151

Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie).
Rang. Exemples et applications.

Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel.

I Familles de vecteurs et dimension

1) Base d'un espace vectoriel [Gri]

Définition 1 Soient $(e_i)_{i\in I}$ une famille de E et $\varphi : \begin{cases} \mathbb{K}^{(I)} \to E \\ (x_i) \mapsto \sum_{i\in I} x_i e_i \end{cases}$

On dit que $(e_i)_{i\in I}$ est libre (resp. génératrice) si φ est injective (resp. surjective), et que c'est une base si φ est bijective.

Dans la suite, on suppose que E est de dimension finie, i.e. qu'il existe une famille génératrice finie.

Exemples
- Si $\mathbb{P}$ est l'ensemble des nombres premiers, $(\ln p)_{p\in\mathbb{P}}$ est libre dans le $\mathbb{Q}$-ev $\mathbb{R}$.
- Base canonique de $\mathbb{K}_n[X]$: $(1, X, \dots, X^n)$
  de $\mathbb{K}^n$: $((1,0,\dots,0),(0,1,0,\dots,0),\dots,(0,\dots,0,1))$

Théorème 2 (Base incomplète)
Si L (resp. G) est libre (resp. génératrice) dans E, alors il existe une base B de E telle que $L \subseteq B \subseteq G$.

Ainsi, tout ev de dim finie admet une base. Le cardinal de cette base est un invariant.

Théorème 3 Deux bases de E ont toujours le même cardinal.
On note ce cardinal $\dim_{\mathbb{K}} E$.

Exemples
- $\dim_{\mathbb{C}}(\mathbb{C}) = 1$ mais $\dim_{\mathbb{R}}(\mathbb{C}) = 2$.
- Si $X = \{a_1,\dots,a_n\}$, $(\{a_1\},\dots,\{a_n\})$ forme une base de $\mathbb{Z}/2\mathbb{Z}$-ev $\mathcal{P}(E)$ muni de la différence symétrique Δ.
- $\dim \mathbb{K}_n[X] = n+1$
- $\dim \mathbb{K}_d[X_1,\dots,X_n] = \binom{n+d}{d}$.

Pour montrer l'importance du thm 2, voyons quelques contre-exemples dans les modules :
$\{2,3\}$ est génératrice minimale de $\mathbb{Z}$, mais ce n'est pas une base.
Les familles libres du $\mathbb{Z}$-module $\mathbb{Q}$ sont des singletons : on ne peut pas les compléter.

Applications linéaires

Prop 4 Soit $f \in \mathcal{L}(E,F)$ et (e_i) une base de E.
f est injective (resp. surjective, bijective) ssi $(f(e_i))$ est libre (resp. génératrice, une base).

Corollaire $f \in \mathrm{End}(E)$ est bijectif ssi injectif ssi surjectif.

⚠ Deux ev sont isomorphes ssi ils ont même dimension.

Exemples
- Si $\dim E = n$ et $\dim F = p$, $\mathcal{L}(E,F) \simeq \mathcal{M}_{p,n}(\mathbb{K})$ de dimension np.
- Si p est premier, un groupe abélien d'exposant p est un $\mathbb{Z}/p\mathbb{Z}$-ev.

Ainsi, le cardinal d'un corps fini est la puissance d'un premier, d'un anneau booléen fini est une puissance de 2.

- Interpolation de Lagrange

Si $(x_i)_{i=1}^n \in \mathbb{K}^n$ est une famille d'éléments deux à deux distincts, et $(y_i) \in \mathbb{K}^n$, il existe un unique $P \in \mathbb{K}_{n-1}[X]$ tel que $P(x_i) = y_i$ $(\forall i \in [\![1,n]\!])$.

2) Sous-espaces vectoriels

Thm 5 Si F est un sev de E, on a $\dim F \leq \dim E$.
(donc F est de dimension finie)

Application Étude de l'algèbre $\mathrm{End}(E)$ [Cog]

Prop 6 Le centre de $\mathrm{End}(E)$ est l'ensemble des homothéties de E.

Prop 7 (Idéaux) I est un idéal bilatère de $\mathrm{End}(E)$ ssi $I = \{0\}$ ou $\mathrm{End}(E)$.
C'est un idéal gauche ssi il existe un sev F tel que $I = \{u \in \mathrm{End}(E) \mid F \subseteq \ker u\}$.
Ce sont des idéaux principaux.
(Des idéaux sont des sev de $\mathrm{End}(E)$)
Note : ce résultat est faux si E n'est qu'un module.
Par exemple, les $\mathcal{M}_n(d\mathbb{Z})$ sont des idéaux de $\mathcal{M}_n(\mathbb{Z})$.

Prop 8 (Thm Skolem-Noether) [H2G2] DEV
Les automorphismes d'algèbre de $\mathrm{End}(E)$ sont tous intérieurs.

Thm 9 Tout sev de E admet un supplémentaire.

La proposition suivante aide à la caractérisation des sommes directes.

Prop 10 (Grassman) Si F et G sont des sev, $\dim(F+G) = \dim F + \dim G - \dim(F \cap G)$

Application Borne de Singleton Un code linéaire de type (n,k,d)
(identifiable à un sev de $(\mathbb{Z}/2\mathbb{Z})^n$ de dimension k et de poids minimal d)
vérifie $n - k \geq d - 1$.

Corollaire Si F et G sont en somme directe, $\dim(F \oplus G) = \dim F + \dim G$.

Prop 11 Soient $E_1, \dots, E_p$ des sev de E.

Alors $E = \bigoplus_{i=1}^{p} E_i$ ssi pour toutes bases $B_1, \dots, B_p$ de $E_1, \dots, E_p$, $B_1 \sqcup \dots \sqcup B_p$ est une base de E.

ssi $\dim E = \sum_{i=1}^{p} \dim E_i$ et $E = \sum_{i=1}^{p} E_i$.

Application $g \in End(E)$ diagonalisable ssi [Gri8]

- Son polynôme caractéristique est scindé : $\chi_g = (-1)^{\dim E}(X-\lambda_1)^{\alpha_1} \dots (X-\lambda_p)^{\alpha_p}$
- Les dimensions des espaces propres sont maximales, i.e. $\dim E_{\lambda_i} = \alpha_i \quad (\forall i \in [\![1, p]\!])$

Par exemple, $\begin{pmatrix} t & 1 \\ 1 & t \end{pmatrix}$ est diagonalisable dans $\mathbb{R}$.

Cette étude des dimensions de sev permet des preuves par récurrence.

Pour rester dans le domaine des réductions d'endomorphisme :

↝ $g \in End(E)$ trigonalisable ssi χ_g est scindé.

↝ Une matrice symétrique réelle est diagonalisable dans une base orthonormée.

II Applications linéaires et rang

Déf 12 Le rang d'une application linéaire (ou d'une matrice) est la dimension de son image.

1) Dualité [Gri8]

Si $E^* = \mathcal{L}(E, \mathbb{K})$, on a $\dim E^* = \dim E$ donc E^* isomorphe à E.

Chaque base (e_i) de E donne une base duale (e_i^*) de E^* t.q. $e_i^*(e_j) = \delta_{i,j}$

Déf 13 Si F est un sev de E, on note

$F^\circ = \{\varphi \in E^* \mid \varphi(g) = 0 \ \forall g \in F\}$ l'annulateur de F.

Exhiber une base de F° donne une méthode efficace pour vérifier qu'un élément est dans F.

Prop 14 $\dim E = \dim F + \dim F^\circ$.

La notion suivante permet de calculer les bases duales ou d'annulateurs et est riche en applications.

Déf 15 Soit $g \in \mathcal{L}(E, F)$. On appelle transposée de g l'application linéaire

$${}^t g : \begin{cases} F^* \longrightarrow E^* \\ \varphi \longmapsto \varphi \circ g \end{cases}$$

Thm 16 Soient (e_i) et (ε_j) des bases de E et F, et (φ_i), (η_j) les bases duales de E^* et F^*.

Alors $M({}^t g)_{\eta_j, \varphi_i} = {}^t A$, où $A = M(g)_{e_i, \varepsilon_j}$.

Applications ↝ Calcul d'une base duale par inversion de la transposée.

↝ Déterminer une base de F° avec le noyau de la transposée d'une matrice de passage de la base canonique à une base de F.

Prop 17 Si $g \in \mathcal{L}(E, F)$, alors $(\mathrm{Im}\, g)^\circ = \mathrm{Ker}({}^t g)$.

Corollaires

- $rg(A) = rg({}^t A)$ si $A \in \mathcal{M}_{n,p}(\mathbb{K})$.
- I est un idéal à droite de $End(E)$ ssi il existe un sev F tel que $I = \{u \in End(E) \mid \mathrm{Im}\, u \subseteq F\}$. [Cog]

Terminons avec un théorème de calcul différentiel lié au rang et aux formes linéaires.

Thm 18 (extrema liés) Soient $g, g_1, \dots, g_p : \mathcal{U} \to \mathbb{R}$ de classe C^1 où [All]

$\mathcal{U}$ est un ouvert de $\mathbb{R}^n$. On note $\Gamma = \{x \in \mathcal{U} \mid g_1(x) = \dots = g_p(x) = 0\}$.

Si $g|_\Gamma$ admet un extremum en $a \in \Gamma$ et $(dg_{1,a}, \dots, dg_{p,a})$ est libre,

Alors il existe $\lambda_1, \dots, \lambda_p \in \mathbb{R}$ t.q.

$$dg_a = \sum_{i=1}^{p} \lambda_i \, dg_{i,a}$$

Application $SO(n)$ est l'ensemble des éléments de $SL_n(\mathbb{R})$ de norme $\|\cdot\|_2$ minimale.

2) Théorème du rang [G2]

On étudie l'action de $G = GL_m(\mathbb{K}) \times GL_n(\mathbb{K})$ sur $\mathcal{M}_{m,n}(\mathbb{K})$ donnée par $(P, Q) \cdot A = PAQ^{-1}$, appelée action de Steinitz.

A et B sont dans la même orbite si ce sont les matrices d'un même endomorphisme dans des bases de départ et d'arrivée potentiellement différentes.

Thm 19 (rang)

A et B sont dans la même orbite ssi $rg(A) = rg(B)$.

La preuve donne en passant une version plus habituelle du thm du rang.

Thm 20 Si $g \in \mathcal{L}(E, F)$, alors $\dim E = rg\, g + \dim(\mathrm{Ker}\, g)$.

En remarquant que $\mathcal{M}_n(\mathbb{K})^* = \{g_A : X \longmapsto \mathrm{Tr}(AX) \mid A \in \mathcal{M}_n(\mathbb{K})\}$ on a une première application de cette classification :

Prop 21 Si $n \geq 3$, tout hyperplan de $\mathcal{M}_n(\mathbb{K})$ intersecte $GL_n(\mathbb{K})$.

Si $\mathbb{K} = \mathbb{C}$, on a aussi des applications topologiques.

Prop 22

- L'ensemble $\mathcal{O}_n = \{M \in \mathcal{M}_n(\mathbb{C}) \mid rg(M) = n\}$ est connexe.
- Les composantes connexes de $\mathcal{P} = \{P \in \mathcal{M}_n(\mathbb{C}) \mid P^2 = P\}$ sont les $\mathcal{P}_n = \{P \in \mathcal{P} \mid rg\, P = n\}$.

Méthode du pivot de Gauss : Permet le calcul effectif du rang.

(Pour justifier sa correction, on remarque que chaque opération élémentaire sur les lignes ou les colonnes est le produit par une matrice inversible, ce qui ne modifie pas le rang.

(3) Utilisations du déterminant

Prop 23 | Une famille de vecteurs est une base (ou la matrice associée est inversible) ssi son déterminant est non nul.

Application $GL_n(\mathbb{C})$ est un ouvert de $\mathcal{M}_n(\mathbb{C})$.

[Grig]

Thm 24 || Le rang d'une matrice est l'ordre du plus grand mineur non nul :

$$\operatorname{rg} A = \max\{ r \in \mathbb{N} \mid \exists I, \exists J, |I| = |J| = r \text{ et } \Delta_{I,J}(A) \neq 0 \}$$

où $\Delta_{I,J} : (a_{i,j})_{\substack{1 \le i \le m \\ 1 \le j \le n}} \longmapsto \det\left(a_{i,j}\right)_{\substack{i \in I \\ j \in J}}$

Corollaire | Si L est une extension de corps de $\mathbb{K}$, et $A \in \mathcal{M}_{n,p}(\mathbb{K})$, alors le rang de A est le même sur L et sur K.

Application | Si K est de caractéristique 0 et L est une extension de K, $U \in \mathcal{M}_n(K)$ est semi-simple dans K ssi U est semi-simple dans L.

Replaçons-nous dans la situation où $\mathbb{K} = \mathbb{C}$ pour donner des applications topologiques au Thm 24.

Prop 25 $\overline{\mathcal{O}_n} = \bigcup_{0 \le k \le n} \mathcal{O}_n$

Corollaires | $\rightsquigarrow$ $GL_n(\mathbb{C})$ est dense dans $\mathcal{M}_n(\mathbb{C})$.
$\rightsquigarrow$ Le rang est semi-continu inférieurement.
Ainsi lorsqu'une suite de matrices A_n converge vers B, on a

$$\operatorname{rg}(B) \le \liminf\left(\operatorname{rg}(A_n)\right)$$

Le résultat de densité permet d'obtenir facilement des théorèmes non triviaux.

Prop 26 | • Si $A, B \in \mathcal{M}_n(K)$, où $\mathbb{K} = \mathbb{C}$, alors $\chi_{AB} = \chi_{BA}$.
• En réutilisant la classification des orbites pour l'action de Steinitz, on voit que $\chi_{AB} = \chi_{BA}$ même si $\mathbb{K} \neq \mathbb{C}$. [How]

III Extensions de corps [Per]

Def 27 | • Si L est une extension de K, on note $[L:K]$ la dimension de L en tant que K-ev.
• $a \in L$ est dit algébrique sur K s'il existe $P \in K[X]$ tel que $P(a) = 0$.

Thm 28 | a est algébrique ssi $K[a] = K(a)$ ssi $[K[a]:K] < \infty$ $\rightsquigarrow$ $[K(a):K]$ est alors le degré du polynôme minimal de a.

Thm 29 (~~Base télescopique~~) || Si $L \supseteq M$ sont des extensions de K, on a $[L:K] = [L:M][M:K]$

Grâce à ces deux résultats, les techniques vectorielles ont de nombreuses applications lorsqu'elles sont combinées à la théorie des corps :

$\rightsquigarrow$ **Prop 30** $\{ x \in L \mid x \text{ est algébrique sur } K \}$ est un corps.
Ainsi, $\sqrt{5} + \sqrt[3]{7}\sqrt[5]{3}$ est algébrique sans que l'on ait besoin d'exhiber un polynôme annulateur.

[Cog] $\rightsquigarrow$ **Prop 31** | Soient $a_1, \dots, a_n$ des entiers naturels deux à deux distincts dont au moins un n'est pas un carré d'entier. Alors $\sum_{i=1}^{n} \sqrt{a_i} \notin \mathbb{Q}$. DEV

Terminons avec un autre théorème pouvant se prouver via les méthodes décrites au long de la leçon.

Thm 32 (Frobenius) [Wiki] || Les seules algèbres à division (corps non commutatifs) de dimension finie sur $\mathbb{R}$ sont $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$ (le corps des quaternions).

Références

[Grig] Joseph Grifone, Algèbre linéaire
[Cog] Michel Cognet, Algèbre linéaire
[Ales] M. Alessandri, Thèmes de géométrie
[H2G2] Caldero & Germoni, Histoire hédoniste des groupes et géométries
[Per] Daniel Perrin, Cours d'Algèbre
[Wiki] Wikipédia — "Théorème de Frobenius (algèbre)"
[How] Ralph Howard, "Characteristic polynomial of a product"

Théorème Soient $a_1, \dots, a_n$ des entiers naturels deux à deux distincts dont au moins un n'est pas un carré d'entier.
Alors $\sum_{i=1}^{n} \sqrt{a_i} \notin \mathbb{Q}$.

Preuve On considère des éléments $p_1, \dots, p_n \geq 2$ sans facteurs carrés, premiers entre eux deux à deux.
Posons pour $i \in [\![1,n]\!]$, $x_i = \sqrt{p_i}$
$$K_i = \mathbb{Q}[x_1, \dots, x_i]$$

Lemme 1 Pour $S \subseteq [\![1,n]\!]$, on pose $X_S = \prod_{s \in S} x_s$.
Alors $K_n = \mathrm{Vect}(G_n)$, où $G_n = \{ X_S \mid S \subseteq [\![1,n]\!] \}$.
(Note : par convention, $X_\emptyset = 1$).

En effet, si S et S' sont des parties de $[\![1,n]\!]$, on a $X_S X_{S'} = \left(\prod_{i \in S \cap S'} p_i\right) X_{S \Delta S'}$
où $S \Delta S'$ est la différence symétrique.
Donc $\mathrm{Vect}(G_n)$ est stable par produit : c'est une algèbre contenant $\mathbb{Q}$ et les x_i.
Or, toute algèbre contenant $\mathbb{Q}$ et les x_i contient G_n, donc $\mathrm{Vect}(G_n) = \mathbb{Q}[x_1, \dots, x_n]$.

Lemme 2 Pour $i \in [\![1,n]\!]$, $[K_i : \mathbb{Q}] = 2^i$. Ainsi, G_n est une base de K_n.

On procède par récurrence sur i :
- le polynôme minimal de x_1 est $X^2 - p_1$, donc $[K_1 : \mathbb{Q}] = 2$.
- supposons le lemme vérifié pour tous les entiers $\leq i-1$.

On a $[K_i : \mathbb{Q}] = [K_i : K_{i-1}][K_{i-1} : \mathbb{Q}] = [K_i : K_{i-1}] \cdot 2^{i-1}$.
Le lemme 1 montre que K_i est engendré par une famille de cardinal 2^i,
donc $[K_i : \mathbb{Q}] \leq 2^i$. Ainsi, $[K_i : K_{i-1}] \in \{1, 2\}$.

Supposons que $[K_i : K_{i-1}] = 1$.

On sait que $[K_{i-1} : K_{i-2}] = 2$, d'où $K_{i-1} = K_{i-2} \oplus x_{i-1} K_{i-2}$.
Puisque $K_i = K_{i-1}$, il existe $\alpha, \beta \in K_{i-2}$ tels que
$$x_i = \alpha + \beta x_{i-1}.$$
Alors $x_i^2 = p_i = (\alpha^2 + p_{i-1}\beta^2) + 2\alpha\beta x_{i-1}$,
donc $\alpha\beta = 0$.

→ Si $\alpha = 0$: $x_i = x_{i-1}\beta$, donc $x_{i-1} x_i = p_{i-1}\beta \in K_{i-2}$.
En posant $y_s = x_s$ si $s \leq i-2$ et $y_{i-1} = x_{i-1}x_i$, $= \sqrt{p_{i-1}p_i}$
et $H = \mathbb{Q}[y_1, \dots, y_{i-1}]$,
on a $[H : \mathbb{Q}] \leq 2^{i-2}$ car $H \subseteq K_{i-2}$,
et $[H : \mathbb{Q}] = 2^{i-1}$ par hypothèse de récurrence car $p_1, \dots, p_{i-2}, p_{i-1}p_i$ sont deux à deux premiers entre eux et sans facteurs carrés.
Ce qui est absurde.

→ Si $\beta = 0$: Alors $x_i \in K_{i-2}$,
si $H = \mathbb{Q}[x_1, \dots, x_{i-2}, x_i]$, on a comme précédemment
$[H : \mathbb{Q}] = 2^{i-1}$ par hypothèse de récurrence
alors que $H \subseteq K_{i-2}$.

Donc $[K_i : K_{i-1}] = 1$ est absurde, et on a $[K_i : K_{i-1}] = 2$.

Choisissons pour les p_i chaque nombre premier facteur d'un a_j, pour $j \in [\![1, k]\!]$.

Si a_j n'est pas un carré d'entier, il existe $J_j \subseteq [\![1, n]\!]$ non vide tel que

$$\sqrt{a_j} / x_{J_j} = \alpha_j \in \mathbb{N}^*.$$

~~Si I est l'ensemble des indices j pour lesquels a_j n'est pas un carré~~

~~On a : Il existe $\alpha_0 \in \mathbb{N}$ et $H \subseteq \mathcal{P}([\![1,n]\!])$ tq $\sum_{i=1}^{k} \sqrt{a_i} = \alpha_0 x_\emptyset + \sum_{J \in H} \beta_J x_J$~~

Il existe donc $H \subseteq \mathcal{P}([\![1, n]\!]) \setminus \{\emptyset\}$, $\alpha_0 \in \mathbb{N}$ et pour chaque $J \in H$ un $\beta_J \in \mathbb{N}^*$ tels que $q := \sum_{i=1}^{k} \sqrt{a_i} = \alpha_0 x_\emptyset + \sum_{J \in H} \beta_J x_J$.

Si q était rationnel, on aurait donc une sous famille $\{x_\emptyset\} \cup H$ de $\mathcal{G}_n$ qui n'est pas libre.

Ce qui est absurde puisque $\mathcal{G}_n$ est une base.

Donc $\sum_{i=1}^{k} \sqrt{a_i} \notin \mathbb{Q}$. □

Idéaux gauches de $\mathcal{L}(E)$: ce sont les ensembles de la forme $\mathcal{I}_F = \{ v \in \mathcal{L}(E) \mid \ker v \supseteq F \}$ et ils sont tous principaux.

Preuve

Lemme 1 Soient E, F, G des ev, $u \in \mathcal{L}(E,F)$ et $u_1, \dots, u_n \in \mathcal{L}(E,G)$.
Il existe $h_1, \dots, h_n \in \mathcal{L}(G,F)$ tels que $u = \sum_{i=1}^{n} h_i \circ u_i$ ssi $\bigcap_{i=1}^{n} \ker(u_i) \subseteq \ker(u)$.

Par récurrence sur n : Si $n=1$, c'est le thm de factorisation

$$\begin{array}{ccc} E & \xrightarrow{u} & F \\ & \searrow^{u_1} & \uparrow h_1 \\ & & G \end{array}$$

h_1 existe ssi $\ker u_1 \subseteq \ker u$.

Pour l'hérédité, supposons $\bigcap_{i=1}^{n} \ker(u_i) \subseteq \ker(u)$, et le lemme vérifié au rang $n-1$.

Alors $\bigcap_{i=1}^{n-1} (\ker(u_i) \cap \ker(u_n)) \subseteq \ker u \cap \ker u_n$.

D'où, en posant $u' = u|_{\ker u_n}$ et $u_i' = u_i|_{\ker u_n}$, $\bigcap_{i=1}^{n-1} \ker(u_i') \subseteq \ker(u')$.

Il existe $h_1, \dots, h_{n-1} \in \mathcal{L}(G,F)$ tq $u' = \sum_{i=1}^{n-1} h_i \circ u_i'$.

Ainsi, $\ker(u_n) \subseteq \ker\left(u - \sum_{i=1}^{n-1} h_i \circ u_i\right)$, et par la première étape,

$u - \sum_{i=1}^{n-1} h_i \circ u_i = h_n \circ u_n$ pour un certain $h_n \in \mathcal{L}(G,F)$.

Soit I un idéal gauche de $\mathcal{L}(E)$.

I est en particulier un ev de dimension finie, soit $(u_1, \dots, u_n)$ une base de I.

Posons $F = \bigcap_{i=1}^{n} \ker(u_i)$.

- Alors si $v \in I$, et $x \in F$, comme v est combinaison linéaire des u_i on a $v(x) = 0$.
  Donc $I \subseteq \mathcal{I}_F$.
- Réciproquement, si $v \in \mathcal{I}_F$, par le lemme 1, il existe $h_1, \dots, h_n \in \mathcal{L}(E)$ tels que
  $v = \sum_{i=1}^{n} h_i \circ u_i \in I$ (car c'est un idéal à gauche)
  Donc $\boxed{\mathcal{I}_F = I}$.

Soit G un supplémentaire de F dans E, et p le projecteur sur G parallèlement à F.

On a $\ker p = F$.

Donc $\mathcal{I}_F = \{ v \in \mathcal{L}(E) \mid \ker p \subseteq \ker v \}$

$= \{ w \circ p \mid w \in \mathcal{L}(E) \}$ par le thm de factorisation.

$= \mathcal{L}(E)\, p$. C'est un idéal principal.

□

Théorème de Skolem-Noether

Les automorphismes d'algèbre de $\mathcal{M}_n(\mathbb{K})$ sont tous intérieurs.

Preuve On considère la base canonique $(E_{ij})_{1\leq i,j\leq n}$ de $\mathcal{M}_n(\mathbb{K})$.

Notons la relation fondamentale $E_{ij}E_{kl} = \delta_{jk}E_{il}$. (*)

Soit $\varphi : \mathcal{M}_n(\mathbb{K}) \to \mathcal{M}_n(\mathbb{K})$ un automorphisme d'algèbre.

Si $G \in \mathcal{M}_n(\mathbb{K})$, $\varphi(G) = \varphi(G)\varphi(I_n)$, en particulier en choisissant G tel que $\varphi(G) \in GL_n(\mathbb{K})$, on a $\varphi(I_n) = I_n$.

φ étant aussi un automorphisme d'ev, il suffit d'exhiber $P \in GL_n(\mathbb{K})$ tel que

$$\varphi(E_{ij}) = PE_{ij}P^{-1} \quad \text{pour } i,j \in [\![1,n]\!].$$

Notons $E_{ij}' = \varphi(E_{ij})$

Lemme 1 Les E_{ii}' sont des projecteurs tels que $\mathbb{K}^n = \bigoplus_{i=1}^{n} \mathrm{Im}(E_{ii}')$

- La relation $I_n = \sum_{i=1}^{n} E_{ii}$ donne $I_n = \sum_{i=1}^{n} E_{ii}'$, et donc $\mathbb{K}^n = \sum_{i=1}^{n} \mathrm{Im}(E_{ii}')$.
- $E_{ii}E_{jj} = \delta_{ij}E_{ii}$, d'où $E_{ii}'E_{jj}' = \delta_{ij}E_{ii}'$ d'après (*). Ainsi, $(E_{ii}')^2 = E_{ii}'$ est un projecteur. De plus, $E_{ii}'E_{jj}' = 0$ si $i \neq j$.
- Si $x = \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$, où $\alpha_i, \beta_i \in \mathrm{Im}(E_{ii}')$, on a $E_{ii}'x = \alpha_i = \beta_i$ pour tout i.

  D'où $\mathbb{K}^n = \bigoplus_{i=1}^{n} \mathrm{Im}(E_{ii}')$.

Comme $E_{ij}' \neq 0$, on a $\mathrm{rg}\, E_{ii}' > 0$, et $\sum_{i=1}^{n} \mathrm{rg}\, E_{ii}' = n$.

Donc $\mathrm{rg}\, E_{ii}' = 1$ pour tout i.

Posons $\mathrm{Im}(E_{11}') = \mathrm{Vect}(e_1')$.

Pour $i \in [\![2,n]\!]$, on pose aussi $e_i' = E_{i1}'e_1'$

Lemme 2 $e' = (e_1', \dots, e_n')$ forme une base de $\mathbb{K}^n$.

- Si $x \in \mathbb{K}^n$, $x = \sum_{i=1}^{n} E_{ii}'x = \sum_{i=1}^{n} E_{i1}'(E_{1i}'x)$

  Or, $E_{1i}'x = E_{11}'(E_{1i}'x) \in \mathrm{Vect}(e_1')$. Posons $E_{1i}'x = \alpha_i e_1'$.

  Alors $x = \sum_{i=1}^{n} \alpha_i E_{i1}'e_1' = \sum_{i=1}^{n} \alpha_i e_i'$.

  Donc $(e_1', \dots, e_n')$ est génératrice.
- On a une famille génératrice de cardinal n, c'est donc bien une base de $\mathbb{K}^n$.

Soit $(e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$.

Posons P la matrice de passage de la base canonique à la base e' :

$$P(e_i) = e_i' \quad \text{pour tout } i.$$

Alors pour tout $i,j \in [\![1,n]\!]$, $k \in [\![1,n]\!]$,

$$E_{ij}'e_k' = E_{ij}'E_{k1}'e_1' \overset{(\text{par } (*))}{=} \delta_{jk}E_{i1}'e_1' = \delta_{jk}e_i'.$$

$$PE_{ij}P^{-1}e_k' = PE_{ij}e_k = P(\delta_{jk}e_i) = \delta_{jk}e_i'$$

Donc $E_{ij}' = PE_{ij}P^{-1}$, et $\varphi : M \longmapsto PMP^{-1}$ est intérieur. □