

I. Calcul matriciel

$[A_{i,j}]_{k,l}$ est le terme (k,l) de la matrice bloc $A_{i,j}$ extraite de la matrice A .

Produit matriciel : $[AB]_{i,j} = \sum_n [A]_{i,n} [B]_{n,j} = L_i(A) \times L_j(B)$

Rappels de sup :

Pour E \mathbb{K} -ev de dimension n , \mathcal{B} base de E et $U = (u_1, \dots, u_p) \in E^p$:

$$\text{Mat}_{\mathcal{B}} U = \text{Mat}_{\mathcal{B}}(u_1, \dots, u_p) = [\mathcal{B}^*(u_1), \dots, \mathcal{B}^*(u_p)] \in \mathfrak{M}_{n,p}(\mathbb{K})$$

Pour $A \in \mathfrak{M}_{m,n}(\mathbb{K})$, $u_A: \begin{cases} \mathbb{K}^n & \longrightarrow \mathbb{K}^m \\ X & \longmapsto AX \end{cases}$ est l'application linéaire canoniquement associée à A .

$\varphi: \begin{cases} \mathfrak{M}_{m,n}(\mathbb{K}) & \longrightarrow L(\mathbb{K}^n, \mathbb{K}^m) \\ A & \longmapsto u_A \end{cases}$ est un isomorphisme de \mathbb{K} -ev, et, pour $A \in \mathfrak{M}_{m,n}(\mathbb{K})$ et $B \in \mathfrak{M}_{n,p}(\mathbb{K})$:

$$u_{AB} = u_A \circ u_B .$$

De plus, $\varphi: \begin{cases} \mathfrak{M}_n(\mathbb{K}) & \longrightarrow L(\mathbb{K}^n) \\ A & \longmapsto u_A \end{cases}$ est un isomorphisme de \mathbb{K} -algèbre.

Proposition - définition : soit E, F des \mathbb{K} -ev de dimensions $\dim E = n$ et $\dim F = m$. Soit \mathcal{B} base de E et \mathcal{C} base de F .

- 1) $\forall f \in L(E, F), \exists! A \in \mathfrak{M}_{m,n}(\mathbb{K}) \mid \forall x \in E, \mathcal{C}^*(f(x)) = A\mathcal{B}^*(x)$.
- 2) $\forall A \in \mathfrak{M}_{m,n}(\mathbb{K}), \exists! f \in L(E, F) \mid \forall x \in E, \mathcal{C}^*(f(x)) = A\mathcal{B}^*(x)$.

Autrement dit, l'application $\text{Mat}_{\mathcal{B}, \mathcal{C}}: \begin{cases} L(E, F) & \longrightarrow \mathfrak{M}_{m,n}(\mathbb{K}) \\ f & \longmapsto \text{Mat}_{\mathcal{B}, \mathcal{C}} f \end{cases}$ est bijective.

$$\left| \begin{array}{l} \text{Preuve : } \forall x \in E, \mathcal{C}^*(f(x)) = A\mathcal{B}^*(x) \iff \mathcal{C}^* \circ f = u_A \circ \mathcal{B}^* = \varphi(A) \circ \mathcal{B}^* \\ \text{Pour } f \in L(E, F), \varphi(A) = \mathcal{C}^* \circ f \circ \mathcal{B}^{*-1}, \text{ soit } A = \varphi^{-1}(\mathcal{C}^* \circ f \circ \mathcal{B}^{*-1}). \\ \text{De même, } f = \mathcal{C}^{*-1} \circ u_A \circ \mathcal{B}^*. \end{array} \right.$$

Remarque : au passage, on a que $\forall k \in \llbracket 1, n \rrbracket, \mathcal{C}^*(f(e_k)) = A\mathcal{B}^*(e_k) = AC_k(I_n) = C_k(A)$.

Corollaires :

- Pour $(f, g) \in L(E, F)^2$ et $\lambda \in \mathbb{K}$, soient $A = \text{Mat}_{\mathcal{B}, \mathcal{C}} f$ et $B = \text{Mat}_{\mathcal{B}, \mathcal{C}} g$:
 $\forall x \in E, \mathcal{C}^*((f + \lambda g)(x)) = \mathcal{C}^*(f(x)) + \lambda \mathcal{C}^*(g(x)) = A\mathcal{B}^*(x) + \lambda B\mathcal{B}^*(x) = (A + \lambda B)\mathcal{B}^*(x)$
Donc $A + \lambda B = \text{Mat}_{\mathcal{B}, \mathcal{C}}(f + \lambda g)$. Donc $\text{Mat}_{\mathcal{B}, \mathcal{C}}$ est linéaire, et puisqu'elle est aussi bijective, c'est un isomorphisme de $L(E, F)$ sur $\mathfrak{M}_{m,n}(\mathbb{K})$ et donc $\boxed{\dim L(E, F) = \dim E \times \dim F}$.
- $\text{Mat}_{\mathcal{B}, \mathcal{C}}(g \circ f) = \text{Mat}_{\mathcal{B}, \mathcal{C}} g \times \text{Mat}_{\mathcal{B}, \mathcal{C}} f$.
- Si $E = F$ et $\mathcal{B} = \mathcal{C}$, $\text{Mat}_{\mathcal{B}} f = \text{Mat}_{\mathcal{B}} f$.
- $\text{Mat}_{\mathcal{B}} Id_E = I_n$. Puisque $\text{Mat}_{\mathcal{B}}(g \circ f) = \text{Mat}_{\mathcal{B}} g \times \text{Mat}_{\mathcal{B}} f$, $\text{Mat}_{\mathcal{B}}$ est un isomorphisme d'algèbres.
- $\text{Mat}_{\mathcal{B}}(f^{-1}) = \left(\text{Mat}_{\mathcal{B}} f \right)^{-1}$.

Remarque :

$\text{Mat}_{\mathcal{B}, \mathcal{C}} : \begin{cases} L(E, F) & \longrightarrow \mathfrak{M}_{m,n}(\mathbb{K}) \\ f & \longmapsto \text{Mat}_{\mathcal{B}, \mathcal{C}} f \end{cases}$ et $\varphi : \begin{cases} \mathfrak{M}_n(\mathbb{K}) & \longrightarrow L(\mathbb{K}^n) \\ A & \longmapsto u_A \end{cases}$ sont des isomorphismes. Quel est leur lien ?

Si $E = \mathbb{K}^n$ et $\mathcal{B} = (C_k(I_n))_{k \in \llbracket 1, n \rrbracket}$ et $F = \mathbb{K}^m$ et $\mathcal{C} = (C_k(I_n))_{k \in \llbracket 1, m \rrbracket}$, on a $\text{Mat}_{\mathcal{B}, \mathcal{C}} = \varphi^{-1}$.

Changements de bases :

Pour \mathcal{B}, \mathcal{C} bases de E : $P_{\mathcal{B}, \mathcal{C}} = P_{\mathcal{B} \rightarrow \mathcal{C}} = \text{Mat}_{\mathcal{B}} \mathcal{C}$ est la matrice de passage de \mathcal{B} à \mathcal{C} .

- $P_{\mathcal{B} \rightarrow \mathcal{C}} = \text{Mat}_{\mathcal{B}} \text{Id}_E(\mathcal{C}) = \text{Mat}_{\mathcal{C}, \mathcal{B}} \text{Id}_E$
- $P_{\mathcal{B} \rightarrow \mathcal{C}} = (P_{\mathcal{C} \rightarrow \mathcal{B}})^{-1} \in GL_n(\mathbb{K})$
- $P_{\mathcal{B} \rightarrow \mathcal{C}}$ est la matrice $\text{Mat}_{\mathcal{C}, \mathcal{B}} \text{Id}_E$ telle que $\forall x \in E, \mathcal{B}^*(\text{Id}_E(x)) = P_{\mathcal{B} \rightarrow \mathcal{C}} \mathcal{C}^*(x)$.

Caractérisation : notant $X = \mathcal{B}^*(x)$ et $X' = \mathcal{B}'^*(x)$, $P = P_{\mathcal{B} \rightarrow \mathcal{B}'} \iff \forall x \in E, X = PX'$.

- $\text{Mat}_{\mathcal{B}'} f = P_{\mathcal{B}' \rightarrow \mathcal{B}} \times \text{Mat}_{\mathcal{B}} f \times P_{\mathcal{B} \rightarrow \mathcal{B}'}$

Réciproquement, une matrice inversible est source d'une nouvelle base.

Définition : pour $(f, g) \in L(E)^2$. f et g sont semblables s'il y a des bases \mathcal{B} et \mathcal{C} de E telles que :

$$\text{Mat}_{\mathcal{B}} f = \text{Mat}_{\mathcal{C}} g$$

Pour $(A, B) \in \mathfrak{M}_n(\mathbb{K})$, A et B sont semblables s'il y a un \mathbb{K} -ev de dimension n , E , et un endomorphisme $f \in L(E)$ et des bases \mathcal{B} et \mathcal{C} de E telles que $A = \text{Mat}_{\mathcal{B}} f$ et $B = \text{Mat}_{\mathcal{C}} f$.

Notations : ici, on notera « eq » pour « équivalente à » et « \sim » pour « semblable à ».

Propriétés sur les relations « eq » et \sim :

- \sim est une relation d'équivalence sur $\mathfrak{M}_n(\mathbb{K})$ ou $L(E)$.
- « eq » est une relation d'équivalence sur $\mathfrak{M}_{m,n}(\mathbb{K})$ ou $L(E, F)$
- Pour $A, B \in \mathfrak{M}_n(\mathbb{K})^2$, $A \sim B \iff \exists P \in GL_n(\mathbb{K}) \mid A = P^{-1}BP$
- Pour $A, B \in \mathfrak{M}_{m,n}(\mathbb{K})^2$, $A \text{ eq } B \iff \exists (P, Q) \in GL_n(\mathbb{K}) \times GL_m(\mathbb{K}) \mid A = Q^{-1}BP$
- Pour $(f, g) \in L(E)$, $f \sim g \iff \exists \varphi \in GL(E) \mid g = \varphi^{-1} \circ f \circ \varphi$
- Pour $(f, g) \in L(E, F)$, $f \text{ eq } g \iff \exists (\varphi, \psi) \in GL(F) \times GL(E) \mid g = \psi^{-1} \circ f \circ \varphi$
- Deux endomorphismes sont équivalents (resp. similaires) ssi leurs matrices dans une base sont équivalentes (resp. similaires).
- $A \sim B \iff u_A \sim u_B$
- $A \text{ eq } B \iff u_A \text{ eq } u_B$
- $A \sim B \implies A \text{ eq } B$
- Multiplier à droite par une inversible conserve l'image et à gauche par une inversible conserve le noyau.

Théorème : pour $(f, g) \in L(E, F)$, $f \text{ eq } g \iff \text{rg } f = \text{rg } g$.

Preuve : si $f \text{ eq } g$, elles ont la même matrice échelonnée et donc le même rang.

Si $\text{rg } f = \text{rg } g = r$, soit $A = \text{Im } f$ et $B = \text{Im } g$, $(\varepsilon_1, \dots, \varepsilon_r)$ base de A et $(\varepsilon'_1, \dots, \varepsilon'_r)$ base de B . Soit $(e_1, \dots, e_r) \in E^r \mid \forall i \in \llbracket 1, r \rrbracket, f(e_i) = \varepsilon_i$ et soit $(e'_1, \dots, e'_r) \in E^r \mid \forall i \in \llbracket 1, r \rrbracket, g(e'_i) = \varepsilon'_i$.

Soit (e_{r+1}, \dots, e_n) une base de $\ker f$ et (e'_{r+1}, \dots, e'_n) une base de $\ker g$.

$\mathcal{B} = (e_i)_{i \in \llbracket 1, n \rrbracket}$ est une base de E et $\mathcal{B}' = (e'_i)_{i \in \llbracket 1, n \rrbracket}$ est une base de E .

On complète $(\varepsilon_1, \dots, \varepsilon_r)$ et $(\varepsilon'_1, \dots, \varepsilon'_r)$ en des bases \mathcal{C} et \mathcal{C}' de F et E respectivement. Alors :

$\text{Mat}_{\mathcal{B}, \mathcal{C}} f = \text{Mat}_{\mathcal{B}', \mathcal{C}'} g$, et donc f et g sont équivalents.

Remarques :

- Cette preuve est concise mais non-constructive. Cf. polycopié pour avoir une preuve constructive.
- Le format et le rang sont les invariants d'équivalence.

Invariants de similitude : deux matrices semblables ont :

- La même trace
- Le même déterminant
- Le même rang
- Le même spectre
- La même dimension spectrale
- Le même polynôme annulateur
- Le même polynôme minimal
- Le même polynôme caractéristique

⚠ Il ne suffit pas que deux matrices aient ces caractéristiques en commun pour être semblables.

Remarque : il y a un algorithme permettant de décider de la similarité de deux matrices, mais il est bien loin du programme.

Proposition : pour $A \in \mathfrak{M}_{n,m}(\mathbb{K})$ et $B \in \mathfrak{M}_{m,n}(\mathbb{K})$, $\text{tr } AB = \text{tr } BA$.

Remarques :

- Ceci explique pourquoi $A \sim B \implies \text{tr } A = \text{tr } B$
- Pour $f \in L(E)$, comme les matrices de f dans les bases de E sont semblables, donc ont la même trace, on définit $\text{tr } f$ comme la valeur commune des traces des matrices de f .
- Il en va de même pour le déterminant : $\det AB = \det A \times \det B = \det BA$ donc on définit de la même manière le déterminant d'un endomorphisme.

Proposition – définition : pour $P = \sum_{k=0}^p a_k X^k$, $A \in \mathfrak{M}_n(\mathbb{K})$ et $f \in L(E)$:

- $P(A) = \sum_{k=0}^p a_k A^k$
- $P(f) = \sum_{k=0}^p a_k f^k$
- $\varphi_A: \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathfrak{M}_n(\mathbb{K}) \\ P & \longmapsto & P(A) \end{cases}$ et $\varphi_f: \begin{cases} \mathbb{K}[X] & \longrightarrow & L(E) \\ P & \longmapsto & P(f) \end{cases}$ sont des morphismes d'algèbres.
- $\mathbb{K}[A] = \{P(A), P \in \mathbb{K}[X]\}$ et $\mathbb{K}[f] = \{P(f), P \in \mathbb{K}[X]\}$ sont des sous-algèbres commutatives de $\mathfrak{M}_n(\mathbb{K})$ et $L(E)$.
- $\ker \varphi_A = \{P \in \mathbb{K}[X] \mid P(A) = 0\}$ est l'idéal annulateur de A .
- $\ker \varphi_f = \{P \in \mathbb{K}[X] \mid P(f) = 0\}$ est l'idéal annulateur de f .

Lorsque $P(f) = 0$ on dit aussi bien que f annule P ou que P annule f .

La clé : pour $P \in \mathbb{K}[X]$ et $(A, B) \in \mathfrak{M}_n(\mathbb{K})^2$ (resp. $(f, g) \in L(E)^2$) :

- $A \sim B \implies P(A) \sim P(B)$ (resp. $f \sim g \implies P(f) \sim P(g)$)
- En fait, si $Q \in GL_n(\mathbb{K})$ est telle que $B = Q^{-1}AQ$, alors $P(B) = Q^{-1}P(A)Q$, et de même pour les endomorphismes.

Proposition : puisque $\text{rg } A = 0 \iff A = 0$, $A \sim B \implies [P(A) = 0 \iff P(B) = 0]$. On énonce :
Les matrices (resp. endomorphismes) semblables ont les mêmes polynômes annulateurs.

Remarque : il en découle que $\dim E_\lambda(f) = \dim E_\lambda(g)$ pour des endomorphismes semblables.

A fortiori, $\lambda \in \text{sp } f \iff E_\lambda(f) \neq \{0\} \iff \dim E_\lambda(f) \neq 0 \iff \dim E_\lambda(g) \neq 0$ et donc $\lambda \in \text{sp } g$.

Il est facile de voir que $\chi_A: \begin{cases} \mathbb{K} & \longrightarrow \mathbb{K} \\ \lambda & \longmapsto \det(A - \lambda I_n) \end{cases}$ est polynômiale et puisque $A \sim B \implies \det(A - \lambda I_n) = \det(B - \lambda I_n)$, on a $\chi_A = \chi_B$.

Remarque : $x \in \ker f \iff f(x) = 0 \iff \mathcal{B}^*(f(x)) = 0 \iff A\mathcal{B}^*(x) = 0 \iff \mathcal{B}^*(x) \in \ker A$, donc si A représente f dans une certaine base, $\dim(\ker A) = \dim(\ker f)$. De même, $\ker(A - \lambda I_n) = E_\lambda(A) = \mathcal{B}^*(E_\lambda(f))$.

II. Notion d'idéal

Preuves dans le polycopié.

Définition : soit $(A, +, \times)$ un anneau. Un idéal \mathcal{I} de A est une partie de A non vide, stable par addition interne et par multiplication externe. $\forall (x, y) \in \mathcal{I}^2, x + y \in \mathcal{I}$ et $\forall (x, y) \in \mathcal{I} \times A, x \times y \in \mathcal{I}$ et $y \times x \in \mathcal{I}$.

Remarque : on peut restreindre à un idéal « à gauche » ou « à droite » avec la stabilité par multiplication externe « à gauche » ou « à droite ».

Proposition :

- 1) Les idéaux sont des sous-groupes.
- 2) Les idéaux stricts (distincts de leur anneau) ne sont jamais des sous-anneaux.
- 3) Les noyaux de morphismes d'anneaux sont des idéaux de l'anneau de départ.
- 4) Les idéaux sont tous des noyaux de morphismes d'anneaux (HP).
- 5) Les idéaux de \mathbb{Z} et de $\mathbb{K}[X]$ sont les $n\mathbb{Z}$ et les $P \cdot \mathbb{K}[X]$

Preuve du 4 : soit \mathcal{I} un idéal. $x \equiv y[\mathcal{I}] \stackrel{\text{def}}{\iff} x - y \in \mathcal{I}$ est une relation d'équivalence sur A .

L'ensemble quotient A/\mathcal{I} existe car on a la compatibilité de $\equiv \mathcal{I}$ avec $+$ et \times .

On peut donc munir A/\mathcal{I} d'une structure d'anneau quotient et notant $\bar{a} = a + \mathcal{I}$ la classe de a modulo \mathcal{I} :

$\forall (\bar{a}, \bar{b}) \in A/\mathcal{I}, \bar{a} + \bar{b} \equiv \overline{a + b}, \bar{a} \times \bar{b} \equiv \overline{a \times b}$ et $\bar{1} = \bar{1}$.

$\varphi: \begin{cases} A & \longrightarrow A/\mathcal{I} \\ a & \longmapsto \bar{a} \end{cases}$ est un morphisme d'anneaux surjectif dont le noyau est $\{a \in A \mid a \equiv 0[\mathcal{I}]\} = \mathcal{I}$.

Proposition : pour A un anneau commutatif et $a \in A$, un idéal principal \mathcal{I} de A est une partie de A de la forme $a \cdot A$. C'est l'idéal principal engendré par a .

Définition : un anneau principal est un anneau commutatif intègre dont tout idéal est principal.

Exemple : \mathbb{Z} et $\mathbb{K}[X]$ sont des anneaux principaux.

Anneaux non principaux : $\mathbb{Z}[X], \mathbb{K}[X, Y]$:

$\mathbb{Z}[X]$: soit $\mathcal{I} = \{P \in \mathbb{Z}[X] \mid P(0) \in 2\mathbb{Z}\}$. C'est un idéal non principal de $\mathbb{Z}[X]$, qui n'est donc pas principal.

$\mathbb{K}[X, Y]$: cf. plus tard.

Proposition : Dans un anneau commutatif quelconque, si $(\mathcal{I}_k)_{k \in K}$ est une famille quelconque d'idéaux (finie ou non), alors :

$$\mathcal{S} = \bigcap_{k \in K} \mathcal{I}_k \text{ est un idéal}$$

Remarque : en revanche, la réunion de deux idéaux n'est pas toujours un idéal :

Si $3\mathbb{Z} \cup 2\mathbb{Z}$ était un idéal de \mathbb{Z} , donc de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$, on aurait $3 \in n\mathbb{Z}$ et $2 \in n\mathbb{Z}$ donc $n \mid 2$ et $n \mid 3$ donc $n \mid 3 \wedge 2$ donc $n = 1$ et donc $3 \mid 7$ ou $2 \mid 7$.

Définition : deux éléments a et b d'un anneau commutatif intègre A sont associés si $aA = bA$.

Proposition : si A est un anneau principal :

- Les PPCM de $a, b \in A^2$ sont les générateurs de l'idéal $aA \cap bA$, i.e les $c \in A$ tels que $cA = aA \cap bA$.
- Les PGCD de $a, b \in A^2$ sont les $d \in A$ tels que $aA + bA = dA$.

Corollaire : si d est un PGCD de a et b , $\exists(u, v) \in A^2 \mid au + bv = d$.

⚠ Ce n'est pas une équivalence.

Néanmoins, si $\exists(u, v) \in A^2 \mid au + bv = 1$, $1 \in dA \iff d \mid 1 \iff d \in \Delta(A) \iff dA = 1A = A$.

Définition : le PGCD de $(a, b) \in \mathbb{Z}^*$ est l'entier positif $a \wedge b$ tel que :

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

Définition : le PGCD de $(A, B) \in \mathbb{K}[X] \setminus \{0\}$ est le polynôme unitaire noté $A \wedge B$ tel que :

$$A\mathbb{K}[X] + B\mathbb{K}[X] = (A \wedge B)\mathbb{K}[X]$$

Théorème de Bézout : pour $(A, B) \in \mathbb{K}[X] \setminus \{0\}$:

$$\begin{aligned} A \wedge B = 1 &\iff \exists(U, V) \in \mathbb{K}[X]^2 \mid AU + BV = 1 \\ A \wedge B = D &\implies \exists(U, V) \in \mathbb{K}[X]^2 \mid AU + BV = D \\ \exists(U, V) \in \mathbb{K}[X]^2 \mid AU + BV = D &\implies D \mid A \wedge B \end{aligned}$$

Propositions : à la louche :

- $(ma \wedge mb) = m(a \wedge b)$
- $(a \wedge b)(a \vee b) = ab$
- $a \mid bc$ et $a \wedge b = 1 \implies a \mid c$
- $a \wedge b = 1$ et $a \wedge c = 1 \implies a \wedge bc = 1$

Proposition : pour $(a, b) \in \mathbb{Z}^{*2}$:

$$\exists! (u, v) \in \mathbb{Z}^2 \mid au + bv = a \wedge b \text{ et } |u| < |b| \text{ et } |v| < |a|$$

Pour $(A, B) \in \mathbb{K}[X] \setminus \{0\}$:

$$\exists! (U, V) \in \mathbb{K}[X]^2 \mid AU + BV = A \wedge B \text{ et } \deg U < \deg B \text{ et } \deg V < \deg A$$

III. Polynômes caractéristiques et annulateurs

Soit E un \mathbb{K} -ev de dimension pas nécessairement finie.

Pour $u \in L(E)$, on note :

$$\varphi_u : \begin{cases} \mathbb{K}[X] & \longrightarrow & L(E) \\ P = \sum_{k=0}^p a_k X^k & \longmapsto & \sum_{k=0}^p a_k u^k \end{cases}$$

Proposition : pour $u \in L(E)$, φ_u est un morphisme de \mathbb{K} algèbres.

- Son image est $\text{Im } \varphi_u = \mathbb{K}[u] = \{P(u), P \in \mathbb{K}[X]\}$. C'est l'ensemble des polynômes en u , qui est une sous-algèbre de $L(E)$.

• Son noyau $\mathcal{N}_u = \ker \varphi_u = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$ est un noyau de morphismes d'anneaux donc un idéal de $\mathbb{K}[X]$, dit « idéal annulateur de u ».

Preuve : $\forall (P, Q) \in \mathbb{K}[X]^2$ et $\forall \lambda \in \mathbb{K}$:

- $(PQ)(u) = P(u) \circ Q(u)$
- $(\lambda P + Q)(u) = \lambda P(u) + Q(u)$
- $X^0(u) = Id_E$

Remarque : • Si $\dim E < \infty$, $\dim L(E) < \infty$ et comme $\dim \mathbb{K}[X] = \infty$, φ_u n'est jamais injective et donc $\mathcal{N}_u = \ker \varphi_u \neq \{0_{\mathbb{K}[X]}\}$. Il y a donc un unique polynôme unitaire Π_u tel que $\mathcal{N}_u = \Pi_u \mathbb{K}[X]$. Π_u est le générateur unitaire de l'idéal annulateur de u , dit « polynôme minimal » de u .

• $\deg \Pi_u = 1 \iff \exists \lambda \in \mathbb{K} \mid \Pi_u = X - \lambda \implies (X - \lambda)(u) = 0 \implies u = \lambda Id_E$.

Proposition - définition : pour $u \in L(E)$, on appelle commutant de u et on note $\mathcal{C}(u)$ l'ensemble :

$$\mathcal{C}(u) = \{v \in L(E) \mid u \circ v = v \circ u\}$$

$\mathcal{C}(u)$ est une sous-algèbre de $L(E)$.

De plus, $\mathbb{K}[u] \subset \mathcal{C}(u)$.

Remarque : ⚠ L'égalité $\mathbb{K}[u] = \mathcal{C}(u)$ est rarement vérifié. Par exemple : si $u = \alpha Id_E$, alors $P(u) = P(\alpha) Id_E$ pour tout polynôme et donc $\mathbb{K}[u] = \text{vect}(Id_E)$ alors que $\mathcal{C}(u) = L(E)$.

Proposition : soit $u \in L(E)$, Π_u son polynôme minimal et $m = \deg \Pi_u$. Alors :

- $\dim \mathbb{K}[u] = m$
- $(Id_E, u, \dots, u^{m-1})$ est une base de $\mathbb{K}[u]$.

Preuve : si $\sum_{k=0}^{m-1} \lambda_k u^k = 0$, alors posant $P = \sum_{k=0}^{m-1} \lambda_k X^k$, $P(u) = 0$ donc $\Pi_u \mid P$ et comme $\deg P < \deg \Pi_u$, $P = 0$ donc tous les λ_k sont nuls et la famille $(Id_E, u, \dots, u^{m-1})$ est libre.

Pour $v \in \mathbb{K}[u]$, soit $P \in \mathbb{K}[X] \mid P(u) = v$.

Soient Q et R les quotients et restes de P par Π_u .

$P = Q\Pi_u + R$ donne $v = P(u) = Q(u) \circ \Pi_u(u) + R(u) = R(u)$, avec $R \in \mathbb{K}_{m-1}[X]$.

$R = \sum_{k=0}^{m-1} \alpha_k X^k$ donne $v = \sum_{k=0}^{m-1} \alpha_k u^k$ donc la famille $(Id_E, u, \dots, u^{m-1})$ est génératrice.

Remarque : comme $m = \dim \mathbb{K}[u]$ et comme $\mathbb{K}[u]$ est un sev de $L(E)$, $m \leq \dim L(E) = (\dim E)^2$.

Théorème (de l'élément primitif) : pour $u \in L(E)$, $\exists x \in E \mid \Pi_u = \Pi_{u,x}$, avec $\Pi_{u,x}$ le générateur unitaire de $\mathcal{N}_x^u = \{P \in \mathbb{K}[X] \mid P(u)(x) = 0_E\}$.

Preuve : pour $x \in E$, notons $\mathcal{N}_x^u = \{P \in \mathbb{K}[X] \mid P(u)(x) = 0_E\}$. On a bien sûr $\mathcal{N}_u \subset \mathcal{N}_x^u$.

Si $P, Q \in \mathcal{N}_x^u$, $R \in \mathbb{K}[X]$:

$$(P + Q)(u)(x) = P(u)(x) + Q(u)(x) = 0$$

$$(RP)(u)(x) = (R(u) \circ P(u))(x) = 0$$

Et donc \mathcal{N}_x^u est un idéal de $\mathbb{K}[X]$, dit idéal annulateur de u en x .

$\dim E = n < \infty$ donc il y a un polynôme minimal de u , Π_u et comme $\Pi_u \in \mathcal{N}_x^u$, celui-ci n'est pas nul et a donc un générateur unitaire $\Pi_{u,x}$. De plus, $\mathcal{N}_u \subset \mathcal{N}_x^u \implies \Pi_{u,x} \mid \Pi_u$.

Par définition de $\Pi_{u,x}$, $\Pi_{u,x}(u)(x) = 0$ et $\forall x \in E$, $x \in \ker \Pi_{u,x}(u)$, donc $E = \bigcup_{x \in E} \ker \Pi_{u,x}(u)$.

Mais si $\Pi_u = \prod_{k=1}^q Q_k^{m_k}$ est la factorisation en facteurs irréductibles de Π_u , l'ensemble des diviseurs

unitaires de Π_u est $\mathcal{D} = \left\{ \prod_{k=1}^p Q_k^{r_k} \mid (r_k)_{k \in [1,p]} \in \llbracket 0, m_1 \rrbracket \times \dots \times \llbracket 0, m_p \rrbracket \right\}$ et a $\prod_{k=1}^p (m_k + 1)$ éléments.

Comme $\forall x \in E$, $\Pi_{u,x} \in \mathcal{D}$, $\mathcal{P} = \{\Pi_{u,x} \mid x \in E\}$ contenu dans \mathcal{D} est fini. Soit $(P_k)_{k \in [1,s]}$ une énumération de \mathcal{P} . Pour chaque $k \in [1,s]$, y'a un x_k tel que $P_k = \Pi_{u,x_k}$.

Et donc, on a en fait :

$$E = \bigcup_{P \in \mathcal{P}} \ker P(u) = \bigcup_{k=1}^s \ker \Pi_{u, x_k}(u)$$

Or si \mathbb{K} est infini, il faut donc que l'un des $\ker \Pi_{u, x_k}(u)$ soit égal à E .

Ainsi, soit $k \in \llbracket 1, s \rrbracket \mid E = \ker \Pi_{u, x_k}(u)$.

Ainsi, $\exists x \in E \mid E = \ker \Pi_{u, x}(u)$ i.e $\Pi_{u, x} = 0$ et donc $\Pi_u \mid \Pi_{u, x}$. Comme ils sont tous deux unitaires on a donc $\Pi_u = \Pi_{u, x}$.

Corollaire : Pour $x \in E$, comme $(x, u(x), \dots, u^n(x))$ est à $n+1$ éléments donc liée, et il y a une combinaison linéaire de cette famille nulle sans coefficients tous nuls, ce qui nous donne un polynôme P de degré n nul en $u(x)$ donc $P \in \mathcal{N}_x^u$ et donc $\Pi_{u, x} \mid P$ donne $\deg \Pi_{u, x} \leq \deg P \leq n$ et donc enfin $\deg \Pi_u \leq \dim E$.

Remarque : lorsque $E = \mathbb{K}^n$, que $A \in \mathfrak{M}_n(\mathbb{K})$ et que $u = u_A$, $\varphi_A: \begin{cases} \mathbb{K}[X] & \longrightarrow \mathfrak{M}_n(\mathbb{K}) \\ P & \longmapsto P(A) \end{cases}$ est un morphisme d'algèbres, d'image $\mathbb{K}[A] = \{P(A), P \in \mathbb{K}[X]\}$, de noyau $\mathcal{N}_A = \{P \in \mathbb{K}[X] \mid P(A) = 0\}$ et $\Pi_A = \Pi_{u_A}$ étant le générateur unitaire de l'idéal \mathcal{N}_A annulateur de A , $\deg \Pi_A \leq n$.

De plus, $P(A) = 0 \iff \Pi_A \mid P$ et $\dim \mathbb{K}[A] = \deg \Pi_A = q$ car (I_n, A, \dots, A^{q-1}) est une base de $\mathbb{K}[A]$ et $\mathbb{K}[A]$ est une sous-algèbre de $\mathcal{C}(A)$.

Proposition : soit P un polynôme annulateur de $u \in L(E)$.

$$\begin{aligned} \text{sp } u &\subset Z_{\mathbb{K}}(P) = \{z \in \mathbb{K} \mid P(z) = 0\} \\ \text{sp } u &= Z_{\mathbb{K}}(\Pi_u) = \{z \in \mathbb{K} \mid \Pi_u(z) = 0\} \end{aligned}$$

Preuve : soit $P = \sum_{k=0}^p a_k X^k$ et $x \in E_{\lambda}(u)$.

$$\forall k \in \mathbb{N} : u^k(x) = \lambda^k x.$$

$$P(u)(x) = \sum_{k=0}^p a_k u^k(x) = \sum_{k=0}^p a_k \lambda^k x = P(\lambda)x$$

$$\text{Donc } E_{\lambda}(u) \subset E_{P(\lambda)}(P(u)).$$

Si P annule u : soit $\lambda \in \text{sp } u$ et soit $0 \neq x \in E_{\lambda}(u)$:

$$0 = P(u)(x) = P(\lambda)x = 0 \text{ et comme } x \neq 0, P(\lambda) = 0.$$

Soit $\lambda \in Z_{\mathbb{K}}(\Pi_u)$. $\Pi_u = (X - \lambda)Q$ avec $Q \in \mathbb{K}[X]$.

$$\Pi_u(u) = (u - \lambda \text{Id}_E) \circ Q(u) = 0_{L(E)}$$

Si $u - \lambda \text{Id}_E \in GL(E)$, en composant par $(u - \lambda \text{Id}_E)^{-1}$, on aurait $Q(u) = 0$ donc $\Pi_u \mid Q$ alors que $\deg Q < \deg \Pi_u$, ce qui est absurde donc $u - \lambda \text{Id}_E \notin GL(E)$, soit $\lambda \in \text{sp } u$.

Trix :

- Pour $(u, v) \in L(E)^2$, si $u \circ v = v \circ u$, alors $\ker u$, $\text{Im } u$, $E_{\lambda}(u)$ sont stables par v et réciproquement.
- Pour $(P, Q) \in \mathbb{K}[X]^2$ avec $\mathbb{K} \subset \mathbb{C}$, comme $P \wedge_{\mathbb{R}, \mathbb{Q}, \dots} Q = P \wedge_{\mathbb{C}} Q$, et comme sur \mathbb{C} , les facteurs irréductibles sont les $X - \lambda$, $\lambda \in \mathbb{C}$, $P \wedge Q = 1 \iff \exists \lambda \in \mathbb{C} \mid (X - \lambda) \mid P$ et $(X - \lambda) \mid Q \iff \exists \lambda \in \mathbb{C} \mid P(\lambda) = Q(\lambda) = 0$.
 \implies Deux polynômes sont premiers entre eux ssi ils n'ont pas de zéro commun.

Lemme des noyaux : E est un \mathbb{K} -ev (de dimension possiblement infinie).

Soient (A_1, \dots, A_n) n éléments de $\mathbb{K}[X] \setminus \{0\}$ deux à deux premiers entre eux. Soit $P = \prod_{k=1}^n A_k$

Alors :

- $\forall f \in L(E)$, $\ker P(f) = \bigoplus_{k=1}^p \ker A_k(f)$
- Les $\ker A_k$ sont stables par f (puisque les $A_k(f)$ commutent avec f).
- Si $P(f) = 0$, $\ker P(f) = E$ et les projecteurs associés à la décomposition de $E = \bigoplus_{k=1}^p \ker A_k(f)$

sont des polynômes en f .

Preuve : par récurrence sur n .

$n = 1$: rien à montrer

$n = 2$:

Si $A, B \in \mathbb{K}[X] \mid A \wedge B = 1$, posant $P = AB$. Soit $(U, V) \in \mathbb{K}[X] \mid AU + BV = 1$. On a donc :

$A(f) \circ U(f) + B(f) \circ V(f) = U(f) \circ A(f) + V(f) \circ B(f) = Id_E$. Et donc :

$$\forall x \in E : x = \underbrace{[A(f) \circ U(f)](x)}_{x_B} + \underbrace{[B(f) \circ V(f)](x)}_{x_A}$$

- Si $x \in \ker A(f) \cap \ker B(f)$, $x_A = 0$ et $x_B = 0$, d'où $\ker A(f) + \ker B(f) = \ker A(f) \oplus \ker B(f)$
- $x \in \ker A(f) \implies A(f)(x) = 0 \implies B(f)(A(f)(x)) = 0$ donc $P(f)(x) = 0$ d'où $\ker A(f) \subset \ker P(f)$.

De même, $\ker B(f) \subset \ker P(f)$, donc $\ker A(f) \oplus \ker B(f) \subset \ker P(f)$.

- Si $x \in \ker P(f)$, $A(f)(x_A) = V(f)[A(f)(B(f)(x))] = V(f)(P(f)(x)) = 0$ donc $x_A \in \ker A(f)$.

De même, $x_B \in \ker B(f)$ donc $x = x_A + x_B \in \ker A(f) \oplus \ker B(f)$ et enfin :

$$\ker A(f) \oplus \ker B(f) = \ker P(f)$$

De plus, lorsque $P(f) = 0$, on a $\forall x \in E = \ker P(f)$, $x = x_A + x_B \in \ker A(f) \oplus \ker B(f)$ avec :

$x_A = (A(f) \circ U(f))(x)$ et $x_B = (B(f) \circ V(f))(x)$. Ainsi, les projecteurs associés à la décomposition sont $B(f) \circ V(f)$ et $A(f) \circ U(f)$.

Fin de la preuve pour $n = 2$.

$n \geq 2$: et supposons le lemme des noyaux au rang $n - 1$.

Soient (A_1, \dots, A_n) n éléments de $\mathbb{K}[X] \setminus \{0\}$ deux à deux premiers entre eux. Soit $P = \prod_{k=1}^n A_k$

$\forall i \neq j \in \llbracket 1, n \rrbracket$, $A_i \wedge A_j = 1$.

Soit $k \in \llbracket 1, n \rrbracket$. Posons $A = A_k$ et $B = \prod_{i \neq k}^n A_i$. Alors $A \wedge B = 1$. Posons $P = AB$. Alors :

$$\ker P(f) \stackrel{n=2}{=} \ker A_k(f) \oplus \ker B(f) \stackrel{\text{HR}}{=} \bigoplus_{i=1}^p \ker A_i(f)$$

Si $P(f) = 0$, le projecteur sur $\ker A_k(f) = \ker A(f)$ parallèlement à $\ker B(f)$ est un polynôme en f .

Complément : invariances par extension du corps des scalaires.

Définition : \mathbb{L} est un sur-corps de \mathbb{K} si $\mathbb{K} \subset \mathbb{L}$ et \mathbb{L} est un corps.

Proposition : soit \mathbb{L} un sur-corps de \mathbb{K} . Si $E_{\mathbb{L}} = (E, +, \times)$ est un \mathbb{L} -ev, alors $E_{\mathbb{K}} = (E, +, \times_{|\mathbb{K}})$ est un \mathbb{K} -ev. De plus, \mathbb{L} est un \mathbb{K} -ev.

Proposition : soit \mathbb{L} un sur-corps de \mathbb{K} . Si $\dim_{\mathbb{L}} E = m$ et $\dim_{\mathbb{K}} \mathbb{L} = p$, alors :

$$\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} \mathbb{L} \dim_{\mathbb{L}} E = mp$$

Remarque : si E est un \mathbb{C} -ev de dimension n , c'est un \mathbb{R} -ev de dimension $2n$. En effet : si (e_1, \dots, e_n) est une \mathbb{C} -base de E , $(e_1, \dots, e_n, ie_1, \dots, ie_n)$ est une \mathbb{R} -base de E .

Soit \mathbb{K} un sous-corps de \mathbb{L} .

On a évidemment $\mathfrak{M}_n(\mathbb{K}) \subset \mathfrak{M}_n(\mathbb{L})$ et $\mathbb{K}[X] \subset \mathbb{L}[X]$.

Un \mathbb{L} -ev est naturellement par restriction de la multiplication scalaire à \mathbb{K} un \mathbb{K} -ev.

Invariants : pour $P, Q \in \mathbb{K}[X]^2$ et pour $A, B \in \mathfrak{M}_{n,m}(\mathbb{K})^2$:

- $P \mid_{\mathbb{K}} Q = P \mid_{\mathbb{L}} Q$ (mais irréductible sur \mathbb{K} n'entraîne pas irréductible sur \mathbb{L} car $Z_{\mathbb{K}}(P) \neq Z_{\mathbb{L}}(Q)$)
- $\text{rg}_{\mathbb{K}}(A) = \text{rg}_{\mathbb{L}}(A)$ (mais $\text{Im}_{\mathbb{K}}(A) \neq \text{Im}_{\mathbb{L}}(A)$)
- $A \text{ eq}_{\mathbb{K}} B \iff A \text{ eq}_{\mathbb{L}} B$

Si, de plus, $n = m$:

- $\text{sp}_{\mathbb{K}}(A) = \text{sp}_{\mathbb{L}}(A) \cap \mathbb{K}$
- pour $\lambda \in \text{sp}_{\mathbb{K}}(A)$, $\dim E_{\lambda}^{\mathbb{K}}(A) = \dim E_{\lambda}^{\mathbb{L}}(A)$ (mais $E_{\lambda}^{\mathbb{K}}(A) \neq E_{\lambda}^{\mathbb{L}}(A)$)
- $A \sim_{\mathbb{K}} B \iff A \sim_{\mathbb{L}} B$
- $\Pi_A^{\mathbb{K}} = \Pi_A^{\mathbb{L}}$

Fin du complément

Trix : pour $A \in \mathfrak{M}_n(\mathbb{K})$ telle que $\chi_A = \prod_{\lambda \in \text{sp } A} (X - \lambda)^{m_{\lambda}} = \prod_{k=1}^n (X - \lambda_k)$. Les deux écritures permettent de dire que χ_A est scindé mais dans la deuxième, on perd le fait que les λ_k ne sont pas 2 à 2 distincts.

On a alors $\text{tr } A = \sum_{\lambda \in \text{sp } A} m_{\lambda} \lambda = \sum_{k=1}^n \lambda_k$.

Lemme : si $\#I = n$ et $\forall k \in \llbracket 1, n \rrbracket, \sum_{i \in I} \alpha_i^k$, alors $\forall i \in I, \alpha_i = 0$.

Preuve : on développe le polynôme sous forme de produit de $\mathbb{K}[X_1, \dots, X_n, X]$ en un de $\mathbb{K}[X_1, \dots, X_n][X]$:

$$\prod_{i=1}^n (X - X_i) = \sum_{k=0}^n (-1)^{n-k} \sigma_k(X_1 \dots X_n) X^k = \sum_{I \subset \llbracket 1, n \rrbracket} (-1)^{\#I} \left(\prod_{i \in I} X_i \right) X^{n-\#I}$$

On obtient alors que $\sigma_k = \sum_{I \subset \mathcal{P}_{n-k}(\llbracket 1, n \rrbracket)} \left(\prod_{i \in I} X_i \right)$.

On pose $J = \{i \in I \mid \alpha_i \neq 0\}$, $p = \#I$ et $P = \prod_{j \in J} (X - \alpha_j) = \sum_{k=0}^p u_k X^k$ (u_k sont les coefficients du développement). On a $u_p = 1$ et $u_0 = -\prod_{j \in J} \alpha_j$.

$\forall j \in J, P(\alpha_j) = \sum_{k=0}^p u_k \alpha_j^k = 0$. On a donc :

$$0 = \sum_{j \in J} \sum_{k=0}^p u_k \alpha_j^k = \sum_{k=0}^p u_k \sum_{j \in J} \alpha_j^k = u_0 p = -p \prod_{j \in J} \alpha_j = 0$$

Si $p \neq 0$, $\exists j \in J \mid \alpha_j = 0$, absurde donc $p = 0$.

Proposition : $\mathbb{K} \subset \mathbb{C}$, $A \in \mathfrak{M}_n(\mathbb{K}) \mid \forall k \in \llbracket 1, n \rrbracket, \text{tr } A^k = 0$. Alors A nilpote.

Proposition : soient $A, B \in \mathfrak{M}_n(\mathbb{K}) \mid \forall k \in \llbracket 1, n \rrbracket, \text{tr } A^k = \text{tr } B^k$. Alors $\chi_A = \chi_B$.

(se montre avec les formules de Newton, ou par passage à la limite en le supposant $\forall k \in \mathbb{N}^*$, ou encore en faisant un analogue de la preuve précédente en le supposant $\forall k \in \llbracket 1, 2n \rrbracket$.)