathrm{Card}(I)} \\ u &\mapsto (u(e_i))_{i \in I} \end{aligned}$$

est bijective.

Démonstration : Nous allons montrer que cette application est bijective.

- Injectivité
  Supposons que $\varphi(u) = 0$, c'est-à-dire que $u(e_i) = 0$ pour tout $i \in I$. Par linéarité de u, pour tout $x \in E$ s'écrivant comme une combinaison linéaire des éléments de la base :
  $$x = \sum_{i \in I} \lambda_i e_i,$$
  on obtient :
  $$u(x) = u\left(\sum_{i \in I} \lambda_i e_i\right) = \sum_{i \in I} \lambda_i u(e_i) = \sum_{i \in I} \lambda_i \cdot 0 = 0.$$
  Ainsi, u est l'application nulle, ce qui prouve que φ est injective.
- Surjectivité
  Soit une famille $(a_i)_{i \in I} \in K^I$. Nous définissons une application linéaire $u : E \to K$ par :
  $$u\left(\sum_{i \in I} \lambda_i e_i\right) = \sum_{i \in I} \lambda_i a_i.$$

Cette application est bien définie car x s'écrit de manière unique sous la forme d'une combinaison linéaire des e_i, et la somme est finie (dans le cas où I est infini, les λ_i sont presque tous nuls).
Par construction, on a bien :

$$\varphi(u) = (a_i)_{i \in I},$$

ce qui prouve la surjectivité.

L'application φ est donc bijective.

Théorème

Soit $u \in \mathcal{L}(E, F)$.
- u est surjective si et seulement si l'image par u d'au moins une famille génératrice de E est génératrice de F (de plus, l'image par u de toute famille qui engendre E est alors génératrice de F).
- u est injective si et seulement si l'image par u d'au moins une base de E est libre (de plus, l'image par u de toute famille libre est alors libre) ; u est un isomorphisme si et seulement si l'image par u d'au moins une base (ou de toute base) de E est une base de F.

2.3 Projections, Symétries :

2.3.1 Projecteurs :

Définition

Soient E_1 et E_2 deux sous espaces vectoriels de E tel que $E_1 \oplus E_2 = E$ ie : $\forall x \in E, \exists!(x_1, x_2) \in E_1 x E_2$ tel que $x = x_1 + x_2$
L'application $p : E \to E$ $x \mapsto x_1$ s'appelle la projection sur E_1 parallèlement à E_2.
i) $p \in \mathcal{L}(E)$.
ii) $Im(p) = E_1$ et $\ker(p) = E_2$.
iii) $p \circ p = p$.
Reciproquement si $p \in \mathcal{L}(E)$ et $p \circ p = p$ alors p est un projecteur.

Théorème

Soit $p \in \mathcal{L}(E)$ p est un projecteur $\Leftrightarrow$ p est la projection sur $Im(p)$ parallèlement à $\ker(p)$.
Dans ce cas $E = Im(p) \oplus \ker(p)$

Proposition HP

Soient E un espace vectoriel, et p, q deux projecteurs de E tels que $Im(p) \in \ker(q)$,
Si $r = p + q - pq$, alors r est un projecteur et $\ker(r) = \ker(p) \cap \ker(q)$ et $Im(r) = Im(p) \oplus Im(q)$

Démonstration : On note par 0 le 0_E pour aiser la notation :
- r est un projecteur :
  Un opérateur est un projecteur s'il vérifie $r^2 = r$. Calculons :

$$\begin{aligned} r^2 &= (p + q - pq)(p + q - pq) \\ &= p^2 + pq - p^2 q + qp + q^2 - qpq - pq + pq^2 - pqq. \end{aligned}$$

En utilisant $p^2 = p$ et $q^2 = q$, on obtient :

$$\begin{aligned} r^2 &= p + pq - pq + qp + q - qpq - pq + pq - pq \\ &= p + q - pq = r. \end{aligned}$$

Donc r est bien un projecteur.

— $\ker(r) = \ker(p) \cap \ker(q)$:
Soit $x \in \ker(r)$, c'est-à-dire $r(x) = 0$, alors :

$$(p + q - pq)(x) = 0.$$

Ce qui donne :

$$p(x) + q(x) - p(q(x)) = 0.$$

Puisque $\text{Im}(p) \subseteq \ker(q)$, on a $q(p(x)) = 0$, donc :

$$p(x) + q(x) = 0.$$

En appliquant q des deux côtés :

$$q(p(x)) + q(q(x)) = q(0) = 0.$$

Comme $q(q(x)) = q(x)$, on en déduit $q(x) = 0$. Remplaçons dans $p(x) + q(x) = 0$, cela donne $p(x) = 0$.
Ainsi, $x \in \ker(p) \cap \ker(q)$.
Réciproquement, si $x \in \ker(p) \cap \ker(q)$, alors $p(x) = 0$ et $q(x) = 0$, donc :

$$r(x) = p(x) + q(x) - p(q(x)) = 0.$$

D'où $\ker(r) = \ker(p) \cap \ker(q)$.

— $\text{Im}(r) = \text{Im}(p) \oplus \text{Im}(q)$:
Montrons d'abord que $\text{Im}(r) \subseteq \text{Im}(p) + \text{Im}(q)$.
Soit $y \in \text{Im}(r)$, alors il existe $x \in E$ tel que :

$$y = r(x) = p(x) + q(x) - p(q(x)).$$

Posons $y_1 = p(x)$ et $y_2 = q(x) - p(q(x))$. Alors $y_1 \in \text{Im}(p)$ et $y_2 \in \text{Im}(q)$, donc $y \in \text{Im}(p) + \text{Im}(q)$.
Réciproquement, soit $y_1 \in \text{Im}(p)$ et $y_2 \in \text{Im}(q)$. Il existe $x_1, x_2 \in E$ tels que $y_1 = p(x_1)$ et $y_2 = q(x_2)$.
Posons $x = x_1 + x_2$, alors :

$$r(x) = p(x) + q(x) - p(q(x)).$$

Développons :

$$r(x) = p(x_1) + p(x_2) + q(x_1) + q(x_2) - p(q(x_1) + q(x_2)).$$

Or, $p(x_2) \in \text{Im}(p) \subseteq \ker(q)$, donc $q(p(x_2)) = 0$, ce qui donne :

$$r(x) = p(x_1) + q(x_2) = y_1 + y_2.$$

Ainsi, $\text{Im}(r) = \text{Im}(p) + \text{Im}(q)$.
Enfin, pour prouver que la somme est directe, supposons que $y \in \text{Im}(p) \cap \text{Im}(q)$. Il existe x_1, x_2 tels que $y = p(x_1) = q(x_2)$. Puisque $\text{Im}(p) \subseteq \ker(q)$, on a $q(y) = q(p(x_1)) = 0$, donc $y = 0$. Cela prouve que l'intersection est réduite à $\{0\}$, donc la somme est directe.
Finalement nous avons démontré que :

> Si E un espace vectoriel, et p, q deux projecteurs de E tels que $Im(p) \in \ker(q)$, et $r = p + q - pq$, alors :
> — r est un projecteur,
> — $\ker(r) = \ker(p) \cap \ker(q)$,
> — $\text{Im}(r) = \text{Im}(p) \oplus \text{Im}(q)$.

2.3.2 Symétrie :

Définition

Soient E_1 et E_2 deux sous espaces vectoriels de E tel que $E_1 \oplus E_2 = E$ ie : $\forall x \in E, \exists!(x_1, x_2) \in E_1 x E_2$ tel que $x = x_1 + x_2$

L'application $s : E \to E$ $x \mapsto x_1 - x_2$ s'appelle symétrie par rapport à E_1 parallèlement à E_2.

i) $s \in \mathcal{L}(E)$.

ii) Si $p \in \mathcal{L}(E)$ est la projection sur E_1 parallèlement à E_2 alors : $s = 2p - Id_E$

Proposition

Dans le cadre du programme , K=R ou C donc on a le résultat suivant :
$s \in L(E)$ est une symétrie $\Leftrightarrow s \circ s = Id_E$
Dans ce cas si $p = 1/2(s + Id_E)$, p est un projecteur et s est la symétrie par rapport à Im(p) parallèlement à $\ker(p)$.
On expliquera plus loin, plus ce résultat et d'où il vient (Voir Notion Caractéristique d'un corps).

2.4 L'espace $\mathcal{L}(E, F)$:

Théorème

Si E est de dimension finie alors
$\dim(\mathcal{L}(E, F)) = \dim(E) \times \dim(F)$..

Remarque : Si $u \in \mathcal{L}(E, F)$et $v \in \mathcal{L}(F, G)$ alors $v \circ u \in \mathcal{L}(E, G)$.

2.5 Rang :

Définition

Le rang d'une application linéaire est la dimension de son image. Si $u : E \to F$ est une application linéaire alors on note son rang par $rg(u)$ et on a : $rg(u) = dim_K(Im(u))$.

Théorème

La composition par un isomorphisme laisse le rang invariant, c'est à dire : Soit $u \in \mathcal{L}(E, F)$:
$\forall v \in \mathcal{L}(F, G)$ bijective $\mathrm{rg}(v \circ u) = \mathrm{rg}(u)$.
$\forall v \in mathcal L(F, G)$ bijective $\mathrm{rg}(v \circ u) = \mathrm{rg}(u)$.

2.5.1 Théorème du rang :

Théorème du rang

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et F un espace vectoriel , et $u \in L(E, F)$ alors : u est de rang fini et on a :
$dim_K(E) = dim_K(Im(u)) + dim_K(\ker(u))$

Corollaire

Soient E, F deux $\mathbb{K}$-espaces vectoriel de même dimension finie $u \in L(E, F)$, alors les assertions suivantes sont équivalentes :

i) u bijective.
ii) u surjective.
iii) u injective.

2.6 Stabilité :

Définition

Soit $\varphi \in \mathcal{L}(E)$. Un sous-espace F de E est dit **stable par** φ si $\varphi(F) \subset F$, c'est-à-dire :

$$\forall x \in F, \quad \varphi(x) \in F.$$

Proposition

Si deux endomorphismes φ_1 et φ_2 commutent, alors le noyau et l'image de l'un sont stables par l'autre.

Démonstration :

— Montrons que $\ker \varphi_2$ est stable par φ_1. Soit $x \in \ker \varphi_2$. Alors $\varphi_1(\varphi_2(x)) = \varphi_1(0) = 0$ (la dernière égalité étant due au fait que φ_1 est linéaire), donc $\varphi_1(x) \in \ker \varphi_2$.
— Montrons que $\mathrm{Im}\varphi_2$ est stable par φ_1.

$$\varphi_1(\mathrm{Im}\varphi_2) = \varphi_1 \circ \varphi_2(E) = \varphi_2 \circ \varphi_1(E) \subset \mathrm{Im}\varphi_2.$$

2.7 Exercices :

2.7.1 Projecteurs :

2.7.2 Lemmes de factorisation :

Exercice :

Soient E,F,G 3 $\mathbb{K}$-espaces vectoriels de dimension finie, et soit $g : E \to G$ une application linéaire.

1) Soit $f : E \to F$ une application linéaire, montrer que :
$(\exists h : F \to G \in L(F, G)$ telle que $g = h \circ f.) \Leftrightarrow (\ker f \subset \ker g.)$
2) Soit $h : F \to G$ une application linéaire, montrer que :
$(\exists f : E \to F \in \mathcal{L}(E, F)$, tel que $g = h \circ f.) \Leftrightarrow (Img \subset Imh.)$
3) On suppose maintenant que $g : E \to F \in \mathcal{L}(E, F)$, montrer que :
$(rgg \leq rgf.) \Leftrightarrow (\exists h \in \mathcal{GL}(F)$ et $k \in \mathcal{L}(E)$ tels que $h \circ g = f \circ k.)$

Correction :

1) $(\Rightarrow)$
Supposant que : $(\exists h : F \to G \in \mathcal{L}(F, G)$ tel que $g = h \circ f.)$,
On a donc : $\forall x \in \ker(f), g(x) = h(f(x)) = h(0_F) = 0_G$, donc $x \in \ker(g)$.
$\forall x \in \ker(f), x \in \ker(g)$, donc $\ker(f) \in \ker(g)$.

$$(\exists h : F \to G \in \mathcal{L}(F, G) \text{ telle que } g = h \circ f.) \Rightarrow (\ker f \subset \ker g.)$$

$(\Leftarrow)$
Reciproquement, supposant $\ker(f) \in \ker(g)$
On pose $h_{Im(f)}$ une application telle que :

$$\forall y \in Im(f), h_{Im(f)} = g(x) \text{ avec } x \in E, f(x) = y, \text{ on peut faire ca car } g(x) \text{ ne dépend pas de x.}$$

En effet si

$$(x, x') \in E^2, f(x) = f(x') \text{ alors } f(x - x') = 0_F \text{ (car f est linéaire)}$$

Donc,

$$x - x' \in \ker(f) \text{ donc } x - x' \in \ker(g) \text{ et donc } g(x) = g(x')$$

.

$$\forall x \in E, h_{Im(f)}(f(x)) = g(x) \text{ donc } h_{Im(f)} \circ f = g$$

$h_{Im(f)}$ est aussi linéaire car

$$\forall (y, y') \in (Im(f))^2, \exists (x, x') \in E^2, f(x) = y, f(x') = y'$$

,

$$\forall (\alpha, \beta) \in \mathbb{K}^2, h_{Im(f)}(\alpha.y+\beta.y') = h_{Im(f)}(\alpha.f(x)+\beta.f(x')) = h_{Im(f)}(f(\alpha.x+\beta.x'))) = g(\alpha.x+\beta.x') = \alpha.g(x)+\beta.g(x') =$$

.
Si une application $h \in L(F, G)$ a sa restriction à $Im(f)$ égale à $h_{Im(f)}$ alors elle répond à notre question donc :

$$(\ker f \subset \ker g.) \Rightarrow ($$

$$\exists h : F \to G \in \mathcal{L}(F, G)$$

$$\text{telle que } g = h \circ f.)$$

Finalement :

$$\boxed{(\exists h : F \to G \in L(F, G) \text{ telle que } g = h \circ f.) \Leftrightarrow (\ker f \subset \ker g.)}$$

2) $(\Rightarrow)$
Pour qu'il existe $f \in \mathcal{L}(E, F)$ telle que $g = h \circ f$, il est nécessaire que ca ce soit $Im(g) \subset Im(h)$
$(\Leftarrow)$ Reciproquement, supposant que $Im(g) \subset Im(h)$.
On considère un supplémentaire H dans $\mathbb{F}$, notant l'isomorphisme induit par h sur H par h_H.
L'application $f = h_H^{-1} \circ g$ est linéaire et bien définie car $Im(g) \subset Im(h)$ et on a :
$\forall x \in Eh(f(x)) = h(H)^{-1}(g(x))) = g(x)$ alors $g = h \circ f$.
donc :

$$(Im(g) \subset Im(h).) \Rightarrow (\exists f : E \to F \in L(E, F), \text{ tel que } g = h \circ f.)$$

Finalement :

$$\boxed{(\exists f : E \to F \in L(E, F), \text{ tel que } g = h \circ f.) \Leftrightarrow (Img \subset Imh.)}$$

3) $(\Rightarrow)$
On suppose que $rg(g) \leq rg(f)$:
Notant $rg(f) = p, rg(g) = q$ et posant $B_f = (x_1, \ldots, x_p, \ldots, x_n)$ base de E avec $(x_{p+1}, \ldots, x_n)$ base de $\ker(f)$
posant aussi $B_g = (y_1, \ldots, y_p, \ldots, y_n)$ base de E avec $(y_{+1}, \ldots, y_n)$ base de $\ker(g)$
Les familles $(f(x_1), \ldots, f(x_p))$, $(g(y_1), \ldots, g(y_q))$ étant des bases de $Im(f)$ et $Im(g)$ respectivement, on les complète en deux bases de F : $(f(x_1), \ldots, f(x_p), f_{p+1}, f_m)$ et $(g(y_1), \ldots, g(y_q), g_{q+1}, g_m)$.
On définit maintenant $k \in \mathbb{L}(E)$ et $h \in \mathbb{GL}(F)$ par : $\forall i \in [|1, q|], k(y_i) = x_i, , \forall j \in [|q + 1, n|], k(y_j) = 0_E$ et $\forall i \in [|1, q|]h(g(y_i)) = f(x_i), \forall j \in [|q + 1, m|]h(g_j) = f_j$.
On a donc :
$\forall i \in [|1, q|], (f \circ k)(y_i)f(k(y_i)) = f(x_i) = h(g(y_i)) = (h \circ g)(y_i)$ et
$\forall i > q, (f \circ k)(y_i) = (h \circ g)(y_i) = 0_F$
Donc $h \circ g = f \circ k$.
Finalement :

$$(rg(g) < rg(f)) \Rightarrow ()(\exists h \in GL(F) \text{ et } k \in L(E) \text{ tels que } h \circ g = f \circ k.)$$

2.7.3 Inégalité de Sylvester :

Exercice :

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, F un $\mathbb{K}$-espace vectoriel et $f, g \in L(E, F)$:

1) Montrer que $|rgf - rgg| \leq rg(f+g) \leq rgf + rgg$.
2) Supposant maintenant que f et g sont les deux des endomorphismes de E, montrer que : $(rg(f+g) = rg(f) + rg(g).) \Leftrightarrow (Im(f) \cap Im(g) = \{0_{\mathbb{F}}\} et \ker(f) + \ker(g) = E.)$
3) Montrer l'inégalité de Sylvester :
$rg(f) + rg(g) - dim_K(E) \leq rg(fg) \leq min(rg(f), rg(g))$.

Correction :

1) Soient $f, g \in \mathbb{L}(E, \mathbb{F})$.
On a alors :
$Im(f+g) \subset Im(f) + Im(g)$ donc $rg(f+g) \leq dim(Im(f) + Im(g)) \leq rg(f) + rg(g)$
donc $rg((f+g) + (-g)) \leq rg(f+g) + rg(-g)$ or $rg(g) = rg(-g)$
donc $rg(f) \leq rg(f+g) + rg(g)$
du coup $rg(f) - rg(g) \leq rg(f+g)$
Si on refait la même démarche avec $f+g$ et $-f$ on obtient :
$rg(g) - rg(f) \leq rg(f+g)$ donc $|rg(f) - rg(g)| \leq rg(f+g)$. et puisque on a démontré que : $rg(f+g) \leq rg(f) + rg(g)$, on a donc :

$$\boxed{\forall f, g \in \mathbb{L}(E, \mathbb{F}) \ |rg(f) - rg(g)| \leq rg(f+g) \leq rg(f) + rg(g).}$$

2) $\Rightarrow$
Supposant $rg(f+g) = rg(f) + rg(g)$,
i) On avait vu que :

$$rg(f+g) \leq dim_{\mathbb{K}}(Im(f+g)) \leq dim_{\mathbb{K}}(Im(f) + Im(g)) \leq rg(f) + rg(g)$$

donc $dim_{\mathbb{K}}(Im(f) + Im(g)) = rg(f) + rg(g)$
Or on a :

$$dim_{\mathbb{K}}(Im(f) + Im(g)) = dim_{\mathbb{K}}(Im(f)) + dim_{\mathbb{K}}(Im(g)) - dim_{\mathbb{K}}(Im(f) \cap Im(g))$$

donc

$$dim_{\mathbb{K}}(Im(f) + Im(g)) = rg(f) + rg(g) - dim_{\mathbb{K}}(Im(f) \cap Im(g))$$

donc

$$dim_{\mathbb{K}}(Im(f) \cap Im(g)) = 0_{\mathbb{K}}$$

donc

$$Im(f) \cap Im(g) = \{0_{\mathbb{F}}\}.$$

ii) On a

$$dim_{\mathbb{K}}(\ker(f) + \ker(g)) = dim_{\mathbb{K}}(\ker(f)) + dim_{\mathbb{K}}(\ker(g)) - dim_{\mathbb{K}}(\ker(f) \cap \ker(g))$$

donc

$$dim_{\mathbb{K}}(\ker(f) + \ker(g)) = dim_{\mathbb{K}}(E) - rg(f) + dim_{\mathbb{K}}(E) - rg(g) - dim_{\mathbb{K}}(\ker(f) \cap \ker(g))$$

.
On a $\ker(f) \cap \ker(g) = \ker(f+g)$.
En effet, si $x \in \ker(f+g), (f+g)(x) = 0_F$ or puisque $f(x) = -g(x)$ on a $f(x) \in Im(f)$et$Im(g)$ de même pour $g(x) \in Im(g)$ et $Im(f)$
donc

$$f(x), g(x) \in Im(f) \cap Im(g) \text{ or } Im(f) \cap Im(g) = \{0_F\} \text{ donc } f(x) = g(x) = 0_F$$

donc

$$x \in \ker(f) \cap \ker(g)$$

On obtient donc $\ker(f+g) \subset \ker(f) \cap \ker(g)$ et puisque on sait que $\ker(f) \cap \ker(g) \subset \ker(f+g)$ donc $\ker(f) \cap \ker(g) = \ker(f+g)$.
On a maintenant :

$$dim_{\mathbb{K}}(\ker(f)+\ker(g)) = dim_{\mathbb{K}}(E) - rg(f) + dim_{\mathbb{K}}(E) - rg(g) - dim_{\mathbb{K}}(\ker(f+g))$$

$$\begin{aligned} \dim_{\mathbb{K}}(\ker(f)+\ker(g)) &= \dim_{\mathbb{K}}(E) - \mathrm{rg}(f) + \dim_{\mathbb{K}}(E) - \mathrm{rg}(g) - \dim_{\mathbb{K}}(E) + \mathrm{rg}(f+g) && (2.1)\\ &= \dim_{\mathbb{K}}(E) - \mathrm{rg}(f) - \mathrm{rg}(g) + \mathrm{rg}(f+g). && (2.2) \end{aligned}$$

Finalement on a :

$$dim_{\mathbb{K}}(\ker(f)+\ker(g)) = dim_{\mathbb{K}}(E) \text{ et puisque } \ker(f)+\ker(g) \subset E$$

On conclut que :

$$\ker(f)+\ker(g) = E$$

On a montré que :

$$\boxed{(rg(f+g) = rg(f) + rg(g).) \Rightarrow (Im(f) \cap Im(g) = \{0_{\mathbb{F}}\} et \ker(f)+\ker(g) = E.)}$$

$\Leftarrow$
Tout élément de E s'écrit comme :

$$x = x_1 + x_2, \quad \text{avec } x_1 \in \ker(f) \text{ et } x_2 \in \ker(g).$$

Appliquons $f+g$:

$$(f+g)(x) = f(x_2) + g(x_1).$$

Puisque $x_2 \in \ker(g)$, on a $g(x_1) \in \mathrm{Im}(g)$ et $f(x_2) \in \mathrm{Im}(f)$.
Or, $\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\}$, donc la somme est directe :

$$\mathrm{Im}(f+g) = \mathrm{Im}(f) \oplus \mathrm{Im}(g).$$

Par conséquent :

$$\mathrm{rg}(f+g) = \mathrm{rg}(f) + \mathrm{rg}(g).$$

3) — Borne supérieure :
Puisque $\mathrm{Im}(fg) \subseteq \mathrm{Im}(f)$, on a :

$$\mathrm{rg}(fg) \leq \mathrm{rg}(f).$$

De même, comme $fg(x)$ est une image par g :

$$\mathrm{Im}(fg) \subseteq \mathrm{Im}(g).$$

Ainsi :

$$\mathrm{rg}(fg) \leq \mathrm{rg}(g).$$

D'où :

$$\mathrm{rg}(fg) \leq \min(\mathrm{rg}(f), \mathrm{rg}(g)).$$

— Borne inférieure
On sait que :

$$\dim_K(E) = \mathrm{rg}(g) + \dim_K(\ker g).$$

Appliquons f :

$$\mathrm{Im}(fg) = f(\mathrm{Im}(g)).$$

Par conséquent :

$$\mathrm{rg}(fg) = \dim(f(\mathrm{Im}(g))) \geq \mathrm{rg}(f) + \mathrm{rg}(g) - \dim_K(E).$$

D'où l'inégalité :

$$\mathrm{rg}(f) + \mathrm{rg}(g) - \dim_K(E) \leq \mathrm{rg}(fg).$$

Finalement nous avons démontré que *l'inégalité de Sylvester* :

$$rg(f) + rg(g) - dim_K(E) \leq rg(fg) \leq min(rg(f), rg(g)).$$

2.7.4 Endomrophismes particuliers :

Exercice :

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in L(E)$:

1) Montrer que les assertions sont équivalentes :
   i) $E = \ker u \oplus Imu$.
   ii) $\exists v \in L(E), v \circ u = 0etv + u \in GL(E)$.
   iii) $\ker u = \ker u^2$.
   iv) $Imu = Imu^2$.

Correction : Nous allons prouver cette équivalence en montrant successivement que :

$$(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i).$$

— $(i) \Rightarrow (ii)$
Supposons que $E = \ker u \oplus \mathrm{Im}\, u$. Cela signifie que tout vecteur $x \in E$ peut s'écrire de manière unique sous la forme :

$$x = x_1 + x_2, \quad \text{avec } x_1 \in \ker u \text{ et } x_2 \in \mathrm{Im}\, u.$$

Nous définissons alors une application linéaire v comme suit :
— $v(x_2) = 0$ pour tout $x_2 \in \mathrm{Im}\, u$,
— $v(x_1) = -x_1$ pour tout $x_1 \in \ker u$.
Par construction, v est bien linéaire. De plus, pour tout $x \in E$, on a :

$$(v + u)(x) = v(x_1 + x_2) + u(x_1 + x_2).$$

Or, $v(x_2) = 0$ et $u(x_1) = 0$, donc :

$$(v + u)(x) = v(x_1) + u(x_2) = -x_1 + x_2.$$

Puisque $x_1 + x_2$ est une décomposition unique de tout élément de E, l'application $v + u$ est bijective, donc appartient à $GL(E)$. Enfin, $v \circ u = 0$ car $u(x_2) \in \mathrm{Im}\, u$ et v est nul sur $\mathrm{Im}\, u$. Cela prouve (ii).

— $(ii) \Rightarrow (iii)$
Supposons qu'il existe une application linéaire v telle que $v \circ u = 0$ et $v + u$ est inversible.
Prenons $x \in \ker u^2$, c'est-à-dire $u^2(x) = 0$. Posons $y = u(x)$, alors $u(y) = 0$, donc $y \in \ker u$.
Puisque $v \circ u = 0$, on a aussi $v(y) = 0$. Comme $v + u$ est bijective, on en déduit que si $u(x) \in \ker u$, alors $u(x) = 0$, donc $x \in \ker u$. Ainsi, $\ker u^2 \subseteq \ker u$, et comme l'inclusion inverse est triviale, on a $\ker u = \ker u^2$, ce qui prouve (iii).

— $(iii) \Rightarrow (iv)$
Supposons que $\ker u = \ker u^2$. Nous voulons montrer que $\mathrm{Im}\, u = \mathrm{Im}\, u^2$.
Prenons $y \in \mathrm{Im}\, u^2$, c'est-à-dire qu'il existe $x \in E$ tel que :

$$y = u^2(x).$$

Posons $z = u(x)$. Alors $u(z) = u^2(x) = y$, donc $y \in \operatorname{Im} u$. Ainsi, $\operatorname{Im} u^2 \subseteq \operatorname{Im} u$. L'inclusion inverse étant évidente, on a $\operatorname{Im} u = \operatorname{Im} u^2$, ce qui prouve (iv).

— $(iv) \Rightarrow (i)$
Supposons que $\operatorname{Im} u = \operatorname{Im} u^2$. Nous voulons prouver que $E = \ker u \oplus \operatorname{Im} u$.
D'abord, montrons que $\ker u \cap \operatorname{Im} u = \{0\}$.
Soit $x \in \ker u \cap \operatorname{Im} u$. Alors, il existe y tel que $x = u(y)$, et on a $u(x) = 0$, donc $u^2(y) = 0$. Par hypothèse, il existe z tel que $u^2(y) = u(z)$, donc $u(z) = 0$, c'est-à-dire $z \in \ker u$. Mais alors,

$$u(y - z) = u(y) - u(z) = x - 0 = x.$$

Or, $y - z \in \ker u$, donc $x = 0$. Ainsi, $\ker u \cap \operatorname{Im} u = \{0\}$.
Enfin, comme la dimension de $\ker u$ plus celle de $\operatorname{Im} u$ est égale à celle de E, on en conclut que :

$$E = \ker u \oplus \operatorname{Im} u.$$

Cela prouve (i), et donc l'équivalence des quatre assertions est démontrée.

Finalement nous avons montré que :

Si E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in L(E)$ alors les assertions suivantes sont équivalentes :
i) $E = \ker u \oplus Imu$.
ii) $\exists v \in L(E), v \circ u = 0 et v + u \in GL(E)$.
iii) $\ker u = \ker u^2$.
iv) $Imu = Imu^2$.

2.8 Compléments :

2.8.1 Drapeaux :

1 **Drapeau dans un espace vectoriel**

Un **drapeau** dans un espace vectoriel E de dimension n est une suite croissante de sous-espaces vectoriels :

$$\{0\} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = E,$$

où chaque F_k est de dimension k, c'est-à-dire que $\dim(F_k) = k$ pour tout $k = 1, 2, \ldots, n$.

Dimension stricte croissante

Soit E un espace vectoriel de dimension n et $\mathcal{F} = \{F_0, F_1, \ldots, F_n\}$ un drapeau dans E. Les sous-espaces doivent satisfaire la condition de **dimension croissante stricte** :

$$\dim(F_0) < \dim(F_1) < \cdots < \dim(F_n).$$

Démonstration : Soit $\mathcal{F} = \{F_0, F_1, \ldots, F_n\}$ un drapeau dans un espace vectoriel E, avec $F_0 = \{0\}$ et $F_n = E$. Chaque sous-espace F_k a une dimension $\dim(F_k) = k$ et $F_k \subseteq F_{k+1}$.

- Par construction, $F_0 = \{0\}$ a une dimension de 0, et $F_n = E$ a une dimension n. - Puisque chaque sous-espace F_k est strictement inclus dans F_{k+1}, cela signifie que $\dim(F_k) < \dim(F_{k+1})$ pour tout k, car une inclusion stricte entre sous-espaces vectoriels entraîne une différence strictement positive de dimension.

Cela montre que la dimension des sous-espaces augmente de manière stricte.

Inclusivité stricte

Un drapeau est une **séquence croissante de sous-espaces** stricts :

$$\{0\} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = E,$$

ce qui signifie que $F_k \neq F_{k+1}$ pour tout k.

Démonstration : Soit $\mathcal{F} = \{F_0, F_1, \ldots, F_n\}$ un drapeau dans un espace vectoriel E, avec $F_0 = \{0\}$ et $F_n = E$. La condition $F_k \subseteq F_{k+1}$ pour chaque k implique que chaque sous-espace est contenu dans le suivant, mais la condition d'inclusivité stricte exige que $F_k \neq F_{k+1}$.

- Supposons, par contradiction, que $F_k = F_{k+1}$ pour un certain k. Cela violerait la condition de dimension stricte croissante , car $\dim(F_k) = \dim(F_{k+1})$. Cela contredirait l'hypothèse que les sous-espaces de la chaîne ont des dimensions strictement croissantes.

Ainsi, $F_k \neq F_{k+1}$ pour tout k, ce qui prouve que les inclusions sont strictes.

Unicité des dimensions

Dans un drapeau, chaque sous-espace F_k doit être de dimension k. Par conséquent, les sous-espaces de dimensions $0, 1, 2, \ldots, n$ sont associés à des sous-espaces successivement plus grands dans l'inclusion.

Démonstration : Soit $\mathcal{F} = \{F_0, F_1, \ldots, F_n\}$ un drapeau dans un espace vectoriel E. Nous savons que $F_0 = \{0\}$ et $F_n = E$, et que la dimension de chaque sous-espace F_k est croissante et distincte.

- Par la définition de drapeau, chaque sous-espace F_k est strictement inclus dans F_{k+1}. Cela signifie que $\dim(F_k)$ est plus petit que $\dim(F_{k+1})$. - La dimension stricte croissante garantit que $\dim(F_0) = 0$, $\dim(F_1) = 1$, ..., $\dim(F_n) = n$.

Ainsi, les sous-espaces $F_0, F_1, \ldots, F_n$ ont des dimensions distinctes et successivement plus grandes.

Drapeau et décomposition de Jordan

Un drapeau est fortement lié à la **décomposition de Jordan** d'une matrice. Dans le cas d'une décomposition de Jordan, les sous-espaces associés à chaque valeur propre et à chaque vecteur généralisé forment un drapeau.

Démonstration : Soit A une matrice carrée associée à un opérateur linéaire f sur un espace vectoriel E. La décomposition de Jordan de A consiste à trouver une base de E qui décompose l'opérateur A en blocs de Jordan, où chaque bloc est associé à une valeur propre et à un ensemble de vecteurs généralisés.

- La décomposition de Jordan fournit une suite croissante de sous-espaces $\{F_0, F_1, \ldots, F_n\}$ qui sont associés aux vecteurs propres et généralisés de A. Chaque sous-espace F_k dans ce cas est un sous-espace invariant associé à un bloc de Jordan. - Cette suite de sous-espaces forme un drapeau, car chaque sous-espace F_k est strictement inclus dans F_{k+1} et a une dimension strictement croissante.

Ainsi, le drapeau qui apparaît dans la décomposition de Jordan correspond aux sous-espaces invariants associés aux blocs de Jordan.

Drapeaux et chaînes de sous-espaces

U

n drapeau peut être vu comme une **chaîne de sous-espaces** de dimension croissante dans l'espace vectoriel.

Démonstration : Un drapeau dans un espace vectoriel E est une séquence de sous-espaces $F_0 \subset F_1 \subset \cdots \subset F_n$, où chaque sous-espace est de dimension strictement croissante. Cela correspond à une chaîne de sous-espaces .

- En termes algébriques, un drapeau est une chaîne d'inclusions strictes de sous-espaces, avec des dimensions strictement croissantes, ce qui correspond à une chaîne ordonnée de sous-espaces vectoriels. - Cette chaîne peut être utilisée pour analyser l'action d'un opérateur linéaire f sur l'espace E, où chaque sous-espace de la chaîne peut être invariant sous f.

Drapeaux et invariance sous les transformations

L

es drapeaux sont utilisés pour **analyser l'invariance sous transformation**.

Démonstration : Soit $f : E \to E$ un endomorphisme linéaire et $\mathcal{F} = \{F_0, F_1, \ldots, F_n\}$ un drapeau dans E. Par définition, un drapeau est une chaîne de sous-espaces invariants sous f, c'est-à-dire que $f(F_k) \subseteq F_k$ pour chaque k.

- Si f est appliqué à chaque sous-espace F_k dans le drapeau, alors les sous-espaces F_k restent invariants sous f, ce qui montre l'invariance de chaque sous-espace de la chaîne. - Cette propriété permet d'analyser la dynamique de f de manière systématique, car elle découpe E en sous-espaces invariants associés à f.

2.8.2 Espace vectoriel quotient :

Définitions

Soient E un $\mathbb{K}$-espace vectoriel et F un sous espace vectoriel de E,
La relation R() définit une relation d'equivalence sur E. L'espace quotient E/F muni des lois "+" :$x+y = x+y$, "." :$\lambda.x = \lambda.x$ est un $\mathbb{K}$-espace vectoriel
si E/F est de dimension finie, On appele codimension de F la dimension de E/f tel que : $dim_{\mathbb{K}}(E/F) = codim_E(F)$.
Dans ce cas on dit que F est de codimension finie.

Proposition

Soit E un $\mathbb{K}$-espace vectoriel et F un sous espace vectoriel de E.
(F est de codimension finie) $\Leftrightarrow$ (F admet un supplémentaire S dans E).
Dans ce cas $dim_K(S) = codim_E(F)$.

Démonstration :

— Preuve de l'implication directe $\Rightarrow$:
Supposons que F est de codimension finie, c'est-à-dire que :

$$\mathrm{codim}_E(F) = \dim_K(E) - \dim_K(F) \text{ est fini.}$$

Cela signifie qu'il existe une famille finie de vecteurs $(v_1, \ldots, v_r)$ dans E telle que :

$$E = F + \mathrm{Vect}(v_1, \ldots, v_r).$$

Montrons que $\mathrm{Vect}(v_1, \ldots, v_r)$ est un supplémentaire de F.

— **Existence d'une décomposition directe :** Tout élément $x \in E$ peut s'écrire comme :

$$x = f + \sum_{i=1}^{r} \lambda_i v_i, \quad \text{avec } f \in F, \lambda_i \in K.$$

— **Vérification de la somme directe :** Nous devons prouver que la somme est directe, c'est-à-dire que :

$$F \cap \mathrm{Vect}(v_1, \ldots, v_r) = \{0\}.$$

Si un vecteur $x \in F \cap \mathrm{Vect}(v_1, \ldots, v_r)$, alors $x \in F$ et il existe $\lambda_1, \ldots, \lambda_r$ tels que :

$$x = \sum_{i=1}^{r} \lambda_i v_i.$$

Mais $x \in F$ implique que x appartient à la fois à F et à $\mathrm{Vect}(v_1, \ldots, v_r)$. Comme F et $\mathrm{Vect}(v_1, \ldots, v_r)$ sont en somme directe, on en déduit que $x = 0$. Ainsi, l'intersection est réduite à $\{0\}$.

On pose alors $S = \mathrm{Vect}(v_1, \ldots, v_r)$. Comme S est de dimension r et que $r = \mathrm{codim}_E(F)$, on a :

$$\dim_K(S) = \mathrm{codim}_E(F).$$

Cela montre que F admet bien un supplémentaire S dans E.

— Preuve de l'implication réciproque $\Leftarrow$:
Supposons maintenant que F admet un supplémentaire S dans E, c'est-à-dire que :

$$E = F \oplus S.$$

Cela signifie que tout élément de E peut s'écrire de manière unique comme une somme :

$$x = f + s, \quad \text{avec } f \in F, s \in S.$$

— **Calcul de la codimension :** La dimension de E s'exprime alors comme la somme des dimensions de F et S :

$$\dim_K(E) = \dim_K(F) + \dim_K(S).$$

— Par définition de la codimension, on a :

$$\operatorname{codim}_E(F) = \dim_K(E) - \dim_K(F).$$

En remplaçant par l'égalité précédente, on obtient :

$$\operatorname{codim}_E(F) = \dim_K(S).$$

Or, S étant un sous-espace de dimension finie, cela prouve que $\operatorname{codim}_E(F)$ est fini. Ainsi, F est bien de codimension finie.

Nous avons démontré que :

$$(F \text{ est de codimension finie}) \iff (F \text{ admet un supplémentaire } S \text{ dans } E)$$

et que dans ce cas :

$$\dim_K(S) = \operatorname{codim}_E(F).$$

Corollaire

Si E est un $\mathbb{K}$-espace vectoriel de dimension finie et F un sous espace vectoriel de E , alors F est de codimension finie et :
$dim_K(E/F) = dim_K(E) - dim_K(F)$.

Corollaire

Si E, F sont deux $\mathbb{K}$-espaces vectoriel et $u \in L(E, F)$, alors Im(u) est isomorphe à E/ker(u).

2.8.3 L'espace $\mathcal{L}(E)$:

Théorème-Programme

$(\mathcal{L}(E), +, \cdot, \circ)$ est une K-algèbre associative unifère (non commutative si $\dim(E) \geq 2$).

Démonstration : Soit E un espace vectoriel sur un corps K. On note $\mathcal{L}(E)$ l'ensemble des endomorphismes de E, c'est-à-dire l'ensemble des applications linéaires $f : E \to E$.

Nous considérons les opérations suivantes sur $\mathcal{L}(E)$:
— **Addition** : Pour $f, g \in \mathcal{L}(E)$, on définit $(f + g)(x) = f(x) + g(x)$ pour tout $x \in E$.
— **Multiplication scalaire** : Pour $\lambda \in K$ et $f \in L(E)$, on définit $(\lambda f)(x) = \lambda f(x)$.
— **Composition** : Pour $f, g \in \mathcal{L}(E)$, on définit $(f \circ g)(x) = f(g(x))$.

$\mathcal{L}(E)$ est un espace vectoriel

L'ensemble $\mathcal{L}(E)$, muni de l'addition et de la multiplication scalaire, est un espace vectoriel sur K. En effet :
— L'addition est associative et commutative : $(f + g) + h = f + (g + h)$ et $f + g = g + f$.
— Il existe un élément neutre : l'endomorphisme nul 0 tel que $0(x) = 0$ pour tout $x \in E$.
— Chaque $f \in \mathcal{L}(E)$ possède un opposé $-f$ tel que $f + (-f) = 0$.
— La multiplication scalaire est distributive et compatible avec les scalaires de K.

$\mathcal{L}(E)$ est une algèbre sur K

Une K-algèbre est un espace vectoriel muni d'une multiplication bilinéaire. Ici, la multiplication est la composition des applications.

Bilinéarité de la composition

— Pour tous $f, g \in L(E)$ et $\lambda \in K$, on a :

$$(\lambda f) \circ g = \lambda(f \circ g),$$
$$f \circ (\lambda g) = \lambda(f \circ g).$$

Cela prouve que $\circ$ est bilinéaire.

Associativité de la composition

— Pour tous $f, g, h \in \mathcal{L}(E)$ et tout $x \in E$,

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))),$$
$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))).$$

Ainsi, $(f \circ g) \circ h = f \circ (g \circ h)$, donc la composition est associative.

Existence de l'élément neutre

— L'identité Id_E, définie par $\mathrm{Id}_E(x) = x$ pour tout $x \in E$, est un élément neutre :

$$\mathrm{Id}_E \circ f = f,$$
$$f \circ \mathrm{Id}_E = f.$$

Donc $L(E)$ est une algèbre unifère.

Non-commutativité si $\dim(E) \geq 2$

Si $\dim(E) \geq 2$, il existe des endomorphismes f, g tels que $f \circ g \neq g \circ f$.

Finalement nous avons démontré que

$(\mathcal{L}(E), +, \cdot, \circ)$ est une K-algèbre associative unifère et qu'elle est non commutative dès que $\dim(E) \geq 2$.

Définition

On appelle homothétie $u \in \mathcal{L}(E)$ de rapport $\lambda \in K$ l'endomorphisme $\lambda.Id_E$

Proposition

Soit $u \in \mathcal{L}(E)$,

(u est une homothétie) $\Leftrightarrow$ ($\forall x \in E$, la famille $(x, f(x))$ est liée.)

Démonstration :

— Supposons que u est une homothétie, c'est-à-dire qu'il existe un scalaire $\lambda \in K$ tel que :

$$\forall x \in E, \ u(x) = \lambda x.$$

— Par définition, une famille de deux vecteurs $(x, u(x))$ est liée si l'un des vecteurs est un multiple de l'autre.

— Or, par l'hypothèse d'homothétie, nous avons :

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

— Il existe donc un scalaire λ tel que $u(x)$ est un multiple de x, ce qui prouve que la famille $(x, u(x))$ est liée.

— Réciproquement, supposons que $\forall x \in E$, la famille $(x, u(x))$ est liée.

— Cela signifie qu'il existe un scalaire $\lambda_x \in K$ tel que :

$$u(x) = \lambda_x x, \quad \forall x \in E \setminus \{0\}.$$

— Montrons que λ_x est constant, c'est-à-dire indépendant de x.

— Prenons deux vecteurs $x, y \in E$ linéairement indépendants.

— On a :

$$u(x) = \lambda_x x, \quad u(y) = \lambda_y y.$$

— Considérons leur somme $x + y$. Comme la famille $(x + y, u(x + y))$ est liée, il existe $\mu \in K$ tel que :

$$u(x + y) = \mu(x + y).$$

— Or, par linéarité de u, on a aussi :

$$u(x+y) = u(x) + u(y) = \lambda_x x + \lambda_y y.$$

— Puisque la famille (x, y) est libre, il doit exister un unique λ tel que :

$$\lambda_x = \lambda_y = \lambda.$$

— Cela montre que u est bien une homothétie de rapport λ.
Finalement nous avons démontré que :

$$\boxed{u \text{ est une homothétie} \iff \forall x \in E,\ \text{la famille } (x, u(x)) \text{ est liée.}}$$

Ce résultat exprime une autre caractérisation des homothéties.

Proposition-HP

Le centre du groupe linéare $\mathcal{G}\updownarrow(E)$ est l'ensemble des homotéthie de rapport non nul.

Démonstration :

— **Définitions et Notations :**
  — Soit E un espace vectoriel sur un corps K.
  — Le groupe linéaire $Gl(E)$ est l'ensemble des automorphismes de E, c'est-à-dire les applications linéaires bijectives de E dans lui-même.
  — Le centre de $Gl(E)$, noté $Z(Gl(E))$, est l'ensemble des éléments de $\mathcal{G}\updownarrow(E)$ qui commutent avec tous les éléments de $\mathcal{G}\updownarrow(E)$:

$$Z(\mathcal{G}\updownarrow(E)) = \{\phi \in Gl(E) \mid \forall g \in \mathcal{G}\updownarrow(E), \phi \circ g = g \circ \phi\}.$$

  — Une homothétie de rapport $\lambda \neq 0$ est une application linéaire h de E définie par :

$$h(v) = \lambda v, \quad \forall v \in E.$$

— **Preuve :**
  — **Inclusion :** $Z(\mathcal{G}\updownarrow(E)) \subseteq$ **Homothéties**
    — Soit $\phi \in Z(\mathcal{G}\updownarrow(E))$, c'est-à-dire que pour tout $g \in Gl(E)$, on a :

$$\phi \circ g = g \circ \phi.$$

    Nous devons montrer que ϕ est une homothétie.
    — Soit $(e_1, \ldots, e_n)$ une base de E. Comme ϕ est un automorphisme, son action sur la base s'écrit sous la forme :

$$\phi(e_i) = \sum_{j=1}^{n} a_{ij} e_j,$$

    où $A = (a_{ij})$ est une matrice inversible.
    — Prenons une matrice de permutation $P \in \mathcal{G}\updownarrow(E)$, qui échange certains vecteurs de la base. Comme ϕ commute avec P, on a :

$$\phi \circ P = P \circ \phi.$$

    Appliquons ceci aux vecteurs de la base :
    — Si $P(e_i) = e_k$, alors $\phi(P(e_i)) = \phi(e_k) = \sum_{j=1}^{n} a_{kj} e_j$.
    — D'un autre côté, $P(\phi(e_i)) = P\left(\sum_{j=1}^{n} a_{ij} e_j\right) = \sum_{j=1}^{n} a_{ij} P(e_j)$.
    Pour que ces deux expressions soient égales pour toute permutation P, la matrice A doit être scalaire, c'est-à-dire qu'il existe $\lambda \neq 0$ tel que :

$$A = \lambda I.$$

    Cela signifie que $\phi(v) = \lambda v$ pour tout $v \in E$, donc ϕ est une homothétie.

— **Inclusion : Homothéties** $\subseteq Z(\mathcal{G}\updownarrow(E))$
  — Soit h une homothétie de rapport $\lambda \neq 0$, définie par :

$$h(v) = \lambda v, \quad \forall v \in E.$$

  — Prenons un élément quelconque $g \in \mathcal{G}\updownarrow(E)$. Alors, pour tout $v \in E$:

$$(g \circ h)(v) = g(h(v)) = g(\lambda v) = \lambda g(v).$$

  D'un autre côté :

$$(h \circ g)(v) = h(g(v)) = \lambda g(v).$$

  — On obtient donc $g \circ h = h \circ g$, ce qui montre que toute homothétie appartient au centre de $\mathcal{G}\updownarrow(E)$.

Finalement nous avons montré que :

$$Z(Gl(E)) = \{\lambda I \mid \lambda \neq 0, \lambda \in K\}.$$

Ainsi, le centre du groupe linéaire $\mathcal{G}\updownarrow(E)$ est exactement l'ensemble des homothéties de rapport non nul.

Proposition-HP

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ $u \in \mathcal{L}(E)$, (u est une homothétie) $\Leftrightarrow$ (si $k \in [|1, n-1|]$ u stabilise tous les sous-espace vectoriels de E de dimension k)

Démonstration :

— **Une homothétie stabilise tous les sous-espaces $\Rightarrow$:**
  — Supposons que u est une homothétie, c'est-à-dire qu'il existe un scalaire $\lambda \in K$ tel que :

$$\forall v \in E, \quad u(v) = \lambda v.$$

  — Considérons un sous-espace vectoriel F de E de dimension k avec $1 \leq k \leq n-1$.
  — Soit $\{e_1, \ldots, e_k\}$ une base de F. Par hypothèse, l'application u agit sur chaque vecteur de F comme suit :

$$u(e_i) = \lambda e_i, \quad \forall i \in \{1, \ldots, k\}.$$

  — Tout vecteur $x \in F$ s'écrit comme combinaison linéaire :

$$x = \sum_{i=1}^{k} \alpha_i e_i.$$

  — L'application de u à x donne :

$$u(x) = \sum_{i=1}^{k} \alpha_i u(e_i) = \sum_{i=1}^{k} \alpha_i \lambda e_i = \lambda \sum_{i=1}^{k} \alpha_i e_i.$$

  — Comme $u(x) \in F$, cela signifie que F est stable par u.
  — Puisque F était un sous-espace quelconque de dimension k, on conclut que u stabilise tous les sous-espaces de E de dimension k.

— **Si u stabilise tous les sous-espaces de dimension k, alors u est une homothétie $\Leftarrow$:**
  — Supposons maintenant que u stabilise tous les sous-espaces vectoriels de E de dimension k pour tout $k \in \{1, \ldots, n-1\}$. Nous allons montrer que u est nécessairement une homothétie.
  — Prenons une base $\{e_1, ..., e_n\}$ de E. Chaque sous-espace vectoriel de dimension 1 est de la forme $F_i = \text{Vect}(e_i)$.
  — Comme u stabilise ces sous-espaces, on a :

$$u(e_i) = \lambda_i e_i, \quad \text{pour un certain } \lambda_i \in K.$$

— Prenons maintenant un sous-espace de dimension 2 de la forme $F = \text{Vect}(e_1, e_2)$. Puisque F est stable par u, tout vecteur $x = \alpha e_1 + \beta e_2 \in F$ est transformé en :

$$u(x) = \alpha u(e_1) + \beta u(e_2) = \alpha\lambda_1 e_1 + \beta\lambda_2 e_2.$$

— Comme F est stable, cela signifie que si $e_1 + e_2 \in F$, alors son image reste dans F, soit :

$$u(e_1 + e_2) = \lambda_1 e_1 + \lambda_2 e_2 \in F.$$

— Autrement dit, u est diagonalisable dans cette base et les λ_i doivent être égaux pour assurer la compatibilité pour tout sous-espace de dimension 2.

— En généralisant ce raisonnement aux sous-espaces de dimensions croissantes jusqu'à $n-1$, on obtient :

$$\lambda_1 = \lambda_2 = ... = \lambda_n = \lambda.$$

— Donc, pour tout $v \in E$, on a bien :

$$u(v) = \lambda v,$$

ce qui montre que u est une homothétie.

Finalement nous avons démontré que :

$$\boxed{u \text{ est une homothétie} \iff u \text{ stabilise tous les sous-espaces vectoriels de dimension } k, \forall k \in \{1, \ldots, n-1\}.}$$

Ce résultat caractérise les homothéties en termes de stabilité des sous-espaces.

Chapitre 3

Les Matrices

3.1 Généralités :

Définition

Une matrice à coefficients dans K est une famille $(a_{i,j})_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]}$ d'éléments de K.
Les nombres m et n sont appelés dimensions de la matrice. On dit qu'une matrice est de taille m $\times$ n.
Les éléments $a_{i,j}$ sont appelés coefficients de la matrice.
Une matrice $A = (a_{i,j})_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]}$est notée de la manière suivante :

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & a_{m,3} & \cdots & a_{m,n} \end{pmatrix}$$

Remarques :

- L'ensemble des matrices de dimensions données à coefficients dans K est noté $\mathrm{M}_{m,n}(\mathbb{K})$.
- L'ensemble $\mathrm{M}_{n,n}(\mathbb{K})$ est noté plus simplement $\mathrm{M}_n(\mathbb{K})$.
- Une matrice de largeur n = 1 est appelée vecteur, ou plus spécifiquement vecteur colonne.
- Une matrice de hauteur m = 1 est appelée vecteur ligne.
- Une matrice telle que m = n est appelée matrice carrée.

3.1.1 Opérations sur les matrices :

Définition — **Addition**

Soient A et B deux matrices de même taille à coefficients dans K. Alors il est possible de les additionner.
Leur somme est une matrice $A + B$ à coefficients dans K, de même taille que A et B :
$(a_{i,j})_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]} + (b_{i,j})_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]} := (a_{i,j} + b_{i,j})_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]}$.

Définition — **Produit par un scalaire**

Le produit d'une matrice $A \in \mathrm{M}_{m,n}(\mathbb{K})$ par un scalaire $\lambda \in \mathbb{K}$ est la matrice $\lambda A \in \mathrm{M}_{m,n}(\mathbb{K})$dont les coefficients sont ceux de A multipliés par λ :

$$\lambda\ (a_{i,j})_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]} := (\lambda a_{i,j})_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]}.$$

Définition — **Produit de deux matrices**

Soient $A = (a_{i,j})_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]} \in \mathrm{M}_{m,n(\mathbb{K})}$ et $B = (b_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} \in \mathrm{M}_{n,p(\mathbb{K})}$ deux matrices telles que . Le produit de A par B est la matrice suivante :

$$AB = \left(\sum_{k=1}^{n} a_{i,k}b_{k,j}\right)_{(i,j)\in[\![1,m]\!]\times[\![1,p]\!]} \in \mathrm{M}_{m,p(\mathbb{K})}.$$

Remarque : La condition pour la possibilité du produit matricielle est que le nombre de colonnes de la première matrice est égale au nombre de lignes de la deuxième.

Propriété

Le produit matriciel est associatif.

Démonstration : Laissée exercise pour le lecteur.

3.1.2 Matrices élémentaires :

Définition — **Matrice nulle**

La matrice nulle de $\mathrm{M}_{m,n}(\mathbb{K})$, notée 0 ou $\mathbf{0}_{\mathrm{M}_{m,n}(\mathbb{K})}$, est : $\mathbf{0}_{\mathrm{M}_{m,n}(\mathbb{K})} := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \mathbf{0}_{\mathrm{M}_{m,n}(\mathbb{K})} := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$

où 0 est l'élément neutre pour l'addition dans l'anneau K — si$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, c'est simplement le zéro habituel.

Définition — **Matrice identité**

On appelle matrice identité de taille n la matrice :

$$\mathrm{I}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Propriétés

- — $\forall A \in \mathrm{M}_{m,n}(\mathbb{K}) \quad A\mathrm{I}_n = A.$
- — $\forall B \in \mathrm{M}_{n,p}(\mathbb{K}) \quad \mathrm{I}_n B = B$

Définitions — **Matrice triangulaire**

Soit A une matrice de $M_n(K)$
On appele A triangulaire supérieure si $a_{i,j} = 0$ pour $i \geq j$.
On appale A triangulaire inférieure si $a_{i,j} = 0$ pour $i \leq j$.

Définitions — **Matrice diagonale**

Soit A une matrice de $M_n(K)$
On appele A diagonale si $a_{i,j} = 0$ pour $i \neq j$.

Définition — **Matrice scalaire**

Soit A une matrice de $M_n(K)$
On appelle A matrice scalaire si $\exists \lambda \in K^*$ tel que $A = \lambda I_n$

3.2 $M_n(\mathbb{K})$

Proposition

$\mathrm{M}_n(\mathbb{K})$, muni de l'addition des matrices et du produit matriciel, est un anneau unifère.

Remarque : $\mathrm{M}_n(\mathbb{K})$ n'est pas un anneau intègre du coup $AB = 0$ n'implique pas $A = 0$ ou $B = 0$

Définition — **Transposition d'une matrice**

La matrice transposée ou la transposée d'une matrice $A \in \mathrm{M}_{m,n}(\mathbb{K})$ est la matrice notée ${}^{\mathrm{t}}A \in \mathrm{M}_{n,m}(\mathbb{K})$ (aussi notée A^{T}ou A^{t}), B telle que :

$$\forall (i,j) \in \{1,\ldots,n\} \times \{1,\ldots,m\} \qquad b_{i,j} = a_{j,i}.$$

Définition — **Inverse d'une matrice**

Soit A une matrice carrée de taille n × n. Lorsqu'elle existe, on appelle inverse à gauche (resp à droite) de A, une matrice telle que : $A_G^{-1}\, A = I_n$.(resp $A\, A_D^{-1} = I_n$) Lorsqu'une matrice admet un inverse à gauche et à droite on dit que cette matrice est inversible , cet inverse ainsi est unique et l'on note A^{-1},

Remarque :

- L'ensemble des matrice inversible est un groupe qu'on note $\mathcal{G}\updownarrow_n(\mathbb{K})$, on étudiera prochainement ce groupe plus profondèment dans son propre chapitre.
- Le produit de deux matrices inversible est aussi une matrice inversible : A, B deux matrices de$M_n(\mathbb{K})$ inversibles d'inverses respectivement A^{-1}, B^{-1} alors AB est inversible d'inverse $B^{-1}A^{-1}$ (il est facile de voir que $B^{-1}A^{-1}AB = ABB^{-1}A^{-1} = I_n$.

Théorème

Une matrice carrée A est inversible si et seulement si $\det A \neq 0$, et dans ce cas, on a :

$$A^{-1} = \frac{1}{\det A}\, {}^{t}(\mathrm{com}\, A)$$

Remarque : Ce résultat ne reste pas vérifié si $\mathbb{K}$ n'est pas un corps commutatif , en fait la condition $\det A \neq 0$ faut être compris en tant que $\det A$ est inversible dans K ce qui sera différent si $\mathbb{K}$ n'était pas un corps commutatif, comme par exemple dans $A \in \mathrm{M}_n(Z)$, la condition deviendra $\det A = 1$ ou $\det A = -1$

Proposition

Soit $A \in \mathrm{M}_n(\mathbb{K})$. Les propositions suivantes (dans lesquelles on identifie $M_{n,1}(\mathbb{K})$ à $\mathbb{K}_n$) sont équivalentes :

i) A est inversible.

ii) l'application linéaire $K^n \to K^n$, $X \mapsto AX$ est bijective (ou, ce qui est équivalent : injective, ou encore : surjective).

iii) A est inversible à gauche, c'est-à-dire qu'il existe une matrice B telle que BA = In.

iv) A est inversible à droite, c'est-à-dire qu'il existe une matrice B telle que AB = In.

v) les colonnes de A forment une base de $\mathbb{K}_n$; la transposée de A est inversible (et dans ce cas, on a $({}^{t}A)^{-1} = {}^{t}(A^{-1})$.

Propriétés

- Si $\lambda \in \mathbb{K}^*\lambda \in \mathbb{K}^*$, la matrice scalaire $\lambda \mathrm{I}_n$ est inversible : $(\lambda \mathrm{I}_n)^{-1} = \frac{1}{\lambda}\mathrm{I}_n$.
- Plus généralement, une matrice diagonale diag $(\lambda_1, \ldots, \lambda_n)$est inversible si et seulement si tous ses termes diagonaux λ_i sont non nuls, et son inverse est alors diag $\left(\frac{1}{\lambda_1}, \ldots, \frac{1}{\lambda_n}\right)$.
- Si une matrice carrée Aest inversible, alors sa transposée l'est aussi, et la transposée de l'inverse de Aest égale à l'inverse de sa transposée : ${}^{t}(A^{-1}) = ({}^{t}A)^{-1}$.
- (n, dim =2)

Définitions — **Matrices symétriques et antisymétriques**

Soit A une matrice de $M_n(\mathbb{K})$,
- On appelle A matrice symétrique si
  $\forall (i,j) \in [|1,n|]^2, a_{i,j} = a_{j,i}$
  (c'est à dire si ${}^{t}A = A$).
- On appelle A matrice antisymétrique
  $\forall (i,j) \in [|1,n|]^2, a_{i,j} = -a_{j,i}$
  (c'est à dire si ${}^{t}A = -A$).

Définitions — **Matrice nilpotente**

Soit A une matrice de $M_n(\mathbb{K})$, on dit que A est nilpotente s'il existe $p \in \mathbf{N}^*$ tel que : $A^p = \mathbf{0}_{\mathrm{M}_{m,n}(K)}$

3.3 Matrice d'une application linéaire

Soient E, F, G trois espace vectoriels, avec : $B = (e_1, ..., e_m)$ base de E, $C = (f_1, ..., f_n)$ base de F, et D base de G.

Définition

Une application $u : E \to F$ est linéaire si et seulement s'il existe une matrice $A \in \mathrm{M}_{m,n}(\mathbb{K})$ telle que pour tout vecteur x de E :
Si X désigne la matrice colonne des coordonnées de x dans la base B c'est à dire si X=.. avec $x = \sum i \in [|1,m|] x_i e_i$ et Y celle des coordonnées de $u(x)$ dans la base C, c'est à dire si $Y =$ avec $u(x) = \sum i \in [|1,n|] y_i f_i$, alors

$$Y = AX.$$

De plus, cette matrice A est alors unique : pour tout $j \in [\![1,n]\!]$, sa j-ème colonne est constituée des coordonnées de $u(e_j)$ dans la base C.
La matrice A est donc appelée la matrice de u dans les bases B, C et notée $\mathrm{Mat}_{B,C}(u)$.

Remarque : Si $F = E$ et $C = B$, on l'appelle la matrice de $u$dans la base B.

Exemples : L'endomorphisme identité I sur un espace vectoriel E est l'application linéaire qui envoie chaque vecteur sur lui-même. La matrice associée à l'endomorphisme identité dans une base $\{e_1, e_2, \ldots, e_n\}$ est la matrice identité.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Une projection est une application linéaire P telle que $P^2 = P$. Par exemple, la projection sur l'axe des x dans $\mathbb{R}^2$ est définie par :

$$P(x, y) = (x, 0)$$

La matrice associée à cette projection est :

$$P = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

La multiplication par un scalaire λ dans un espace vectoriel est une application linéaire définie par :

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

La matrice de multiplication par λ dans une base canonique est simplement λ fois la matrice identité.

$$M = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$$

Une rotation dans $\mathbb{R}^2$ d'un angle θ est une application linéaire R_θ définie par :

$$R_\theta(x, y) = (x\cos(\theta) - y\sin(\theta), x\sin(\theta) + y\cos(\theta))$$

La matrice associée à cette rotation est :

$$R_\theta = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

Une dilatation dans $\mathbb{R}^2$ par un facteur k est une application linéaire D_k définie par :

$$D_k(x, y) = (kx, ky)$$

La matrice associée à cette dilatation est :

$$D_k = \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix}$$

La réflexion par rapport à l'axe des x dans $\mathbb{R}^2$ est une application linéaire R_x définie par :

$$R_x(x, y) = (x, -y)$$

La matrice associée à cette réflexion est :

$$R_x = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

L'application linéaire de la transposition T dans un espace vectoriel E de dimension n est définie comme l'application qui échange les vecteurs avec leurs composants dans une base duale. Si E est un espace vectoriel de dimension 2, la matrice de la transposition est la même que la matrice identité, car l'opération de transposition ne change pas les composantes :

$$T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Soit P_y l'application linéaire qui projette un vecteur (x, y) sur l'axe des y. Cette projection est définie par :

$$P_y(x, y) = (0, y)$$

La matrice de cette projection est :

$$P_y = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

La réflexion par rapport à une droite passant par l'origine dans $\mathbb{R}^2$ et formant un angle θ avec l'axe des x est une application linéaire R_θ. La matrice associée à cette réflexion est donnée par :

$$R_\theta = \begin{bmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{bmatrix}$$

La contraction est une application linéaire qui rétrécit toutes les directions d'un facteur k (avec $0 < k < 1$). Par exemple, une contraction de $\mathbb{R}^2$ par un facteur $k = \frac{1}{2}$ est une application qui diminue toutes les distances par un facteur constant.

La matrice associée à cette contraction est :

$$C_k = \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix}$$

Pour $k = \frac{1}{2}$, cela devient :

$$C_{\frac{1}{2}} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$$

Une transformation affine dans $\mathbb{R}^2$ peut être décomposée en une combinaison d'une application linéaire suivie d'une translation. Par exemple, une translation de vecteur $\mathbf{t} = (t_1, t_2)$ et une transformation linéaire L donnée par :

$$L(x, y) = (x + 1, y - 2)$$

Pour une transformation affine qui effectue cette opération, la matrice augmentée devient :

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

La partie linéaire de la transformation est la matrice $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, et la dernière colonne correspond à la translation.

Un endomorphisme f est dit **nilpotent** s'il existe un entier k tel que $f^k = 0$. Par exemple, l'endomorphisme $f : \mathbb{R}^2 \to \mathbb{R}^2$ défini par :

$$f(x, y) = (y, 0)$$

est nilpotent car $f^2 = 0$. La matrice de f est :

$$f = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

et on a bien $f^2 = 0$.

Un endomorphisme f est **symétrique** si sa matrice est égale à sa transposée. Par exemple, une matrice symétrique dans $\mathbb{R}^2$ pourrait être :

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

Cette matrice est symétrique car $A = A^T$.

Considérons l'opérateur différentiel $D = \frac{d}{dx}$, qui est une application linéaire agissant sur l'espace des polynômes. Si nous appliquons cet opérateur à un polynôme de degré 2, $f(x) = ax^2 + bx + c$, la matrice associée à cet opérateur (dans la base $\{1, x, x^2\}$) est :

$$D = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 0 \end{bmatrix}$$

Cela montre comment cet opérateur agit sur chaque terme du polynôme.

Théorème

L'application $\mathrm{Mat}_{B,C} : \mathrm{L}(E, F) \to \mathrm{M}_{m,n}(K)$ est un isomorphisme d'espaces vectoriels.

Propriété

Si E est muni d'une base « adaptée à F » (c'est-à-dire une base de F complétée en une base de E), la matrice représentative de φ peut être notée par blocs :

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

Alors, F est stable par φ si et seulement si $C = 0$, et dans ce cas la matrice de l'endomorphisme induit sur F est A.

3.3.1 Proposition :

Proposition

Soient $u : E \to F$ et $v : F \to G$ deux applications linéaires. Alors,
$\mathrm{Mat}_{B,D}(v \circ u) = \mathrm{Mat}_{C,D}(v)\ \mathrm{Mat}_{B,C}(u)$.

3.4 Changement de bases :

Définition

La matrice de passage de Bà B' est :
la matrice $\mathrm{Mat}_{B',B}(\mathrm{Id}_\mathrm{E})$ de l'application identité IdE, de E muni de la base B' dans E muni de la base B ou, ce qui est équivalent :
la matrice dont les colonnes sont les coordonnées dans Bdes vecteurs de B'.

3.4.1 Remarque :

Définition

Soit P la matrice de passage de B à B'. Il résulte immédiatement de la définition que :
Pest inversible : son inverse est la matrice de passage de B'à B ; si un même vecteur de E a pour coordonnées X dans B et X' dans B', alors $X = PX'$.

3.4.2 Proposition :

Proposition

Soient :
$u : E \to F$ une application linéaire ; Pla matrice de passage de B à B' (bases de E) ; Q la matrice de passage de C à C' (bases de F). Alors,
$\mathrm{Mat}_{B',C'}(u) = Q^{-1}\ \mathrm{Mat}_{B,C}(u)\ P$.

3.5 Rang :

Définition

Soit A une matrice de $M_{(p,q)}(\mathbb{K})$, on appelle rang de A , le rang de ses vecteurs colonnes dans K^p, et on le note rg(A). Dans le cas oû A est une matrice d'une application linéaire u , on a : rg(A)=rg(u).

Propriétés

- Si $A \in M_{p,q}(K), rg(A) \leq inf\{p, q\}$.
- Si $A \in M_n(K)$ alors
  (A est inversible.) $\Leftrightarrow$ (rg(A)=n.)

Définition

Soit $A = (a_{i,j})_{(i,j)\in[|1,p|]*[|1,q|]} \in M_{(p,q)}(\mathbb{K})$, et soient deux sous-ensembles non vide $I \subset \{1, ..., p\}$ et $J \subset \{1, ..., q\}$. On appelle la matrice $(a_{i,j})_{(i,j)\in I*J} \in M_{(p,q)}(\mathbb{K})$ matrice extraite et A matrice bordante.

Théorème

Soient $A \in M_{p,q}(\mathbb{K})$, son rang est égale à la taille de la plus grande matrice carrée inversible qu'on peut extraire de cette dernière.

Corollaire

Le rang de la transposée d'une matrice est égal à celui de la dernière.

3.6 Equivalence, similitude et trace :

3.6.1 Equivalence :

Définition

Deux matrices M et N sont dites équivalentes s'ils existent deux matrices inversibles P et Qtelles que : $N = Q^{-1}MP$.

Théorème

Soient $A \in M_{p,q}(K)$ et $r \in N^*$, rg(A)=r si et seulement si A est équivalent à J_r avec
$J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$

Théorème

Deux matrices de même taille sont équivalentes si et seulement si elles ont même rang.

Démonstration : Soit B matrice de rang r équivalent à A alors : ils existent deux matrices inversibles P et Qtelles que :

$A = Q^{-1}BP$. or B étant de rang r elle est équivalent à J_r donc de plus ils existent deux matrices inversibles P' et Q'telles que :

$B = Q'^{-1}J_rP'$. donc $A = Q^{-1}Q'^{-1}J_rP'P$. avec $Q^{-1}Q'^{-1}$ et $P'P$ les deux inversibles (produit de deux matrices inversibles) donc A est équivalente à J_r, finalement A est de rang r le même que B.

3.6.2 Similitude :

Définition

Deux matrices carrées M et N sont dites semblables s'il existe une matrice inversible Ptelle que : $N = P^{-1}MP$.

3.6.3 Trace

Définition

Soit A une matrice carrée. La trace de A est la somme des « éléments diagonaux » de A (les éléments de sa diagonale principale). Elle est notée : tr **A**, ou Tr **A**.

Propriété

L'application $tr : M_n(\mathbb{K}) \to K$ est une forme linéaire.

Propriétés

Soient $\mathbf{A}$ et $\mathbf{B}$ deux matrices carrées de même taille et a un scalaire. Alors : $\mathrm{tr}\,(\mathbf{A}+\mathbf{B}) = \mathrm{tr}\,\mathbf{A} + \mathrm{tr}\,\mathbf{B}$; $\mathrm{tr}\,(a\,\mathbf{A}) = a\,\mathrm{tr}\,\mathbf{A}$; $\mathrm{tr}({}^{t}\mathbf{A}) = \mathrm{tr}\ \mathbf{A}$;

Démonstration : Laissée exercise pour le lecteur.

Remarque : Si $A, B, C \in M_n(K)$ on peut avoir $tr(ABC) = tr(CAB) = tr(BCA)$ mais $tr(ABC) \neq tr(ACB)$.

Corollaire

Soient $\mathbf{A} \in \mathrm{M}_{m,n}(\mathbb{K})$ et $\mathbf{B} \in \mathrm{M}_{n,m}(\mathbb{K})$. Alors : $\mathrm{tr}\ (\mathbf{AB}) = \mathrm{tr}\ (\mathbf{BA})$.

Démonstration : Laissée exercise pour le lecteur.

Propriété

Deux matrices semblables ont même trace.

Propriété

Soit E un K-espace vectoriel et $p \in \mathcal{L}(E)$ un projecteur, alors
$trp = rg(p).1_{\mathbb{K}}$

Démonstration : Notons r le rang de p, p étant projecteur on a : $E = \ker p \oplus Imp$, considèrant les deux bases $(e_1, ..., e_r)$ de Imp et $(e_{r+1}, ..., e_n)$ puisque $E = \ker p \oplus Imp$, la base B obtenue par concatenation des deux bases $(e_1, ..., e_r)$ et $(e_{r+1}, ..., e_n)$ est base de E, et donc la matrice de p dans cette base est $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$
Finalement, sa trace $trp = r = rg(p).1_{\mathbb{K}}$.

3.7 Compléments :

3.7.1 Matrice diagonalement dominantes -HP

Définition

Soit $A = (a_{i,j})_{1 \leq i,j \leq n} \in M_n(\mathbb{K})$ A est dite de diagonale dominante si :

$$\forall i \in [|1, n|], \sum_{1 \leq j \leq n, j \neq i} |a_{i,j}| \leq |a_{i,i}|$$

Lemme de Hadamard

Si A une matrice de diagonale dominante, alors A est inversible.

Démonstration Dire que A est inversible est équivalent à dire que les vecteurs colonnes de A forment une famille libre, on montrera par raisonnement par absurde le résultat dérnier.
Supposant que les vecteurs colonnes de A forment une famille liée,
On note les coéfficients de A par $a_{i,j}, i, j \in [|1, n|]$, d'après notre supposition :

$$\exists (\lambda_1, \ldots, \lambda_n) \in \mathbb{C}^n \text{ non tous nuls tels que } \forall i \in [|1, n|], \sum_{j=1}^n \lambda_j a_{i,j} = 0_{\mathbb{C}},$$

Posant $k \in [|1, n|]$ tel que $|\lambda_k| = sup_{j \in [|1,n|]} |\lambda_j|$, puisque les $(\lambda_j)_{j \in [|1,n|]}$ sont non tous nuls cette définition a un sens et $\lambda_k \neq 0$.
On a maintenant $\sum_{j=1}^n \lambda_j a_{k,j} = 0_{\mathbb{C}}$ donc $\sum_{j=1, j \neq k}^n (\lambda_j a_{k,j}) + \lambda_k a_{k,k} = 0_{\mathbb{C}}$ donc $a_{k,k} = \sum_{j=1, j \neq k}^n \lambda_j / \lambda_k a_{k,j}$
du coup $|a_{k,k}| \leq \sum_{j=1, j \neq k}^n |\lambda_j| / |\lambda_k| |a_{k,j}| \leq \sum_{j=1, j \neq k}^n |a_{k,j}|$(puisque $\forall j \in [|1, n|] |\lambda_j| \leq |\lambda_k|$)
ce qui est contradictoire avec l'hypothèse que A est de diagonale dominante, finalement :

$$\boxed{\text{Si A est de diagonale dominante alors A est inversible.}}$$

3.7.2 Matrice circulantes-HP

Définition

Soit $M \in M_n(\mathbb{C})$, on dit que M est une matrice circulante si elle s'écrit sous la forme suivante : $M = \begin{pmatrix} c_1 & c_2 & ... & c_n \\ c_n & c_1 & ... & c_{n-1} \\ c_{n-1} & c_n & ... & c_{n-2} \\ \vdots & \ddots & \vdots & \\ c_2 & c_3 & ... & c_1 \end{pmatrix}$
avec $\forall i \in [|1, n|]\, c_i \in \mathbb{C})$

Proposition

On note une matrice circulante de sorte que la matrice précédente est noté $M(c_1, ..., c_n)$

On pose alors $J = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$ de sorte que
$J = M(0, 1, ..., 0)$, on a donc :

(M est une matrice circulante) $\Leftrightarrow$ (M est un polynôme en J)

Démonstration :

— **Sens direct ($\Rightarrow$) :** Si M est une matrice circulante, alors elle s'écrit sous la forme :

$$M = \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_n \\ c_n & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_n & c_1 & \cdots & c_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & c_4 & \cdots & c_1 \end{pmatrix}.$$

Chaque ligne est obtenue en multipliant la précédente par J, où J est la matrice de permutation circulaire :

$$J = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Ainsi, M est une combinaison linéaire des puissances de J :

$$M = c_1 I + c_2 J + c_3 J^2 + \cdots + c_n J^{n-1}.$$

Donc M est un polynôme en J.

— **Sens réciproque ($\Leftarrow$) :** Supposons que M soit un polynôme en J, soit :

$$M = c_1 I + c_2 J + c_3 J^2 + \cdots + c_n J^{n-1}.$$

Comme les puissances de J correspondent aux décalages cycliques des vecteurs de base, toute combinaison linéaire de ces puissances conserve cette structure.
Par conséquent, M est nécessairement une matrice circulante.

$$(M \text{ est circulante}) \iff (M \text{ est un polynôme en } J).$$

Proposition

L'ensemble des matrice circulantes est une sous-algèbre commutative de $M_n(\mathbb{C})$

Démonstration :

- **Stabilité de $C_n(\mathbb{C})$ sous les opérations algébriques :**
  - **Addition :** Soient $A = \operatorname{circ}(a_1, a_2, \ldots, a_n)$ et $B = \operatorname{circ}(b_1, b_2, \ldots, b_n)$ deux matrices circulantes. Leur somme est :
  $$A + B = \operatorname{circ}(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$
  Comme la somme des coefficients suit la même structure, $A + B$ est encore circulante.
  - **Multiplication par un scalaire :** Pour tout $\lambda \in \mathbb{C}$, on a :
  $$\lambda A = \operatorname{circ}(\lambda a_1, \lambda a_2, \ldots, \lambda a_n),$$
  ce qui reste une matrice circulante.
  - **Multiplication matricielle :** Toute matrice circulante M peut s'écrire comme un polynôme en la matrice de permutation J :
  $$M = c_1 I + c_2 J + c_3 J^2 + \cdots + c_n J^{n-1}.$$
  La multiplication de deux matrices circulantes correspond à la multiplication de polynômes en J, ce qui donne encore une matrice circulante. Ainsi, $C_n(\mathbb{C})$ est une **sous-algèbre** de $M_n(\mathbb{C})$.
- **Commutativité de $C_n(\mathbb{C})$:** Soient $A, B \in C_n(\mathbb{C})$, alors il existe deux polynômes $P(X)$ et $Q(X)$ tels que :
  $$A = P(J), \quad B = Q(J).$$
  Comme J est une **matrice de permutation cyclique** et que les polynômes appliqués à une même matrice commutent, on a :
  $$AB = P(J)Q(J) = Q(J)P(J) = BA.$$
  Ainsi, $C_n(\mathbb{C})$ est **commutatif**.

L'ensemble des matrices circulantes est une sous-algèbre commutative de $M_n(\mathbb{C})$.

3.7.3 Matrice de Toeplitz

Définition

Une **matrice de Toeplitz** de dimension $n \times n$ est une matrice de la forme :

$$T = \begin{bmatrix} t_0 & t_1 & t_2 & \cdots & t_{n-2} & t_{n-1} \\ t_{-1} & t_0 & t_1 & \cdots & t_{n-3} & t_{n-2} \\ t_{-2} & t_{-1} & t_0 & \cdots & t_{n-4} & t_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ t_{-n+2} & t_{-n+3} & t_{-n+4} & \cdots & t_0 & t_1 \\ t_{-n+1} & t_{-n+2} & t_{-n+3} & \cdots & t_{-1} & t_0 \end{bmatrix}$$

où chaque élément de la matrice est défini par la relation :

$$T_{i,j} = t_{j-i}, \quad \forall i, j \in \{1, 2, \ldots, n\}.$$

Ainsi, une matrice de Toeplitz est complètement déterminée par son premier élément de chaque ligne et de chaque colonne.

Définition

Une **matrice de Toeplitz tridiagonale** est une matrice de la forme :

$$T = \begin{bmatrix} a & b & 0 & 0 & \cdots & 0 \\ c & a & b & 0 & \cdots & 0 \\ 0 & c & a & b & \cdots & 0 \\ 0 & 0 & c & a & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & b \\ 0 & 0 & \cdots & 0 & c & a \end{bmatrix}$$

où :

$$T_{i,j} = \begin{cases} a, & \text{si } i = j \\ b, & \text{si } j = i + 1 \\ c, & \text{si } j = i - 1 \\ 0, & \text{sinon} \end{cases}$$

3.7.4 Matrice de Hankel

Définition

Une matrice de Hankel H est donnée par :

$$H = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{m-1} \\ h_1 & h_2 & h_3 & \cdots & h_m \\ h_2 & h_3 & h_4 & \cdots & h_{m+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n-1} & h_n & h_{n+1} & \cdots & h_{n+m-2} \end{bmatrix}$$

où chaque élément $H(i, j)$ est défini par h_{i+j}. Ainsi, toutes les valeurs situées sur une même anti-diagonale sont égales.

3.7.5 Matrice de Hankel symétrique

Définition

Une **matrice de Hankel symétrique** est une matrice carrée dans laquelle les éléments sont constants sur chaque anti-diagonale (diagonales parallèles à la diagonale secondaire). Autrement dit, une matrice H de taille $n \times n$ est dite de Hankel si :

$$H_{i,j} = H_{i-1,j+1}, \quad \forall i, j \text{ tels que } 1 \leq i, j \leq n-1.$$

En notation matricielle, une matrice de Hankel symétrique prend la forme :

$$H = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{n-1} \\ h_1 & h_2 & h_3 & \cdots & h_n \\ h_2 & h_3 & h_4 & \cdots & h_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n-1} & h_n & h_{n+1} & \cdots & h_{2n-2} \end{bmatrix}$$

où chaque élément est défini uniquement par un indice unique h_k correspondant à la somme des indices de ligne et de colonne :

$$H_{i,j} = h_{i+j-2}, \quad \forall i, j.$$

Une matrice de Hankel est dite **symétrique** si et seulement si elle satisfait la condition :

$$H_{i,j} = H_{j,i}, \quad \forall i, j.$$

Chapitre 4

Dualité

4.1 Définitions

4.1.1 Espace et base duale

Définition

On rappelle qu'une **forme linéaire** sur E est toute application linéaire de E dans $\mathbb{K}$.
L'ensemble $\mathcal{L}(E, K)$ des formes linéaires sur E est aussi noté E^*.
C'est un $\mathbb{K}$-espace vectoriel appelé **espace dual** de E.

4.1.2 Bidual

Définition

On appelle **bidual** de E l'espace dual de E^*, noté E.

On considère maintenant que E est de dimension finie $n \in \mathbb{N}^*$.

Définition

Soit $B = (e_1, \ldots, e_n)$ une base de E. Pour tout i, $1 \leq i \leq n$, la forme linéaire e^i définie sur B par :

$$e^i(e_j) = 0 \quad \text{si } j \neq i, \quad e^i(e_i) = 1$$

s'appelle **forme linéaire coordonnée d'indice** i.

4.1.3 Théorème

Définition-Théorème

Soit $B = (e_1, \ldots, e_n)$ une base de E. Alors $B^* = (e^1, \ldots, e^n)$ est une base de E^* appelée **base duale de** B, et donc $\dim E^* = \dim E$. Pour tout $\varphi \in E^*$, on a :

$$\varphi = \sum_{i=1}^{n} \varphi(e_i) e^i.$$

Démonstration : Nous devons prouver que B^* est une base de E^*, c'est-à-dire qu'elle est :

- **Libre** : les éléments sont linéairement indépendants.
- **Génératrice** : tout $\varphi \in E^*$ s'écrit comme une combinaison linéaire des e^i.
- **Preuve que B^* est libre**
  Une famille $(v_1, \ldots, v_n)$ est libre si la seule combinaison linéaire nulle est la combinaison triviale :

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0 \quad \Rightarrow \quad \lambda_1 = \cdots = \lambda_n = 0.$$

Supposons qu'il existe $\lambda_1, \ldots, \lambda_n$ tels que :

$$\lambda_1 e^1 + \lambda_2 e^2 + \cdots + \lambda_n e^n = 0.$$

Cela signifie que l'application $\psi \in E^*$ définie par :

$$\psi = \sum_{i=1}^{n} \lambda_i e^i$$

est la fonction nulle, c'est-à-dire $\psi(x) = 0$ pour tout $x \in E$. En particulier, en prenant $x = e_j$, on obtient :

$$\psi(e_j) = \sum_{i=1}^{n} \lambda_i e^i(e_j) = 0.$$

Par définition de e^i, on sait que $e^i(e_j) = \delta_{ij}$, donc :

$$\lambda_j = 0, \quad \forall j \in \{1, \ldots, n\}.$$

Ainsi, $\lambda_1 = \cdots = \lambda_n = 0$, donc B^* est libre.

— **Preuve que B^* est génératrice**
Nous devons montrer que tout $\varphi \in E^*$ s'écrit comme :

$$\varphi = \sum_{i=1}^{n} c_i e^i.$$

Prenons un $\varphi \in E^*$. Nous cherchons $c_1, \ldots, c_n$ tels que :

$$\varphi(x) = \sum_{i=1}^{n} c_i e^i(x), \quad \forall x \in E.$$

En appliquant cette égalité à $x = e_j$, on obtient :

$$\varphi(e_j) = \sum_{i=1}^{n} c_i e^i(e_j).$$

Or, $e^i(e_j) = \delta_{ij}$, donc l'équation devient simplement :

$$\varphi(e_j) = c_j.$$

Ainsi, les coefficients c_i sont déterminés par :

$$c_i = \varphi(e_i), \quad \forall i.$$

On en déduit :

$$\varphi = \sum_{i=1}^{n} \varphi(e_i) e^i.$$

Cela prouve que B^* est une famille génératrice.

— **Conclusion**
Comme B^* est libre et génératrice dans E^*, c'est une base de E^*.
De plus, B^* contient n éléments, donc $\dim E^* = n = \dim E$.
$\square$

Théorème

Si $x \in E$, on note $\tilde{x} : E^* \to K$ par $\varphi \mapsto \varphi(x)$. On a $\tilde{x} \in E$ et l'application :

$$f : E \to E, \quad x \mapsto \tilde{x}$$

est un isomorphisme.

Démonstration : Nous allons démontrer cette affirmation en plusieurs étapes :

— **1. Vérification que f est bien définie**
L'espace E est, par définition, l'ensemble des applications linéaires de E^* dans K. Vérifions que $\tilde{x}$ est bien un élément de E, c'est-à-dire qu'elle est une application linéaire.
Soient $\varphi, \psi \in E^*$ et $\lambda, \mu \in K$. Calculons :

$$\tilde{x}(\lambda\varphi + \mu\psi) = (\lambda\varphi + \mu\psi)(x).$$

Par linéarité de φ et ψ, on a :

$$(\lambda\varphi + \mu\psi)(x) = \lambda\varphi(x) + \mu\psi(x).$$

Or, par définition de $\tilde{x}$, on a $\tilde{x}(\varphi) = \varphi(x)$ et $\tilde{x}(\psi) = \psi(x)$, donc :

$$\tilde{x}(\lambda\varphi + \mu\psi) = \lambda\tilde{x}(\varphi) + \mu\tilde{x}(\psi).$$

Cela montre que $\tilde{x}$ est bien linéaire, donc $\tilde{x} \in E$, et l'application f est bien définie.

— **2. Injectivité de f**
Montrons que f est injective, c'est-à-dire que :

$$f(x) = 0 \quad \Rightarrow \quad x = 0.$$

Soit $x \in \ker f$, c'est-à-dire que $f(x) = \tilde{x}$ est l'application nulle :

$$\tilde{x}(\varphi) = 0, \quad \forall \varphi \in E^*.$$

Cela signifie que :

$$\varphi(x) = 0, \quad \forall \varphi \in E^*.$$

Si $x \neq 0$, on peut compléter x en une base $(x, e_2, \ldots, e_n)$ de E. Soit $x^* \in E^*$ la forme linéaire définie par :

$$x^*(x) = 1 \quad \text{et} \quad x^*(e_j) = 0 \quad \text{pour } j \geq 2.$$

En particulier, $x^*(x) \neq 0$, mais par hypothèse $\tilde{x}(x^*) = 0$, donc :

$$x^*(x) = 0.$$

Contradiction. On en déduit que $x = 0$, donc $\ker f = \{0\}$, et f est injective.

— **3. Surjectivité de f**
Pour montrer que f est un isomorphisme, il reste à prouver que f est surjective, c'est-à-dire que tout élément de E est de la forme $\tilde{x}$ pour un certain $x \in E$.
Par le 4.1.3, nous savons que :

$$\dim E = \dim E^* = \dim E.$$

Or, nous avons montré que f est injective, donc :

$$\dim \operatorname{Im}(f) = \dim E.$$

Comme E a la même dimension que E, on en déduit que f est aussi surjective, car une application linéaire injective entre deux espaces de même dimension est nécessairement bijective.

Ainsi, f est un isomorphisme entre E et E, ce qui conclut la démonstration.

Remarque : Cet isomorphisme est **canonique** (c'est-à-dire qu'il ne dépend pas du choix d'une base). On convient alors d'**identifier** E et E en identifiant x à $\tilde{x}$ pour $x \in E$. En dimension infinie, $f : x \mapsto \tilde{x}$ est injective mais **pas surjective**.

4.1.4 Base antéduale

Propriété-Définition

Soit $(f_1, \ldots, f_n)$ une base de E^*. Il existe une **unique** base $(e_1, \ldots, e_n)$ de E telle que, pour tout i, $e^i = f_i$. Cette base s'appelle **base antéduale** de $(f_1, \ldots, f_n)$.

4.2 Orthogonalité

Définition

Des éléments $x \in E$ et $\varphi \in E^*$ sont dits **orthogonaux** si $\varphi(x) = \langle \varphi, x \rangle = 0$.

— Si $A \subset E$, on note $A^\perp = \{\varphi \in E^* \mid \forall x \in A, \varphi(x) = 0\}$. L'ensemble $A^\perp$ est un sous-espace vectoriel de E^* appelé **orthogonal de** A.

— Si $B \subset E^*$, on note $B^\perp = \{x \in E \mid \forall \varphi \in B, \varphi(x) = 0\}$. L'ensemble $B^\perp$ est un sous-espace vectoriel de E appelé **orthogonal de** B.

Remarque Si $\varphi \in E^*$, alors $\{\varphi\}^\perp$ est le noyau de φ.

Propriété

La proposition qui suit se prouve facilement.

— Si $A_1 \subset A_2 \subset E$, alors $A_2^\perp \subset A_1^\perp$.

— Si $B_1 \subset B_2 \subset E^*$, alors $B_2^\perp \subset B_1^\perp$.

— Si $A \subset E$, alors $A^\perp = (\mathrm{Vect}(A))^\perp$.

— Si $B \subset E^*$, alors $B^\perp = (\mathrm{Vect}(B))^\perp$.

Théorème

Soit E un K-espace vectoriel de dimension finie. Alors :

(i) Si F est un sous-espace vectoriel de E, alors $\dim F + \dim F^\perp = \dim E$ et $(F^\perp)^\perp = F$.

(ii) Si G est un sous-espace vectoriel de E^*, alors $\dim G + \dim G^\perp = \dim E$ et $(G^\perp)^\perp = G$.

Démonstration : Nous devons démontrer les deux propriétés suivantes :

(i) Si F est un sous-espace vectoriel de E, alors :

$$\dim F + \dim F^\perp = \dim E \quad \text{et} \quad (F^\perp)^\perp = F.$$

(ii) Si G est un sous-espace vectoriel de E^*, alors :

$$\dim G + \dim G^\perp = \dim E \quad \text{et} \quad (G^\perp)^\perp = G.$$

— **1. Rappels et définitions**

— L'orthogonal $F^\perp$ d'un sous-espace $F \subset E$ est défini par :

$$F^\perp = \{\varphi \in E^* \mid \forall x \in F, \varphi(x) = 0\}.$$

— L'orthogonal $G^\perp$ d'un sous-espace $G \subset E^*$ est donné par :

$$G^\perp = \{x \in E \mid \forall \varphi \in G, \varphi(x) = 0\}.$$

— L'orthogonal d'un sous-espace est toujours un sous-espace vectoriel.

— En dimension finie, nous allons exploiter le fait que F et $F^\perp$ sont en correspondance via l'application bilinéaire naturelle :

$$\langle \varphi, x \rangle = \varphi(x).$$

— **2. Preuve de (i) :** $\dim F + \dim F^\perp = \dim E$ **et** $(F^\perp)^\perp = F$

— Soit F un sous-espace de E de dimension r, soit $B = (e_1, \dots, e_n)$ une base de E.

— On peut choisir une base adaptée $(e_1, \dots, e_r)$ de F, et compléter en une base $(e_{r+1}, \dots, e_n)$ de E.

— L'ensemble des formes linéaires $(e^{r+1}, \dots, e^n)$ définit alors une base de $F^\perp$.

— Comme ces formes sont indépendantes et forment un complément de F, on a :

$$\dim F^\perp = n - r.$$

— D'où l'égalité :

$$\dim F + \dim F^\perp = r + (n - r) = n = \dim E.$$

- Pour prouver que $(F^\perp)^\perp = F$, nous devons montrer que F est exactement l'ensemble des vecteurs qui sont orthogonaux à $F^\perp$.
- Comme $F^\perp$ est défini par l'ensemble des formes annulant F, les vecteurs de $(F^\perp)^\perp$ sont exactement ceux qui ne peuvent être distingués de F.
- Puisque nous avons l'égalité des dimensions, nous concluons :

$$(F^\perp)^\perp = F.$$

- **3. Preuve de (ii) :** $\dim G + \dim G^\perp = \dim E$ **et** $(G^\perp)^\perp = G$
  - Soit G un sous-espace de E^*, et soit $r = \dim G$.
  - L'espace $G^\perp$ est l'ensemble des vecteurs de E qui sont annulés par toutes les formes de G.
  - Comme G est de dimension r, nous avons un système maximal de formes linéaires indépendantes $(\varphi_1, \dots, \varphi_r)$.
  - L'espace des vecteurs $G^\perp$ est donc un sous-espace de dimension $n - r$.
  - Ainsi, on obtient bien :
  $$\dim G + \dim G^\perp = r + (n - r) = n = \dim E.$$
  - Pour prouver que $(G^\perp)^\perp = G$, nous utilisons le même raisonnement que précédemment.
  - Les formes qui s'annulent sur $G^\perp$ sont exactement celles qui appartiennent à G.
  - Étant donné que les dimensions correspondent, nous avons :
  $$(G^\perp)^\perp = G.$$
- **4. Conclusion**
  - Nous avons montré que :
    (i) $\dim F + \dim F^\perp = \dim E$ et $(F^\perp)^\perp = F$.
    (ii) $\dim G + \dim G^\perp = \dim E$ et $(G^\perp)^\perp = G$.
  - Ce qui termine la démonstration. □

Conséquence En dimension finie, un sous-espace est égal à l'espace tout entier si et seulement si son orthogonal est nul.

Remarque L'égalité $F^{\perp\perp} = F$ reste vraie en dimension infinie. En revanche, l'égalité $B^{\perp\perp} = B$ est **fausse** en dimension infinie.

Par exemple, prenons $E = \mathbb{R}[X]$ et B le sous-espace de E^* engendré par :

$$\varphi_n : P \mapsto P^{(n)}(0), \quad n \in \mathbb{N}.$$

Si $P \in B^\perp$, alors pour tout $n \in \mathbb{N}$, $P^{(n)}(0) = 0$. D'après la formule de Taylor, $P = 0$. Donc $B^\perp = \{0\}$ et $B^{\perp\perp} = E^*$, mais $B \neq B^{\perp\perp}$.

Cependant, **l'inclusion** $B \subset B^{\perp\perp}$ est **toujours vraie** en dimension infinie.

Propriété

Corollaire 1 (Équations d'un s.e.v en dimension finie). Soit E un K-espace vectoriel de dimension finie n.
- Soient p formes linéaires $\varphi_1, \dots, \varphi_p$ de E^* telles que :
$$\operatorname{rg}(\varphi_1, \dots, \varphi_p) = r.$$
Le sous-espace vectoriel :
$$F = \{x \in E \mid \forall i, \varphi_i(x) = 0\}$$
est de dimension $n - r$.

Remarque Réciproquement, si F est un sous-espace vectoriel de E de dimension q, il existe $n - q$ formes linéaires linéairement indépendantes $\varphi_1, \dots, \varphi_{n-q}$ telles que :

$$F = \{x \in E \mid \forall i, 1 \leq i \leq n - q, \varphi_i(x) = 0\}.$$

Propriété

Soit E un K-espace vectoriel de dimension finie et A_1, A_2 deux sous-espaces vectoriels de E. Alors :
(i) $(A_1 + A_2)^\perp = A_1^\perp \cap A_2^\perp$.
(ii) $(A_1 \cap A_2)^\perp = A_1^\perp + A_2^\perp$.
Soient B_1 et B_2 deux sous-espaces de E^*. Alors :
(iii) $(B_1 + B_2)^\perp = B_1^\perp \cap B_2^\perp$.
(iv) $(B_1 \cap B_2)^\perp = B_1^\perp + B_2^\perp$.

Démonstration : Nous devons prouver les relations suivantes concernant les orthogonaux de sommes et d'intersections de sous-espaces vectoriels.
(i) $(A_1 + A_2)^\perp = A_1^\perp \cap A_2^\perp$.
(ii) $(A_1 \cap A_2)^\perp = A_1^\perp + A_2^\perp$.
(iii) $(B_1 + B_2)^\perp = B_1^\perp \cap B_2^\perp$.
(iv) $(B_1 \cap B_2)^\perp = B_1^\perp + B_2^\perp$.

— **1. Rappels et définitions**
  — Pour un sous-espace A de E, son orthogonal est défini par :

$$A^\perp = \{\varphi \in E^* \mid \forall x \in A, \varphi(x) = 0\}.$$

  — Pour un sous-espace B de E^*, son orthogonal est :

$$B^\perp = \{x \in E \mid \forall \varphi \in B, \varphi(x) = 0\}.$$

  — Nous allons démontrer chaque égalité en deux inclusions.

— **2. Preuve de (i) :** $(A_1 + A_2)^\perp = A_1^\perp \cap A_2^\perp$
  — Montrons d'abord que $(A_1 + A_2)^\perp \subset A_1^\perp \cap A_2^\perp$.
  — Soit $\varphi \in (A_1 + A_2)^\perp$. Alors, pour tout $x_1 \in A_1$ et $x_2 \in A_2$, on a :

$$\varphi(x_1 + x_2) = 0.$$

  — En prenant $x_2 = 0$, on obtient $\varphi(x_1) = 0$, donc $\varphi \in A_1^\perp$.
  — En prenant $x_1 = 0$, on obtient $\varphi(x_2) = 0$, donc $\varphi \in A_2^\perp$.
  — Ainsi, $\varphi \in A_1^\perp \cap A_2^\perp$, ce qui prouve l'inclusion.
  — Montrons maintenant que $A_1^\perp \cap A_2^\perp \subset (A_1 + A_2)^\perp$.
  — Soit $\varphi \in A_1^\perp \cap A_2^\perp$. Alors $\varphi(x) = 0$ pour tout $x \in A_1$ et tout $x \in A_2$.
  — Pour tout $x \in A_1 + A_2$, il existe $x_1 \in A_1$ et $x_2 \in A_2$ tels que $x = x_1 + x_2$.
  — Alors :

$$\varphi(x) = \varphi(x_1) + \varphi(x_2) = 0 + 0 = 0.$$

  — Donc $\varphi \in (A_1 + A_2)^\perp$, ce qui prouve la seconde inclusion.

— **3. Preuve de (ii) :** $(A_1 \cap A_2)^\perp = A_1^\perp + A_2^\perp$
  — Montrons d'abord que $(A_1 \cap A_2)^\perp \subset A_1^\perp + A_2^\perp$.
  — Soit $\varphi \in (A_1 \cap A_2)^\perp$, c'est-à-dire que $\varphi(x) = 0$ pour tout $x \in A_1 \cap A_2$.
  — Par le théorème de prolongement des formes linéaires, il existe $\varphi_1 \in A_1^\perp$ et $\varphi_2 \in A_2^\perp$ tels que :

$$\varphi = \varphi_1 + \varphi_2.$$

  — Ainsi, $\varphi \in A_1^\perp + A_2^\perp$, ce qui prouve cette inclusion.
  — Montrons maintenant que $A_1^\perp + A_2^\perp \subset (A_1 \cap A_2)^\perp$.
  — Soit $\varphi_1 \in A_1^\perp$ et $\varphi_2 \in A_2^\perp$, alors pour tout $x \in A_1 \cap A_2$, on a :

$$(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x) = 0 + 0 = 0.$$

  — Donc $\varphi_1 + \varphi_2 \in (A_1 \cap A_2)^\perp$, ce qui termine la preuve.

— **4. Preuve de (iii) :** $(B_1 + B_2)^\perp = B_1^\perp \cap B_2^\perp$
  — Cette preuve suit le même raisonnement que celle de (i), en remplaçant les A_i par B_i dans l'espace dual.

— **5. Preuve de (iv) :** $(B_1 \cap B_2)^\perp = B_1^\perp + B_2^\perp$
  — Cette preuve suit le même raisonnement que celle de (ii), en remplaçant les A_i par B_i dans l'espace dual.

— **6. Conclusion**
  — Nous avons montré que :
    (i) $(A_1 + A_2)^\perp = A_1^\perp \cap A_2^\perp$.
    (ii) $(A_1 \cap A_2)^\perp = A_1^\perp + A_2^\perp$.
    (iii) $(B_1 + B_2)^\perp = B_1^\perp \cap B_2^\perp$.
    (iv) $(B_1 \cap B_2)^\perp = B_1^\perp + B_2^\perp$.
  — Ce qui termine la démonstration. □

Remarque La preuve est simple. Pour montrer chaque assertion, on montre une inclusion triviale puis l'égalité des dimensions grâce au théorème 3.

Orthogonalité et hyperplans

Propriété

Soit $\varphi \in E^*$ une forme linéaire non nulle. Alors $\ker\varphi$ est un hyperplan de E. Réciproquement, tout hyperplan de E est le noyau d'une forme linéaire non nulle.

Démonstration : Nous devons prouver deux affirmations :
(i) Si $\varphi \in E^*$ est une forme linéaire non nulle, alors son noyau $\ker\varphi$ est un hyperplan de E.
(ii) Réciproquement, tout hyperplan de E est le noyau d'une forme linéaire non nulle.

— **1. Preuve de (i) : $\ker\varphi$ est un hyperplan**
  — Soit $\varphi \in E^*$ une forme linéaire non nulle.
  — Son noyau est défini par :
$$\ker\varphi = \{x \in E \mid \varphi(x) = 0\}.$$
  — Nous devons prouver que $\ker\varphi$ est un sous-espace vectoriel de E de codimension 1.
  — Comme φ est linéaire, pour tous $x, y \in \ker\varphi$ et tout scalaire λ, nous avons :
$$\varphi(x + y) = \varphi(x) + \varphi(y) = 0 + 0 = 0.$$
$$\varphi(\lambda x) = \lambda\varphi(x) = \lambda \cdot 0 = 0.$$
  — Ainsi, $\ker\varphi$ est un sous-espace vectoriel de E.
  — Montrons maintenant que sa dimension est $\dim E - 1$.
  — Puisque $\varphi \neq 0$, il existe $x_0 \in E$ tel que $\varphi(x_0) \neq 0$.
  — Considérons l'application linéaire sur l'espace quotient :
$$\bar{\varphi} : E/\ker\varphi \to K, \quad \bar{\varphi}([x]) = \varphi(x).$$
  — Cette application est bien définie et injective car si $\bar{\varphi}([x]) = 0$, alors $x \in \ker\varphi$.
  — Or, un espace vectoriel injectif vers un espace de dimension 1 est de dimension au plus 1, donc :
$$\dim E/\ker\varphi = 1.$$
  — Ainsi, on obtient bien :
$$\dim\ker\varphi = \dim E - 1.$$
  — Par définition, $\ker\varphi$ est donc un hyperplan de E.

— **2. Preuve de (ii) : Tout hyperplan est un noyau d'une forme linéaire non nulle**
  — Soit H un hyperplan de E, c'est-à-dire un sous-espace vectoriel de E de dimension $\dim H = \dim E - 1$.
  — Nous devons exhiber une forme linéaire $\varphi \in E^*$ telle que :
$$\ker\varphi = H.$$
  — Puisque H est un sous-espace de codimension 1, il existe un vecteur $x_0 \notin H$ tel que :
$$E = H \oplus Kx_0.$$
  — Définissons $\varphi \in E^*$ par :
$$\varphi(x_0) = 1, \quad \varphi(x) = 0, \quad \forall x \in H.$$
  — Montrons que φ est bien une forme linéaire :

- Pour $x, y \in E$, on écrit $x = h_1 + \lambda_1 x_0$ et $y = h_2 + \lambda_2 x_0$ avec $h_1, h_2 \in H$.
- Alors :
$$\varphi(x+y) = \varphi(h_1 + h_2 + (\lambda_1 + \lambda_2)x_0).$$
- Comme $h_1, h_2 \in H$, on a $\varphi(h_1) = \varphi(h_2) = 0$, donc :
$$\varphi(x+y) = (\lambda_1 + \lambda_2)\varphi(x_0) = (\lambda_1 + \lambda_2).$$
- D'autre part :
$$\varphi(x) + \varphi(y) = \lambda_1 + \lambda_2.$$
- Donc $\varphi(x+y) = \varphi(x) + \varphi(y)$, ce qui prouve l'additivité.
- La linéarité en général découle du même raisonnement.

- Par construction, nous avons $\ker \varphi = H$, ce qui prouve que tout hyperplan est le noyau d'une forme linéaire non nulle.

- **3. Conclusion**
  - Nous avons montré que :
    (i) Si $\varphi \in E^*$ est une forme linéaire non nulle, alors $\ker \varphi$ est un hyperplan.
    (ii) Réciproquement, tout hyperplan est le noyau d'une forme linéaire non nulle.
  - Ce qui termine la démonstration. □

Propriété

Soit H un hyperplan de E. L'ensemble $H^\perp$ des formes linéaires sur E qui s'annulent sur H est une droite de E^*.

Démonstration : Nous devons prouver que si H est un hyperplan de E, alors l'ensemble :
$$H^\perp = \{\varphi \in E^* \mid \forall x \in H, \varphi(x) = 0\}$$
est une droite de E^*, c'est-à-dire qu'il est un sous-espace vectoriel de dimension 1.

- **1. Définition de $H^\perp$ et rappel des propriétés d'un hyperplan**
  - Un **hyperplan** H de E est un sous-espace vectoriel de E de codimension 1, ce qui signifie que :
$$\dim H = \dim E - 1.$$
  - Par définition de l'orthogonal $H^\perp$, un fonctionnel $\varphi \in E^*$ appartient à $H^\perp$ si et seulement si :
$$\varphi(x) = 0, \quad \forall x \in H.$$
  - Nous devons montrer que $H^\perp$ est un sous-espace vectoriel de E^* de dimension 1.
- **2. Existence d'un élément non nul dans $H^\perp$**
  - Comme H est un hyperplan, il existe un vecteur $x_0 \in E \setminus H$ tel que :
$$E = H \oplus Kx_0.$$
  - Considérons la forme linéaire $\varphi_0 \in E^*$ définie par :
$$\varphi_0(x_0) = 1 \quad \text{et} \quad \varphi_0(x) = 0, \quad \forall x \in H.$$
  - Par construction, φ_0 est non nulle et appartient à $H^\perp$.
- **3. Dimension de $H^\perp$**
  - Nous devons montrer que tout $\varphi \in H^\perp$ est un multiple de φ_0, ce qui prouvera que $H^\perp$ est de dimension 1.
  - Soit $\varphi \in H^\perp$. Par définition, nous avons :
$$\varphi(x) = 0, \quad \forall x \in H.$$
  - Écrivons un vecteur $y \in E$ sous la forme :
$$y = h + \lambda x_0, \quad \text{où } h \in H \text{ et } \lambda \in K.$$

— En appliquant φ à ce vecteur, on obtient :

$$\varphi(y) = \varphi(h + \lambda x_0) = \varphi(h) + \lambda\varphi(x_0).$$

— Or, comme $h \in H$, on sait que $\varphi(h) = 0$, donc :

$$\varphi(y) = \lambda\varphi(x_0).$$

— On en déduit que φ est proportionnelle à φ_0, soit :

$$\varphi = \lambda\varphi_0, \quad \text{pour un certain } \lambda \in K.$$

— Cela montre que $H^\perp$ est de dimension 1.

— **4. Conclusion**

— Nous avons prouvé que $H^\perp$ est engendré par un seul vecteur φ_0, donc :

$$\dim H^\perp = 1.$$

— Ainsi, $H^\perp$ est une droite de E^*, ce qui termine la démonstration. □

Remarque On peut montrer de manière plus générale que si F est un sous-espace de E de codimension finie, alors $F^\perp$ est de dimension égale à cette codimension.

4.3 Transposée

Définition

Soient E et F deux K-espaces vectoriels de dimension quelconque. Soit $u \in \mathcal{L}(E, F)$. Pour tout $f \in F^*$, on a $f \circ u \in E^*$. L'application linéaire $F^* \to E^*$ définie par :

$$f \mapsto f \circ u$$

est appelée application transposée de u et notée ${}^t u$.

Propriété

Soient E et F deux K-espaces vectoriels. Si E et F sont de dimension finie, alors :
(i) $\operatorname{rg} u = \operatorname{rg}({}^t u)$.
(ii) $\operatorname{Im}(u) = (\ker {}^t u)^\perp$.
Et en dimension quelconque :
(iii) $\ker({}^t u) = (\operatorname{Im} u)^\perp$.

Démonstration : Nous devons prouver que pour toute application linéaire $u \in \mathcal{L}(E, F)$, nous avons :
(i) $\operatorname{rg} u = \operatorname{rg}({}^t u)$.
(ii) $\operatorname{Im}(u) = (\ker {}^t u)^\perp$.
(iii) $\ker({}^t u) = (\operatorname{Im} u)^\perp$ (en dimension quelconque).

— **1. Rappel des définitions**

— L'application transposée ${}^t u : F^* \to E^*$ est définie par :

$${}^t u(f) = f \circ u, \quad \forall f \in F^*.$$

— L'image de u est définie comme :

$$\operatorname{Im}(u) = \{u(x) \mid x \in E\}.$$

— Le noyau de u est défini par :

$$\ker u = \{x \in E \mid u(x) = 0\}.$$

— L'orthogonal d'un sous-espace $V \subset E$ est :

$$V^\perp = \{f \in E^* \mid \forall x \in V, f(x) = 0\}.$$

- **2. Preuve de (i) :** rg $u = \mathrm{rg}({}^t u)$
  - Soit $u \in \mathcal{L}(E, F)$.
  - Par le théorème du rang, on a :

$$\dim E = \dim \ker u + \dim \operatorname{Im} u.$$

  - De même, en appliquant ce théorème à l'application transposée ${}^t u$, on obtient :

$$\dim F^* = \dim \ker({}^t u) + \dim \operatorname{Im}({}^t u).$$

  - Il suffit alors d'utiliser l'égalité $\ker({}^t u) = (\operatorname{Im} u)^\perp$ (démontrée plus bas).
  - En dimension finie, on a $\dim(\operatorname{Im} u) + \dim(\operatorname{Im} u)^\perp = \dim F$.
  - Ainsi :

$$\dim \operatorname{Im} u = \dim \operatorname{Im}({}^t u).$$

  - D'où l'égalité :

$$\mathrm{rg}\ u = \mathrm{rg}({}^t u).$$

- **3. Preuve de (ii) :** $\operatorname{Im}(u) = (\ker {}^t u)^\perp$
  - Montrons que $\varphi \in \ker {}^t u$ si et seulement si φ est dans l'orthogonal de $\operatorname{Im} u$.
  - Par définition de ${}^t u$, on a :

$$\ker({}^t u) = \{\varphi \in F^* \mid {}^t u(\varphi) = 0\}.$$

  - Or, par définition de ${}^t u$:

$${}^t u(\varphi)(x) = \varphi(u(x)), \quad \forall x \in E.$$

  - Donc $\varphi \in \ker({}^t u)$ signifie que :

$$\varphi(u(x)) = 0, \quad \forall x \in E.$$

  - Ce qui revient à dire que φ est nul sur $\operatorname{Im} u$, c'est-à-dire :

$$\varphi \in (\operatorname{Im} u)^\perp.$$

  - D'où l'égalité :

$$\ker({}^t u) = (\operatorname{Im} u)^\perp.$$

  - En passant à l'orthogonal dans un espace de dimension finie, on obtient :

$$\operatorname{Im}(u) = (\ker {}^t u)^\perp.$$

- **4. Preuve de (iii) :** $\ker({}^t u) = (\operatorname{Im} u)^\perp$ **en dimension quelconque**
  - En toute dimension, la démonstration de (ii) nous donne déjà que :

$$\ker({}^t u) = (\operatorname{Im} u)^\perp.$$

  - Contrairement au cas de dimension finie, on ne peut pas nécessairement conclure que $\operatorname{Im}(u) = (\ker {}^t u)^\perp$, car l'orthogonal d'un sous-espace n'a pas toujours la même dimension.
  - Ainsi, cette relation reste valable sans restriction de dimension.
- **5. Conclusion**
  - Nous avons montré :
    (i) rg $u = \mathrm{rg}({}^t u)$.
    (ii) $\operatorname{Im}(u) = (\ker {}^t u)^\perp$.
    (iii) $\ker({}^t u) = (\operatorname{Im} u)^\perp$ (en toute dimension).
  - Ce qui termine la démonstration. □

Propriété

Soient E, F, G trois K-espaces vectoriels, $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(F, G)$. Alors :

$${}^t(v \circ u) = {}^t u \circ {}^t v.$$

Démonstration : Nous devons prouver que pour toute composition d'applications linéaires u et v, on a l'égalité :

$$^t(v \circ u) = {}^tu \circ {}^tv.$$

- **1. Définition de l'application transposée**
  - Soit E, F, G trois K-espaces vectoriels.
  - Soient $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(F, G)$.
  - Nous avons la composition $v \circ u$ définie par :
  $$(v \circ u)(x) = v(u(x)), \quad \forall x \in E.$$
  - L'application transposée ${}^tu : F^* \to E^*$ est définie par :
  $${}^tu(f) = f \circ u, \quad \forall f \in F^*.$$
  - De même, ${}^tv : G^* \to F^*$ est définie par :
  $${}^tv(g) = g \circ v, \quad \forall g \in G^*.$$
  - Enfin, l'application transposée de $v \circ u$ est définie par :
  $${}^t(v \circ u) : G^* \to E^* \quad \text{avec} \quad {}^t(v \circ u)(g) = g \circ (v \circ u), \quad \forall g \in G^*.$$
- **2. Calcul de ${}^tu \circ {}^tv$**
  - Prenons $g \in G^*$.
  - Par définition de ${}^tv$, on a :
  $${}^tv(g) = g \circ v.$$
  - Appliquons ensuite ${}^tu$ à ${}^tv(g)$:
  $${}^tu({}^tv(g)) = {}^tu(g \circ v).$$
  - Par définition de ${}^tu$, on a :
  $${}^tu(g \circ v) = (g \circ v) \circ u.$$
  - Par associativité de la composition des applications, on obtient :
  $${}^tu(g \circ v) = g \circ (v \circ u).$$
  - Or, par définition de ${}^t(v \circ u)$, on sait que :
  $${}^t(v \circ u)(g) = g \circ (v \circ u).$$
  - Donc, nous avons bien :
  $${}^t(v \circ u)(g) = {}^tu({}^tv(g)).$$
- **3. Conclusion**
  - L'égalité précédente étant vraie pour tout $g \in G^*$, on en déduit que :
  $${}^t(v \circ u) = {}^tu \circ {}^tv.$$
  - Ce qui achève la démonstration. $\square$

Propriété

Supposons E de dimension finie. Soit $u \in \mathcal{L}(E)$. Un sous-espace F de E est stable par u si et seulement si $F^\perp$ est stable par ${}^tu$.

Démonstration : Nous devons prouver que pour tout sous-espace F de E, celui-ci est stable par u si et seulement si $F^\perp$ est stable par ${}^tu$.

- **Sens direct : si F est stable par u, alors $F^\perp$ est stable par ${}^tu$.**
  - Supposons que F est stable par u, c'est-à-dire que :
  $$u(F) \subset F.$$
  - Par définition de l'orthogonal, nous avons :
  $$F^\perp = \{\varphi \in E^* \mid \forall x \in F, \varphi(x) = 0\}.$$
  - Prenons maintenant $\varphi \in F^\perp$. Nous devons montrer que ${}^tu(\varphi)$ appartient aussi à $F^\perp$.
  - Par définition de l'application transposée :
  $$({}^tu(\varphi))(x) = \varphi(u(x)), \quad \forall x \in E.$$
  - En particulier, si $x \in F$, alors $u(x) \in F$ (par hypothèse de stabilité).
  - Comme $\varphi \in F^\perp$, on sait que $\varphi(u(x)) = 0$.
  - Donc, par définition de ${}^tu$, on obtient :
  $${}^tu(\varphi)(x) = \varphi(u(x)) = 0, \quad \forall x \in F.$$
  - Cela signifie que ${}^tu(\varphi) \in F^\perp$, donc $F^\perp$ est stable par ${}^tu$.
- **Sens réciproque : si $F^\perp$ est stable par ${}^tu$, alors F est stable par u.**
  - Supposons maintenant que $F^\perp$ est stable par ${}^tu$, c'est-à-dire que :
  $${}^tu(F^\perp) \subset F^\perp.$$
  - Nous devons prouver que $u(F) \subset F$.
  - Soit $x \in F$. Nous devons montrer que $u(x) \in F$.
  - Prenons une forme linéaire quelconque $\varphi \in F^\perp$.
  - Par hypothèse de stabilité de $F^\perp$, nous savons que ${}^tu(\varphi) \in F^\perp$.
  - Ainsi, pour tout $x \in F$, on a :
  $$({}^tu(\varphi))(x) = \varphi(u(x)) = 0.$$
  - Cela signifie que pour toute $\varphi \in F^\perp$, on a $\varphi(u(x)) = 0$.
  - Autrement dit, $u(x)$ appartient à $(F^\perp)^\perp$.
  - Or, en dimension finie, on a l'égalité $(F^\perp)^\perp = F$.
  - Donc $u(x) \in F$, ce qui prouve que $u(F) \subset F$, donc F est stable par u.
- **Conclusion :** Nous avons montré que :
  $$F \text{ est stable par } u \quad \Longleftrightarrow \quad F^\perp \text{ est stable par } {}^tu.$$

  Ce qui achève la démonstration. □

Chapitre 5

Déterminants

5.1 Formes multilinéaires

Soit E un $K-$ev.

Définition

Soient $E_1, ..., E_n$ et F des K-ev. Une application f, à valeurs dans F, est dite n-linéaire lorsque $f : E_1 * ... * E_n \to F$ f est linéaire par rapport à chacune de ses variables, c'est-à-dire : $\forall i \in \{1, \dots, n\} \quad \forall x \in E^n \quad \forall y_i \in E \quad \forall \lambda \in K$

$$f(x_1, \dots, x_{i-1}, \lambda x_i + y_i, x_{i+1}, \dots, x_n) = \lambda f(x_1, \dots, x_i, \dots, x_n) + f(x_1, \dots, y_i, \dots, x_n)$$

Lorsque $E_1 = ... = E_n = E$ et $F = K$ f est une forme n-linéaire sur E.

Remarque :

- Une application $f : E_1 * E_2 \to F$ est bilinéaire si : $\forall \lambda \in K \quad \forall (x, y, z) \in E_1 * E_1 * E_2 f(\lambda x + y, z) = \lambda f(x, z) + f(y, z)$ et $\forall \lambda \in K \quad \forall (x, y, z) \in E_1 * E_2 * E_2 f(x, \lambda y + z) = f(x, z) + \lambda f(x, y)$.
- L'ensemble des formes n-linéaire est noté $Ł_n(E, K)$.

Exemples : r

Proposition

$dim_K(L_n(E, K)) = (dim_K(E))^n$.

Définitions

- Une application n-linéaire f est dite symétrique si $\forall i < j \quad f(x_1, \dots, x_{i-1}, \dots, x_j, \dots, xi, x_{j+1}, \dots, x_n) = f(x_1, \dots, x_n)$.
- Une application n-linéaire f est dite antisymétrique si $\forall i < j \quad f(x_1, \dots, x_{i-1}, \dots, x_j, \dots, xi, x_{j+1}, \dots, x_n) = -f(x_1, \dots, x_n)$.
- Une application n-linéaire f est dite alternée si, appliquée à un n-uplet où deux vecteurs sont égaux, elle s'annule, c'est-à-dire si $\forall i < j \quad f(x_1, \dots, x_i, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_n) = 0$.

Propriété

Puisque une permutation $\sigma \in S_n$ est composée de transpositions alors :f est symétrique si et seulement si $\forall \sigma \in S_n f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n)$ f est antisymétrique si et seulement si $\forall \sigma \in S_n f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \epsilon(\sigma) f(x_1, \dots, x_n)$

Proposition

Soient E un K-ev et $f \in L_n(E, K)$ alternée.
Si $(x_1, ..., x_n) \in E^n$ une famille de vecteurs liée alors $f(x_1, ..., x_n) = 0_K$.

5.2 Déterminant d'une famille de vecteurs dans une base

Définition

Soit B base de E, il existe une seule forme n-linéaire alternée sur E prenant la valeur 1 sur B et telle que toute forme n-linéaire dans B est multiple de celle ci. On la note par det_B et on l'appelle déterminant dans la base B.
Soit $x_1, \dots, x_n$ une famille de vecteurs dans B alors leur déterminant s'exprime ainsi :

— $det_B(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) x_{1,\sigma(1)} \dots x_{n,\sigma(n)}$

Démonstration : Soit B une base de E, et soit ω la forme n-linéaire alternée unique définie sur E qui prend la valeur 1 sur la base B. Cela signifie que :

$$\omega(x_1, \dots, x_n) = 1 \quad \text{pour} \quad (x_1, \dots, x_n) \in B.$$

Étant donné que B est une base de E, la forme ω est unique, et toute autre forme n-linéaire sur E est un multiple scalaire de ω.

Maintenant, supposons que $x_1, \dots, x_n$ soient des vecteurs dans B. Nous souhaitons exprimer le déterminant de cet ensemble de vecteurs, noté $\det_B(x_1, \dots, x_n)$, en termes du groupe des permutations S_n.

Le déterminant est défini comme la somme sur toutes les permutations σ des indices $1, \dots, n$, chaque permutation contribuant par un terme. Le signe de chaque permutation σ est donné par $\varepsilon(\sigma)$, qui est égal à $+1$ pour une permutation paire (celle qui peut être obtenue par un nombre pair de transpositions) et -1 pour une permutation impaire.

Le déterminant dans la base B est alors donné par la somme suivante :

$$\det_B(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}.$$

Cette formule découle directement des propriétés de la forme n-linéaire alternée et de la manière dont les permutations interagissent avec la base. Le terme $\varepsilon(\sigma)$ garantit que le déterminant change de signe lorsque deux vecteurs de la famille sont échangés, ce qui reflète la nature alternée de la forme. Ainsi, nous arrivons à la définition du déterminant dans la base B.

En résumé, le déterminant des vecteurs $x_1, \dots, x_n$ est calculé comme la somme sur toutes les permutations des indices, pondérée par le signe de chaque permutation. Cela garantit que le déterminant respecte les propriétés alternées de la forme.

Propriété

Si B et B' sont deux bases de E,
alors pour toute famille $(x_1, \dots, x_n) \in E, det_{B'}(x_1, \dots, x_n) = det_{B'}B.det_B(x_1, \dots, x_n)$ et on a $det_{B'}B.det_B B' = 1$.

Thoérème

Une famille $(x_1, \dots, x_n) \in E$ est base de E $\Leftrightarrow$ pour toute base B de E $det_B(x_1, \dots, x_n) \neq 0 \Leftrightarrow$ pour une base B de E $det_B(x_1, \dots, x_n) \neq 0$.

5.3 Déterminant d'un endomorphisme

Définition

Soit u un endomorphisme de E et $B = (e_1, \ldots, e_n)$ base de E. On appelle déterminant de e $det_B(u(e_1), \ldots, u(e_n))$, il ne dépend pas de la base choisie et on le note $detu$.

Proposition

- Si $u, v \in L(E), det(u \circ v) = detu * detv$.
- $detId_E = 1$.
- Soit $u \in L(E)$,
  $inGl(E) \Leftrightarrow detu \neq 0$, et $(detu)^{-1} = det(u^{-1})$.

5.4 Déterminant d'une matrice carrée

Définition

Soit $A \in M_n(K)$ le déterminant de A est défini par :

$$det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j}$$

avec S_n l'ensemble des permutations de l'ensemble $\{1, ..., n\}$, et $\epsilon(\sigma)$ la signature de la permutation σ.

Remarque On note souvent le déterminant de A sous la forme suivante :

- le déterminant d'une matrice ne change pas de valeur quand on ajoute à une colonne ou une matrice une combinaison linéaire des autres.
- Si A est la matrice d'un endomorphisme alors leurs déterminants sont égaux.

Propriétés

Soient $A, B \in M_n(K)$, on a alors :

- Le déterminant est invariant par transposition : $detA = detA^{\mathrm{T}}$.
- $\forall \lambda \in \mathbf{K}, det(\lambda A) = \lambda^n.det(A)$.
- $det(AB) = detA * detB$.
- Si A et B sont semblables alors $detA = detB$.
- $detA \neq 0 \Leftrightarrow A \in Gl_n(\mathbf{K})$.
- Si $A = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$
  (ie. triangulaire) alors $detA = \prod_{i=1}^{n} a_i$.

Définitions

Soit $A = (a_{i,j})_{i,j \in [|1,n|]} \in M_n(\mathbf{K})$. Pour tout $(i,j) \in [|1,n|]$ on appelle cofacteur de $a_{i,j}$, le scalaire $(-1)^{i+j} detA_{i,j}$ avec $A_{i,j}$ la matrice obtenue de A en éliminant la i-ème ligne et la j-ième colonne.

Remarque On appelle aussi le scalaire $detA_{i,j}$ mineur de l'élément $a_{i,j}$ et mineurs principaux de A les déterminants $det(a_{i,j})_{i,j \in [|1,k|]}$ pour $k \in [|1,n|]$, mais ces définitions sont hors-programme.

Définitions

Soit $A \in M_n(\mathbf{K})$, la matrice des cofacteurs des élements de A s'appelle comatrice de A et est notée $com(A)$.

Proposition

Si $A \in M_n(\mathbf{K})$ alors $com(A).A^{\mathrm{T}} = com(A)^{\mathrm{T}}.A = (detA).I_n$.

Corollaire

Si A est inversible alors $A^{-1} = (1/detA).com(A)^{\mathrm{T}}$.

Remarque Si $A \in M_2(\mathbb{K})$ inversible telle que A=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ alors $A^{-1} = 1/(ad-bc) * \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Propriété-HP

Soit $M \in \mathcal{M}_n(\mathbb{Z})$ (*i.e.* une matrice à coefficients dans $\mathbb{Z}$).

$$(M \text{ est inversible et } M^{-1} \in \mathcal{M}_n(\mathbb{Z})) \Leftrightarrow (\det M = \pm 1).$$

Démonstration :

— $\Rightarrow$ On a $M \in \mathcal{M}_n(\mathbb{Z})$ donc $\det(M) \in \mathbb{Z}$. De même, $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$ donc $\det(M^{-1}) = 1/\det(M) \in \mathbb{Z}$. Ainsi, $\det(M)$ est un entier d'inverse entier, d'où $\det(M) = \pm 1$.

— $\Leftarrow$ On a $M \in \mathcal{M}_n(\mathbb{Z})$ donc les cofacteurs de M sont des entiers, donc la comatrice $\widetilde{M}$ de M vérifie $\widetilde{M} \in \mathcal{M}_n(\mathbb{Z})$. Or $\det(M) = \pm 1$ donc $1/\det(M) \in \mathbb{Z}$. Donc M est inversible et :

$$M^{-1} = \frac{1}{\det(M)} {}^{\mathrm{t}}\widetilde{M} \in \mathcal{M}_n(\mathbb{Z}).$$

5.5 Calcul d'un déterminant

Proposition

Soit $A = (a_{i,j})_{i,j \in [|1,n|]} \in M_n(\mathbf{K})$ avec $A_{i,j}$ les cofacteurs des élements de A, on calcule généralement un déterminant en développant par rapport à la i-ème ligne ou la j-ième colonne selon :

— Développement par rapport à la i-ème ligne :

$$detA \sum_{j=1}^{n} (a_{i,j} A_{i,j}).$$

— Développement par rapport à la i-ème ligne :

$$detA \sum_{i=1}^{n} (a_{i,j} A_{i,j}).$$

5.6 Exemples de calcul de déterminants

5.6.1 Déterminant de Vandermonde

Définition

Soient $x_1, x_2, \ldots, x_n$ des éléments d'un corps commutatif K. Le déterminant de Vandermonde associé à ces éléments est défini par :

$$V(x_1, x_2, \ldots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{vmatrix}$$

Propriété

Soient $x_1, x_2, \ldots, x_n$ des éléments d'un corps commutatif K. Le déterminant de Vandermonde associé à ces éléments est donné par :

$$V(x_1, x_2, \ldots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

Démonstration : On procède par récurrence :

Initialisation $(n = 2)$ **:**

Pour $n = 2$, la matrice est :

$$\begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix} = x_2 - x_1$$

La formule est donc vérifiée.

Hypothèse de récurrence :

Supposons que la formule soit vraie pour une matrice de taille $(n-1) \times (n-1)$, c'est-à-dire :

$$V(x_1, x_2, \ldots, x_{n-1}) = \prod_{1 \leq i < j \leq n-1} (x_j - x_i)$$

Étape de récurrence (passage à n**) :**

Considérons maintenant une matrice de Vandermonde de taille n :

$$V(x_1, \ldots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{vmatrix}$$

Développons ce déterminant selon la dernière colonne. Le déterminant prend la forme :

$$V(x_1, \ldots, x_n) = \sum_{k=1}^{n} (-1)^{n+k} x_k^{n-1} \begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k-1} & \ldots & x_{k-1}^{n-2} \\ 1 & x_{k+1} & \ldots & x_{k+1}^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \ldots & x_n^{n-2} \end{vmatrix}$$

Chaque déterminant de taille $(n-1)$ qui apparaît est lui-même un déterminant de Vandermonde d'ordre inférieur, auquel s'applique l'hypothèse de récurrence. Après factorisation, on obtient finalement :

$$V(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

Ce qui conclut la récurrence et prouve la formule pour tout entier naturel n.

5.6.2 Déterminant circulant

Déterminant circulant

Le déterminant d'une **matrice circulante** est donné par le produit de ses valeurs propres. Pour une matrice circulante C de taille $n \times n$, définie à partir du vecteur $c = (c_0, c_1, \ldots, c_{n-1})$, on a :

$$\det(C) = \prod_{k=0}^{n-1} \lambda_k$$

où λ_k sont les valeurs propres de la matrice circulante, obtenues à partir des coefficients c_j.

Démonstration : Le déterminant d'une matrice circulante peut être obtenu en utilisant des opérations élémentaires sur les lignes, exploitant le fait que chaque ligne est une permutation circulaire de la précédente. En appliquant des combinaisons linéaires successives sur les lignes de la matrice, il est possible de la transformer en une matrice triangulaire.

Après ces manipulations, on obtient l'expression suivante pour le déterminant de C :

$$\det(C) = \prod_{k=0}^{n-1} \left(c_0 + c_1 e^{2i\pi k/n} + c_2 e^{4i\pi k/n} + \cdots + c_{n-1} e^{2i\pi(n-1)k/n} \right).$$

Cette formule montre que le déterminant dépend de la somme pondérée des coefficients c_j avec des puissances de racines de l'unité. La singularité de la matrice est alors caractérisée par l'existence d'un facteur nul dans ce produit.

Ainsi, le déterminant d'une matrice circulante est gouverné par les relations entre ses coefficients, et sa nullité dépend des combinaisons linéaires des c_j.

5.6.3 Déterminant de Cauchy :

Déterminant de Cauchy

Soient $(x_1, x_2, \ldots, x_n)$ et $(y_1, y_2, \ldots, y_n)$ deux familles de nombres complexes distincts deux à deux. Alors, le déterminant de la matrice de Cauchy définie par :

$$C = \left(\frac{1}{x_i - y_j} \right)_{1 \leq i,j \leq n}$$

est donné par :

$$\det(C) = \frac{\displaystyle\prod_{1 \leq i < j \leq n} (x_j - x_i)(y_i - y_j)}{\displaystyle\prod_{i=1}^{n} \prod_{j=1}^{n} (x_i - y_j)}.$$

Démonstration : Considérons le déterminant comme une fonction rationnelle des variables (x_i) et (y_j). On remarque que le déterminant s'annule dès que deux lignes ou deux colonnes sont égales, ce qui se produit précisément lorsque deux x_i ou deux y_j coïncident. Ainsi, le déterminant est divisible par les produits :

$$\prod_{1 \leq i < j \leq n} (x_j - x_i) \quad \text{et} \quad \prod_{1 \leq i < j \leq n} (y_i - y_j).$$

Par ailleurs, le déterminant présente des pôles évidents en les points $x_i = y_j$, avec $1 \leq i, j \leq n$. Ceci implique que le dénominateur doit nécessairement être le produit complet :

$$\prod_{i=1}^{n} \prod_{j=1}^{n} (x_i - y_j).$$

Par conséquent, il existe une constante k telle que :

$$\det(C) = k \frac{\displaystyle\prod_{1 \leq i < j \leq n} (x_j - x_i)(y_i - y_j)}{\displaystyle\prod_{i=1}^{n} \prod_{j=1}^{n} (x_i - y_j)}.$$

Pour déterminer k, évaluons ce déterminant pour une valeur spécifique des variables afin de simplifier les calculs. Prenons par exemple la limite $x_i \to y_i$ pour tout i. Dans ce cas particulier, on retrouve la forme limite et on obtient aisément que $k = 1$.

On en déduit donc finalement la formule explicite du déterminant de Cauchy :

$$\det\left(\frac{1}{x_i - y_j}\right)_{1\le i,j\le n} = \frac{\displaystyle\prod_{1\le i<j\le n} (x_j - x_i)(y_i - y_j)}{\displaystyle\prod_{i=1}^{n}\prod_{j=1}^{n}(x_i - y_j)}.$$

Chapitre 6

Problèmes

6.1 Traces :

6.1.1 Matrice de trace nulle

Matrice de trace nulle

Soit $A \in M_n(\mathbb{R})$ telle que $TrA = 0_R$
1) Montrer que A est semblable à une matrice n'ayant que de 0_R dans sa diagonale.
2) Montrer que $\exists X, Y \in M_n(\mathbb{R})$ tels que $A = XY - YX$

Correction

1) On montre par récurrence sur $n \in \mathbf{N}^*$ la proposition suivante :

P :$\forall n \in \mathbb{N}^*$, Si $A \in M_n(\mathbb{R})$ est de trace nulle alors elle est semblable à une matrice n'ayant que des 0 sur la diagonale principale.

Initialisation : $P(1)$
On a $M = tr(M) = 0_{\mathbf{R}}$.
Hérédité :$P(n-1) \to P(n)$
Supposant que la proposition P est vrai pour le rang n-1 et montrant la pour le rang n.
Soit u un endomorphisme de $\mathbf{R}^n$ dont la matrice dans la base canonique $\mathbb{R}^n$ est notée A. On traitera deux cas :

i) $\forall x \in \mathbb{R}^n$, la famille $(x, u(x))$ est liée.
On a vu donc que u est une homothétie ie : $\exists \lambda \in \mathbb{R}$ tel que $u = \lambda Id_E$ donc $tr(\lambda Id_E) = n\lambda = tr(u) = tr(A) = 0_{\mathbb{R}}$ du coup $\lambda = 0_{\mathbb{R}}$ et donc $u = 0_{L(\mathbb{R}^n)}$, finalement A est la matrice nulle.

ii) $\exists x \in \mathbb{R}^n$ tel que la famille $(x, u(x))$ soit libre. On complète cette famille en base $B = (x, u(x), e_3, \ldots, e_n)$ de $\mathbb{R}^n$, la matrice de u dans cette base est : $[u]_B = \begin{pmatrix} 0 & \ldots\ldots\ldots \\ 1 & N \\ 0 & \end{pmatrix}$
On a $tr(N) = tr([u]_B) = 0_{\mathbb{R}}$, donc d'après l'hypothèse de récurrence $\exists Q \in \mathbb{G}\lessdot_{n-1}(\mathbb{R})$ telle que $Q^{-1}NQ$ n'ait que des zéros sur la diagonale principale. On pose $Q' \in \mathbb{G}\lessdot_n(\mathbb{R})$, telle que $Q' = \begin{pmatrix} 1 & \ldots\ldots\ldots \\ 0 & Q \\ 0 & \end{pmatrix}$
$Q^{-1}[u]_B Q = \begin{pmatrix} 0 & \ldots\ldots\ldots \\ 0 & Q^{-1}NQ \\ 0 & \end{pmatrix}$ et puisque $Q^{-1}NQ$ n'a que des zéros dans sa diagonale principale et puisque A est semblable à $[u]_B$ A est semblable à $Q^{-1}[u]_B Q$, la récurrence étante établie, on a prouvé :

P :$\forall n \in \mathbb{N}^*$, Si $A \in M_n(\mathbb{R})$ est de trace nulle alors elle est semblable à une matrice n'ayant que des 0 sur la diagonale principale.

2) On déduit de la question précedente que $\exists Q \in \mathbb{G}\lessdot_n(\mathbb{R})$ telle que $A = Q^{-1}NQ$ avec $N = (n_{i,j})_{i,j\in[|1,n|]}$ n'ayant que des zéros sur sa diagonale principale.
Posant X'=$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ 0 & x_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & x_n \end{pmatrix} \in \mathbb{M}_n((R)), x_i \neq x_j sii \neq j$
$Y' = (y_{i,j})_{i,j\in[|1,n|]} \in M_n(\mathbb{R}), y_{i,j} = n_{i,j}/(x_i - x_j) sii \neq j$ et $y_{i,i} = 0_{\mathbb{R}}$ sinon.
On a $(X'Y' - Y'X')_{i,j} = n_{i,j}(x_i - x_j)/(x_i - x_j) = n_{i,j} sii \neq j$ et $(X'Y' - Y'X')_{i,j} = 0_{\mathbb{R}}$ sinon, alors $X'Y' - Y'X' = N$ donc $A = (P^{-1}X'P)(P^{-1}Y'P) - (P^{-1}Y'P)(P^{-1}X'P)$
On pose $X = P^{-1}X'P, Y = P^{-1}Y'P$, finalement :

$$\exists X, Y \in \mathbb{M}_n(\mathbb{R}), A = XY - YX.$$

6.1.2 Traces modulo p

Exercice :

Soit p un nombre premier et $A, B \in M_n(\mathbb{Z})$.
1) Montrer que $Tr((A + B)^p) = Tr(A^p) + Tr(B^p)[p$.
2) En déduire que $Tr(A^p) = Tr(A)[p]$.
3) Soit la suite récurrente (u_n) définie par $u_0 = 3, u_1 = 0, u_2 = 2$
$\forall n \in \mathbb{N}, u_{n+3} = u_{n+1} + u_n$.
Montrer p divise u_p.

Correction : 1) Montrer que $\mathrm{Tr}((A + B)^p) = \mathrm{Tr}(A^p) + \mathrm{Tr}(B^p) \pmod p$
La trace est une fonction linéaire, donc $\mathrm{Tr}((A + B)^p)$ peut être développée à l'aide du binôme de Newton. On a :

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

En prenant la trace des deux côtés, on obtient :

$$\mathrm{Tr}((A + B)^p) = \sum_{k=0}^{p} \binom{p}{k} \mathrm{Tr}(A^k B^{p-k}).$$

Ensuite, on utilise la propriété de la trace $\mathrm{Tr}(XY) = \mathrm{Tr}(YX)$, ce qui permet de réécrire chaque terme sous la forme $\mathrm{Tr}(A^k B^{p-k}) = \mathrm{Tr}(A^k)\mathrm{Tr}(B^{p-k})$. Comme p est un nombre premier, tous les termes où $k \neq p$ seront divisibles par p. Cela donne :

$$\mathrm{Tr}((A + B)^p) = \mathrm{Tr}(A^p) + \mathrm{Tr}(B^p) \pmod p.$$

2) En déduire que $\mathrm{Tr}(A^p) = \mathrm{Tr}(A) \pmod p$
En appliquant le résultat précédent avec $B = 0$, on obtient :

$$\mathrm{Tr}(A^p) = \mathrm{Tr}((A + 0)^p) = \mathrm{Tr}(A^p) + \mathrm{Tr}(0^p) \pmod p.$$

Or, $\mathrm{Tr}(0^p) = 0$, donc :

$$\mathrm{Tr}(A^p) = \mathrm{Tr}(A) \pmod p.$$

3) Soit la suite récurrente (u_n) définie par $u_0 = 3$, $u_1 = 0$, $u_2 = 2$, et $u_{n+3} = u_{n+1} + u_n$. Montrer que p divise u_p.

Nous allons utiliser l'induction pour montrer que p divise u_p.

Pour $p = 0$, $u_0 = 3$, donc p divise u_0. Supposons que p divise u_n et u_{n+1}. On a la relation récurrente $u_{n+3} = u_{n+1} + u_n$. Par hypothèse d'induction, p divise u_n et u_{n+1}, donc p divise leur somme, ce qui montre que p divise u_{n+3}.

Par récurrence, on conclut que p divise tous les termes de la suite, y compris u_p.

6.2 Décomposition de Fitting

Exercice :

Soient E un K-espace vectoriel de dimension finie $n \in^*$, et $u \in L(E)$:

1) Montrer que les suites $(Imu^k)_{k\in N}$ et $(Keru^k)_{k\in N}$ sont strictement monotones pour l'inclusion jusqu'un certain rang m d'oû elle deviennent stationnaire.
2) Montrer que la suite $(dim_K Ker(u^{k+1}) - dim_K Ker(u^k))_{k\geq 0}$ est décroissante.
3) Montrer que $E = keru^m \oplus Imu^m$.

Correction : La suite des images est décroissante pour l'inclusion :

$$\operatorname{Im} u \supseteq \operatorname{Im} u^2 \supseteq \operatorname{Im} u^3 \supseteq \dots$$

De même, la suite des noyaux est croissante :

$$\operatorname{Ker} u \subseteq \operatorname{Ker} u^2 \subseteq \operatorname{Ker} u^3 \subseteq \dots$$

Puisque E est de dimension finie, les dimensions des sous-espaces ne peuvent pas croître ou décroître indéfiniment. Par conséquent, il existe un entier m tel que :

$$\operatorname{Im} u^m = \operatorname{Im} u^{m+1} = \operatorname{Im} u^{m+2} = \dots$$

et

$$\operatorname{Ker} u^m = \operatorname{Ker} u^{m+1} = \operatorname{Ker} u^{m+2} = \dots$$

Ces suites deviennent donc stationnaires à partir de ce rang m, appelé l'indice de stabilisation de l'endomorphisme u.

2. (u^k))$_{k\geq 0}$ est décroissante.

D'après le théorème du rang, pour tout entier k :

$$\dim_K E = \dim_K \operatorname{Ker}(u^k) + \dim_K \operatorname{Im}(u^k).$$

Puisque $\operatorname{Im} u^k \supseteq \operatorname{Im} u^{k+1}$, la suite $(\dim_K \operatorname{Im} u^k)_{k\geq 0}$ est décroissante. En conséquence, la suite $(\dim_K \operatorname{Ker} u^k)_{k\geq 0}$ est croissante, et la quantité :

$$\dim_K \operatorname{Ker}(u^{k+1}) - \dim_K \operatorname{Ker}(u^k)$$

diminue avec k. Ainsi, la suite demandée est décroissante.

3.

Montrons d'abord que l'intersection $\operatorname{Ker} u^m \cap \operatorname{Im} u^m$ est réduite à $\{0\}$. Soit $x \in \operatorname{Ker} u^m \cap \operatorname{Im} u^m$. Alors il existe $y \in E$ tel que :

$$x = u^m(y).$$

Or, comme $x \in \operatorname{Ker} u^m$, on a :

$$u^m(x) = u^m(u^m(y)) = 0.$$

Mais par stabilisation, $\operatorname{Im} u^m = \operatorname{Im} u^{2m}$, ce qui implique que u^m est injective sur $\operatorname{Im} u^m$. Ainsi, l'égalité $u^m(x) = 0$ entraîne directement $x = 0$. Donc :

$$\operatorname{Ker} u^m \cap \operatorname{Im} u^m = \{0\}.$$

Montrons maintenant que tout élément de E peut se décomposer sous la forme $x + y$ avec $x \in \operatorname{Ker} u^m$ et $y \in \operatorname{Im} u^m$. Soit $z \in E$. Nous définissons $y = u^m(z)$ et posons $x = z - y$. Alors :

$$u^m(x) = u^m(z - y) = u^m(z) - u^m(y) = u^m(z) - u^m(z) = 0.$$

Donc $x \in \operatorname{Ker} u^m$. Par ailleurs, par construction, $y = u^m(z) \in \operatorname{Im} u^m$.

Ainsi, tout vecteur $z \in E$ s'écrit de manière unique comme la somme d'un élément de $\operatorname{Ker} u^m$ et d'un élément de $\operatorname{Im} u^m$, ce qui établit la somme directe :

$$E = \operatorname{Ker} u^m \oplus \operatorname{Im} u^m.$$

6.3 Identité de Sylvester, Identité de Jacobi

Exercice :

1) Identité de Jacobi : Soit $A \in Gl_n(\mathbb{K})$. On note $T = A^{-1}$ et on considère l'écriture par blocs des matrices A et T :
A=$\begin{pmatrix} B & C \\ S & E \end{pmatrix}$ T=$\begin{pmatrix} W & X \\ Y & Z \end{pmatrix}$ avec $B, W \in M_r(\mathbb{K})$ et $1 \leq r \leq n$.
Montrer que $(det(A))(det(W)) = det(E)$.
2) Soient $I, J \subset \{1, ..., n\}, card(I) = card(J) = r, A = (a_{i,j})_{(i,j) \in [|1,n|]^2} \in \mathbb{M}_n(\mathbb{K})$ On note $A_{I,J} \in M_r(\mathbb{K})$ la matrice extraite de A.
Notons I^*, J^* les complémentaires de I, J das $\{1, ..., n\}$ et $S(I,J) = \sum_{i \in I} i + \sum_{j \in J} j$.
Montrer que :
$(A \in Gl_n(\mathbb{C})$ avec $T = A^{-1}) \Rightarrow ((det(A))(det(T_{J,I})) = (-1)^{S(I,J)}(det(A_{I^*,J^*})))$
3) Identité de Sylvester : Soit $A = (a_{i,j})_{(i,j) \in [|1,n|]^2} \in M_n(\mathbb{K})$, on pose :
$\Gamma_{I,J} = det(com(A))_{I,J}, \Delta_{I,J} = det(A_{I^*,J^*})$.
Montrer que :
$$\Gamma_{I,J} = (-1)^{S(I,J)}.\Delta_{I,J}.(det(A))^{r-1}$$
*

Correction :

1) On a $TA = I_n$, par bloc ca donne :
$$\begin{pmatrix} BW + CY & BX + CZ \\ SW + EY & SX + EZ \end{pmatrix} = \begin{pmatrix} I_r & 0 \\ 0 & I_{n-r} \end{pmatrix}$$
Donc
$$BW + CY = I_r \text{ et } SW + EY = 0$$
Posons
$$N = \begin{pmatrix} W & 0 \\ Y & I_{n-r} \end{pmatrix}$$
On a
$$AN = \begin{pmatrix} B & C \\ S & E \end{pmatrix} \begin{pmatrix} W & 0 \\ Y & I_{n-r} \end{pmatrix} = \begin{pmatrix} BW + CY & C \\ SW + EY & E \end{pmatrix} = \begin{pmatrix} I_r & C \\ 0 & E \end{pmatrix}$$
Et donc en passant par le déterminant :
$$det(AN) = det(A) \cdot det(N) = det(A) \cdot det(W) = det(E)$$

2) L'idée est de réutiliser le résultat précedent, mais cette fois ci on pourrai pas l'appliquer directement car les élements des deux ensembles I, J étant parti de $\{1, \ldots, n\}$ ne garrantissent pas le même ordre ce qui explique la présence du terme $(-1)^{S(I,J)}$.
En effet, notons réspectivement : $(i_k)_{k \leq r}$,$(i'_k)_{k \leq r}$ $(j_{k'})_{k' \leq r}$, $(j'_{k'})_{k' \leq r}$ les éléments de I, J.
On obtient $T_{J,I} = W$ en faisant r permutations sur les lignes de T du type : $\forall 1 \leq k' \leq r, \sigma(j_{k'}) = k'$ et $\forall 1 \leq k' \leq n - r, \sigma(j'_{k'}) = j' + r$ Et d'autres r permutations sur les colonnes du mêmes type.
Avec les permutations faites on aura $E = A_{I^*,J^*}$ et
$$\Pi_{k=1}^r (-1)^{i_k - k} \cdot \Pi_{k'=1}^r (-1)^{j_{k'} - k'} det(A) \cdot det(T_{J,I}) = det(A_{I^*,J^*})$$
Donc
$$det(A) \cdot det(T_{J,I}) = (-1)^{S(I,J)} det(A_{I^*,J^*})$$

3) Si $\det A = 0$, la comatrice de A est de rang 0 ou 1, donc comme $r \geq 2$, on a $\Gamma_{I,J} = 0$, sinon l'égalité :

$$\hat{A} = (\det A)T$$

avec $T = A^{-1}$ montre que

$$(\hat{A})_{I,J} = (\det A)T_{I,J}$$

donc

$$\Gamma_{I,J} = (\det A)^r \det T_{I,J}.$$

On conclue aisément car d'après le résultat de la question $1/b$, on a

$$(\det A) \det T_{J,I} = (-1)^{S(I,J)} \Delta_{I,J}.$$

6.4 Dual de Mn(K)

Exercice :

Si $A \in \mathbb{M}_n(\mathbb{K})$, on note ϕ_A la forme linéaire définie par : $\phi_A : \mathbb{M}_n(\mathbb{K}) \to \mathbb{K}$
$X \mapsto Tr(AX)$
Montrer que $\phi : \mathbb{M}_n(\mathbb{K}) \to \mathbb{M}_n(\mathbb{K})^*$
$A \mapsto \phi_A$
est un isomorphisme.

Correction : On commence par montrer que l'application ϕ est injective.

Soit $A \in \ker \phi$, on rappelle que la base canonique de $M_n(\mathbb{K})$ est $(E_{i,j})$, la matrice ayant que des 0 pour coefficient sauf celui d'indice (i, j) dont la valeur est 1.

On a :

$$\forall (i, j) \in [|1, n|], \phi_A(E_{i,j}) = 0_{M_n(\mathbb{K})}$$

Donc

$$\forall (i, j) \in [|1, n|], tr(AE_{i,j}) = a_{j,i} = 0_{M_n(\mathbb{K})}$$

Donc A est la matrice nulle alors $\ker \phi = \{0_{M_n(\mathbb{K})}\}$, donc ϕ est injective.

Mais alors $dim_{\mathbb{K}}(M_n(\mathbb{K})) = dim_{\mathbb{K}}(M_n(\mathbb{K})^*)$, donc finalement ϕ est bijective et étant une forme linéaire ϕ est un isomorphisme.

6.5 Intersection des hyperplans avec GLn(K)

Exercice :

Soit $n \geq 2$, Montrer que tout hyperplan de $\mathbb{M}_n(\mathbb{K})$ coupe $\mathbb{G}\lessdot_n(\mathbb{K})$ c'est à dire :

$$H \subset \mathbb{M}_n(\mathbb{K}) \Rightarrow \mathbb{G}\lessdot_n(\mathbb{K}) \cap H \neq \varnothing.$$

Correction : Soit H un hyperplan de $M_n(\mathbb{K})$.

$\exists \phi \in M_n(\mathbb{K})^*, H = \ker \phi$ et $\exists A \in M_n(\mathbb{K}), \forall M \in M_n(\mathbb{R}), \phi(M) = tr(AM)$

Puisque $\phi \neq 0_{M_n(\mathbb{K})^*}, A \neq 0_{M_n(\mathbb{K})}$ et donc :

$$H = \ker \phi = \{M \in M_n(R) | tr(AM) = 0_{\mathbb{R}}\}$$

Posons $r = rg(A)$, donc A est équivalente à J_r :

$$\exists P, Q \in Gl_n(\mathbb{K}), PAQ = J_r \text{ avec } J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

(les 0 étant des matrices nulles.) Soit M une matrice inversible n'ayant que des 0 sur sa diagonale, l'écriture par bloc de M s'exprime ainsi :

$$M = \begin{pmatrix} A_r & B_r \\ C_r & D_r \end{pmatrix} \text{ avec } A_r \in M_r(\mathbb{K})$$

On a donc ;

$$J_r M = \begin{pmatrix} A_r & B_r \\ 0 & 0 \end{pmatrix}$$

Donc la matrice $J_r M$ n'a que des 0 dans sa diagonale et donc $tr(J_r M) = 0_R$
On pose $N = QMP \in Gl_n(\mathbb{K})$, on a $M = Q^{-1}NP^{-1}$ et donc :
$tr(AN) = tr(P(AN)P^{-1}) = tr(PAQQ^{-1}NP^{-1})$ et puisque $J_r = PAQ$ finalement :

$$tr(AN) = tr(J_r M) = 0_R$$

Donc il existe $N \in Gl_n(\mathbb{K}), tr(AN) = 0_{\mathbb{R}}$ donc $N \in H$
Finalement puisque H est un hyperplan quelconque de $M_n(\mathbb{K})$, on conclut que tout hyperplan de $M_n(\mathbb{K})$ coupe $Gl_n(\mathbb{K})$.

6.6 Conservation de similitude par passage vers un surcorps

Exercice :

1) Soient$A, B \in M_n(\mathbb{R})$ semblabes sur $\mathbb{C}$.
   Montrer qu'elles sont sembalbes sur $\mathbb{R}$.
2) Cas general :
   Soient $\mathbb{K}$ un corps infini et $\mathbb{L}$ une extension de $\mathbb{K}$.
   Montrer que si $A, B \in M_n(\mathbb{K})$ semblabes sur $\mathbb{L}$, alors elles sont sembalbes sur $\mathbb{K}$.

Correction :

— On suppose que $A, B \in M_n(\mathbb{R})$ sont semblables sur $\mathbb{C}$, c'est-à-dire qu'il existe une matrice inversible $P \in GL_n(\mathbb{C})$ telle que :
$$A = P^{-1}BP.$$
On écrit P sous la forme :
$$P = P_1 + iP_2, \quad P_1, P_2 \in M_n(\mathbb{R}).$$
En séparant les parties réelles et imaginaires, on obtient les relations :
$$P_1 A = BP_1, \quad P_2 A = BP_2.$$
On définit le polynôme :
$$\varphi(X) = \det(P_1 + XP_2) \in \mathbb{R}[X].$$
Comme $\varphi(0) = \det(P_1) \neq 0$, il existe $x \in \mathbb{R}$ tel que $\varphi(x) \neq 0$.
On pose :
$$Q = P_1 + xP_2.$$
Alors Q est inversible et satisfait :
$$QA = BQ.$$
Finalement :

$$\boxed{A \text{ et } B \text{ sont semblables sur } \mathbb{R}.}$$

— On suppose que $A, B \in M_n(\mathbb{K})$ sont semblables sur L, c'est-à-dire qu'il existe une matrice $P \in GL_n(L)$ telle que :
$$A = P^{-1}BP.$$
On écrit les coefficients de P dans une base de L sur $\mathbb{K}$. Soit :
$$P = (p_{ij})_{1\leq i,j\leq n}, \quad p_{ij} \in L.$$
On exprime chaque p_{ij} dans une base $(e_1, \dots, e_m)$ de L sur $\mathbb{K}$:
$$p_{ij} = \sum_{k=1}^{m} p_{ij}^{(k)} e_k, \quad p_{ij}^{(k)} \in K.$$
On définit alors les matrices :
$$P_k = (p_{ij}^{(k)}) \in M_n(\mathbb{K}),$$
et on réécrit P comme :
$$P = \sum_{k=1}^{m} e_k P_k.$$
On considère le polynôme déterminant :
$$F(X_1, \dots, X_m) = \det(X_1P_1 + \cdots + X_mP_m) \in K[X_1, \dots, X_m].$$
Ce polynôme n'est pas identiquement nul car $\det(P) \neq 0$.
Puisque $\mathbb{K}$ est un corps infini, il existe $(x_1, \dots, x_m)$ dans $\mathbb{K}^m$ telle que :
$$F(x_1, \dots, x_m) \neq 0.$$
On définit :
$$Q = x_1P_1 + \cdots + x_mP_m \in M_n(\mathbb{K}).$$
On vérifie que :
$$QA = BQ.$$
De plus, Q est inversible car $\det(Q) \neq 0$.
Finalement :

$$\boxed{A \text{ et } B \text{ sont semblables sur } \mathbb{K}.}$$

6.7 Stabilisation du GLn(K)

Exercice

Soit $A \in M_n(\mathbb{C})$ et $\phi \in \mathbb{L}(M_n(\mathbb{C})$ tel que : $(A \in \mathbb{G}\lessdot_n(\mathbb{C})) \Rightarrow (\phi(A) \in \mathbb{G}\lessdot_n(\mathbb{C}))$

1) Montrer que : $(A \in \mathbb{G}\lessdot_n(\mathbb{C})) \Leftrightarrow (\exists P \in \mathbb{G}\lessdot_n(\mathbb{C}), \forall \lambda \in \mathbb{C}, P - \lambda.A \in \mathbb{G}\lessdot_n(\mathbb{C}))$
2) Montrer que $(\phi(A) \in \mathbb{G}\lessdot_n(\mathbb{C}))\Rightarrow (A \in \mathbb{G}\lessdot_n(\mathbb{C}))$

Correction :

— $\Rightarrow$ Supposons que M est non inversible. Si $r = \text{rg}(M)$, on sait que M est équivalente à la matrice :
$$K_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$
Il existe donc $A, B \in GL_n(\mathbb{C})$ tels que :
$$M = AK_rB.$$
Posons la matrice
$$J = \begin{pmatrix} I_{n-1} & 0 \\ 1 & 0 \end{pmatrix} \in GL_n(\mathbb{C}).$$

Pour tout $\lambda \in \mathbb{C}$, on a :

$$J - \lambda K_r = \begin{pmatrix} -\lambda & 0 & \cdots & 0 \\ 0 & -\lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

En ajoutant les lignes de l'identité, on voit que le rang ne change pas, donc $\mathrm{rg}(J - \lambda K_r) = \mathrm{rg}\, J = n$. Ainsi, $J - \lambda K_r \in GL_n(\mathbb{C})$ et donc :

$$A(J - \lambda K_r)B = P - \lambda M \in GL_n(\mathbb{C}).$$

$\Leftarrow$ Supposons que M est inversible mais que $P - \lambda M$ est inversible pour tout $\lambda \in \mathbb{C}$. On a alors :

$$\forall \lambda \in \mathbb{C}, \quad \det(P - \lambda M) = (\det M)(\det(Q - \lambda I_n)) \neq 0.$$

Mais $\det(Q - \lambda I_n)$ est un polynôme de degré n en λ, qui doit donc s'annuler pour au moins une valeur de λ. Cette contradiction montre que notre hypothèse est fausse, d'où la condition suffisante.

Soit φ un endomorphisme de $M_n(\mathbb{C})$ tel que :

$$\forall M \in GL_n(\mathbb{C}), \quad \varphi(M) \in GL_n(\mathbb{C}).$$

— Raisonnons par l'absurde. Supposons que $M \notin GL_n(\mathbb{C})$, c'est-à-dire que M est singulière ($\det M = 0$). Par hypothèse, $\varphi(M) \in GL_n(\mathbb{C})$, donc $\varphi(M)$ est inversible.
Or, si M est singulière, alors son image par un morphisme linéaire conserve sa structure de rang. Ce qui impliquerait que $\varphi(M)$ est aussi singulière, ce qui contredit le fait que $\varphi(M) \in GL_n(\mathbb{C})$.
Finalement, M doit être inversible, d'où $M \in GL_n(\mathbb{C})$.

6.8 Formule de Burnside

Exercice :

1. Soit V un espace vectoriel complexe de dimension finie $m \geq 1$, et soit H un sous-groupe fini de $\mathrm{GL}(V)$. On définit le sous-espace des points fixes sous l'action de H par :

$$V^H = \{v \in V \mid \forall h \in H,\ h(v) = v\}.$$

Montrer que

$$\dim V^H = \frac{1}{|H|} \sum_{h \in H} \mathrm{Tr}(h).$$

2. Soit H un sous-groupe de S_m. Pour tout $h \in H$, notons $\mathrm{Fix}(h)$ le nombre d'éléments de $\{1, \ldots, m\}$ laissés invariants par h. Soit t le nombre d'orbites de l'action de H sur $\{1, \ldots, m\}$. Déduire de la question précédente que :

$$t = \frac{1}{|H|} \sum_{h \in H} \mathrm{Fix}(h).$$

3. Donner une démonstration directe de la formule obtenue à la question 2 en comptant de deux manières différentes un certain ensemble.

Correction : 1. Définissons l'opérateur

$$P = \frac{1}{|H|} \sum_{h \in H} h.$$

On remarque que, pour tout $h \in H$, on a $hP = P$, ce qui implique que P commute avec chaque h.

En appliquant P à un vecteur $v \in V$, on obtient :

$$Pv = \frac{1}{|H|} \sum_{h \in H} h(v).$$

Si v appartient à V^H, alors pour tout $h \in H$, $h(v) = v$, d'où $Pv = v$. Réciproquement, si $Pv = v$, alors pour tout $h \in H$,

$$h(v) = h(Pv) = Pv = v.$$

Ainsi, V^H est exactement l'image de P, ce qui signifie que P est un projecteur sur V^H.

Or, en caractéristique nulle (ce qui est le cas ici), la trace d'un projecteur est égale à sa dimension. La trace de P est donc donnée par :

$$\mathrm{Tr}(P) = \frac{1}{|H|} \sum_{h \in H} \mathrm{Tr}(h),$$

ce qui prouve la formule demandée.

2. Identifions H à un sous-groupe de $\mathrm{GL}_m(\mathbb{C})$ en considérant les matrices de permutation associées : pour chaque $h \in H$, on définit la matrice M_h dont les coefficients sont $(M_h)_{i,j} = \delta_{i,h(j)}$, où δ est le symbole de Kronecker.

On vérifie que l'application $h \mapsto M_h$ est un morphisme de groupes injectif de H dans $\mathrm{GL}_m(\mathbb{C})$, ce qui permet d'identifier H à un sous-groupe de matrices de permutation. Par ailleurs, le nombre de points fixes de h, noté $\mathrm{Fix}(h)$, est précisément la trace de M_h, c'est-à-dire le nombre de 1 sur la diagonale.

L'application du résultat précédent donne alors :

$$\dim V^H = \frac{1}{|H|} \sum_{h \in H} \mathrm{Tr}(M_h) = \frac{1}{|H|} \sum_{h \in H} \mathrm{Fix}(h).$$

Il reste à montrer que cette dimension est égale au nombre t d'orbites de l'action de H sur $\{1, \ldots, m\}$.

Notons $\{O_1, \ldots, O_t\}$ les orbites de cette action et définissons pour chaque k l'espace vectoriel engendré par les vecteurs e_i associés aux indices i de l'orbite O_k :

$$W_k = \mathrm{Vect}(e_i)_{i \in O_k}.$$

Ces sous-espaces sont globalement stables par H et forment une décomposition directe de $\mathbb{C}^m$:

$$\mathbb{C}^m = W_1 \oplus \cdots \oplus W_t.$$

On montre alors que V^H est la somme directe des sous-espaces invariants $V^H \cap W_k$, chacun de dimension 1, ce qui prouve que $\dim V^H = t$.

3. Pour obtenir une preuve directe, comptons de deux manières différentes la taille de l'ensemble

$$A = \{(h, i) \in H \times \{1, \ldots, m\} \mid h(i) = i\}.$$

D'une part, en sommant selon H, on obtient :

$$|A| = \sum_{h \in H} \mathrm{Fix}(h).$$

D'autre part, en sommant selon les éléments de $\{1, \ldots, m\}$, on obtient :

$$|A| = \sum_{i=1}^{m} |H_i|,$$

où H_i est le stabilisateur de i sous l'action de H.

Or, en regroupant selon les orbites $O_1, \ldots, O_t$, on a :

$$\sum_{i=1}^{m} |H_i| = \sum_{k=1}^{t} \sum_{i \in O_k} |H_i|.$$

Comme H_i a toujours la même taille pour tous les éléments d'une orbite donnée, on obtient :

$$\sum_{i \in O_k} |H_i| = |O_k| \cdot |H_i| = |H|.$$

Ainsi, en sommant sur toutes les orbites :

$$|A| = \sum_{k=1}^{t} |H| = t|H|.$$

En comparant avec la première expression de $|A|$, on conclut :

$$t = \frac{1}{|H|} \sum_{h \in H} \mathrm{Fix}(h).$$

$\triangleleft$

6.9 Famille strictement positive engendrant l'espace :

Problème :

Soit V un espace vectoriel réel de dimension $d \geq 1$, et considérons une famille de vecteurs $\mathcal{G} = (v_1, v_2, \ldots, v_m)$ dans V qui est extbfstrictement positive engendrant, c'est-à-dire que pour tout $y \in V$, il existe des scalaires $\alpha_1, \ldots, \alpha_m \in \mathbb{R}_+^*$ tels que :

$$y = \alpha_1 v_1 + \cdots + \alpha_m v_m.$$

1. Montrer que $m \geq d+1$. Trouver un exemple de famille strictement positive engendrant l'espace avec $m = d+1$.
2. Supposons que $m \geq 2d+1$. Montrer qu'il est possible d'extraire de $\mathcal{G}$ une sous-famille propre qui reste strictement positive engendrant. Donner un exemple de famille ayant exactement $2d+1$ éléments et telle qu'aucune de ses sous-familles propres ne possède cette propriété.

Correction : 1. Puisque $\mathcal{G}$ engendre l'espace, on a immédiatement $m \geq d$. Si l'on suppose que $m = d$, alors $\mathcal{G}$ forme une base de V. Cependant, dans ce cas, le vecteur opposé à l'un des éléments de la base, par exemple $-v_1$, ne peut pas être écrit comme une combinaison des v_i avec des coefficients strictement positifs, ce qui est en contradiction avec notre hypothèse. Ainsi, il est nécessaire que $m \geq d+1$.

Prenons une base $(w_1, \ldots, w_d)$ de V et considérons la famille $\mathcal{H} = (w_1, \ldots, w_d, -w_1 - \cdots - w_d)$. Montrons qu'elle est strictement positive engendrant.

Pour tout élément $y \in V$, on peut écrire y sous la forme $y = \beta_1 w_1 + \cdots + \beta_d w_d$. En ajoutant un paramètre positif s, on obtient :

$$y = (\beta_1 + s)w_1 + \cdots + (\beta_d + s)w_d + s(-w_1 - \cdots - w_d).$$

En choisissant s suffisamment grand, tous les coefficients deviennent strictement positifs, prouvant que $\mathcal{H}$ satisfait la propriété demandée.

Un raisonnement similaire montre que si une famille $\{w_1, \ldots, w_m\}$ satisfait une relation du type :

$$\gamma_1 w_1 + \cdots + \gamma_m w_m = 0,$$

avec tous les γ_i strictement positifs, alors cette famille est strictement positive engendrant.

2. Comme la famille $\mathcal{G}$ possède au moins $2d+1$ vecteurs, on sait qu'il existe un sous-ensemble $I \subseteq \{1, \ldots, m\}$ de taille d tel que $\{v_i\}_{i \in I}$ forme une base de V. Considérons le complémentaire $J = \{1, \ldots, m\} \setminus I$. Comme $|J| \geq d+1$, la famille $\{v_j\}_{j \in J}$ est nécessairement liée, ce qui signifie qu'il existe des coefficients δ_j non tous nuls tels que :

$$\sum_{j \in J} \delta_j v_j = 0.$$

Par l'hypothèse de positivité, on peut écrire tout vecteur de V sous la forme :

$$y = \sum_{i \in I} \mu_i v_i + \mu_s v_s,$$

avec $\mu_i, \mu_s > 0$. En ajoutant un paramètre r, on obtient :

$$\sum_{i \in I} \mu_i v_i + \sum_{j \in J} (\mu_j + r\delta_j) v_j = 0.$$

En choisissant r de façon appropriée (par exemple $r = \frac{\mu_s}{\delta_k}$ pour un certain $k \in J$ avec $\delta_k \neq 0$ et un quotient minimal), on obtient une sous-famille de $\mathcal{G}$ qui reste strictement positive engendrant.

On peut ainsi réduire progressivement la taille de la famille sans perdre la propriété d'engendrement strictement positif, jusqu'à ce qu'on atteigne une taille minimale. Lorsque $m = 2d+1$, il existe des configurations où aucune sous-famille plus petite ne possède cette propriété, par exemple en choisissant des vecteurs tels que chaque sous-ensemble strict perde la capacité d'engendrer l'espace de manière strictement positive.

Chapitre 7

Réduction des endomorphismes et matrice carrées

7.1 Généralités :

7.1.1 Elements propres d'un endomorphisme et de matrice carrée

Cas d'endomorphisme :

Soient K un corps, E un K-espace vectoriel et u un endomorphisme de $L(E)$.

Définition

Soit $\lambda \in K$, on dit que λ est une valeur propre de u si $\exists x \in E \setminus \{0_E\}$ tel que : $u(x) = \lambda x$ ce qui est équivalent aux assetions suivantes :

i) $ker(u - \lambda.Id_E) \neq \{0_E\}$.

ii) $u - \lambda.Id_E$ n'est pas injective.

iii) $u - \lambda.Id_E$ n'est pas inversible (Seulement si E est de dimension finie).

L'ensemble des valeurs propres d'un endomorphisme s'appelle son spectre et il dépend du corps de base de l'espace vectoriel ainsi on note :

$$\boxed{Sp_K(u) = \{\lambda \in K | \exists x \in E \setminus \{0_E\}, u(x) = \lambda.x\}}$$

Définition

Soit $x \in E \setminus \{0_E\}$, on dit que x est une valeur propre de u si $\exists \lambda \in K$ tel que : $u(x) = \lambda x$

Remarque :

— Une valeur propre peut être nulle.
— Un vecteur propre ne peut jamais être nul.

Définition

Si λ est une valeur propre, on appelle sous-espace propre : l'ensemble des vecteurs propres associées à cette valeur qu'on note $E_\lambda(u)$ ainsi on a :

$$\boxed{E_\lambda(u) = ker(u - \lambda.Id_E)}$$

Cas d'une matrice carrée :

Définitions

Toutes les définitions précédentes s'étend pour les matrices carrées en considérant, pour une matrice $A \in \mathrm{M}_n(K)$ l'endomorphisme : $\varphi_A : K^n \to K^n,\ X \mapsto AX$. c'est à dire :

— $\lambda \in K$ est une valeur propre de u si $\exists X \in K^n \setminus \{0_{K^n}\}$ tel que : $AX = \lambda X$ ce qui est équivalent à $ker(A - \lambda.I_n) \neq \{0_{K^n}\} cequiestaussiéquivalentàrg(A - \lambda \cdot I_n) < n$

— $X \in K^n \setminus \{0_{K^n}\}$ est une valeur propre de A si $\exists \lambda \in K$ tel que : $AX = \lambda X$.

— $E_\lambda(A) = ker(A - \lambda.I_n)$ est le sous-espace propre associé à la valeur propre λ.

Théorème

Soit $k \in \mathbb{N}^*$ si $\lambda_1, ..., \lambda_k$ des valeurs propres distincts deux à deux d'un endomorphisme u alors les sous-espaces propres $E_{\lambda_1}, ..., E_{\lambda_k}$ sont en somme directe.

Démonstration : Soient $(x_i)_{1 \leq i \leq k} \in E^k$ tels que $\forall i \in [|1, k|], x_i \in E_{\lambda_i}$ et $\sum_{i=1}^k x_i = 0_E$
Pour chaque j de [—1,k—] on va appliquer la composée des endomorphismes $(u - \lambda_i ide)$ avec $i \in [|1, k|], i \neq j$
Puique $\forall i \in [|1, k|], i \neq j, u(x_i) = \lambda_i x_i$ donc $\forall i \in [|1, k|], i \neq j, (u - \lambda_i ide)(x_i) = 0_E$
Donc on aura :

$$(u - \lambda_i ide)(\sum_{i=1, i\neq j}^{k} x_i) = \sum_{i=1, i\neq j}^{k} (u - \lambda_i ide)(x_i) = \lambda_j x_j = (u - \lambda_i ide)(0_E) = 0_E$$

Donc :

$$\lambda_j x_j = 0_E$$

Quitte à perdre de généralité on considère que toutes les valeurs propres sont non nulles alors,

$$\forall j \in [|1, k|], x_j = 0_E$$

Et donc on a montré que :

$$\text{Si } (x_i)_{1 \leq i \leq k} \in E^k \text{ tels que } \forall i \in [|1, k|], x_i \in E_{\lambda_i} \text{et} \sum_{i=1}^{k} x_i = 0_E, \text{ alors } \forall j \in [|1, k|], x_j = 0_E$$

Finalement, les espaces $E_{\lambda_1}, ..., E_{\lambda_k}$ sont en somme directe.

Proposition

Si E est un $\mathbb{K}$-espace vectoriel de dimension finie $n \in K^*$ alors si u est un endomorphisme de E, il admet au plus n valeurs propres.

Démonstration : Soient $\lambda_1, \ldots, \lambda_k$ des valeurs propres distinctes de u. À chaque λ_i est associé son sous-espace propre :

$$E_{\lambda_i} = \{v \in E \mid u(v) = \lambda_i v\}.$$

On sait que si $\lambda_1, \ldots, \lambda_k$ sont distinctes, alors leurs sous-espaces propres sont en somme directe :

$$E_{\lambda_1} \oplus E_{\lambda_2} \oplus \cdots \oplus E_{\lambda_k} \subseteq E.$$

En prenant les dimensions, on obtient :

$$\dim(E_{\lambda_1}) + \dim(E_{\lambda_2}) + \cdots + \dim(E_{\lambda_k}) \leq \dim(E) = n.$$

Or, chaque E_{λ_i} contient au moins un vecteur non nul, donc $\dim(E_{\lambda_i}) \geq 1$, ce qui implique :

$$k \leq n.$$

Ainsi, u admet au plus n valeurs propres distinctes.

7.1.2 Polynome caractéristique

Depuis maintenant, on considera que E est un espace vectoriel de dimension $n \in \mathbb{N}^*$

Définition

Soit $A \in M_n(\mathbb{K})$, on appelle polynôme caractéristique de A , le polynôme noté χ_A définit par :

$$\boxed{\chi_A(X) = det(A - X.I_n)}$$

Définition

Soit $u \in L(E)$, on appelle polynôme caractéristique de u , le polynôme caractéristique de sa matrice dans une base quelconque de E, et on le note χ_u.

Remarque : Par convention, le polynôme caractéristique est unitaire.

Proposition

Soit $A \in M_n(\mathbb{K})$, alors $\chi_A = \chi_A^{\intercal}$

Proposition

Deux matrices semblables ont le même polynôme caractéristique.

Démonstration : Soient A, B deux matrices carrées d'ordre n à coefficients dans un corps $\mathbb{K}$. On dit que A et B sont *semblables* s'il existe une matrice inversible P telle que :

$$B = P^{-1}AP.$$

Le *polynôme caractéristique* d'une matrice M est défini par :

$$\chi_M(X) = \det(XI - M),$$

où I est la matrice identité de taille n.
Nous devons montrer que :

$$\chi_A(X) = \chi_B(X).$$

Calcul du polynôme caractéristique de B :

$$\chi_B(X) = \det(XI - B).$$

En remplaçant $B = P^{-1}AP$, on obtient :

$$\chi_B(X) = \det(XI - P^{-1}AP).$$

Factorisons P^{-1} :

$$\chi_B(X) = \det(P^{-1}(XI - A)P).$$

En utilisant la propriété du déterminant $\det(P^{-1}MP) = \det(M)$ pour toute matrice M, on en déduit :

$$\chi_B(X) = \det(XI - A).$$

Donc,

$$\chi_B(X) = \chi_A(X).$$

Remarque : Cette propriété s'appelle l'invariance par similitude.

□

Proposition

Soit $u \in L(E)$, on a :

$$(\lambda \text{ valeur propre de } u) \Leftrightarrow (\chi_u(\lambda) = 0_K)$$

Définition

Soit $u \in L(E)$ et $\lambda \in Sp_K(u)$, on appelle multiplicité de λ sa multiplicité en tant que racine du polynôme caractéristique de u et on la note par m_λ.

Proposition

Soit $u \in L(E)$ et $\lambda \in Sp_K(u)$ on a :

$$dim_K(E_\lambda) \leq m_\lambda.$$

7.1.3 Diagonalisation

Définition

Soit $u \in L(E)$, u est diagonalisable s'il existe une base de E composée seulement de vecteurs propres de u.
Dans une telle base, sa matrice est diagonale d'oû la définition suivante :
Un endomorphisme est diagonalisable si sa matrice est semblable à une matrice diagonale.

Définition

Une matrice $A \in M_n(K)$ est diagonalisable si elle est semblable à une matrice diagonale c'est à dire si :

$$\boxed{\exists P \in Gl_n(K), \exists \Lambda = diag(\lambda_1, ..., \lambda n) \in M_n(K), A = P\Lambda P^{-1}.}$$

Conditions de diagonalisabilité

Soit $u \in L(E)$, avec $r = card(Sp_K(u)), Sp_K(u) = \{\lambda_1, ..., \lambda_r\}$. Conditions nécessaires de diagonalisabilité :
Les assertions suivantes sont équivalentes :

i) u est diagonalisable.
ii) χ_u est scindé et $\forall i \in [|1, r|]\lambda_i$, $m_{\lambda_i} = dim_K(E_{\lambda_i})$.
iii) $E = \bigoplus_{i \in [|1,r|]} E_{\lambda_i}$

Conditions suffisantes de diagonalisabilité :
Les assertions suivantes sont équivalentes :

i) $r = dim_K(E)$.
ii) χ_u est scindé et à racines simples.
iii) les valeurs propres de u sont distinctes deux à deux.

Dans le cas oû une des assertions ci-dessus est verifié alors u est diagonalisable.

Démonstration :

i) $\Rightarrow$ ii) Si u est diagonalisable, il existe une base de E formée de vecteurs propres. Dans ce cas, u est représenté par une matrice diagonale, donc son polynôme caractéristique est scindé. De plus, la dimension de chaque sous-espace propre E_{λ_i} est égale à la multiplicité algébrique m_{λ_i}, d'où la deuxième assertion.

ii) $\Rightarrow$ iii) Réciproquement, si χ_u est scindé et que chaque $m_{\lambda_i} = \dim(E_{\lambda_i})$, alors la somme des sous-espaces propres est directe et engendre E :

$$\sum_{i=1}^{r} \dim(E_{\lambda_i}) = \sum_{i=1}^{r} m_{\lambda_i} = n.$$

Ainsi, $E = \bigoplus_{i=1}^{r} E_{\lambda_i}$, ce qui prouve la diagonalisabilité.

iii) $\Rightarrow$ i) Si $r = \dim(E)$, alors chaque valeur propre possède au moins un vecteur propre et leurs sous-espaces propres sont en somme directe. Cela fournit une base de E constituée de vecteurs propres, donc u est diagonalisable.

Maintenant pour les conditions suffisantes de diagonalisabilité :

i) Soient $\lambda_1, \ldots, \lambda_r$ les valeurs propres distinctes de u et leurs sous-espaces propres associés :

$$E_{\lambda_i} = \{v \in E \mid u(v) = \lambda_i v\}.$$

Les sous-espaces propres E_{λ_i} sont en somme directe :

$$E_{\lambda_1} \oplus E_{\lambda_2} \oplus \cdots \oplus E_{\lambda_r} \subseteq E.$$

En prenant les dimensions :

$$\sum_{i=1}^{r} \dim(E_{\lambda_i}) \leq \dim(E) = n.$$

Chaque sous-espace propre E_{λ_i} contient au moins un vecteur propre non nul, donc $\dim(E_{\lambda_i}) \geq 1$. Puisque $r = n$, on obtient :

$$\sum_{i=1}^{r} \dim(E_{\lambda_i}) = n.$$

Ainsi,

$$E = \bigoplus_{i=1}^{r} E_{\lambda_i}.$$

Cela signifie que E possède une base formée de vecteurs propres, donc u est diagonalisable.

□

ii) Si χ_u est scindé et à racines simples, alors chaque E_{λ_i} est de dimension 1. La somme de ces espaces propres engendre E, assurant ainsi la diagonalisabilité.

iii) Si toutes les valeurs propres sont distinctes, alors χ_u est scindé à racines simples, ce qui implique la diagonalisabilité par le raisonnement précédent.

□

Proposition

Si $u \in \mathbb{L}(E)$ est diagonalisable et F un sous-espace vectoriel de E stable par u alors $u_{|F}$ est diagonalisable.

Démonstration : Puisque u est diagonalisable, il existe une base de E formée de vecteurs propres de u. Autrement dit, on peut écrire :

$$E = \bigoplus_{\lambda \in Sp(u)} E_\lambda,$$

où E_λ est le sous-espace propre associé à la valeur propre λ :

$$E_\lambda = \{v \in E \mid u(v) = \lambda v\}.$$

Étant donné que F est stable par u, cela signifie que pour tout $v \in F$, on a $u(v) \in F$. Prenons un vecteur $v \in F$, qui peut s'écrire comme somme de vecteurs propres :

$$v = v_1 + v_2 + \cdots + v_k, \quad \text{avec } v_i \in E_{\lambda_i}.$$

En appliquant u :

$$u(v) = u(v_1) + u(v_2) + \cdots + u(v_k) = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k.$$

Comme $u(v) \in F$, chaque v_i appartient aussi à F, ce qui implique que :

$$F = \bigoplus_{\lambda \in Sp(u)} (F \cap E_\lambda).$$

Cela signifie que F est engendré par des vecteurs propres de u, donc la restriction $u|_F$ possède une base formée de vecteurs propres. Ainsi, $u|_F$ est diagonalisable.

□

Proposition-HP **Lemme**

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$ de rang 1.

$$\text{u est diagonalisable} \Leftrightarrow tr(u) \neq 0_{\mathbb{K}}.$$

Démonstration :

— $\Rightarrow$ Supposant que u est diagonalisable.
u étant de rang 1, on aura $dim_{\mathbb{K}} \ker u = dim_{\mathbb{K}}(E) - 1$, son polynôme caractéristique est $_u = (X - \lambda)X^{dim_{\mathbb{K}}(E)-1}$ avec λ sa valeur propre.
La trace de u étant la somme des valeurs propres de u verifie : $tr(u) = \lambda$, si $tr(u) = 0_{\mathbb{K}}$, en notant la multiplicité de $0_{\mathbb{K}}$ par $m_{0_{\mathbb{K}}}$, on a :

$$m_{0_{\mathbb{K}}} = dim_{\mathbb{K}}(E) > dim_{\mathbb{K}}(E_{0_{\mathbb{K}}}) = dim_{\mathbb{K}} \ker u = dim_{\mathbb{K}}(E) - 1$$

Ce qui est absurde puisque u est diagonalisable donc :

$$u \text{ est diagonalisable } \Rightarrow tr(u) \neq 0_{\mathbb{K}}.$$

— $\Leftarrow$ Supposant que $tr(u) \neq 0_{\mathbb{K}}$.
u étant de rang 1, on a $dim_{\mathbb{K}} \ker u = dim_{\mathbb{K}}(E) - 1$, donc $0_{\mathbb{K}}$ est valeur propre de u d'ordre $dim_{\mathbb{K}}(E) - 1$, il en reste qu'une valeur propre qu'on note λ.
Puisque $tr(u) \neq 0_K$ alors $\lambda \neq 0_K$ et donc en notant $_u$ le polynôme caractéristique de u, on a $_u = (X - \lambda)X^{dim_{\mathbb{K}}(E)-1}$ qui est scindé avec

$$dim_{\mathbb{K}}(E_{0_{\mathbb{K}}}) = dim_{\mathbb{K}}(\ker u) = dim_{\mathbb{K}}(E) - 1 \text{ et } dim_{\mathbb{K}}(\ker(u - \lambda.ide)) = 1$$

et donc :

$$tr(u) \neq 0_{\mathbb{K}} \Rightarrow uestdiagonalisable$$

Finalement, on a :

$$\boxed{u \text{ est diagonalisable } \Leftrightarrow tr(u) \neq 0_{\mathbb{K}}.}$$

7.1.4 Trigonalisation

Définition

Soit $u \in L(E)$, u est trigonalisable s'il existe une base dans laquelle sa matrice est triangulaire supérieure.

Définition

Soit $A \in M_n(K)$, A est trigonalisable si elle est semblable à une matrice triangulaire supérieure c'est à dire si :

Proposition

Soit $u \in L(E)$(resp $A \in M_n(K)$), u (resp A) est diagonalisable si χ_u(resp χ_A) est scindé sur K.

Démonstration : Soit u un endomorphisme d'un espace vectoriel E de dimension finie sur un corps K. On sait que u est **diagonalisable** s'il existe une base de E constituée de vecteurs propres de u, c'est-à-dire si l'on peut écrire :

$$E = \bigoplus_{\lambda \in \sigma(u)} \ker(u - \lambda I).$$

où $\sigma(u)$ est l'ensemble des valeurs propres de u.

Le polynôme caractéristique de u est défini par :

$$\chi_u(X) = \det(XI - A),$$

où A est la matrice de u dans une base quelconque de E.

Si u est diagonalisable, alors il existe une base de vecteurs propres de E, et la matrice associée à u dans cette base est diagonale. Dans ce cas, son polynôme caractéristique s'écrit :

$$\chi_u(X) = (X - \lambda_1)(X - \lambda_2) \dots (X - \lambda_n),$$

ce qui montre qu'il est un produit de facteurs de degré 1 à coefficients dans K, donc **scindé sur** K.

Réciproquement, supposons que $\chi_u(X)$ est scindé sur K :

$$\chi_u(X) = (X - \lambda_1)^{n_1}(X - \lambda_2)^{n_2} \dots (X - \lambda_k)^{n_k}, \quad \text{avec } \lambda_i \in K.$$

Pour que u soit diagonalisable, il faut que E admette une décomposition en somme directe des sous-espaces propres. Ce critère est assuré si et seulement si le polynôme **minimal** de u est scindé et sans facteur carré :

$$\mu_u(X) = (X - \lambda_1)(X - \lambda_2) \dots (X - \lambda_k).$$

Dans notre hypothèse, $\chi_u(X)$ est scindé et chaque sous-espace propre a une dimension égale à la multiplicité de sa valeur propre. Cela signifie que E est engendré par une base de vecteurs propres, et donc que u est **diagonalisable**.

On conclut donc :

$$\boxed{u \text{ est diagonalisable} \iff \chi_u(X) \text{ est scindé sur } K.}$$

Le même raisonnement s'applique pour une matrice $A \in \mathcal{M}_n(K)$.

□

7.1.5 Nilpotence :

Définition

Un endomorphisme u d'un espace vectoriel E est dit **nilpotent** s'il existe un entier k tel que :

$$u^k = 0$$

Cela signifie qu'après un certain nombre d'itérations, l'application de u devient l'application nulle.

Propriété

Si u est un endomorphisme nilpotent d'un espace vectoriel de dimension n, alors :

$$u^n = 0.$$

Démonstration : On considère la suite des sous-espaces :

$$\ker u, \quad \ker u^2, \quad \ker u^3, \quad \ldots$$

Chaque noyau est inclus dans le suivant :

$$\ker u \subseteq \ker u^2 \subseteq \ker u^3 \subseteq \ldots$$

Puisque la dimension de E est finie, cette suite devient stationnaire à un certain rang, c'est-à-dire qu'il existe un entier k tel que :

$$\ker u^k = \ker u^{k+1}.$$

Cela signifie que l'application u envoie tout vecteur de E dans $\ker u^k$, et donc que u^n annule tout vecteur. Ainsi, on obtient bien $u^n = 0$.

Propriété

Si u est nilpotent, alors la seule valeur propre possible de u est 0.

Démonstration : Soit λ une valeur propre de u, et soit $v \neq 0$ un vecteur propre associé, tel que :

$$uv = \lambda v.$$

En appliquant u plusieurs fois, on obtient :

$$u^2 v = \lambda uv = \lambda^2 v,$$

$$u^3 v = \lambda^3 v,$$

et plus généralement,

$$u^k v = \lambda^k v.$$

Mais puisque u est nilpotent, il existe un entier k tel que $u^k = 0$. En appliquant cela à v, on obtient :

$$u^k v = 0 \Rightarrow \lambda^k v = 0.$$

Comme $v \neq 0$, on en déduit que $\lambda^k = 0$, donc $\lambda = 0$.

Ainsi, toutes les valeurs propres d'un endomorphisme nilpotent sont nulles.

7.1.6 Réduction simultanée-HP

Proposition-HP

Soient $u, v \in \mathcal{L}(E)$ tels que $u \circ v = v \circ u$. Alors

i) Tout sous-espace propre de u est stable par v (en particulier $\ker u$).

ii) $\operatorname{Im} u$ est stable par v.

Démonstration

i) Soit E_λ un sous-espace propre de u. Pour tout $x \in E_\lambda$,

$$u[v(x)] = v[f(x)] = v(\lambda x) = \lambda v(x)$$

donc $v(x) \in E_\lambda$.

ii) Soit $y \in \operatorname{Im} u$, et $x \in E$ tel que $y = u(x)$. On a

$$v(y) = v[u(x)] = u[v(x)] \in \operatorname{Im} u.$$

□

Diagonalisation simultanée

Théorème

Si u et $v \in \mathcal{L}(E)$ sont diagonalisables et commutent, il existe une base commune de diagonalisation de u et v, on dit alors que u et v sont *codiagonalisables*.

Démonstration. Soient $\lambda_1, \ldots, \lambda_k$ les valeurs propres de u, et $E_{\lambda_1}, \ldots, E_{\lambda_k}$ les sous-espaces propres correspondants. Pour tout i, E_{λ_i} est stable par v. La restriction de v à E_{λ_i}, notée $v|E_{\lambda_i}$, induit un endomorphisme de E_{λ_i}, qui est diagonalisable.

Il existe donc une base B_i de E_{λ_i} constituée de vecteurs propres de v (et bien sûr de u, car $u|E_{\lambda_i} = \lambda_i \operatorname{Id}|E_{\lambda_i}$).

Or,

$$E = \bigoplus_{i=1}^{k} E_{\lambda_i},$$

donc

$$B = (B_1, \ldots, B_k)$$

est une base de diagonalisation commune de u et v. □

Théorème

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.
Si $(u_i)_{i \in I}$ est une famille d'endomorphismes diagonalisables qui commutent deux à deux, il existe une base commune de diagonalisation pour cette famille.

Démonstration : Procédons par récurrence sur n.

- **Initialisation :**
  Pour $n = 1$, c'est évident.
- **Hérédité :**
  Supposons le résultat vrai jusqu'au rang $n-1$ et montrons le au rang n. Si tous les f_i sont des homothéties, c'est terminé.
  Sinon il existe i_0 tel que u_{i_0} n'est pas une homothétie.
  Notons $E_{\lambda_1}, \ldots, E_{\lambda_r}$ ses sous-espaces propres, on a donc $r \geq 2$, et pour tout j, $\dim E_{\lambda_j} < n$. Pour tout j, E_{λ_j} est stable par tous les u_i, et chaque $u_i|_{E_{\lambda_j}}$ est diagonalisable.
  Donc d'après l'hypothèse de récurrence il existe une base B_j de E_{λ_j}, qui soit une base de diagonalisation de tous les $u_i|_{E_{\lambda_j}}$. Donc $B = (B_1, \ldots, B_r)$ est une base de diagonalisation de tous les $(u_i)_{i \in I}$.

Trigonalisation simultanée

Théorème

Soient $u, v \in \mathcal{L}(E)$ tels qu'ils sont trigonalisables et commuttent, alors il existe une base commune des deux de trigonalisation, on dit alors qu'ils sont cotrigonalisable.

Démonstration : On raisonne par récurrence sur $\dim E$.

- Cas de base : Si $\dim E = 1$, alors u et v sont des homothéties dans toute base, et la propriété est trivialement vérifiée.

- Hérédité : Supposons le théorème vrai en dimension n et montrons-le en dimension $n+1$. Comme u est trigonalizable, il admet un vecteur propre e_1. Le sous-espace $F = \operatorname{Vect}(e_1)^{\perp}$ est stable par u et par v, car u et v commutent. Par hypothèse de récurrence, il existe une base de F dans laquelle u et v sont simultanément triangulaires. En ajoutant e_1 à cette base, on obtient une base de E où u et v sont tous deux triangulaires.

Ainsi, par récurrence, le résultat est établi pour toute dimension finie. □

Théorème

Si $(u_i)_{i \in I}$ est une famille d'endomorphismes trigonalisables qui commutent deux à deux, il existe une base commune de trigonalisation pour cette famille.

Démonstration : On raisonne par récurrence sur la dimension n de E :

— **Cas** $n = 1$ **:** Trivial, toute base convient.

— **Hérédité :** Supposons que le résultat est vrai en dimension $n-1$. Montrons-le pour n.

Étant donné que les endomorphismes sont trigonalizables et commutent, on considère un vecteur propre commun v de l'un d'eux (grâce au théorème de Schur). Comme tous les u_i commutent, ils stabilisent le sous-espace engendré par v, ainsi que son complément $F = \ker(v)^{\perp}$, de dimension $n-1$.

Par hypothèse de récurrence, il existe une base triangulaire de F pour tous les u_i. En ajoutant v, on obtient une base triangulaire de E, ce qui prouve le résultat.

Conclusion

Par récurrence, on conclut qu'il existe une base commune de trigonalisabilité pour toute la famille $(u_i)_{i\in I}$.

□

7.1.7 Lemme de Schur

On dit qu'une matrice est irréductible si les seuls sous-espaces de E stables par tous les éléments de cette matrice sont $\{0_E\}$ et E

Lemme de Schur

a) Soit E un $\mathbb{C}$-e.v de dimension finie. Soit $Q \subset \mathcal{L}(E)$.

a) Les seuls éléments commutant avec tous les éléments de Q sont les homothéties.

b) Si E est un $\mathbb{R}$-e.v de dimension finie, le résultat est faux que si $dim_{\mathbb{K}}(E)$ est impair.

Démonstration : **a)** Soit $f \in \mathcal{L}(E)$ commutant avec tous les éléments de Q. Le corps $\mathbb{C}$ étant algébriquement clos, f admet au moins une valeur propre λ. Soit E_λ le sous-espace propre correspondant. On a $E_\lambda \neq \{0\}$. Par hypothèse sur f, pour tout $g \in Q$, on a $f \circ g = g \circ f$. E_λ est stable par tous les éléments de Q. Comme $E_\lambda \neq \{0\}$ et que Q est irréductible, ceci entraîne $E_\lambda = E$. Donc $f = \lambda\,\mathrm{Id}_E$ est une homothétie.

b) Sur un $\mathbb{R}$-e.v, le résultat est faux dans le cas général. Par exemple, en dimension 2, l'ensemble Q des rotations est irréductible car aucune droite n'est stable par toutes les rotations. Or tous les éléments de Q commutent avec tous les éléments de Q. Il existe donc des éléments de $\mathcal{L}(E)$ qui ne sont pas des homothéties qui commutent avec tous les éléments de Q.

Supposant $n = \dim E$ est impair, soit $f \in \mathcal{L}(E)$ commutant avec tous les éléments de Q. Le polynôme caractéristique P_f de f est un polynôme réel de degré impair, donc P_f admet au moins une racine réelle λ, donc f admet une valeur propre λ. En procédant comme au a), on en déduit que f est une homothétie.

7.1.8 Disque de Gerschgorin

Définition

Soit A une matrice **complexe** de taille $n \times n$, de terme général (a_{ij}). Pour chaque indice de ligne i entre 1 et n, on introduit le **disque de Gerschgorin** correspondant

$$D_i = \left\{ z \in \mathbb{C}, |a_{ii} - z| \leq \sum_{j\neq i} |a_{ij}| \right\} = D(a_{ii}, R_i),$$

qui constitue effectivement un **disque** dans le plan complexe, de rayon $R_i = \sum_{j\neq i} |a_{ij}|$.

Théorème

Toute valeur propre de A appartient au moins à l'un des disques de Gerschgorin.

Démonstration : Soit $\lambda \in \mathrm{Sp}(A)$. Comme $A - \lambda I_n$ n'est pas inversible, il existe $i_0 \in 1, n$ tel que $|a_{i_0 i_0} - \lambda| \leq R_{i_0}$, *i.e.* $\lambda \in \{z \in \mathbb{C} \mid |z - a_{i_0 i_0}| \leq R_{i_0}\}$.

Finalement,

$$\lambda \in \bigcup_{i=1}^{n} \{z \in \mathbb{C} \mid |z - a_{ii}| \leq R_i\}.$$

7.2 Polynome d'endomorphisme, et de matrice carrée

7.2.1 Généralités

Définition

Soient $u \in \mathbb{L}(E)$,$A \in M_n(\mathbb{K})$ les applications $f_u : K[X] \to L(E)$ $P \mapsto P(u)$, $f_A : K[X] \to M_n(K)$ $P \mapsto P(A)$ sont des morphismes d'algèbres tels que :

$$\boxed{\forall P \in K[X] \ f_u(P) = P(u) = \text{ et } f_A(P) = P(A) =}$$

Si $\exists r \in \mathbb{N}^*$ et $\exists (a_i)_{i\in[|0,r|]} \in K^r$ tel que $P(X) = \sum_{i\in[|1,r|]} a_i.X^i$ alors

$$\boxed{P = \sum_{i\in[|1,r|]} a_i.u^i,\ P = \sum_{i\in[|1,r|]} a_i.A^i}$$

on a donc : $\forall x \in E, f_u(P)(x) = \sum_{i\in[|1,r|]} a_i.u^i(x)$

Remarque :
- Notons que pour $i \in \mathbb{N}^*, u^i = u \circ u \circ ... \circ u$ (i fois).
- $P(u) \in L(E)$, ie : P(u) est un endomorphisme!!
- $P(A) \in M_n(K)$, ie : P(A) est une matrice!!
- Si $u \in L(E), \forall P, Q \in \mathbb{K}[X]$ on a $P(u) \circ Q(u) = (PQ)(u)$.

Proposition

Considérons l'application :

$$f_u : \mathbb{K}[X] \to L(E), \quad P(X) \mapsto P(u).$$

i) $Kerf_u = \{P \in K[X]|P(u) = 0_{L(E)}\}$ est un idéal de $\mathbb{K}[X]$.
ii) $Imf_u = \{P(u)|P \in K[X]\}$ est une sous algèbre commutative de $L(E)$ noté $K[u]$.

Démonstration :
- **1.** $\ker f_u$ **est un idéal de** $\mathbb{K}[X]$
  f_u étant un morphisme d'anneau , son noyau $\ker f_u$ est un idéal.

- **2.** $\operatorname{Im} f_u$ **est une sous-algèbre commutative de** $L(E)$
  L'image de f_u est définie par :
  $$\operatorname{Im} f_u = \{P(u) \mid P \in \mathbb{K}[X]\}.$$
  Nous montrons que c'est une sous-algèbre de $L(E)$:
  -**Stabilité par addition** : Soient $P, Q \in \mathbb{K}[X]$, alors :
  $$f_u(P + Q) = P(u) + Q(u).$$
  Donc $P(u) + Q(u) \in \operatorname{Im} f_u$, ce qui prouve la stabilité par addition.
  - **Stabilité par multiplication** : Pour $P, Q \in \mathbb{K}[X]$, on a :
  $$f_u(PQ) = P(u)Q(u).$$
  Donc $P(u)Q(u) \in \operatorname{Im} f_u$, montrant la stabilité par multiplication.
  - Stabilité par multiplication scalaire : Pour $\alpha \in \mathbb{K}$ et $P \in \mathbb{K}[X]$,
  $$f_u(\alpha P) = \alpha P(u),$$
  donc $\operatorname{Im} f_u$ est aussi un espace vectoriel.
  - **Commutativité** : Comme les polynômes commutent dans $\mathbb{K}[X]$, alors pour tous $P, Q \in \mathbb{K}[X]$,

$$P(u)Q(u) = Q(u)P(u).$$

Ainsi, Im f_u est une sous-algèbre commutative de $L(E)$, notée $\mathbb{K}[u]$.

□

7.2.2 Polynôme minimal

Définition

On considère l'ideal $\mathbb{I} = Ker f_u = \{P \in \mathbb{K}[X] | P(u) = 0_{L(E)}\}$, on a $\mathbb{I} \neq \{0_{\mathbb{K}[X]}\}$ alors il est généré par un seul élément noté "μ_u" ou "π_u" c'est à dire :

$$\boxed{I = \pi_u \mathbb{K}[X]}$$

On a donc :

$$\boxed{(\forall P \in \mathbb{K}[X], P(u) = 0.) \Leftrightarrow (\pi_u | P.)}$$

Démonstration : On considère l'idéal :

$$I = \ker f_u = \{P \in \mathbb{K}[X] \mid P(u) = 0\}.$$

On suppose que $I \neq \{0\}$, c'est-à-dire qu'il existe des polynômes non nuls qui s'annulent en u. Nous allons montrer qu'il existe un unique polynôme unitaire de degré minimal dans I, et que cet élément engendre I.

On note π_u un polynôme non nul de degré minimal dans I. Nous allons montrer que π_u engendre I.

Prenons un polynôme quelconque $P \in I$, c'est-à-dire un polynôme qui s'annule en u. Effectuons la division euclidienne de P par π_u :

$$P = Q\pi_u + R$$

où $Q, R \in \mathbb{K}[X]$ et R est soit nul, soit un polynôme de degré strictement inférieur à celui de π_u.

Comme $P \in I$, on a $P(u) = 0$. En évaluant cette égalité en u, on obtient :

$$P(u) = Q(u)\pi_u(u) + R(u) = 0.$$

Or, $\pi_u(u) = 0$, donc il reste :

$$R(u) = 0.$$

Puisque R est un polynôme de degré strictement inférieur à celui de π_u, et que π_u est un polynôme de degré minimal dans I, il s'ensuit que $R = 0$. Ainsi, on a :

$$P = Q\pi_u.$$

Cela montre que tout polynôme de I est un multiple de π_u, donc :

$$I = (\pi_u) = \pi_u \mathbb{K}[X].$$

On en déduit que :

$$\boxed{(\forall P \in \mathbb{K}[X], P(u) = 0) \iff (\pi_u \mid P).}$$

Remarque : Le polynôme minimal est unitaire.

Définition

De même on considère l'ideal $\mathbb{I} = Kerf_A = \{P \in K[X] | P(A) = 0_{M_n(\mathbb{K})}\}$, on a $\mathbb{I} \neq \{0_{K[X]}\}$ alors il est généré par un seul élément noté "μ_A" ou "π_A" c'est à dire :

$$\boxed{\mathbb{I} = \pi_A \mathbb{K}[X]}$$

On a donc :

$$\boxed{(\forall P \in \mathbb{K}[X], P(A) = 0.) \Leftrightarrow (\pi_A | P.)}$$

Démonstration : De même comme on a fait précédement pour le cas d'endormorphisme.

Proposition

Si d est le degré du Polynôme minimal d'un endomorphisme alors la famille $(u^k)_{1 \leq k \leq d-1}$ est une base de $\mathbb{K}[u]$.

Proposition

Soit $u \in L(E), \lambda \in K$ on a :
Les racines de μ_λ dans $\mathbb{K}$ sont les valeurs propres de u. ce qui est equivalent à

$$(\mu_\lambda(\lambda) = 0_K) \Leftrightarrow (\lambda \in Sp_{\mathbb{K}}(u).)$$

Lemme de décomposition de noyaux

Soient $P_1, ..., P_r$ des polynômes premiers entre eux deux à deux tel que $P = \Pi_{i=1}^r Pi$ alors :

$$\boxed{Ker(P(u)) = \bigoplus_{i=1}^r Ker(P_i(u)).}$$

Démonstration : **Étape 1 : Inclusion $\subseteq$**

Soit $v \in \ker(P(u))$, c'est-à-dire que :

$$P(u)v = 0.$$

Par l'identité de Bézout, il existe des polynômes $Q_1, \ldots, Q_r$ tels que :

$$\sum_{i=1}^r Q_i P_i = 1.$$

En appliquant cette relation à u et en multipliant par v, on obtient :

$$v = \sum_{i=1}^r Q_i(u) P_i(u) v.$$

Or, chaque $P_i(u)v$ appartient à $\ker(P_i(u))$, donc :

$$\ker(P(u)) \subseteq \sum_{i=1}^r \ker(P_i(u)).$$

Étape 2 : Inclusion $\supseteq$

Prenons $v_i \in \ker(P_i(u))$ et posons $v = \sum_{i=1}^{r} v_i$. On a :

$$P_i(u)v_i = 0 \quad \text{pour tout } i.$$

Alors :

$$P(u)v = \sum_{i=1}^{r} P(u)v_i = 0.$$

Donc $v \in \ker(P(u))$, et :

$$\sum_{i=1}^{r} \ker(P_i(u)) \subseteq \ker(P(u)).$$

Étape 3 : La somme est directe
Si $v = v_1 + \cdots + v_r = 0$ avec $v_i \in \ker(P_i(u))$, alors en appliquant $P_j(u)$, on obtient :

$$P_j(u)v_j = 0.$$

Ce qui implique $v_j = 0$ pour tout j, donc la somme est directe.
Conclusion :

$$\boxed{\ker(P(u)) = \bigoplus_{i=1}^{r} \ker(P_i(u)).}$$

Proposition

Soit $u \in L(E)$, les assertions suivantes sont équivalentes :
i) u est diagonalisable.
ii) μ_u est scindé dans $\mathbb{K}$ à racines simples.
iii) $\exists P \in \mathbb{K}[X]$ scindé à racines simples tel que $P(u) = 0_{L(E)}$.

Démonstration :

— **1.** $(i) \Rightarrow (ii)$ **: Un endomorphisme diagonalisable a un polynôme minimal scindé à racines simples**
Un endomorphisme u est diagonalisable si et seulement si E admet une base de vecteurs propres de u. Cela signifie que la matrice de u est diagonale, et que son polynôme minimal est :

$$\mu_u(X) = \prod_{i=1}^{r} (X - \lambda_i),$$

où les λ_i sont les valeurs propres distinctes de u. Puisque u est diagonalisable, chaque valeur propre a une multiplicité géométrique égale à sa multiplicité algébrique, donc μ_u est scindé à racines simples. D'où $(i) \Rightarrow (ii)$.

— **2.** $(ii) \Rightarrow (iii)$ **: Le polynôme minimal scindé à racines simples donne un polynôme annulateur avec la même propriété**
Si μ_u est scindé à racines simples, on peut prendre $P(X) = \mu_u(X)$, qui est un polynôme scindé avec des racines simples tel que :

$$P(u) = \mu_u(u) = 0_{L(E)}.$$

D'où $(ii) \Rightarrow (iii)$.

— **3.** $(iii) \Rightarrow (i)$ **: Un polynôme annulateur scindé à racines simples implique la diagonalisabilité**
On suppose qu'il existe un polynôme P scindé avec des racines simples tel que :

$$P(u) = 0_{L(E)}.$$

Cela signifie que les valeurs propres de u ont toutes une multiplicité algébrique égale à 1. Or, un endomorphisme est diagonalisable si ses multiplicités algébriques et géométriques coïncident, donc u est diagonalisable.
Ainsi, nous avons prouvé $(iii) \Rightarrow (i)$, ce qui termine la démonstration.

$$(i) \Leftrightarrow (ii) \Leftrightarrow (iii).$$

□

Proposition

De même si $A \in M_n(\mathbb{K})$, les assertions suivantes sont équivalentes :

i) A est diagonalisable.
ii) μ_A est scindé dans $\mathbb{K}$ à racines simples.
iii) $\exists P \in \mathbb{K}[X]$ scindé à racines simples tel que $P(A) = 0_{M_n(\mathbb{K})}$.

Démonstration : De même comme ce qu'on a fait pour le cas de l'endomorphisme.

Proposition

Si F est un sous-espace vectoriel de E, stable par u et $u_{|F}$ l'endomorphisme induit par u sur F alors $\mu_{u_{|F}}$ divise μ_u.
Et si u est diagonalisable alors $u_{|F}$ est aussi diagonalisable.

Proposition

Soit $u \in L(E)$, les assertions suivantes sont équivalentes :

i) u est trigonalisable.
ii) μ_u est scindé dans $\mathbb{K}$.
iii) $\exists P \in K[X]$ scindé tel que $P(u) = 0_{L(E)}$.

Proposition

De même si $A \in M_n(\mathbb{K}$, les assertions suivantes sont équivalentes :

i) A est trigonalisable.
ii) μ_A est scindé dans $\mathbb{K}$.
iii) $\exists P \in K[X]$ scindé tel que $P(u) = 0_{M_n K}$.

Proposition-HP

Soit E un $\mathbb{K}$-espace vectoriel et $u \in \mathcal{GL}(E)$ admettant un polynôme minimal, u^{-1} est un polynôme en u

Démonstration : Le monôme X ne divise pas le polynôme minimal Π_u de u.

En effet, s'il existe $P \in \mathbb{K}[X]$ tel que $\Pi_u = XP$, alors $0 = \Pi_u(u) = f \circ P(u)$, et comme f est inversible, $P(u) = 0$. Comme $\deg P < \deg \Pi_u$, ceci contredit le fait que Π_u est le polynôme minimal de u.

Donc $X \nmid \Pi_u$. Comme X est irréductible, X et Π_u sont premiers entre eux, donc il existe $A, B \in \mathbb{K}[X]$ tels que $AX + B\Pi_u = 1$, d'où on tire $A(u) \circ u + B(u) \circ \Pi_u(u) = \mathrm{Id}_E$, c'est-à-dire $A(u) \circ u = \mathrm{Id}_E$.

Donc $u^{-1} = B(u)$.

Proposition-HP

Soient $\mathbb{K}$ un corps commutatif fini à m élements, E un $\mathbb{K}-$espace vectoriel de dimension finie n et $u \in \mathcal{L}(E)$ on a :

$$(u \text{ est diagonalisable}) \Leftrightarrow (u^m = u).$$

Démonstration : On a :

$$X^m - X = \prod_{\alpha \in \mathbb{K}} (X - \alpha). \quad (*)$$

En effet, muni de la loi produit, $\mathbb{K}^*$ est un groupe multiplicatif à $m-1$ éléments, donc pour tout $x \in \mathbb{K}^*$, $x^{m-1} = 1$, d'où pour tout $x \in \mathbb{K}$, $x^m = x$. On a ainsi déterminé m racines distinctes du polynôme $X^m - X$ qui est de degré m, d'où $(*)$.

u est diagonalisable si et seulement s'il existe $P \in \mathbb{K}[X]$, scindé sur $\mathbb{K}$, à racines toutes simples, tel que $P(u) = 0_{\mathcal{L}(E)}$, autrement dit si et seulement s'il existe $P \in \mathbb{K}[X]$, $P \mid \prod_{\alpha \in \mathbb{K}} (X - \alpha) = X^m - X$ tel que $P(u) = 0_{\mathcal{L}(E)}$. En d'autres termes, u est diagonalisable si et seulement si $u^m - u = 0_{\mathcal{L}(E)}$.

7.2.3 Théorème de Cayley-Hamilton

Théorème

Soit $u \in L(E)$, χ_u son polynôme caractéristique, alors $\chi_u = 0_{L(E)}$

Démonstration : Soit $x \in E \backslash \{0_E\}$, il existe un entier minimal m pour lequel la famille : $(x, u(x), u^2(x), \ldots, u^m(x))$ est liée, donc la famille $(x, u(x), u^2(x), \ldots, u^{m-1}(x))$ est libre.

$$\exists (c_1, \ldots, c_{m-1}), u^m + \sum_{i=0}^{m-1} c_i \cdot u^i(x) = 0_{\mathbb{K}}$$

Complétons la en une base de E, la matrice de u en cette base s'exprime en bloc par :
$\begin{pmatrix} C & B \\ 0 & D \end{pmatrix}$

$$\text{Avec } C = \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ -c_0 & -c_1 & -c_2 & -c_3 & \ldots & -c_{n-1} \end{pmatrix}$$

La matrice C s'appelle la matrice compagnon des éléments $(c_1, \ldots, c_{m-1})$ et son polynôme caractéristique s'exprime ainsi : ${}_C(X) = X^m + \sum_{i=0}^{m-1} c_i \cdot X^i$

En effet en raisonnant par récurrence sur m : H(m) : Le polynôme caractéristique de la matrice compagnon des éléments $(c_1, \ldots, c_{m-1})$ s'exprime ainsi : ${}_C(X) = X^m + \sum_{i=0}^{m-1} c_i \cdot X^i$

— **Initialisation :** $H(1)$ On a

$$C = \begin{pmatrix} 0 & 1 \\ -c_0 & -c_1 \end{pmatrix}$$

Et on a donc pour $\lambda \in \mathbb{K}$

$${}_C(\lambda) = det(C - \lambda \cdot I_2) = \lambda^2 + \lambda \cdot c_1 + c_0$$

Donc l'hypothèse est vérifié au rang 1, l'initialisation a été établie.

— **Hérédité :** $H(m) \Rightarrow H(m+1)$ Supposant la propriété étant établie au rang m et prouvant la au rang $m+1$: Soit $\lambda \in \mathbb{K}$:

En développant par la première colonne du $det(C - \lambda I_{m+1})$, on obtient :

$${}_C(\lambda) = \lambda det(C_{[|1,m|],[|1,m|]} - \lambda I_m) + c_0$$

Et d'après l'hypothèse de récurrence :

$$det(C_{[|1,m|],[|1,m|]} - \lambda I_m) = \lambda^m + \sum_{i=0}^{m-1} c_i + 1 \cdot \lambda^i$$

Et donc :

$${}_C(\lambda) = \lambda \cdot (\lambda^m + \sum_{i=0}^{m-1} c_i + 1 \cdot \lambda^i) + c_0 = \lambda^{m+1} + \sum_{i=0}^{m} c_i \cdot \lambda^i$$

On a établie l'hérédité.

Finalement Le polynôme caractéristique de la matrice compagnon des éléments $(c_1, \ldots, c_{m-1})$ s'exprime ainsi : $_C(X) = X^m + \sum_{i=0}^{m-1} c_i \cdot X^i$.

On a aussi d'après ce qui précède :

$$_u =_C \ _D, \text{ donc } \forall x \in E\backslash\{0_E\}_u(u)(x) =_C (u)(x)_D(u)(x)$$

Or,

$$\forall x \in E\backslash\{0_E\}_u(u)(x) =_C (u)(x) = x^m + \sum_{i=0}^{m-1} c_i \cdot x^i = 0_E$$

Donc,

$$_u(u) = 0_E$$

Ce qui conclut la preuve.

7.2.4 Sous-espace caractéristiques

Définition

Soit $u \in \mathbb{L}(E)$ tel que son polynôme caractéristique χ_u est scindé dans $\mathbb{K}$ ie : $\exists s \in \mathbb{N}^*$ tel que $\exists(\lambda_1, ..., \lambda_s) \in \mathbb{K}^s, (\alpha_1, ..., \alpha_s) \in \mathbb{N}^s$,
$P = (X - \lambda_1)^\alpha_1 ...(X - \lambda_s)^\alpha_s$
Pour tout $i \in [|1, s|]$ on appelle sous-espace caractéristique le sous-espace vectoriel $Ker(u - \lambda_i.Id)^\alpha_i$.

Proposition

Les assertions suivantes sont équivalentes :

i) Pour tout $i \in [|1, s|]$, $Ker(u - \lambda_i.Id)^\alpha_i$ est stable par u.

ii) $E = \bigoplus_{i=1}^{s} Ker(u - \lambda_i.Id)^\alpha_i$.

iii) Pour tout $i \in [|1, s|], dim_K(Ker(u - \lambda_i.Id)^\alpha_i) = \alpha_i$.

7.3 Exercices

7.3.1 Polynôme minimal

Exercice

Soit E un espace vectoriel sur un corps $\mathbb{K}$, et soit $T \in \mathcal{L}(E)$ admettant un polynôme minimal μ_T. Pour tout $a \in E$, on note Q_a le polynôme unitaire de degré minimal dans $\mathbb{K}[X]$ vérifiant :

$$Q_a(T)(a) = 0.$$

Ce polynôme est appelé le **polynôme minimal de a relatif à T**.

1/a) Montrer l'existence et l'unicité de Q_a. Si $P(T)(a) = 0$ avec $P \in \mathbb{K}[X]$, montrer que Q_a divise P.

b) Montrer que l'ensemble

$$E_a = \{P(T)(a) \mid P \in \mathbb{K}[X]\}$$

est un sous-espace vectoriel de E de dimension $\deg(Q_a)$.

2/a) Si $E_a \cap E_b = \{0\}$, montrer que $Q_{a+b} = \text{ppcm}(Q_a, Q_b)$. Généraliser à p vecteurs $a_1, \ldots, a_p$.

b) Si Q_a et Q_b sont premiers entre eux, montrer que $E_{a+b} = E_a \oplus E_b$. Généraliser à p vecteurs $a_1, \ldots, a_p$.

3/a) Soit $M \in \mathbb{K}[X]$ un facteur irréductible de μ_T, et soit k sa multiplicité dans la décomposition de μ_T en facteurs irréductibles sur $\mathbb{K}[X]$. Montrer qu'il existe $a \in \ker M^k(T)$ tel que $Q_a = M^k$.

b) Montrer qu'il existe $a \in E$ tel que $Q_a = \mu_T$.

Correction : 1a) Existence et unicité du polynôme minimal Q_v

Définissons l'ensemble des polynômes qui annulent v sous l'action de T :

$$J_v = \{P \in \mathbb{K}[X] \mid P(T)(v) = 0\}.$$

Cet ensemble est un **idéal** de $\mathbb{K}[X]$ et contient le polynôme minimal μ_T de T, donc $J_v \neq \{0\}$. D'après la structure des idéaux principaux dans $\mathbb{K}[X]$, il existe un unique polynôme unitaire Q_v tel que :

$$J_v = (Q_v).$$

Ainsi, Q_v est le plus petit polynôme unitaire satisfaisant $Q_v(T)(v) = 0$, ce qui prouve son existence et son unicité.

Si un polynôme $P \in \mathbb{K}[X]$ vérifie $P(T)(v) = 0$, alors $P \in J_v = (Q_v)$, ce qui implique que Q_v divise P.

1b) Dimension de E_v

Considérons l'application linéaire suivante :

$$\psi : \mathbb{K}[X] \to E_v, \quad P \mapsto P(T)(v).$$

Cette application est surjective par définition de E_v, qui est engendré par les images de v sous l'action de T.

Le noyau de ψ est précisément $J_v = (Q_v)$, donc par le théorème du noyau , on obtient l'isomorphisme :

$$E_v \simeq \mathbb{K}[X]/(Q_v).$$

Ainsi, la dimension de E_v est donnée par :

$$\dim(E_v) = \deg(Q_v).$$

2a) Polynôme minimal de la somme de deux vecteurs

Définissons $R = \text{ppcm}(Q_v, Q_w)$. Nous allons montrer que $Q_{v+w} = R$.

Puisque $Q_{v+w}(T)(v + w) = 0$, nous avons aussi :

$$Q_{v+w}(T)(v) = -Q_{v+w}(T)(w).$$

Or, ces deux vecteurs appartiennent à $E_v \cap E_w$, et si cette intersection est réduite à $\{0\}$, cela entraîne :

$$Q_v \mid Q_{v+w} \quad \text{et} \quad Q_w \mid Q_{v+w}.$$

Par définition du ppcm, nous obtenons alors :

$$R \mid Q_{v+w}.$$

Réciproquement, comme $R(T)$ annule $v + w$, on a $Q_{v+w} \mid R$, ce qui conduit à :

$$Q_{v+w} = R = \text{ppcm}(Q_v, Q_w).$$

Ce raisonnement se généralise par récurrence à une famille de p vecteurs $v_1, \ldots, v_p$, sous l'hypothèse que les sous-espaces E_{v_i} sont en somme directe :

$$Q_{v_1+\cdots+v_p} = \text{ppcm}(Q_{v_1}, \ldots, Q_{v_p}).$$

2b) Décomposition en somme directe des espaces E_v et E_w

Commençons par montrer que $E_v \cap E_w = \{0\}$. Soit $z \in E_v \cap E_w$, alors il existe deux polynômes $P, Q \in \mathbb{K}[X]$ tels que :

$$z = P(T)(v) = Q(T)(w).$$

En exploitant la définition des polynômes minimaux, nous avons :

$$0 = P(T)(v) - P(T)(v) = P_x(T)(v).$$

Ce qui implique $Q_v \mid P_x Q$. Or, si Q_v et Q_w sont premiers entre eux, alors d'après le théorème de Gauss , on obtient $Q_w \mid Q$, et donc $z = Q(T)(w) = 0$. Ainsi, $E_v \cap E_w = \{0\}$.

D'après **2a)**, nous avons :

$$Q_{v+w} = \text{ppcm}(Q_v, Q_w) = Q_v Q_w.$$

Ce qui entraîne :

$$\dim E_{v+w} = \deg(Q_{v+w}) = \deg(Q_v) + \deg(Q_w) = \dim E_v + \dim E_w.$$

Puisque $P(T)(v+w) = P(T)(v) + P(T)(w)$, il en résulte que $E_{v+w} \subseteq E_v \oplus E_w$, et donc :

$$E_{v+w} = E_v \oplus E_w.$$

Par récurrence, nous en déduisons que si $Q_{v_1}, \ldots, Q_{v_p}$ sont premiers entre eux deux à deux, alors :

$$E_{v_1+\cdots+v_p} = E_{v_1} \oplus \cdots \oplus E_{v_p}.$$

3a) Construction d'un vecteur ayant un polynôme minimal donné
Décomposons le polynôme minimal μ_T sous la forme :

$$\mu_T = M^k N,$$

où N est premier avec M. Le théorème de la décomposition des noyaux donne :

$$E = \ker M^k(T) \oplus \ker N(T).$$

Pour tout $v \in \ker M^k(T)$, nous avons $M^k(T)(v) = 0$, donc d'après **1a)**, Q_v divise M^k. Comme M est irréductible, il existe un entier $m_v \leq k$ tel que $Q_v = M^{m_v}$.

Si aucun vecteur de $\ker M^k(T)$ ne vérifiait $Q_v = M^k$, cela signifierait que tous les vecteurs sont annihilés par $M^{k-1}(T)$, ce qui est absurde car cela contredirait la minimalité de μ_T. Nous concluons donc qu'il existe un $v \in \ker M^k(T)$ tel que $Q_v = M^k$.

3b) Existence d'un vecteur ayant μ_T comme polynôme minimal
Soit la décomposition de μ_T en facteurs irréductibles :

$$\mu_T = \prod_{i=1}^{r} M_i^{k_i}.$$

D'après **3a)**, pour chaque i, il existe $v_i \in \ker M_i^{k_i}(T)$ tel que $Q_{v_i} = M_i^{k_i}$.

Par **2b)**, nous avons :

$$E_{v_1+\cdots+v_r} = E_{v_1} \oplus \cdots \oplus E_{v_r}.$$

D'après **2a)**, cela entraîne :

$$Q_{v_1+\cdots+v_r} = \prod_{i=1}^{r} Q_{v_i} = \prod_{i=1}^{r} M_i^{k_i} = \mu_T.$$

Ce qui conclut la démonstration.

□

7.3.2 Commutant d'un endomorphisme

Exercice

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$. Soit $u \in \mathcal{L}(E)$. On note Γ_u le s.e.v de $\mathcal{L}(E)$ défini par

$$\Gamma_u = \{v \in \mathcal{L}(E) \mid u \circ v = v \circ u\}.$$

1. a) Si u est diagonalisable, déterminer $\dim \Gamma_u$.
   b) Si de plus les valeurs propres de u sont toutes distinctes, montrer que

$$\Gamma_u = \{P(u) \mid P \in \mathbb{K}[X]\}.$$

2. On suppose que le polynôme minimal Π_u de u est de degré n. En utilisant le résultat établi à l'exercice 3 (il existe $x \in E, P_x = \Pi_u$), montrer que

$$\Gamma_u = \{P(u), P \in \mathbb{K}[X]\}.$$

Correction : 1/a) Soient $\lambda_1, \dots, \lambda_r$ les valeurs propres de u, $E_{\lambda_1}, \dots, E_{\lambda_r}$ les sous-espaces propres correspondants.

Si $v \in \Gamma_u$, alors pour tout i, E_{λ_i} est stable par v.

Réciproquement, si E_{λ_i} est stable par v pour tout i, alors :

$$\forall x \in E_{\lambda_i}, \quad u(v(x)) = \lambda_i v(x) = v(u(x)),$$

donc comme $E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_r}$, on a $v \in \Gamma_u$.

Donc $\Gamma_u = \{v \in \mathcal{L}(E) \mid \forall i, E_{\lambda_i} \text{ est stable par } v\}$.

Pour tout i, soit B_i une base de E_{λ_i}, de sorte que $B = B_1 \cup \cdots \cup B_r$ est une base de E. Les matrices des endomorphismes de Γ_u dans la base B sont celles de la forme

$$\begin{bmatrix} M_1 & 0 & \dots & 0 \\ 0 & M_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M_r \end{bmatrix}$$

avec $\forall i, M_i \in M_{\dim E_{\lambda_i}}(\mathbb{K})$.

On voit donc que

$$\dim \Gamma_u = \sum_{i=1}^{r} (\dim E_{\lambda_i})^2.$$

1/b) Ici, pour tout i, $\dim E_{\lambda_i} = 1$, donc $\dim \Gamma_u = \sum_{i=1}^{n} 1^2 = n$.

Pour tout i, $\Pi_u(\lambda_i) = 0$, donc $(X - \lambda_i)$ divise $\Pi_u(X)$, et comme les λ_i sont distincts deux à deux, $\prod_{i=1}^{n}(X - \lambda_i)$ divise Π_u, donc $\deg(\Pi_u) \geq n$.

Or Π_u divise le polynôme caractéristique de u, donc $\deg(\Pi_u) \leq n$.

On en déduit que $\deg(\Pi_u) = n$.

Soit $C = \{P(u) \mid P \in \mathbb{K}[X]\}$.

L'application

$$\varphi : \mathbb{K}[X] \to C, \quad P \mapsto P(u)$$

est linéaire surjective, donc C est isomorphe comme $\mathbb{K}$-e.v. à $\mathbb{K}[X]/\ker\varphi = \mathbb{K}[X]/(\Pi_u)$, donc

$$\dim C = \deg(\Pi_u) = n.$$

Or $C \subseteq \Gamma_u$ et $\dim \Gamma_u = n$, donc $C = \Gamma_u$.

L'inclusion réciproque est évidente.

2/ D'après la question **1b)** de l'exercice précédent, il existe $w \in E$ tel que son polynôme minimal est exactement celui de T, soit :

$$Q_w = \mu_T.$$

Par conséquent, nous avons :

$$\deg(Q_w) = \dim(E_w) = n.$$

Or, comme $\dim(E) = n$, il en résulte que $E_w = E$, ce qui signifie que l'ensemble E_w coïncide avec tout l'espace E.

Soit maintenant $S \in \Gamma_T$. Comme nous avons montré que $E_w = E$, il existe un polynôme $P \in \mathbb{K}[X]$ tel que :

$$S(w) = P(T)(w).$$

Par ailleurs, pour tout $v \in E_w$, on a :

$$S(v) = Q \circ S(v) = Q(S(v)) = Q(P(T)(v)) = Q(P)(T)(v) = P(v).$$

Ainsi, S et $P(T)$ coïncident sur tout E_w.

Mais comme $E_w = E$, nous obtenons :

$$S = P(T).$$

Nous avons donc établi l'inclusion :

$$\Gamma_T \subseteq \{P(T) \mid P \in \mathbb{K}[X]\}.$$

L'inclusion réciproque étant immédiate, nous en déduisons l'égalité :

$$\Gamma_T = \{P(T) \mid P \in \mathbb{K}[X]\}.$$

□

7.3.3 Résultant de deux polynômes

Exercice :

1/ a) 1/

a) Soient f et g deux polynômes non constants de $\mathbb{C}[X]$. Montrer que f et g possèdent un diviseur commun non trivial si et seulement si

$$(\exists U, V \in \mathbb{C}[X], U \neq 0, V \neq 0), \quad Uf = Vg$$

avec

$$\deg(U) < \deg(g), \quad \deg(V) < \deg(f).$$

b) Pour tout $d \in \mathbb{R}$, on définit

$$\Lambda_d = \{h \in \mathbb{C}[X] \mid \deg h = d\}.$$

Pour tout $p, q \in \mathbb{N}^*$, déterminer une fonction continue

$$S : \Lambda_p \times \Lambda_q \to \mathbb{C}$$

vérifiant

$$(f \text{ et } g \text{ sont premiers entre eux}) \iff (S(f,g) \neq 0).$$

2/

Soit $n \in \mathbb{N}$ avec $n \geq 2$. On note $\mathcal{D}$ l'ensemble des matrices diagonalisables dans $\mathcal{M}_n(\mathbb{C})$. Déterminer l'intérieur de $\mathcal{D}$, noté $\mathring{\mathcal{D}}$.

Correction : 1a) Condition nécessaire

Supposons qu'il existe un polynôme $R \in \mathbb{C}[X]$ tel que $\deg(R) \geq 1$ et qui divise à la fois f et g. Ainsi, on peut écrire :

$$f = Rf_1, \quad g = Rg_1,$$

où $f_1, g_1 \in \mathbb{C}[X]$.

Posons alors $U = g_1$ et $V = f_1$. On obtient immédiatement :

$$Uf = Rf_1g_1 = Vg.$$

Par ailleurs, nous avons $\deg(U) = \deg(g_1) < \deg(g)$ et $\deg(V) = \deg(f_1) < \deg(f)$, ce qui prouve la nécessité de cette condition.

Condition suffisante

Supposons maintenant que f et g soient premiers entre eux , c'est-à-dire qu'ils ne possèdent pas de facteur commun autre que les constantes. Si nous avons $Uf = Vg$ pour des polynômes U, V, alors d'après le théorème de Gauss , le polynôme f doit nécessairement diviser V. Or, comme $V \neq 0$, cela implique que :

$$\deg(V) \geq \deg(f),$$

ce qui contredit notre hypothèse $\deg(V) < \deg(f)$.

On en conclut que si $Uf = Vg$ avec $\deg(U) < \deg(g)$ et $\deg(V) < \deg(f)$, alors f et g doivent nécessairement partager un diviseur commun non constant.

1b) Définition d'une fonction continue $S(f, g)$

Considérons les polynômes :

$$f = a_0 + a_1X + \cdots + a_pX^p \in \Lambda_p, \quad g = b_0 + b_1X + \cdots + b_qX^q \in \Lambda_q.$$

D'après la question précédente, f et g possèdent un facteur commun non trivial si et seulement s'il existe deux polynômes $U, V \in \mathbb{C}[X]$ non nuls tels que :

$$Uf = Vg,$$

avec $\deg(U) < \deg(g)$ et $\deg(V) < \deg(f)$.

Cette condition équivaut au fait que la famille de polynômes :

$$f, Xf, \dots, X^{q-1}f, g, Xg, \dots, X^{p-1}g$$

est **linéairement dépendante** dans $\mathbb{C}[X]$. Autrement dit, leur déterminant dans une base de $\mathbb{C}_{p+q-1}[X]$ s'annule :

$$\det_{\mathcal{B}}(f, Xf, \dots, X^{q-1}f, g, Xg, \dots, X^{p-1}g) = 0.$$

En particulier, f et g sont premiers entre eux si et seulement si le déterminant :

$$S(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & a_p & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_p & 0 & \dots & 0 \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & 0 & \dots & a_0 & a_1 & \dots & a_p & 0 \\ b_0 & b_1 & \dots & b_q & 0 & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_q & 0 & \dots & 0 \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & 0 & \dots & b_0 & b_1 & \dots & b_q & \end{vmatrix}$$

est non nul. Ce déterminant, appelé **résultant** de f et g, définit une fonction :

$$S : \Lambda_p \times \Lambda_q \to \mathbb{C}$$

qui est continue (car polynomiale en les coefficients de f et g). Ainsi, f et g sont premiers entre eux si et seulement si $S(f,g) \neq 0$.

2) Intérieur de l'ensemble des matrices diagonalisables

Nous devons déterminer l'intérieur de :

$$\mathcal{D} = \{M \in \mathcal{M}_n(\mathbb{C}) \mid M \text{ est diagonalisable}\}.$$

Une intuition forte nous suggère que $\mathring{\mathcal{D}}$ est constitué des matrices ayant **uniquement des valeurs propres distinctes**. Définissons :

$$\Gamma = \{M \in \mathcal{D} \mid M \text{ possède } n \text{ valeurs propres distinctes}\}.$$

Nous allons démontrer que :

$$\mathring{\mathcal{D}} = \Gamma.$$

Inclusion $\Gamma \subset \mathring{\mathcal{D}}$

Si $M \in \Gamma$, alors son polynôme caractéristique P_M possède uniquement des racines simples. Cela implique que P_M et son dérivé P'_M sont premiers entre eux, donc leur résultant $S(P_M, P'_M)$ est non nul. La fonction :

$$\varphi : \mathcal{M}_n(\mathbb{C}) \to \mathbb{C}, \quad M \mapsto S(P_M, P'_M)$$

est continue, et comme :

$$\Gamma = \varphi^{-1}(\mathbb{C}^*),$$

on en conclut que Γ est un ouvert . Puisque $\Gamma \subset \mathcal{D}$, on en déduit $\Gamma \subset \mathring{\mathcal{D}}$.

Inclusion $\mathring{\mathcal{D}} \subset \Gamma$

Supposons qu'une matrice $M \in \mathring{\mathcal{D}}$ possède une valeur propre multiple λ. On peut alors construire une suite de matrices N_p légèrement perturbées qui ne sont pas diagonalisables, et dont la limite est M. Cela montre que $M \notin \mathring{\mathcal{D}}$, ce qui contredit notre hypothèse. Ainsi, M doit nécessairement appartenir à Γ, d'où :

$$\mathring{\mathcal{D}} = \Gamma.$$

Conclusion : L'intérieur de l'ensemble des matrices diagonalisables est l'ensemble des matrices ayant des valeurs propres distinctes :

$$\mathring{\mathcal{D}} = \{M \in \mathcal{D} \mid M \text{ a } n \text{ valeurs propres distinctes}\}.$$

Cet ensemble est ouvert et dense dans $\mathcal{D}$. □

7.3.4 Dérivée d'un déterminant

Exercice :

On considère

$$M : \mathbb{R} \to \mathcal{M}_n(\mathbb{R}), \quad t \mapsto M(t) = (m_{i,j}(t))_{1 \le i,j \le n}$$

une application dérivable sur $\mathbb{R}$. Montrer que l'application $\varphi : t \mapsto \det(M(t))$ est dérivable sur $\mathbb{R}$ et que

$$\varphi'(t) = \sum_{i=1}^{n} \det(C_1(t), \dots, C_{i-1}(t), C_i'(t), C_{i+1}(t), \dots, C_n(t)),$$

où $C_1(t), \dots, C_n(t)$ désignent les vecteurs colonnes de la matrice $M(t)$.

Correction : L'expression du déterminant d'une matrice $M(t)$ est donnée par la formule de Leibniz :

$$\det M(t) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\, m_{\sigma(1),1}(t) \cdots m_{\sigma(n),n}(t)$$

où $\mathfrak{S}_n$ est le groupe symétrique des permutations de $\{1, 2, \dots, n\}$, $\varepsilon(\sigma)$ est le signe de la permutation σ, et chaque terme est un produit de coefficients de la matrice suivant une permutation spécifique des lignes.

La fonction $\varphi(t) = \det M(t)$ est dérivable car elle est une somme finie de fonctions différentiables. En dérivant cette expression, on applique la règle du produit :

$$\frac{d}{dt}\left(m_{\sigma(1),1}(t) \cdots m_{\sigma(n),n}(t)\right) = \sum_{k=1}^{n} m_{\sigma(1),1}(t) \cdots m_{\sigma(k-1),k-1}(t)\, m'_{\sigma(k),k}(t)\, m_{\sigma(k+1),k+1}(t) \cdots m_{\sigma(n),n}(t).$$

En injectant cette relation dans la somme définissant $\varphi'(t)$, on obtient :

$$\varphi'(t) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \sum_{k=1}^{n} m_{\sigma(1),1}(t) \cdots m_{\sigma(k-1),k-1}(t)\, m'_{\sigma(k),k}(t)\, m_{\sigma(k+1),k+1}(t) \cdots m_{\sigma(n),n}(t).$$

Chaque terme de cette somme correspond à un déterminant où la k-ième colonne est remplacée par sa dérivée. En échangeant l'ordre des sommes, cela donne :

$$\varphi'(t) = \sum_{i=1}^{n} \det(C_1(t), \dots, C_{i-1}(t), C_i'(t), C_{i+1}(t), \dots, C_n(t)).$$

On retrouve ainsi exactement le résultat demandé. Ce résultat montre que la dérivée du déterminant s'obtient en dérivant chaque colonne séparément, ce qui est une propriété essentielle en calcul différentiel matriciel.

7.4 Compléments

7.4.1 Réduction des matrice circulantes

Réduction de la matrice J

La matrice J est diagonalisable, ses valeurs propres sont les racines n-ièmes de l'unité et ses vecteurs propres s'expriment ainsi :
On pose $w = exp(2i\pi/n)$ alors pour tout $k \in [|1,n|], w^k$ est valeur propre de J et : $\forall k \in [|1,n|], X_k = \begin{pmatrix} 1 \\ w^k \\ w^{2k} \\ \vdots \\ w^{(n-1)k} \end{pmatrix}$ est vecteur propre de J.

Démonstration On a $J^n = I_n$ donc le polynôme $X^n - 1$ est annulateur de J, ce dernier étant scindé a racines simples dans $\mathbb{C}$, J est diagonalisable.
Les valeurs propres de J sont les racines de $X^n - 1$, du coup elles sont les racines n-ièmes de l'unité

Réduction d'une matrice circulante

Toute matrice circulante est diagonalisable, avec ses **valeurs propres** données par :

$$\lambda_k = \sum_{j=0}^{n-1} c_j \omega_n^{kj}, \quad k = 0, \ldots, n-1,$$

où :
- c_j sont les coefficients définissant la première ligne de la matrice circulante,
- $\omega_n = e^{2\pi i/n}$ est une **racine primitive n-ième de l'unité**.

Démonstration : Comme M est un polynôme en J, en utilisant la diagonalisation de J, on obtient :

$$M = c_0 I + c_1(PD_J P^{-1}) + c_2(PD_J^2 P^{-1}) + \cdots + c_{n-1}(PD_J^{n-1} P^{-1}).$$

En factorisant P et P^{-1}, on a :

$$M = P(c_0 I + c_1 D_J + c_2 D_J^2 + \cdots + c_{n-1} D_J^{n-1})P^{-1}.$$

L'expression entre parenthèses est une matrice diagonale notée D, dont les coefficients diagonaux sont :

$$\lambda_k = c_0 + c_1\omega_n^k + c_2\omega_n^{2k} + \cdots + c_{n-1}\omega_n^{(n-1)k}, \quad k = 0, \ldots, n-1.$$

Ainsi, M est **diagonalisable**, avec une matrice diagonale D contenant ses valeurs propres, et sa diagonalisation s'écrit :

$$M = PDP^{-1}.$$

7.4.2 Réduction des matrices de Toeplitz tridiagonale

Valeurs propres

Les valeurs propres λ_k d'une matrice de Toeplitz tridiagonale de taille $n \times n$, ayant a sur la diagonale principale et b, c sur les diagonales adjacentes, sont données par :

$$\lambda_k = a + 2\sqrt{bc}\cos\left(\frac{k\pi}{n+1}\right), \quad k = 1, 2, \ldots, n.$$

Démonstration :

$$T = \begin{bmatrix} a & b & 0 & 0 & \cdots & 0 \\ c & a & b & 0 & \cdots & 0 \\ 0 & c & a & b & \cdots & 0 \\ 0 & 0 & c & a & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & b \\ 0 & 0 & \cdots & 0 & c & a \end{bmatrix}$$

Nous cherchons ses valeurs propres λ et les vecteurs propres $\mathbf{v} = (v_1, v_2, \dots, v_n)^T$ satisfaisant :

$$cv_{i-1} + av_i + bv_{i+1} = \lambda v_i.$$

En posant :

$$v_i = \sin\left(\frac{ki\pi}{n+1}\right),$$

et en substituant dans l'équation de récurrence, nous obtenons :

$$\lambda_k = a + 2\sqrt{bc}\cos\left(\frac{k\pi}{n+1}\right), \quad k = 1, 2, \dots, n.$$

7.4.3 Endomorphismes cycliques

Définition

Un **endomorphisme cyclique** est un endomorphisme linéaire $f : E \to E$ d'un espace vectoriel E qui admet un **vecteur cyclique**, c'est-à-dire un vecteur $v \in E$ tel que l'ensemble des images successives de v par f engendre tout l'espace E :

$$E = \mathrm{Vect}\{v, f(v), f^2(v), \dots, f^{n-1}(v)\}$$

où $\dim(E) = n$.

Polynôme minimal et polynôme caractéristique

Si un endomorphisme f de E est cyclique, alors son **polynôme minimal** $\mu_f(X)$ est égal à son **polynôme caractéristique** $\chi_f(X)$:

$$\mu_f(X) = \chi_f(X).$$

Démonstration : Par définition, f est cyclique s'il existe un vecteur v tel que :

$$E = \mathrm{Vect}\{v, f(v), f^2(v), \dots, f^{n-1}(v)\}.$$

Cela signifie que l'application linéaire f admet une base de type compagnon, c'est-à-dire que sa matrice M_f dans cette base est une matrice compagnon associée à un polynôme minimal $P(X)$:

$$M_f = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

Or, la matrice compagnon admet toujours un polynôme caractéristique qui est égal à son polynôme minimal :

$$\chi_f(X) = \mu_f(X).$$

Cela prouve que le polynôme minimal et le polynôme caractéristique sont égaux.

Matrice compagnon associée à un endomorphisme cyclique

Si f est un endomorphisme cyclique sur un espace vectoriel de dimension n, alors sa matrice dans une base bien choisie est une **matrice compagnon** :

$$C = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

où les coefficients a_i proviennent du polynôme minimal $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$.

Démonstration : Puisque f est cyclique, il existe un vecteur v tel que :

$$\{v, f(v), f^2(v), \ldots, f^{n-1}(v)\}$$

forme une base de E. Alors, f est complètement déterminé par son action sur ce vecteur :

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

En exprimant f dans cette base, on obtient la matrice compagnon.

Existence d'un vecteur cyclique unique (généralement)

Si f est un endomorphisme cyclique, alors **tout vecteur de l'espace n'est pas forcément cyclique**. Toutefois, il existe un **unique vecteur cyclique à un scalaire près**.

Démonstration : Un vecteur v est dit cyclique si f appliqué à ses puissances successives engendre tout l'espace :

$$E = \text{Vect}\{v, f(v), f^2(v), \ldots, f^{n-1}(v)\}.$$

Si f est représenté par une matrice compagnon, alors seul le premier vecteur de la base naturelle est un vecteur cyclique. Si l'on prend un autre vecteur v', alors la structure de la matrice compagnon implique que les puissances successives de v' ne généreront pas nécessairement tout E, sauf s'il est une combinaison linéaire non triviale de v. Ainsi, il existe un unique vecteur cyclique, sauf multiplication par un scalaire.

Irréductibilité de l'endomorphisme cyclique

Si un endomorphisme f est cyclique, alors il est **irréductible**, c'est-à-dire qu'il ne possède aucun sous-espace stable non trivial.

Démonstration : Supposons que f possède un sous-espace propre non trivial $F \subset E$, stable par f. Cela signifierait que f admet un sous-polynôme minimal diviseur strict de $\mu_f(X)$. Mais, par la propriété 1, nous savons que :

$$\chi_f(X) = \mu_f(X).$$

Or, cela signifie que $\mu_f(X)$ est irréductible, donc ne peut pas avoir de sous-diviseur propre. Il ne peut donc pas exister de sous-espace stable non trivial. Ainsi, f est irréductible.

Relation avec la décomposition de Jordan

Tout endomorphisme peut être décomposé en une somme d'endomorphismes cycliques. C'est ce qu'on appelle le **théorème des cycles**.

Démonstration : Soit f un endomorphisme d'un espace vectoriel E. On peut décomposer E en sous-espaces où f agit comme un endomorphisme cyclique :

$$E = V_1 \oplus V_2 \oplus \cdots \oplus V_k,$$

où chaque $f_i = f_{|V_i}$ est cyclique. Cela vient du fait que l'algèbre des matrices sur un corps est semi-simple, ce qui implique que toute matrice peut être écrite comme une somme de blocs cycliques de Jordan. Cette propriété est cruciale en réduction de Jordan, car elle permet de transformer une matrice quelconque en une somme d'endomorphismes cycliques.

Applications en systèmes dynamiques

Un endomorphisme cyclique est **idéal** pour modéliser des systèmes dynamiques linéaires, où un **unique état initial** engendre toute l'évolution.

Démonstration : Si f est cyclique, alors tout état du système peut être exprimé en fonction des états précédents, ce qui correspond exactement à la dynamique d'un système d'équations aux différences :

$$X_{n+1} = AX_n.$$

Puisque f est cyclique, l'état initial X_0 génère toute la trajectoire X_n, ce qui montre que les équations différentielles linéaires peuvent être étudiées sous l'angle des endomorphismes cycliques.

7.4.4 Endomorphismes simples et semi-simples

Endomorphisme simple

Un **endomorphisme simple** est un endomorphisme $f : E \to E$ tel que les seuls sous-espaces vectoriels invariants sous f sont $\{0\}$ et E.

Sous-espaces invariants

Soit $f : E \to E$ un endomorphisme simple. Alors les seuls sous-espaces vectoriels $F \subset E$ tels que $f(F) \subset F$ sont $\{0\}$ et E.

Démonstration : Par définition, un endomorphisme simple est tel que tout sous-espace invariant est soit $\{0\}$, soit E. Supposons qu'il existe un sous-espace propre F (c'est-à-dire $0 \subsetneq F \subsetneq E$) tel que $f(F) \subseteq F$. Alors F est stable par f, ce qui contredit la définition de la simplicité de f. Donc, les seuls sous-espaces invariants sont bien $\{0\}$ et E.

Diagonalisabilité

Un endomorphisme simple n'est pas nécessairement diagonalisable.

Démonstration : Considérons l'espace $E = \mathbb{R}^2$ et l'endomorphisme f défini par la matrice :

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

Cette matrice représente une rotation d'angle $\frac{\pi}{2}$. Aucun sous-espace propre n'est invariant sous cette transformation, sauf $\{0\}$ et E. La matrice n'est pas diagonalisable car son polynôme caractéristique :

$$\det(A - \lambda I) = \begin{vmatrix} -\lambda & -1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 + 1$$

a des racines complexes $\pm i$, ce qui signifie qu'elle n'est pas diagonalisable sur $\mathbb{R}$. Ainsi, f est simple mais non diagonalisable.

Endomorphisme semi-simple

U

n **endomorphisme semi-simple** est un endomorphisme $f : E \to E$ qui est diagonalisable ou qui admet une décomposition en somme directe de sous-espaces invariants.

Décomposition en sous-espaces invariants

Si f est un endomorphisme semi-simple sur E, alors E est somme directe de sous-espaces stables sous f.

Démonstration : Par définition, un endomorphisme semi-simple est un endomorphisme complètement réductible, ce qui signifie qu'il est diagonalisable ou qu'il admet une décomposition en sous-espaces invariants. Soit $P_f(X)$ le polynôme caractéristique de f, qui est supposé scindé en produit de facteurs linéaires :

$$P_f(X) = (X - \lambda_1)^{m_1} \cdots (X - \lambda_k)^{m_k}.$$

D'après le théorème de décomposition primaire, E peut être écrit comme somme directe des sous-espaces caractéristiques associés aux valeurs propres :

$$E = E_{\lambda_1} \oplus E_{\lambda_2} \oplus \cdots \oplus E_{\lambda_k}.$$

Chaque E_{λ_i} est invariant par f, ce qui prouve que f est bien décomposable en sous-espaces propres.

Diagonalisabilité sur un corps algébriquement clos

Si f est un endomorphisme semi-simple et que le corps $\mathbb{K}$ est algébriquement clos, alors f est diagonalisable.

Démonstration : Par définition, un endomorphisme semi-simple est un endomorphisme dont le polynôme minimal est scindé en facteurs distincts. Puisque $\mathbb{K}$ est algébriquement clos, toute matrice carrée sur $\mathbb{K}$ a un polynôme caractéristique scindé :

$$P_f(X) = (X - \lambda_1)^{m_1} \cdots (X - \lambda_k)^{m_k}.$$

De plus, pour que f soit semi-simple, son polynôme minimal doit être sans facteur répété :

$$m_f(X) = (X - \lambda_1) \cdots (X - \lambda_k).$$

Cela implique que la matrice associée à f est diagonalisable, car il existe une base de vecteurs propres. Par conséquent, un endomorphisme semi-simple est toujours diagonalisable sur un corps algébriquement clos.

Stabilité par somme et composition

La somme et la composition de deux endomorphismes semi-simples sont encore semi-simples.

Démonstration : Puisque f et g sont semi-simples, ils sont diagonalisables dans une base de E. Supposons que les matrices de f et g dans une certaine base sont diagonales :

$$F = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}, \quad G = \begin{bmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{bmatrix}.$$

Alors la matrice de $f + g$ est également diagonale :

$$F + G = \begin{bmatrix} \lambda_1 + \mu_1 & 0 \\ 0 & \lambda_2 + \mu_2 \end{bmatrix}.$$

Donc $f + g$ est diagonalisable et donc semi-simple. De même, la matrice de $f \circ g$ est :

$$FG = \begin{bmatrix} \lambda_1\mu_1 & 0 \\ 0 & \lambda_2\mu_2 \end{bmatrix}.$$

Ce qui prouve que $f \circ g$ est aussi semi-simple. Ainsi, la stabilité par somme et composition est démontrée.

7.4.5 La réduction de Dunford

Endomorphisme nilpotent

Un endomorphisme $f : E \to E$ est nilpotent s'il existe un entier k tel que $f^k = 0$, où f^k désigne l'application f composée k-fois. Autrement dit, l'endomorphisme f est nilpotent si, après un certain nombre d'itérations, f annihile tous les vecteurs de l'espace E.

Partie semi-simple de f

La partie semi-simple f_s d'un endomorphisme f est l'endomorphisme obtenu en éliminant la partie nilpotente de f, c'est-à-dire la partie qui agit de manière diagonalisable. Cette partie f_s est donc diagonalisable et contient toutes les informations liées aux valeurs propres de f.

Partie nilpotente de f

La partie nilpotente f_n d'un endomorphisme f est l'endomorphisme qui capture les effets nilpotents de f, c'est-à-dire qui ne joue aucun rôle dans la partie diagonalisable, mais qui peut avoir des effets non nuls lorsqu'on applique plusieurs fois f.

Théorème de la Réduction de Dunford

Soit $f : E \to E$ un endomorphisme d'un espace vectoriel E de dimension finie sur un corps $\mathbb{K}$. Il existe une décomposition unique de f sous la forme :

$$f = f_s + f_n$$

où : - f_s est la partie semi-simple (diagonalisable) de f, - f_n est la partie nilpotente de f, - f_s et f_n commutent : $f_s f_n = f_n f_s$.
Cette décomposition est unique, et chaque partie f_s et f_n est associée à un polynôme minimal distinct.

Démonstration : La décomposition de Dunford repose sur l'analyse du polynôme minimal de f. Le polynôme minimal de f se décompose en un produit de facteurs de la forme $(X - \lambda)^m$, où λ est une valeur propre de f et m est la multiplicité de λ.

1. Partie semi-simple : La partie semi-simple de f, notée f_s, est la somme des projecteurs spectraux associés aux valeurs propres distinctes. On peut écrire f_s comme suit :

$$f_s = \sum_{\lambda} \lambda P_\lambda$$

où P_λ est le projecteur spectral associé à λ.

2. Partie nilpotente : La partie nilpotente f_n est alors définie comme :

$$f_n = f - f_s.$$

Par construction, f_n est nilpotent, car il contient les effets de f qui ne sont pas capturés par les valeurs propres distinctes.

3. Commutation de f_s et f_n : Les projecteurs spectraux P_λ vérifient $P_\lambda P_\mu = \delta_{\lambda,\mu} P_\lambda$, ce qui implique que f_s et f_n commutent.

Cela démontre la décomposition de f en f_s et f_n, et prouve qu'elles commutent et sont uniques.

Unicité de la Décomposition

La décomposition de Dunford $f = f_s + f_n$ est unique.

Démonstration : Soient $f = f'_s + f'_n$ une autre décomposition de f, où f'_s est semi-simple et f'_n est nilpotente. Nous voulons prouver que $f_s = f'_s$ et $f_n = f'_n$.

1. f_s et f'_s doivent être les mêmes, car ils agissent de manière identique sur les espaces propres associés aux valeurs propres distinctes. 2. f_n et f'_n sont également les mêmes, car f_n capture toute la partie nilpotente de f, et si deux décompositions diffèrent, elles doivent nécessairement correspondre à la même partie nilpotente.

Ainsi, $f_s = f'_s$ et $f_n = f'_n$, prouvant l'unicité de la décomposition.

Commutation entre f_s et f_n

f_s et f_n commutent, c'est-à-dire $f_s f_n = f_n f_s$.

Démonstration : 1. Par construction, f_s est la somme des projecteurs spectraux associés aux valeurs propres de f. 2. Chaque projecteur P_λ associé à une valeur propre λ satisfait la relation $P_\lambda P_\mu = \delta_{\lambda,\mu} P_\lambda$, où $\delta_{\lambda,\mu}$ est le symbole de Kronecker. 3. En appliquant cette propriété aux projections de f_s et à la partie nilpotente f_n, on montre que $f_s f_n = f_n f_s$, car les projecteurs P_λ et la partie nilpotente f_n agissent indépendamment.

Partie Nilpotente de f est Nilpotente

f_n est nilpotent.

Démonstration : 1. Par construction, $f_n = f - f_s$. 2. Comme f_s est semi-simple (diagonalisable), f_s n'a aucun effet sur les puissances successives de f. 3. f_n, qui est constitué des effets nilpotents de f, satisfait donc $f_n^k = 0$ pour un certain k, ce qui définit f_n comme un endomorphisme nilpotent.

Propriétés de f_s : Diagonalisabilité et Commutativité

La partie f_s est diagonalisable et commute avec la partie f_n.

Démonstration : 1. Comme f_s est la partie semi-simple de f, cela signifie que les valeurs propres de f_s sont distinctes et que f_s est diagonalisable. 2. En raison de la commutation entre f_s et f_n, f_s peut être transformé en une matrice diagonale par un changement de base approprié. 3. La diagonalisabilité de f_s suit donc directement de la structure de f_s, qui est une somme de projecteurs spectraux associés à des valeurs propres distinctes.

7.5 Problèmes

7.5.1 Algorithme de Fadeev

Algorithme de Fadeev

L'algorithme de Faddéev est un algorithme conçu pour le calcul du polynôme caractéristique d'une matrice.
Soient K un corps commutatif et une matrice $A \in M_n(K)$. On note $\chi_A = \det(XI_n - A)$.
a) Montrer que

$$\chi'_A = \operatorname{tr}(\operatorname{com}(XI_n - A))$$

où $\operatorname{com}(XI_n - A)$ désigne la comatrice de $XI_n - A$.
b) On définit des matrices $B_0, \dots, B_{n-1} \in M_n(K)$ par

$$B_0 = I_n \quad \text{et} \quad \forall k, 1 \leq k \leq n-1, \quad B_k = AB_{k-1} - \frac{\operatorname{tr}(AB_{k-1})}{k} I_n.$$

Montrer

$$\chi_A(X) = X^n - \operatorname{tr}(AB_0)X^{n-1} - \frac{\operatorname{tr}(AB_1)}{2}X^{n-2} - \dots - \frac{\operatorname{tr}(AB_{n-1})}{n},$$

et si A est inversible,

$$A^{-1} = \frac{n}{\operatorname{tr}(AB_{n-1})} B_{n-1}.$$

Correction : Le raisonnement mené dans l'exercice 7.5.3 s'applique également aux polynômes dérivés. En l'appliquant au polynôme caractéristique $\chi_A(X) = \det(XI_n - A)$, on met en évidence que sa dérivée $\chi'_A(X)$ correspond à la somme des cofacteurs des termes diagonaux de la matrice $XI_n - A$. Cela conduit à l'expression :

$$\chi'_A(X) = \operatorname{tr}(\operatorname{com}(XI_n - A)),$$

où $\operatorname{com}(XI_n - A)$ est la matrice des cofacteurs associée à $XI_n - A$.
En développant explicitement $\chi_A(X)$, on obtient :

$$\chi_A(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n.$$

Les éléments de $\operatorname{com}(XI_n - A)$ étant des polynômes en X de degré au plus $n-1$, il existe des matrices $B_0, B_1, \ldots, B_{n-1}$ telles que :

$$\operatorname{com}(XI_n - A) = B_0 X^{n-1} + B_1 X^{n-2} + \cdots + B_{n-1}.$$

En combinant cette expression avec l'égalité $\chi'_A(X) = \operatorname{tr}(\operatorname{com}(XI_n - A))$, on obtient les relations :

$$(n-1)a_1 = \operatorname{tr}(B_1), \quad \ldots, \quad 1 \cdot a_{n-1} = \operatorname{tr}(B_{n-1}).$$

D'autre part, la relation matricielle fondamentale :

$$(XI_n - A)\operatorname{com}(XI_n - A) = \det(XI_n - A)I_n$$

donne, en développant les termes en X :

$$B_0 X^n + (B_1 - AB_0)X^{n-1} + \cdots + (B_{n-1} - AB_{n-2})X - AB_{n-1} = \chi_A(X)I_n.$$

En comparant les coefficients pour chaque puissance de X, on obtient les relations suivantes :

$$B_0 = I_n, \quad B_1 - AB_0 = a_1 I_n, \quad \ldots, \quad B_{n-1} - AB_{n-2} = a_{n-1}I_n, \quad -AB_{n-1} = a_n I_n.$$

En appliquant l'opérateur trace sur ces équations :

$$na_1 = \operatorname{tr}(B_1) - \operatorname{tr}(AB_0), \quad \ldots, \quad na_{n-1} = \operatorname{tr}(B_{n-1} - AB_{n-2}), \quad na_n = -\operatorname{tr}(AB_{n-1}).$$

En comparant avec les relations précédentes, nous avons :

$$1 \cdot a_1 = -\operatorname{tr}(AB_0), \quad \ldots, \quad (n-1)a_{n-1} = -\operatorname{tr}(AB_{n-2}), \quad na_n = -\operatorname{tr}(AB_{n-1}).$$

Il en découle que les coefficients du polynôme caractéristique peuvent être exprimés sous la forme :

$$a_k = -\frac{\operatorname{tr}(AB_{k-1})}{k}.$$

En injectant ces valeurs dans les relations obtenues, nous établissons la récurrence suivante pour les matrices B_k :

$$B_0 = I_n, \quad B_1 = AB_0 - \frac{\operatorname{tr}(AB_0)}{1}I_n, \quad \ldots, \quad B_{n-1} = AB_{n-2} - \frac{\operatorname{tr}(AB_{n-2})}{n-1}I_n.$$

Cette construction permet d'obtenir successivement chaque B_k à partir de B_0.
Dans le cas où A est inversible, l'expression finale devient :

$$-AB_{n-1} = a_n I_n.$$

En multipliant de part et d'autre par $-A^{-1}$, on en déduit immédiatement :

$$A^{-1} = -\frac{1}{a_n}B_{n-1}.$$

En utilisant $a_n = -\frac{\operatorname{tr}(AB_{n-1})}{n}$, on obtient finalement :

$$A^{-1} = \frac{n}{\operatorname{tr}(AB_{n-1})}B_{n-1}.$$

Cette expression explicite relie l'inverse de A aux cofacteurs associés.

7.5.2 Théorème de Perron-Frobenius

Théorème de Perron-Frobenius

Si $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{R})$ est une matrice, on note $A \geq 0$ si $a_{i,j} \geq 0$ pour tout (i, j), et on note $A > 0$ si $a_{i,j} > 0$ pour tout (i, j). Pour un vecteur $X \in \mathbb{R}^n$, on définit de la même manière les notations $X \geq 0$ et $X > 0$. Si X, Y sont deux vecteurs de $\mathbb{R}^n$, on note $X \geq Y$ (resp. $X > Y$) lorsque $X - Y \geq 0$ (resp. $X - Y > 0$).

1/ . Soit une matrice $A \in \mathcal{M}_n(\mathbb{R})$ telle que $A > 0$. On note S l'ensemble des vecteurs $X = (x_i) \in \mathbb{R}^n$ tels que $X \geq 0$ et $\sum_{i=1}^n x_i = 1$ (de tels vecteurs sont appelés *vecteurs de probabilité*). Montrer que l'ensemble

$$\Lambda = \{\lambda \in \mathbb{R} \mid (\exists X \in S), AX \geq \lambda X\}$$

est majoré et que sa borne supérieure λ_0 est une valeur propre de A strictement positive associée à un vecteur propre $X > 0$.

a) Montrer que pour toute valeur propre complexe $\lambda \neq \lambda_0$ de A, on a $|\lambda| < \lambda_0$, alors que λ_0 est *valeur propre dominante* de A.

b) Montrer que le sous-espace propre E_{λ_0} de A associé à la valeur propre λ_0 est de dimension 1.

c) Montrer que λ_0 est racine simple du polynôme caractéristique de A (on dit alors que λ_0 est *valeur propre simple* de A). (Indication : raisonner par l'absurde en considérant deux vecteurs indépendants X et Y tels que $X > 0$ avec $AX = \lambda_0 X$ et $AY = \lambda_0 Y + \alpha X$, puis considérer $A^k Y$).

Correction : 1/ a) L'ensemble Λ est non vide (puisque $0 \in \Lambda$) et possède une borne supérieure évidente (par exemple la somme des coefficients de A).

Par définition de λ_0, on peut construire une suite (X_n) dans S et une suite réelle (γ_n) telle que :

$$\lim_{n\to\infty} \gamma_n = \lambda_0, \quad \text{et} \quad \forall n, \quad AX_n \geq \gamma_n X_n.$$

L'espace S étant un compact de $\mathbb{R}^n$, il existe une sous-suite $(X_{\varphi(n)})$ convergeant vers un certain $X \in S$. En passant à la limite dans l'inégalité $AX_{\varphi(n)} \geq \gamma_{\varphi(n)} X_{\varphi(n)}$, on en déduit :

$$AX \geq \lambda_0 X.$$

Si cette relation n'était pas une égalité, on aurait strictement $AX > \lambda_0 X$. Définissant alors $Y = AX - \lambda_0 X$, on en déduirait $AY > \lambda_0 Y$. Dès lors, il existerait $\varepsilon > 0$ tel que $AY > (\lambda_0 + \varepsilon) Y$, ce qui contredit la définition de λ_0. On conclut donc que $AX = \lambda_0 X$. Comme $A > 0$, il en résulte que $AX > 0$, donc $\lambda_0 X > 0$, ce qui implique que $X > 0$ et $\lambda_0 > 0$.

b) Soit λ une valeur propre de A et Z un vecteur propre associé. En notant (z_i) les composantes de Z, on a :

$$\forall i, \quad \sum_{j=1}^n a_{i,j} z_j = \lambda z_i.$$

En appliquant la valeur absolue de chaque terme :

$$\forall i, \quad \sum_{j=1}^n a_{i,j} |z_j| \geq |\lambda||z_i|.$$

Le vecteur $|Z| = (|z_i|)$ appartient ainsi à S, ce qui prouve que $|\lambda| \leq \lambda_0$.

Supposons maintenant que $|\lambda| = \lambda_0$ mais que $\lambda \neq \lambda_0$. On définit alors la matrice perturbée $A_\delta = A - \delta I_n$ avec $\delta > 0$ suffisamment petit. Il est possible de démontrer que A_δ possède une plus grande valeur propre strictement inférieure à λ_0, ce qui contredit l'hypothèse initiale. On en conclut que $|\lambda| < \lambda_0$.

c) Il existe un vecteur propre $X > 0$ associé à λ_0. Supposons que l'espace propre associé à λ_0 soit de dimension au moins 2, c'est-à-dire qu'il existe un vecteur propre Y linéairement indépendant de X. On choisit un scalaire μ tel que $X - \mu Y \geq 0$ avec au moins une composante strictement positive, ce qui entraîne :

$$A(X - \mu Y) = \lambda_0 (X - \mu Y).$$

Puisque $A > 0$ et que $X - \mu Y > 0$, on en déduit que :

$$A(X - \mu Y) > \lambda_0(X - \mu Y),$$

ce qui est absurde. On conclut donc que $\dim E_{\lambda_0} = 1$.

d) Supposons que λ_0 soit une racine d'ordre au moins 2 du polynôme caractéristique P_A. Il existe un vecteur propre $X > 0$ tel que $AX = \lambda_0 X$. En complétant X en une base $B = (X, X_2, \dots, X_n)$ et en considérant la matrice de passage P, on obtient la forme :

$$P^{-1}AP = \begin{pmatrix} \lambda_0 & x & \cdots & x \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$$

où B est une matrice de dimension $(n-1) \times (n-1)$.

Cela implique que λ_0 est une racine du polynôme caractéristique de B. Si λ_0 était une racine de multiplicité au moins 2 dans P_B, il existerait un vecteur Y vérifiant :

$$AY = \lambda_0 Y + \alpha X.$$

En itérant cette relation, on obtient la suite :

$$A^k Y = \lambda_0^k Y + k\alpha\lambda_0^{k-1} X.$$

Étant donné que $A \geq 0$, on en déduit l'inégalité :

$$|A^k Y| \geq |\lambda_0^k Y|.$$

Or, les valeurs propres de A^k sont précisément λ_0^k, ce qui conduit à une contradiction avec l'unicité de la valeur propre dominante. On conclut donc que λ_0 est une racine simple du polynôme caractéristique de A.

7.5.3 Endomorphismes de $\mathcal{L}(E)$

Exercice :

Soit E un K-e.v de dimension finie n. Si $f, g \in \mathcal{L}(E)$, on note $L_f \in \mathcal{L}(\mathcal{L}(E))$ l'endomorphisme défini sur $\mathcal{L}(E)$ par $L_f(u) = f \circ u$ et on note $R_g \in \mathcal{L}(\mathcal{L}(E))$ celui défini par $R_g(u) = u \circ g$.

1. (a) Calculer $\dim(\ker L_f)$ et $\dim(\ker R_g)$ en fonction de $\dim(\ker f)$ et de $\dim(\ker g)$.
   (b) Montrer que f (resp. g) est diagonalisable si et seulement si L_f (resp. R_g) est diagonalisable.
   (c) Donner les matrices de L_f et R_g dans des bases commodes.
2. On note $A_{f,g} = L_f - R_g \in \mathcal{L}(\mathcal{L}(E))$.
   (a) Si f et g sont diagonalisables, montrer que $A_{f,g}$ est diagonalisable.
   (b) On suppose que P_f, le polynôme caractéristique de f, est scindé sur K. Si $A_{f,f}$ est diagonalisable, montrer que f est diagonalisable.

Correction : 1a) Calcul des dimensions des noyaux de L_f et R_g

On commence par examiner le noyau de l'application L_f, qui est défini par :

$$u \in \ker(L_f) \iff f \circ u = 0.$$

Cela signifie que tout opérateur u appartenant à $\ker(L_f)$ annule l'image de f, autrement dit :

$$\operatorname{Im} f \subset \ker u.$$

Ainsi, les applications linéaires u qui vérifient cette propriété sont exactement celles qui ont pour image un sous-espace inclus dans $\ker f$. On en déduit que :

$$\ker(L_f) = \mathcal{L}(E, \ker f),$$

ce qui implique la relation sur les dimensions :

$$\dim(\ker L_f) = n\dim(\ker f).$$

De manière similaire, pour l'application R_g, on a :

$$u \in \ker(R_g) \iff u \circ g = 0.$$

Cela revient à dire que l'image de g est incluse dans le noyau de u :

$$\operatorname{Im} g \subset \ker u.$$

Si l'on choisit un sous-espace supplémentaire S de $\operatorname{Im} g$ dans E, alors $\ker R_g$ est isomorphe à l'espace des applications linéaires de S dans E, soit :

$$\dim(\ker R_g) = \dim S \cdot n = (n - \dim(\operatorname{Im} g)) \cdot n = n\dim(\ker g).$$

1b) Diagonalisation de L_f et R_g
Soit $P \in K[X]$. On peut vérifier directement que :

$$P(L_f) = L_{P(f)}.$$

Ainsi, on a l'équivalence :

$$P(f) = 0 \iff \forall u, P(f) \circ u = 0 \iff L_{P(f)} = 0 \iff P(L_f) = 0.$$

Cela montre que f et L_f possèdent le même polynôme minimal. Par conséquent, d'après le théorème 2 page 185, f est diagonalisable si et seulement si L_f l'est également.
Un raisonnement similaire permet de conclure pour R_g.

1c) Matrices des applications L_f et R_g
Soit $B = (e_1, \dots, e_n)$ une base de E. On définit la famille de base des endomorphismes élémentaires $(e_{i,j})_{1\le i,j\le n}$ par la règle suivante :

$$e_{i,j}(e_k) = \delta_{j,k} e_i, \quad \text{où } \delta_{j,k} = \begin{cases} 1 & \text{si } j = k, \\ 0 & \text{sinon.} \end{cases}$$

Si $[f]_B = (a_{i,j})_{1\le i,j\le n}$ est la matrice de f dans la base B, alors :

$$f \circ e_{i_0,j_0}(e_k) = \delta_{j_0,k} f(e_{i_0}) = \delta_{j_0,k} \sum_{i=1}^{n} a_{i,i_0} e_i = \sum_{i=1}^{n} a_{i,i_0} e_{i,j_0}(e_k).$$

Ce qui implique que :

$$L_f(e_{i,j}) = \sum_{k=1}^{n} a_{k,i} e_{k,j}.$$

Dans la base :

$$B_1 = (e_{1,1}, \dots, e_{1,n}, e_{2,1}, e_{2,2}, \dots, e_{n,n}),$$

la matrice de L_f est donnée par blocs sous la forme :

$$[L_f]_{B_1} = \begin{pmatrix} M & (0) & \cdots & (0) \\ (0) & M & \cdots & (0) \\ \vdots & \vdots & \ddots & \vdots \\ (0) & (0) & \cdots & M \end{pmatrix}, \quad \text{où } M = [f]_B.$$

Un raisonnement similaire avec la matrice $[g]_B = (b_{i,j})_{1\le i,j\le n}$ permet d'obtenir :

$$R_g(e_{i,j}) = \sum_{k=1}^{n} b_{j,k} e_{i,k}.$$

Ainsi, la matrice de R_g dans la base :

$$B_2 = (e_{1,1}, \dots, e_{1,n}, e_{2,1}, e_{2,2}, \dots, e_{n,n}),$$

s'écrit :

$$[R_g]_{B_2} = \begin{pmatrix} {}^tN & (0) & \cdots & (0) \\ (0) & {}^tN & \cdots & (0) \\ \vdots & \vdots & \ddots & \vdots \\ (0) & (0) & \cdots & {}^tN \end{pmatrix}, \quad \text{où } N = [g]_B.$$

2a) Commutation et diagonalisation de L_f et R_g

D'après la question 1b), L_f et R_g sont diagonalisables. De plus, on vérifie que pour tout $u \in \mathcal{L}(E)$:

$$L_f \circ R_g(u) = f \circ u \circ g = R_g(f \circ u) = R_g \circ L_f(u).$$

Ainsi, L_f et R_g commutent, ce qui permet de les diagonaliser simultanément. Par conséquent, $A_{f,g} = L_f - R_g$ est également diagonalisable.

2b) Décomposition de Dunford et diagonalisabilité de f

Puisque le polynôme minimal de f est scindé sur K, on peut écrire la décomposition de Dunford :

$$f = d + n,$$

où d est un endomorphisme diagonalisable et n un endomorphisme nilpotent, vérifiant $n \circ d = d \circ n$.

Si l'on pose $A_u = A_{f,f}$ pour tout $u \in \mathcal{L}(E)$, on a :

$$A_u = A_d + A_n.$$

Puisque $n^p = 0$ pour un certain p, on en déduit que $A_n^p = 0$, donc A_n est nilpotent. De plus, A_d est diagonalisable et A_d commute avec A_n, donc $A_u = A_d + A_n$ est sa décomposition de Dunford.

Étant donné que A_u est diagonalisable, il s'ensuit que $A_n = 0$, donc n commute avec tout opérateur de $\mathcal{L}(E)$. Par conséquent, n est une homothétie nilpotente, donc $n = 0$, ce qui implique $f = d$ est diagonalisable.

□