151 - Dimension d'un espace vectoriel (finie). Rang. Exemples et applications

E est un espace vectoriel sur un corps commutatif K.

1 - Dimension finie en algèbre linéaire

a) Espaces vectoriels

Déf. 1 : Toutes les bases de E ont le même nombre d'éléments, appelé dimension de E et noté $\dim_K E$ (ou $\dim E$).

À partir de maintenant, E est de dimension finie.

Thm 2 (existence d'une base) : Si $E \neq \{0\}$, G une famille génératrice de E, $L \subset G$ une famille libre de E, alors il existe une base $\mathcal{B}$ de E telle que $L \subset \mathcal{B} \subset G$.

Thm 3 (thm de la base incomplète) : Toute famille libre peut être complétée de manière à former une base.

Prop. 4 : Si $\dim E = n$, toute famille libre / génératrice de E à n éléments est une base de E.

ex. 5 : $\alpha, \beta \in \mathbb{R}^*$, $E = \{(u_n)_{n \geq 0} \in \mathbb{R}^{\mathbb{N}}, u_{n+2} = \alpha u_{n+1} + \beta u_n\}$ est un $\mathbb{R}$-ev de dimension 2.

b) Sous-espaces vectoriels

Prop. 6 : Soit $F \subset E$ un sev. Alors F est de dimension finie et on a :
- $\dim_K F \leq \dim_K E$.
- $\dim_K F = \dim_K E \iff F = E$.

ex. 7 : Le sev $\mathbb{R}_n[X] \subset \mathbb{R}[X]$ des polynômes de degré $\leq n$ est de dimension finie $n+1$.

Formule de Grassmann : F, G deux sev de E
$$\dim(F+G) = \dim F + \dim G - \dim(F \cap G).$$

FAUX

Thm 8 : $E = E_1 \oplus \dots \oplus E_r \Rightarrow \begin{cases} E_1 \cap \dots \cap E_r = \{0\} \\ \dim E = \dim E_1 + \dots + \dim E_r \end{cases}$

pour $\Leftarrow$: $r = 2$

On dit alors que E est somme directe des E_i, ou que les E_i sont supplémentaires.

Prop. 9 : • Soit $\mathcal{B}_i$ une base de E_i, $\forall i \in [\![1, r]\!]$.
$E = \bigoplus_{i=1}^{r} E_i \iff \{\mathcal{B}_1, \dots, \mathcal{B}_r\}$ est une base de E.

• Pour tout sev de E, il existe toujours un supplémentaire (non unique). Si E est de dimension finie, tous les supplémentaires d'un même sev sont de même dimension.

c) Applications linéaires

Déf. 10 : E, E' deux e.v. de dimension finie, $f \in \mathcal{L}(E, E')$. $\mathrm{Im} f \subset E'$ est un sev de dimension finie appelée rang de f, notée $\mathrm{rg}\, f$.

Si A est la matrice de f dans une certaine base, le rang de A est égal à la dimension du sev engendré par les vecteurs lignes (colonnes) de A. De plus $\mathrm{rg}\, f = \mathrm{rg}\, A$.

Calcul effectif du rang :
- via le pivot de Gauss.
- via le déterminant :

Thm 11 : Soit $A \in \mathcal{M}_{p,n}(K)$. Alors $\mathrm{rg}\, A = r$ ssi on peut extraire de A un mineur non nul δ d'ordre r dont tous les bordants dans A sont nuls.

Thm 12 (thm du rang) : Soient E, E' de dimension finie, $f \in \mathcal{L}(E, E')$. $\dim E = \dim(\ker f) + \mathrm{rg}\, f$.

Cor. 13 : Si $\dim E = \dim E'$, alors on a :
f injective $\iff$ f surjective $\iff$ f bijective.

C.-ex 14 : $D : \begin{array}{l} \mathbb{R}[X] \to \mathbb{R}[X] \\ P \mapsto P' \end{array}$ est surjective et non injective.

Prop. 15 : Soit $f \in \mathcal{L}(E)$, $F \subset E$ un sev stable par f. Alors $f_{|F} \in \mathcal{L}(F)$.

Prop. 16 : E, E' de dimension finie, $f \in \mathcal{L}(E,E')$, $(v_i)_{i=1}^n \in E$.
- Si f est injective et $(v_i)_{i=1}^n$ libre, alors $(f(v_i))_{i=1}^n$ est libre.
- — surjective — génératrice, — est génératrice de E'.

Thm 17 (d'isomorphisme) : Deux espaces vectoriels de même dimension (finie) sont isomorphes.

d) Quotient d'espaces vectoriels

Prop 18 : Soit $F \subset E$ un sev. L'espace quotient E/F est de dimension finie, appelée codimension de F dans E, et on a :
$\mathrm{codim}_E F = \dim(E/F) = \dim E - \dim F$.

Rmq 19 : Si E est de dimension infinie et F de dimension finie, la codimension de F sur E est finie ssi F admet un supplémentaire de dimension finie dans E.

e) Espace dual

[GOU]

Prop. 20 : On a $\dim_K E = \dim_K E^*$.

Prop. 21 : En dimension finie, E est isomorphe à son bidual E^{**}.

Déf. 22 :
- Si $F \subset E$, on note $F^\perp = \{\varphi \in E^* \mid \forall x \in F, \varphi(x) = 0\}$.
$F^\perp$ est appelé annulateur de F.
- Si $G \subset E^*$, on note $G^\circ = \{x \in E \mid \forall \varphi \in G, \varphi(x) = 0\}$.
G° est appelé orthogonal de G.

Thm 23 : $F \subset E$, $G \subset E^*$. $\dim E = \dim F + \dim F^\perp$.
$\dim E^* = \dim G + \dim G^\circ$.

Appli 24 [invariants de similitude]. Soit $f \in \mathcal{L}(E)$.
Il existe $F_1, \dots, F_r$ sev de E stables par f, tels que :
1. $E = F_1 \oplus \dots \oplus F_r$
2. $\forall i$, $f_i = f|_{F_i}$ est un endomorphisme cyclique de F_i.
3. Si $P_i = \mathrm{polmin}(f_i)$, on a $P_{i+1} | P_i$, $\forall i$.

La suite $(P_i)_{i=1}^r$ est appelée suite des invariants de similitude de f.

DEV

2 - Espaces euclidiens

a) Généralités

ex. 25 : $\mathcal{M}_2(\mathbb{R})$ muni du produit scalaire $(A,B) \mapsto \mathrm{tr}({}^tAB)$.

Thm 26 (thm fondamental) : Dans les espaces euclidiens, il existe toujours une base orthonormée (BON).

Cor. 27 : Si E est euclidien de dimension n, le choix d'une BON permet d'identifier E à $\mathbb{R}^n$ muni de son produit scalaire usuel.

Appli 28 [Classification des formes quadratiques] $K = \mathbb{R}$ ou $\mathbb{C}$. Cela revient à étudier les orbites de l'action de $GL_n(K)$ sur $S_n(K)$ par congruence.
Soit q une forme quadratique sur K^n.
$p(q) = \max\{\dim F \,;\, F \subset K^n, \forall x \in F, x \neq 0 \Rightarrow q(x) > 0\}$
- si $K = \mathbb{C}$; $A, A' \in S_n(K)$ sont dans la même orbite ssi $\mathrm{rg} A = \mathrm{rg} A'$.
- si $K = \mathbb{R}$; $A, A' \in S_n(K)$ sont dans la même orbite ssi
  - $\mathrm{rg} A = \mathrm{rg} A'$.
  - $p(q) = p(q')$ (q (resp. q') forme quad correspondant à A (resp. A'))

[C.G]

b) Endomorphisme adjoint

Prop. 29 : Soit $(E, \langle \cdot,\cdot \rangle)$ euclidien et $f \in \mathcal{L}(E)$. Il existe un unique endomorphisme f^* de E tel que
$\forall x, y \in E, \ \langle f(x), y \rangle = \langle x, f^*(y) \rangle$
f^* est dit adjoint de f. Si $\mathcal{B}$ est une BON de E et A la matrice de f dans cette base, alors $\mathrm{Mat}_{\mathcal{B}}(f^*) = A^* = {}^tA$.

Prop. 30 : Soit $f \in \mathcal{L}(E)$, alors $\mathrm{rg} f = \mathrm{rg} f^*$
(d'où $\mathrm{rg}\, A = \mathrm{rg}\, {}^tA$)

Thm 31 : Si $f \in \mathcal{L}(E)$ autoadjoint ($f = f^*$), alors :
f est diagonalisable ~~et~~ ses sous-espaces propres sont deux à deux orthogonaux.

c) Isométries

Déf. 32 : $f \in \mathcal{L}(E)$ (E euclidien) est une isométrie si pour tout $x, y \in E$, on a $\langle f(x), f(y)\rangle = \langle x, y\rangle$.

thm 33 (réduction des isométries). Soit $u \in \mathcal{L}(E)$ une isométrie. Il existe une base $\mathcal{D}$ dans laquelle

$$\mathrm{Mat}_{\mathcal{D}}(u) = \begin{pmatrix} R_{\theta_1} & & & & \\ & \ddots & & & \\ & & R_{\theta_s} & & & \\ & & & \varepsilon_1 & & \\ & & & & \ddots & \\ & & & & & \varepsilon_r \end{pmatrix}$$

DEV

où R_{θ_i} est une matrice de rotation d'angle θ_i, $\forall i \in [\![1, s]\!]$ et $\varepsilon_j \in \{-1, 1\}$, $\forall j \in [\![1, r]\!]$.

[GOU]

3 - Extension de corps

On considère ici une extension L du corps K (notée L/K).

[PER]

Prop. 34 : L'extension L est un K-espace vectoriel.

Déf. 35 : On appelle degré de l'extension la quantité $[L : K] = \dim_K L$. L'extension est dite finie si son degré est fini.

thm 36 (multiplicativité des degrés). Soient $L \subset M$ deux extensions finies de K. On a $[M:K] = [M:L][L:K]$.

Cor. 37 : En particulier, si M/L et L/K sont finies, alors M/K l'est aussi.

ex. 38 : $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}] = 6$.

4 - Dimension finie en analyse et en géométrie

thm 39 (de Riesz). Dans un espace vectoriel normé de dimension finie, les compacts sont exactement les fermés bornés.

thm 40 : Les applications linéaires entre e.v. normés de dimension finie sont continues.

[B.G.]

Déf. 41 (dimension d'une sous-variété de $\mathbb{R}^n$) : Lorsqu'on définit une sous-variété M de $\mathbb{R}^n$ par des représentations paramétriques, on appelle dimension de M le nombre d de paramètres réels. Le nombre d'équations est appelé codimension de M, et est égal à $n-d$.

thm 42 (Hahn-Banach géométrique). Soient E un espace affine de dimension finie n, $\mathcal{A}$ un ouvert convexe non vide de E, et L un sous-espace affine de E tel que $\mathcal{A} \cap L = \emptyset$. Alors il existe un hyperplan affine H de E qui contient L et ne rencontre pas $\mathcal{A}$.

[GRI] : J. GRIFONE, *Algèbre linéaire*.

[PER] : D. PERRIN, *Cours d'algèbre*.

[GOU] : X. GOURDON, *Les maths en tête, Algèbre*.

[B.G.] : BERGER, GOSTIAUX, *Géométrie différentielle : variétés, courbes et surfaces*.

[C.G.] : CALDERO, GERMONI, *Groupes et géométries*.

Endomorphismes cycliques, invariants de similitude et réduction de Frobenius

2013 – 2014

Théorème.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.
Soit $u \in \mathcal{L}(E)$.
Alors il existe une suite $F_1, \ldots, F_r$ de sous-espaces vectoriels de E non réduits à $\{0\}$ et stables par u telle que :

(i) $E = F_1 \oplus \ldots \oplus F_r$

(ii) $\forall i \in \{1, \ldots, r\}, u_i := u_{|F_i}$ *est un endomorphisme cyclique*

(iii) si P_i désigne le polynôme minimal de u_i, on a :

$$\forall i \in \{1, \ldots, r-1\}, P_{i+1} \mid P_i$$

La suite de polynômes $P_1, \ldots, P_r$ ne dépend que de u. On l'appelle suite des invariants de similitude de u.

On a alors l'existence d'une base $\mathcal{B}$ de E telle que

$$Mat_{\mathcal{B}}(u) = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix}$$

où $C(P_i)$ désigne la matrice compagnon de P_i.
On a $P_1 = \pi_u$ et $P_1 \ldots P_r = \chi_u$.

Lemme.
Soit $u \in \mathcal{L}(E)$ un endomorphisme cyclique.
Alors il existe une base de E dans laquelle la matrice de u est égale à $C(\pi_u)$.

Démonstration. Il existe $x \in E$ tel que $(x, u(x), \ldots, u^{n-1}(x))$ soit une base de E.
Si $\pi_u = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, alors $u^n(x) = -a_{n-1}u^{n-1}(x) - \ldots - a_0 x$ car π_u annule u. $\square$

Démonstration du théorème. La forme matricielle obtenue se déduit immédiatement du lemme.

- Existence : soit $k = \deg(\pi_u)$, soit $x \in E$.
  On note P_x le polynôme unitaire engeandrant l'idéal :

$$\{P \in \mathbb{K}[X] \ / \ P(u)(x) = 0\}$$

et

$$E_x := \{P(u)(x) \ / \ P \in \mathbb{K}[X]\}.$$

Soit $x \in E$ tel que $P_x = \pi_u$ (une preuve de l'existence d'un tel x est donnée en fin de document).
Le sous-espace vectoriel $F := E_x$ est de dimension k et est stable par u.
On pose :

$$e_1 = x, e_2 = u(x), \ldots, e_k = u^{k-1}(x).$$

Alors $(e_1, \ldots, e_k)$ forme une base de F car $\deg(P_x) = k$ (plus de détails sont donnés en fin de document).
On complète $(e_1, \ldots, e_k)$ en une base $(e_1, \ldots, e_n)$ et on considère la base duale $(e_1^*, \ldots, e_n^*)$.

On note $G = \Gamma^\circ$ où $\Gamma = \mathrm{vect}(\{\,{}^t u^i(e_k^*), i \in \mathbb{N}\})$ (orthogonal vis-à-vis du dual).
G est un sev de E stable par u car Γ est stable par ${}^t u$.
Montrons $F \oplus G = E$:
- $F \cap G = \{0\}$:
  On remarque que l'on a, pour $i + j \leq k$,

$$\begin{aligned} \langle {}^t u^i(e_k^*), e_j \rangle &= \langle e_k^*, u^i(e_j) \rangle \\ &= \langle e_k^*, e_{i+j} \rangle \\ &= \delta_{i+j,k}. \end{aligned} \tag{1}$$

  Donc si $y \in F \cap G$, $\langle {}^t u^i(e_k^*), y \rangle = e_{k-i}^*(y) = 0$ pour $0 \leq i \leq k-1$, donc $y = 0$.

- $\dim F + \dim G = n$:
  On a $\pi_{{}^t u} = \pi_u$ donc $\dim \Gamma \leq k$ (on peut aussi dire que $(\mathrm{id}, u, \ldots, u^k)$ est liée donc $(e_k^*, {}^t u(e_k^*), \ldots, {}^t u^k(e_k^*))$ aussi), donc $\dim G = n - \dim \Gamma \geq n - k$.
  D'où $\dim F + \dim G \geq n$, d'où le résultat.

On note P_1 le polynôme minimal de $u_{|F}$ ($\pi_u = P_x = P_1$) et P_2 le polynôme minimal de $u_{|G}$, on a $P_2 \mid P_1$ car $P_1 = \pi_u$.
Puis on recommence sur $u_{|G}$.

- Unicité : soient $F_1, \ldots, F_r$ et $G_1, \ldots, G_s$ vérifiant les hypothèses du théorème.
  On note $P_i = \pi_{u_{|F_i}}$ et $Q_j = \pi_{u_{|G_j}}$.

Supposons $(P_1, \ldots, P_r) \neq (Q_1, \ldots, Q_s)$.
On note $p = \inf\{i, P_i \neq Q_i\}$, p existe car $\sum_i \deg(P_i) = n = \sum_j \deg(Q_j)$ et $\deg(P_i), \deg(Q_j) \neq 0$.

$$P_p(u)(E) = P_p(u)(F_1) \oplus \ldots \oplus P_p(u)(F_{p-1})$$

car $E = F_1 \oplus \ldots \oplus F_r$ et $P_p(u)(F_k) = 0$ pour $k \geq p$ et les F_i sont stables par u.
Or

$$P_p(u)(E) = P_p(u)(G_1) \oplus \ldots \oplus P_p(u)(G_s)$$

et

$$\dim P_p(u)(F_i) = \dim P_p(u)(G_i) \text{ pour } 1 \leq i \leq p-1$$

car d'après le lemme, il existe $\mathcal{B}_i$ et $\mathcal{B}'_i$ telles que $\mathrm{Mat}_{\mathcal{B}_i}(u_{|F_i}) = \mathrm{Mat}_{\mathcal{B}'_i}(u_{|G_i})$.
D'où :

$$0 = \dim P_p(u)(G_p) = \ldots = \dim P_p(u)(G_s)$$

D'où $Q_p \mid P_p$, donc $Q_p = P_p$ par symétrie.

□

Détails supplémentaires

Proposition.
Si $k = \deg(\pi_u)$, $\mathcal{L}_u := \{P(u) \mid P \in \mathbb{K}[X]\}$ est un sev de $\mathcal{L}(E)$ de dimension k, dont une base est $(Id_E, u, \ldots, u^{k-1})$.

Si $l = \deg(P_x)$, E_x est un sev de E de dimension l, dont une base est $(x, \ldots, u^{l-1}(x))$.

Démonstration.

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow \mathcal{L}(E) \\ P &\longmapsto P(u) \end{aligned}$$

est linéaire, $\mathrm{Im}\,\varphi = \mathcal{L}_u$.

$$\ker \varphi = \{P \in \mathbb{K}[X] \ / \ P(u) = 0\} = (\pi_u)$$

Donc

$$\mathcal{L}_u \cong \mathbb{K}[X]/(\pi_u)$$

dont une base est $(1, X, \ldots, X^{k-1})$

Idem avec

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow E \\ P &\longmapsto P(u)(x) \end{aligned}$$

□

Proposition.
Il existe $x \in E$ tel que $P_x = \pi_u$.

Démonstration. Soit $\pi_u = Q_1^{\alpha_1} \dots Q_l^{\alpha_l}$ avec Q_i irréductible unitaire, $\alpha_i > 0$.

- soit $i \in \{1, \dots, l\}$, soit R tel que $\pi_u = Q_i^{\alpha_i} R$.

$$0 = \pi_u(u) = Q_i^{\alpha_i}(u) \circ R(u)$$

Donc

$$\operatorname{Im} R(u) \subseteq \ker Q_i^{\alpha_i}(u)$$

Si

$$\operatorname{Im} R(u) \subseteq \ker Q_i^{\alpha_i - 1}(u)$$

alors

$$Q_i^{\alpha_i - 1}(u) \circ R(u) = 0$$

donc $\pi_u \mid Q_i^{\alpha_i-1}R$, or $\deg Q_i^{\alpha_i-1}R < \deg \pi_u$, donc il existe $a_i \in \operatorname{Im} R(u)$ tel que $Q_i^{\alpha_i-1}(u)(a_i) \neq 0$.
Mais $Q_i^{\alpha_i}(u)(a_i) = 0$ donc $P_{a_i} \mid Q_i^{\alpha_i}$, donc $P_{a_i} = Q_i^{\alpha_i}$ car $P_{a_i} \nmid Q_i^{\alpha_i-1}$ et Q_i est irréductible.
En résumé, pour $1 \leq i \leq l$, il existe $a_i \in E$ tel que $P_{a_i} = Q_i^{\alpha_i}$.

- Montrons que :

$$P_x \wedge P_y = 1 \Longrightarrow P_{x+y} = P_x P_y$$

On a

$$P_x P_y(u)(x+y) = P_x P_y(u)(x) + P_x P_y(u)(y) = 0$$

Donc $P_{x+y} \mid P_x P_y$.
D'autre part,

$$P_{x+y}(u)(y) = -P_{x+y}(u)(x)$$

Donc

$$P_x P_{x+y}(u)(y) = -P_x P_{x+y}(u)(x) = 0$$

Donc $P_y \mid P_x P_{x+y}$ et $P_x \wedge P_y = 1$ donc $P_y \mid P_{x+y}$.
De même, $P_x \mid P_{x+y}$ donc $P_x P_y \mid P_{x+y}$ car $P_x \wedge P_y = 1$.
D'où $P_x P_y = P_{x+y}$.

- Alors pour $1 \leq i \leq l$, il existe a_i tel que $P_{a_i} = Q_i^{\alpha_i}$ et $Q_i^{\alpha_i} \wedge Q_j^{\alpha_j} = 1$ pour $i \neq j$, donc :

$$P_{\sum_{i=1}^{l} a_i} = \prod_{i=1}^{l} P_{a_i} = \pi_u$$

□

Références

[1] Xavier Gourdon, *Algèbre (2e édition)*, Ellipses, 2009, page 290.
R. Goblot Algèbre Linéaire

Réduction des isométries

...

Thm: soit E un espace euclidien et $u \in \mathcal{L}(E)$ une isométrie. Alors il existe une base $\mathcal{B}$ de E telle que :

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} R_{\theta_1} & & & & & \\ & \ddots & & & & \\ & & R_{\theta_s} & & & \\ & & & \varepsilon_1 & & \\ & & & & \ddots & \\ & & & & & \varepsilon_r \end{pmatrix}$$

où $\begin{cases} R_{\theta_i} \in \mathcal{M}_2(\mathbb{R}) \text{ est une rotation d'angle } \theta_i, & \forall i \in [\![1, s]\!] \\ \varepsilon_j \in \{\pm 1\} & \forall j \in [\![1, r]\!] \end{cases}$

démonstration: En dimension 1, $\mathrm{Mat}_{\mathcal{B}}(u) = (\varepsilon)$ avec $\varepsilon = \pm 1$

Initia Supposons le résultat vrai pour tout sous-espace vectoriel strict de E et montrons que le résultat est vrai sur E (on note $n = \dim E$).

On distingue deux cas.

Cas ①: u admet une valeur propre réelle, que l'on note λ et x son vecteur propre associé. On a $\|u(x)\| = \|\lambda x\| = |\lambda| \cdot \|x\|$ et puisque u est une isométrie, $|\lambda| = 1$ et comme $\lambda \in \mathbb{R}$, on a $\lambda \in \{\pm 1\}$

Posons $F = \mathrm{Vect}\{x\}$. F est stable par u :

$\forall \alpha \in \mathbb{R}, \quad u(\alpha x) = \alpha u(x) = (\alpha \lambda) \cdot x \in F$

Par le lemme suivant, on a alors $F^\perp$ stable par u :

Lemme: si F est un sous-espace vectoriel stable par u, alors $F^\perp$ est stable par u.

preuve: soit $y \in F^\perp$. Alors $\forall \alpha \in \mathbb{R}, \ \langle \alpha x, y \rangle = 0$

$u_{|F} \in \mathcal{L}(F)$ est une isométrie donc bijective

donc pour tout $\alpha \in \mathbb{R}$, il existe $z \in F$ tel que $\alpha x = u(z)$

Alors $\langle \alpha x, u(y) \rangle = \langle u(z), u(y) \rangle = \langle z, y \rangle = 0$

$\square$

Donc $u_{|F^\perp} \in \mathcal{L}(F^\perp)$ et l'hypothèse de récurrence appliquée au sous-espace strict $F^\perp$ entraine l'existence d'une base $\mathcal{B}_0$ dans laquelle $\mathrm{Mat}(u_{|F^\perp})$ est de la forme voulue, de même, on en déduit une base $\mathcal{B}_1$ de $F = \mathrm{Vect}\{x\}$.

Puisque $E = F \oplus F^\perp$, on peut considérer $\mathcal{B} = \{\mathcal{B}_0, \mathcal{B}_1\}$ qui est une base de E, dans laquelle $\mathrm{Mat}_{\mathcal{B}}(u)$ est de la forme voulue.

Cas ②: u n'admet pas de valeur propre réelle. On pose alors $v = u + u^*$ qui est un endomorphisme symétrique et admet donc une valeur propre réelle, que l'on note encore λ et x son vecteur propre associé.

$u(v(x)) = u^2(x) + \cancel{\lambda}\, x = \lambda u(x)$

D'où $\quad u^2(x) = \lambda u(x) - x \quad (1)$

La famille $\{x, u(x)\}$ est libre puisque ~~u~~ u ne possède pas de valeur propre réelle. Posons $F := \mathrm{Vect}(\{x, u(x)\})$. F est stable par u :

$$\forall \alpha, \beta \in \mathbb{R}, \quad u(\alpha x + \beta u(x)) = \alpha u(x) + \beta u^2(x) \overset{(1)}{=} (\alpha + \beta\lambda) u(x) - \beta x$$

donc $u(F) \subset F$ et F est stable par u. Par le lemme précédent, on en déduit que $F^\perp$ est stable par u.

- Soit $\mathcal{B}_0$ une BON de $u_{|F}$ et $N := \mathrm{Mat}_{\mathcal{B}_0}(u_{|F})$

Alors ${}^t NN = N{}^t N = \mathrm{Id}$ et en notant $N = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

on a : $\begin{cases} a^2 + b^2 = a^2 + c^2 = 1 \\ ab + cd = 0 \end{cases}$

donc $b = \pm c$. Si $b = c$ alors N symétrique et u admet une valeur propre réelle, contradiction. Donc $b = -c$ et $a = d$

puisque $a^2 + b^2 = 1$, il existe $\theta \in [0; 2\pi]$ tel que $a = \cos\theta$ et $b = \sin\theta$.

Donc $N = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \mathrm{Mat}_{\mathcal{B}_0}(u_{|F})$

- On applique l'hypothèse de récurrence au sous-espace $F^\perp$: il existe $\mathcal{B}_1$ base de $F^\perp$ dans laquelle $\mathrm{Mat}_{\mathcal{B}_1}(u_{|F^\perp})$ est de la forme voulue.

Comme dans le cas précédent, on peut conclure en considérant $\mathcal{B}$ base de E égale à $\{\mathcal{B}_0, \mathcal{B}_1\}$, ce qui est possible car $E = F \oplus F^\perp$.

$\square$

Référence : Math-en-tête, Gourdon (p.256, 2nd Edition)

Application :

Thm : Le groupe $SO_n(\mathbb{R})$ est connexe.

démonstration : On veut montrer que toute matrice de $SO_n(\mathbb{R})$ peut être relié à $\mathrm{Id} \in \mathcal{M}_n(\mathbb{R})$ par un chemin. Soit $M \in SO_n(\mathbb{R})$.

Puisque E est euclidien, par le théorème précédent, M est semblable à la matrice C donnée par

$$C = \begin{pmatrix} R_{\theta_1} & & & & & \\ & \ddots & & & & \\ & & R_{\theta_r} & & & \\ & & & \varepsilon_1 & & \\ & & & & \ddots & \\ & & & & & \varepsilon_s \end{pmatrix}$$

Puisque $M \in SO_n(\mathbb{R})$ $\det M = \det C = 1$

or $\det C = \left(\prod_{i=1}^{p} \cos^2 \theta_i\right) \cdot (-1)^{\alpha}$ où $\alpha \leq d$

nécessairement α est pair donc les coefficients ε_i valant -1 sont pairs, on peut donc les regrouper en blocs $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\pi & \sin\pi \\ -\sin\pi & \cos\pi \end{pmatrix}$

Pour tout $t \in [0,1]$, on considère $\varphi(t)$ l'endomorphisme ayant pour matrice dans $\mathcal{B}$.

$$\mathrm{Mat}_{\mathcal{B}}(\varphi(t)) = \begin{pmatrix} R_{\theta_1 t} & & & & & & & \\ & \ddots & & & & & & \\ & & R_{\theta_p t} & & & & & \\ & & & R_{\pi t} & & & & \\ & & & & \ddots & & & \\ & & & & & R_{\pi t} & & \\ & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix}$$

où $R_{\theta_i t}$ est une rotation d'angle $\theta_i t$

pour tout $t \in [0,1]$, $\mathrm{Mat}_{\mathcal{B}}\,\varphi(t) \in SO_n(\mathbb{R})$, de plus $\varphi(0) = \mathrm{Id}$ et $\varphi(1) = u$

donc φ est bien un chemin entre Id et u dans $SO_n(\mathbb{R})$. $\square$

Autre application :

prop : soit f une transformation orthogonale de E euclidien. Alors f peut s'écrire sous la forme

$$f = s_1 \circ \dots \circ s_r \quad \text{où } s_i \text{ sont des réflexions}$$

rem : décomposition non unique.

Référence : Mathématiques L3, Szpirglas