Compléments d'algèbre linéaire

La lettre $\mathbb{K}$ désigne indifféremment $\mathbb{R}$ ou $\mathbb{C}$.
Dans tout ce qui suit, E désignera un $\mathbb{K}$-espace vectoriel (sauf mention contraire)

Table des matières

I Interpolation de Lagrange

Dans cette partie, $x_1, x_2, ..., x_n$ désignent des scalaires deux à deux distincts.

Proposition 1 (Problème de l'interpolation.) Pour toute famille $(y_1, y_2, ...y_n)$ de $\mathbb{K}^n$, il existe un unique polynome P de $\mathbb{K}_{n-1}[X]$ tel que $\forall i \in \{1, ..., n\} \quad P(x_i) = y_i$

Proposition 2 (Polynomes de Lagrange.)
On pose pour tout entier $i \in \{1, ..., n\}$, $\quad L_i = \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}$. Alors :

- $\forall (i, j) \in \{1, ..., n\}^2$, $L_i(x_j) = \delta_{i,j}$ (symbole de Kronecker).
- $(L_1, L_2, ..., L_n)$ est une base de l'espace $\mathbb{K}_{n-1}[X]$.
- Tout polynome P de $\mathbb{K}_{n-1}[X]$ s'écrit dans cette base : $\quad P = \sum_{i=1}^{n} P(x_i) L_i$.

  Autrement dit les $(P(x_i))$ sont les coordonnées de P dans la base $(L_1, L_2, ..., L_n)$.
- $\sum_{i=1}^{n} L_i = 1$

II Produits d'espaces vectoriels, sommes de sous-espaces vectoriels

II.1 Produits d'espaces vectoriels

Theorème-Definition 1 Soient $E_1, \cdots, E_m$ des $\mathbb{K}$-espaces vectoriels.
Alors l'ensemble $E_1 \times \cdots \times E_m$ peut être muni d'une structure de K-espace vectoriel.
On l'appelle produit cartésien des espace $E_1, \cdots, E_m$.

Théorème 1 Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie, non nulle.
Soit $\mathcal{B}_1 = (e_1, \ldots, e_n)$ une base de E. Soit $\mathcal{B}_2 = (f_1, \ldots, f_p)$ une base de F.
Pour $i \in \{1, \ldots, n\}$, on pose $g_i = (e_i, 0_F)$ et pour $i \in \{n+1, \ldots, n+p\}$, on pose $g_i = (0_E, f_{i-n})$.
Alors $(g_1, \ldots, g_{n+p})$ est une base de $E \times F$, appelée base de $E \times F$ associée à $\mathcal{B}_1$ et $\mathcal{B}_2$.
On en déduit que $E \times F$ est de dimension finie et $\dim(E \times F) = \dim(E) + \dim(F)$.

Théorème 2 Soient $E_1, \cdots, E_m$ des $\mathbb{K}$-espaces vectoriels de dimension finie, non nulle.
Alors $E_1 \times \cdots \times E_m$ est un $\mathbb{K}$-espace vectoriel de dimension :

II.2 Somme de sous-espace vectoriels

Définition 1 Soient $F_1, \ldots, F_n$ des sous-espaces vectoriels de E.
On définit la **somme** de $F_1, \ldots, F_n$ par :

$$F_1 + \cdots + F_n = \{x_1 + \cdots + x_n \,|\, (x_1, \ldots, x_n) \in F_1 \times \cdots \times F_n\}$$

Proposition 3 Si $F_1, \ldots, F_n$ des sous-espaces vectoriels de E, alors :

$F_1 + \cdots + F_n$ est un **sous-espace vectoriel** de E.

Exemple 1
1. Dans $\mathbb{R}^3$, la somme de deux droites vectorielles (sous-espaces de dimension 1) **distinctes** est un plan (sous-espace de dimension 2) de $\mathbb{R}^3$.
2. Dans $\mathbb{R}[X]$, on a : $\mathbb{R}_2[X] + \mathbb{R}_5[X] + \mathbb{R}_3[X] =$
3. Soit E le $\mathbb{R}$-espace vectoriel des fonctions définies sur $\mathbb{R}$ et à valeurs réelles. Notons f_1, f_2 les fonctions définies sur $\mathbb{R}$ par $f_1(x) = \cos(x)$, $f_2(x) = \sin(x)$ et $F = \mathrm{Vect}(f_1, f_2)$. Soit G le sous-espace vectoriel de E formé des fonctions polynomiales de degré inférieur ou égal à 3. Soit H la droite vectorielle engendrée par la fonction exponentielle. Décrire les éléments du sous-espace vectoriel $F + G + H$.
4. Si (v_1, v_2, v_3, v_4) est une famille génératrice de E, alors $E = \mathrm{vect}(v_1, v_2) + \mathrm{vect}(v_3) + \mathrm{vect}(v_4)$.

Remarque 1 Erreur classique : pour deux sous-espaces, ne pas confondre $F + G$ et $F \cup G$.
En règle générale, l'ensemble $F \cup G$ n'a aucune propriété algébrique intéressante et n'est pas un sous-espace vectoriel de E (sauf si $F \subset G$ ou $G \subset F$).

Définition 2 (Rappel PCSI) Soient F et G deux sous-espaces vectoriels de E.
1. On dit que la somme $F + G$ est **directe** et on la note $F \oplus G$ si pour tout $x \in F + G$, il existe un **unique** couple $(x_1, x_2) \in F \times G$ tel que $x = x_1 + x_2$.
2. On dit que F et G sont **supplémentaires dans** E si la somme est $F + G$ est directe et si $F + G = E$, c'est-à-dire si $F \oplus G = E$.

Exemple 2
- L'ensemble des fonctions définies sur $\mathbb{R}$ est somme directe de l'espace des fonctions paires et de l'espace des fonctions impaires.
- L'espace des matrices carrées (de taille n) est somme directe de l'espace des matrices symétriques et de l'espace des matrices antisymétriques (de taille n), ce qui s'écrit :
$$\mathcal{M}_n(\mathbb{K}) = \mathcal{A}_n(\mathbb{K}) \oplus \mathcal{S}_n(\mathbb{K}).$$
- $\mathbb{R}^2 = \mathrm{vect}\{(1,0)\} \oplus \mathrm{vect}\{(0,1)\}$, $\mathbb{R}^3 = \mathrm{vect}\{(1,0,0)\} \oplus \mathrm{vect}\{(0,1,0),\ (0,0,1)\}$ etc....
- Soit $E = \mathbb{R}^3$, $F = \mathrm{Vect}((2,1,4))$ et G le plan vectoriel d'équation $x + y + z = 0$.
Montrer que $E = F \oplus G$.

Pour de plus amples rappels sur les sommes directes et espaces supplémentaires, voir le poly ≪ Révisions : Algèbre linéaire ≫. (Caractérisation à l'aide de $F \cap G$ et des dimensions,...)

Définition 3 Soient $F_1, \ldots, F_n$ des sous-espaces vectoriels de E.

On dit que la somme $F_1 + \cdots + F_n$ est **directe**, et on la note $F_1 \oplus \cdots \oplus F_n$ ou $\displaystyle\bigoplus_{i=1}^{n} F_i$ lorsque :

pour tout $x \in F_1 + \cdots + F_n$, il **existe un unique** n**-uplet** $(x_1, \ldots, x_n) \in F_1 \times \cdots \times F_n$ tel que :

$$x = x_1 + \cdots + x_n.$$

Remarque 2 On a notamment $E = F_1 \oplus \cdots \oplus F_n$ si et seulement si :

$$\forall x \in E,\ \exists!(x_1, \ldots, x_n) \in F_1 \times \cdots \times F_n \,/\, x = x_1 + \cdots + x_n.$$

Proposition 4 Soient $F_1, \ldots, F_n$ des sous-espaces vectoriels de E.
Alors la somme $F_1 + \cdots + F_n$ est **directe** si et seulement si le **vecteur nul** se décompose de manière unique dans $F_1 + \cdots + F_n$.
Autrement dit, la somme $F_1 + \cdots + F_n$ est **directe** si et seulement si :

$$\forall (x_1, \cdots, x_n) \in F_1 \times \cdots \times F_n, \quad \left(\sum_{i=1}^{n} x_i = 0_E \ \Rightarrow\ x_1 = \cdots = x_n = 0_E \right)$$

Définition 4 Si $E = \displaystyle\bigoplus_{i=1}^{n} F_i$, on dit qu'on a une décomposition en somme directe de E.

Théorème 3 Si $F_1, \ldots, F_p$ sont des sous-espaces de dimension finie d'un espace vectoriel E (de dimension quelconque), alors :

$$\dim\left(\sum_{i=1}^{p} F_i \right) \leqslant \sum_{i=1}^{p} \dim(F_i)$$

avec égalité si et seulement si la somme est directe.

Cas particulier : si E est de dimension finie

Proposition 5 Soit E un espace vectoriel <u>de dimension finie</u> et $F_1 \oplus \cdots \oplus F_n$ une somme directe de sous-espaces vectoriels. Soit $\mathcal{B}_1, \ldots, \mathcal{B}_n$ des bases respectives de $F_1, \ldots, F_n$. Alors la famille obtenue par **concaténation** des bases $\mathcal{B}_1, \ldots, \mathcal{B}_n$ est une base de $F_1 \oplus \cdots \oplus F_n$.
On dit que cette base est **adaptée à la décomposition en somme directe** de $F_1 \oplus \cdots \oplus F_n$.

Corollaire 1 Si $E = F_1 \oplus \cdots \oplus F_n$, et si $\mathcal{B}_1, \ldots, \mathcal{B}_n$ sont des bases respectives de $F_1, \ldots, F_n$, alors la famille obtenue par concaténation des bases $\mathcal{B}_1, \ldots, \mathcal{B}_n$ est une base de E.

Corollaire 2 Soit E un espace vectoriel <u>de dimension finie</u>. Si $E = F_1 \oplus \cdots \oplus F_n$, alors

$$\dim\,(E) =$$

III Matrices par blocs et sous-espaces stables

III.1 Matrices définies par blocs

Considérons une matrice $A \in \mathcal{M}_{n,p}(\mathbb{K})$ ainsi que deux entiers $i \in [\![1\,;\, n-1]\!]$ et $j \in [\![1\,;\, p-1]\!]$.
Divisons les lignes de A en deux ensembles : les lignes dont les indices sont compris entre 1 et i et celles dont les indices sont compris entre $i+1$ et n. Faisons de même avec les colonnes en distinguant celles dont les indices sont compris entre 1 et j de celles dont les indices sont compris entre $j+1$ et p.
En procédant de la sorte, on divise la matrice A en quatre blocs :

$$A = \begin{array}{cc} \begin{pmatrix} \boxed{A_1} & \boxed{A_2} \\ \boxed{A_3} & \boxed{A_4} \end{pmatrix} & \begin{array}{l} \updownarrow i \\ \updownarrow n-i \end{array} \\ \begin{array}{cc} \overset{\longleftrightarrow}{j} & \overset{\longleftrightarrow}{p-j} \end{array} & \end{array} \qquad \text{avec} \quad A_1 \in \mathcal{M}_{i,j}(\mathbb{K}),\ A_2 \in \mathcal{M}_{i,p-j}(\mathbb{K}),\ A_3 \in \mathcal{M}_{n-i,j}(\mathbb{K}),\ A_4 \in \mathcal{M}_{n-i,p-j}(\mathbb{K}).$$

Une telle matrice sera dite *définie par blocs*.
Pour peu que le découpage soit identique, la définition par bloc de deux matrices est évidemment compatible avec l'addition :

$$\text{si } A' = \begin{pmatrix} \boxed{A'_1} & \boxed{A'_2} \\ \boxed{A'_3} & \boxed{A'_4} \end{pmatrix} \quad \text{alors} \quad \lambda A + A' = \begin{pmatrix} \boxed{\lambda A_1 + A'_1} & \boxed{\lambda A_2 + A'_2} \\ \boxed{\lambda A_3 + A'_3} & \boxed{\lambda A_4 + A'_4} \end{pmatrix}$$

mais le fait le plus remarquable est que le découpage par blocs est *compatible avec la multiplication*, pour peu que les découpages conduisent à des produits « licites »de matrices :

$$\text{si } B = \begin{array}{cc} \begin{pmatrix} \boxed{B_1} & \boxed{B_2} \\ \boxed{B_3} & \boxed{B_4} \end{pmatrix} & \begin{array}{l} \updownarrow j \\ \updownarrow p-j \end{array} \\ \begin{array}{cc} \overset{\longleftrightarrow}{k} & \overset{\longleftrightarrow}{q-k} \end{array} & \end{array} \in \mathcal{M}_{p,q}(\mathbb{K}) \quad \text{alors} \quad AB = \begin{array}{cc} \begin{pmatrix} \boxed{A_1B_1 + A_2B_3} & \boxed{A_1B_2 + A_2B_4} \\ \boxed{A_3B_1 + A_4B_3} & \boxed{A_3B_2 + A_4B_4} \end{pmatrix} & \begin{array}{l} \updownarrow i \\ \updownarrow n-i \end{array} \\ \begin{array}{cc} \overset{\longleftrightarrow}{k} & \overset{\longleftrightarrow}{q-k} \end{array} & \end{array} \in \mathcal{M}_{n,q}(\mathbb{K})$$

Autrement dit, les matrices définies par blocs se multiplient entre elles tout comme si les blocs étaient des scalaires, à condition que chaque multiplication corresponde à une multiplication « légale »de matrices (en ce qui concerne les dimensions).

Ces propriétés s'étendent par récurrence au cas d'un découpage des lignes et/ou des colonnes en un nombre arbitraire de subdivisions.

Définition 5 Une matrice carrée $A \in \mathcal{M}_p(\mathbb{K})$ est dite *diagonale par bloc* lorsqu'il existe une subdivision de $[\![1\,;\, p]\!]$ telle que :

$$A = \begin{array}{cc} \begin{pmatrix} \boxed{A_{11}} & & & \\ & \boxed{A_{22}} & & \\ & & \ddots & \\ & & & \boxed{A_{kk}} \end{pmatrix} & \begin{array}{l} \updownarrow i_1 \\ \updownarrow i_2 \\ \vdots \\ \updownarrow i_k \end{array} \\ \begin{array}{cccc} \overset{\longleftrightarrow}{i_1} & \overset{\longleftrightarrow}{i_2} & \cdots & \overset{\longleftrightarrow}{i_k} \end{array} & \end{array}$$

Tous les blocs sont nuls
hormis les blocs diagonaux, qui sont tous carrés.

Une matrice carrée $A \in \mathcal{M}_p(\mathbb{K})$ est dite *triangulaire par bloc* lorsqu'il existe une subdivision de $[\![1\,;\, p]\!]$ telle que :

$$A = \begin{array}{cc} \begin{pmatrix} \boxed{A_{11}} & \boxed{A_{12}} & \cdots & \boxed{A_{1k}} \\ & \boxed{A_{22}} & \cdots & \boxed{A_{2k}} \\ & & \ddots & \vdots \\ & & & \boxed{A_{kk}} \end{pmatrix} & \begin{array}{l} \updownarrow i_1 \\ \updownarrow i_2 \\ \vdots \\ \updownarrow i_k \end{array} \\ \begin{array}{cccc} \overset{\longleftrightarrow}{i_1} & \overset{\longleftrightarrow}{i_2} & \cdots & \overset{\longleftrightarrow}{i_k} \end{array} & \end{array}$$

Tous les blocs diagonaux sont carrés,
et les blocs situés sous la diagonale sont nuls.

Exemple 3 $A = \begin{pmatrix} -3 & 5 & 0 & 0 & 0 \\ 1 & 4 & 0 & 0 & 0 \\ 0 & 0 & 5 & 6 & 9 \\ 0 & 0 & 1 & -2 & 8 \\ 0 & 0 & 1 & 7 & -9 \end{pmatrix}$

III.2 Sous-espaces stables

Définition 6 Soit H un sous-espace vectoriel de E, et $u \in \mathcal{L}(E)$ un endomorphisme.
On dit que H est *stable* par u lorsque $u(H) \subset H$.

Proposition 6 Si u et v sont deux endomorphismes d'un espace vectoriel E tels que $uov = vou$, alors le noyau $\mathrm{Ker}(u)$ et l'image $\mathrm{Im}(u)$ sont des sous-espaces stables par v.

Exemple 4 Soit u l'endomorphisme de $\mathbb{R}^3$ canoniquement associé à la matrice $A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}$.

1. Montrer que le sous-espace F d'équation $x + y + z = 0$ est stable par u.
2. Construire une base de E adaptée à la stabilité de F et déterminer la matrice de u dans cette base.

De manière générale, considérons une base adaptée à un sous-espace vectoriel H, c'est-à-dire construite à partir d'une base $(e_1, \ldots, e_k)$ de H puis complétée pour former une base $\mathcal{B} = (e_1, \ldots, e_k, e_{k+1}, \ldots, e_p)$ de E.
Alors H est stable par u si et seulement si la matrice associée à u dans cette base $(\mathcal{B})$ est de la forme :

$$\begin{array}{cc} \begin{array}{c} k \\ p-k \end{array} & \begin{pmatrix} A & C \\ O & D \end{pmatrix} \\ & \begin{array}{cc} k & p-k \end{array} \end{array}$$

En effet, le fait que la matrice soit de cette forme signifie que :

$$\forall j \in [\![1 \,;\, k]\!], \quad u(e_j) \in H = (e_1, \ldots, e_k).$$

Lorsque H est stable par u, la restriction de u à H définit donc un endomorphisme u_H de H dont la matrice dans la base $(e_1, \ldots, e_k)$ est la matrice A. **Cet endomorphisme s'appelle l'*induit* de u sur H.**

Remarque 3 Dans une base $(e'_1, \ldots, e'_p)$ de E pour laquelle ce sont les vecteurs $(e'_{p-k+1}, \ldots, e'_p)$ qui forment une base de H, la matrice d'un endomorphisme stabilisant H est de la forme :

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

Exemple 5 $\mathrm{Ker}(u)$ et $\mathrm{Im}(u)$ sont des sous-espaces vectoriels stables de u. En effet, dans une base dont les p premiers vecteurs forment une base de $\ker(u)$, la matrice associée à u prend la forme : $\begin{pmatrix} O & C \\ O & D \end{pmatrix}$

De même, dans une base dont les r premiers vecteurs forment une base de $\mathrm{Im}(u)$, la matrice associée à u est alors de la forme suivante : $\begin{pmatrix} A & C \\ O & O \end{pmatrix}$

Théorème 4 (Sous-espaces stables et matrice diagonale par blocs)
Soit $E = F_1 \oplus F_2 \oplus .... \oplus F_p$ une décomposition de E en somme directe.
Pour chaque $i \in \{1, 2, ...p\}$ on note B_i une base de F_i . On note B la base de E obtenue par concaténation des B_i.
Soit f un endomorphisme de E et $A = \mathcal{M}at_B(f)$.
Les propositions suivantes sont équivalentes :

- Les sous-espaces F_i sont tous stables par f.
- La matrice A est diagonale par blocs, la taille du $i$eme bloc étant la dimension de F_i

Exemple 6 Projecteur et symétrie, rotation de $\mathbb{R}^3$

Théorème 5 (Sous espaces stables et matrice triangulaire supérieure)
Soit f un endomorphisme de E et $B = (e_1, e_2, ..., e_n)$ une base de E.
$\forall i \in \{1, 2, ..., n\}$, on note $F_i = vect(e_1, e_2, ...e_i)$.
Les propositions suivantes sont équivalentes :

- Les sous-espaces F_i sont tous stables par f.
- La matrice $A = \mathcal{M}at_B(f)$ est triangulaire supérieure.

IV A propos de matrices carrées

IV.1 Rappels de PCSI

Définition 7 Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, de dimension n.
On appelle matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$ la matrice P de $\mathcal{M}_n(\mathbb{K})$ dont les colonnes contiennent les coordonnées des éléments de $\mathcal{B}'$ relativement à la base $\mathcal{B}$. On a aussi $P = \mathcal{M}_{\mathcal{B}',\mathcal{B}}(Id_E)$.
On note couramment : $P = Pass_{\mathcal{B}\to\mathcal{B}'} = P_{\mathcal{B}\to\mathcal{B}'}$

Proposition 7 Soit $u \in \mathcal{L}(E, F)$, soient $\mathcal{B}_1, \mathcal{B}_1{}'$ des bases de F avec $Q = Pass_{\mathcal{B}_1\to\mathcal{B}'_1}$ et soient $\mathcal{B}$, $\mathcal{B}'$ des bases de E avec $P = Pass_{\mathcal{B}\to\mathcal{B}'}$.

- Pour tout $x \in E$, si on pose $X = \mathcal{M}_{\mathcal{B}}(x)$ et $X' = \mathcal{M}_{\mathcal{B}'}(x)$, alors : $X = PX'$
- P est inversible et $P^{-1} = Pass_{\mathcal{B}'\to\mathcal{B}}$.
- Si $f \in \mathcal{L}(E, F)$ et $A = \mathcal{M}_{\mathcal{B},\mathcal{B}_1}(f)$ et $A' = \mathcal{M}_{\mathcal{B}',\mathcal{B}'_1}(f)$, alors $A' = Q^{-1}AP$.
- Si $E = F$, alors $\mathcal{M}_{\mathcal{B}'}(f) = P^{-1}\mathcal{M}_{\mathcal{B}}(f)P$ (ou : $A' = P^{-1}AP$).

IV.2 Matrices semblables

Définition 8 Soient A, B dans $\mathcal{M}_n(\mathbb{K})$.
Si il existe $P \in \mathcal{GL}_n(\mathbb{K})$ telle que $B = P^{-1}AP$, on dit que A et B sont **semblables**.

Remarque 4 Deux matrices A et B sont semblables si et seulement si elles représentente le même endomorphisme dans deux bases d'un même $\mathbb{K}$-espace vectoriel de dimension finie. La matrice P de la relation « $B = P^{-1}AP$ »s'interprète alors comme la matrice de passage entre ces deux bases.

Exemple 7

1. Si $B = P^{-1}AP$, alors on a : alors $A = PBP^{-1}$.
2. Une matrice est semblable à elle-même.
3. Que dire d'une matrice semblable à I_n ? à $\lambda \cdot I_n$?
4. **Important** : si $B = P^{-1}AP$, alors pour tout $k \in \mathbb{N}$, $B^k = P^{-1}A^kP$ (dém. à écrire au dos).

   En particulier : si A et B sont semblables, alors A^k et B^k sont semblables pour tout $k \in \mathbb{N}$.

Proposition 8 Deux matrices semblables ont même rang.

Preuve On rappelle que : si Q est inversible, alors pour tout matrice $M \in \mathcal{M}_n(\mathbb{K})$, on a rg($QM$)=rg($MQ$) =rg($M$).
Soient A et P deux matrices de $\mathcal{M}_n(\mathbb{K})$. Si P est inversible alors $\text{rg}(P^{-1}(AP)) = \text{rg}(AP) = \text{rg}(A)$.
Deuxième méthode : le rang d'un endomorphisme et de sa matrice dans n'importe quelle(s) base(s) sont égaux. ■

IV.3 Trace d'une matrice carrée, trace d'un endomorphisme

Définition 9 Trace d'une matrice carrée.
La **trace** d'une matrice carrée A est la somme de ses éléments diagonaux. Elle est notée $\text{tr}(A)$.
Si $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{R})$, on a donc $\text{tr}(A) = \displaystyle\sum_{i=1}^{n} a_{i,i}$.

Proposition 9
- L'application Trace est une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$.
- Si $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$, alors : $\text{tr}(AB) = \text{tr}(BA)$.
- Deux matrices semblables ont la même trace.

Remarque 5 L'ensemble $H = \{A \in \mathcal{M}_n(\mathbb{K}) \,/\, \text{tr}(A) = 0\} = \text{Ker}(\text{tr})$ est un hyperplan de $\mathcal{M}_n(\mathbb{K})$.
Exercice : Donner une base de cet hyperplan.

Theorème-Definition 2 Soit E un $\mathbb{K}$-espace vectoriel **de dimension finie** et $f \in \mathcal{L}(E)$.
On considère $\mathcal{B}$ une base de E et $A = \mathcal{M}_{\mathcal{B}}(f)$.
Alors $\text{tr}(A)$ ne dépend pas du choix de $\mathcal{B}$ et est appelé la **trace** de f.
Autrement dit : on a pour toute base B de E : $\text{tr}(f) = \text{tr}(\mathcal{M}_{\mathcal{B}}(f))$.

Proposition 10 Soit E de dimension finie.
- L'application T« trace » est une forme linéaire sur $\mathcal{L}(E)$.
- Pour tout f, g dans $\mathcal{L}(E)$, on a : $\text{Tr}(f \circ g) = \text{Tr}(g \circ f)$

V Polynômes d'endomorphismes et de matrices carrées

V.1 Introduction

Définition 10 Soit A une matrice de $\mathcal{M}_n(\mathbb{K})$. Soit $P = \displaystyle\sum_{k=0}^{p} a_k X^k$ un polynome de $\mathbb{K}[X]$.
On définit la matrice $P(A)$ par :

$$P(A) = \sum_{k=0}^{p} a_k A^k$$

avec la convention : $A^0 = I_n$, et pour tout entier k non nul, $A^k = \underbrace{A \times A ... \times A}_{k \text{ fois}}$.

Exemple 8 Ecrire $P(A)$ pour $P = X^2 + X$ puis pour $P = X^2 + 7$.

Proposition 11
- L'application $\Phi : \left\{ \begin{array}{lcl} \mathbb{K}[X] & \rightarrow & \mathcal{M}_n(\mathbb{K}) \\ P & \mapsto & P(A) \end{array} \right.$ est une application linéaire.
- Pour tous polynomes P et Q de $\mathbb{K}[X]$, et pour toute matrice carrée A, on a :

$$(P \times Q)(A) = P(A) \times Q(A)$$

- Les matrices $P(A)$ et $Q(A)$ commutent.

Exemple 9 Polynome d'une matrice triangulaire par blocs

1. Si M est une matrice triangulaire par blocs, $M = \begin{pmatrix} A & * \\ 0 & B \end{pmatrix}$, et si $P \in \mathbb{K}[X]$, alors : $P(M) = \begin{pmatrix} P(A) & * \\ 0 & P(B) \end{pmatrix}$
2. Si M est diagonale par blocs, $M = \mathrm{Diag}(M_1, M_2, ..., M_k)$, alors pour tout polynome P :
$$P(M) = \mathrm{Diag}(P(M_1), P(M_2)...., P(M_k)).$$

Définition 11 Soit $u \in \mathcal{L}(E)$ et soit $P \in \mathbb{K}[X]$.
Si $P = \sum_{k=0}^{n} a_k X^k$, on définit l'endomorphisme $P(u) = \sum_{k=0}^{n} a_k u^k$.

$$\begin{aligned} P(X) &= a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \\ P(u) &= a_n u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 \mathrm{Id}_E \end{aligned}$$

Proposition 12 L'application qui à P associe $P(u)$ est une application linéaire qui vérifie :
$$\forall (P,Q) \in \mathbb{K}[X]^2, \quad (PQ)(u) = P(u) \circ Q(u).$$
Par ailleurs : $P(u)$ et $Q(u)$ commutent c'est à dire :

Proposition 13 Soit $P \in \mathbb{K}[X]$ et soit $u \in \mathcal{L}(E)$. Alors le noyau de $P(u)$ est stable par u.

ATTENTION : Si P et Q sont deux polynômes vérifiants $PQ = 0$, on sait que l'on peut en déduire que $P = 0$ ou $Q = 0$.
Ce n'est pas le cas des polynômes d'un endomorphisme : on peut avoir $(PQ)(u) = 0$ sans pour autant en déduire que $P(u) = 0$ ou $Q(u) = 0$.
On peut faire la même remarque concernant les polynômes de matrices...
Considérons par exemple une projection vectorielle u : on a $u^2 - u = 0$. Si on pose $P = X$ et $Q = X - 1$ on a $PQ = X^2 - X$ donc $(PQ)(u) = 0$, mais on a pas en général $P(u) = 0$ ou $Q(u) = 0$ (sauf si $u = 0$ ou $u = \mathrm{Id}_E$).

Proposition 14 (Polynome d'endomorphisme et matrice associée)
Soit f un endomorphisme d'un espace vectoriel E de dimension n.
Soit $\mathcal{B}$ une base de E, et A la matrice de f dans la base $\mathcal{B}$.
Pour tout polynome P, la matrice de l'endomorphisme $P(f)$ dans la base $\mathcal{B}$, est la matrice $P(A)$.

V.2 Polynôme annulateur d'un endomorphisme ou d'une matrice

Définition 12 Soit $P \in \mathbb{K}[X]$.

Soit $f \in \mathcal{L}(E)$. On dit que P est un polynôme annulateur de f lorsque $P(f)$ est l'endomorphisme nul.

Soit $A \in \mathcal{M}_n(\mathbb{K})$. On dit que P est un polynôme annulateur de A lorsque la matrice $P(A)$ est la matrice nulle.

Exemple 10 Soit p un projecteur. Donner un polynôme annulateur de p.
Soit s une symétrie vectorielle. Donner un polynôme annulateur de s.

Proposition 15 Lorsque E est un espace vectoriel **de dimension finie**, tout endomorphisme $u \in \mathcal{L}(E)$ possède un polynôme annulateur.
Toute matrice carrée possède un polynôme annulateur.

Exemple 11 Considérons une matrice $A \in \mathcal{M}_2(\mathbb{K})$, et posons $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

$$\begin{aligned} A^2 &= \begin{pmatrix} a^2+bc & (a+d)b \\ (a+d)c & bc+d^2 \end{pmatrix} \\ &= \begin{pmatrix} (a+d)a+bc-ad & (a+d)b \\ (a+d)c & (a+d)d+bc-ad \end{pmatrix} \\ &= (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} - (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \mathrm{tr}(A)\, A - \mathrm{Det}(A)\, I_2 \end{aligned}$$

Autrement dit, le polynôme $P = X^2 - (\mathrm{tr}A)X + (\mathrm{Det}A)$ est un polynôme annulateur de A.

V.3 Application au calcul de l'inverse

Exemple 12 Montrer que $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ admet $X^2 - 5X + 4$ comme polynome annulateur.

En déduire que A est inversible et expliciter son inverse.

Exemple 13 Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a vu que $A^2 - (\mathrm{tr}(A))A + (\mathrm{Det}(A))I_2 = 0$.

Si $\mathrm{Det}(A) \neq 0$, on peut dire que A est inversible et que

$$A^{-1} =$$

Proposition 16 Calcul de l'inverse d'une matrice On suppose qu'une matrice A admet un polynome annulateur P tel que $P(0) \neq 0$.
Alors A est inversible et on peut exprimer A^{-1} à l'aide des puissances de A.
Plus précisément : si $P(X) = a_0 + a_1 X + \cdots + a_n X^n$ alors

$$A^{-1} =$$

A vous de jouer : énoncer des propriétés analogues pour les endomorphismes !

V.4 Application au calcul des puissances d'une matrice ou d'un endomorphisme

Soit A une matrice carrée et soit P un polynôme annulateur de A. On suppose que $\deg(P) = d$.
Pour calculer A^n, on peut réaliser la division euclidienne de X^n par P :

$$X^n = PQ + R, \text{ avec } \deg(R) < d.$$

Ainsi, $A^n = P(A)\, Q(A) + R(A) = R(A)$ puisque $P(A) = 0$.
Le calcul de A^n se ramène à celui de $R(A)$, ce qui peut être intéressant lorsque le degré d du polynôme annulateur est petit, puisque $\deg R < d$.

Exemple 14 On a vu que la matrice $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ admet $X^2 - 5X + 4$ comme polynome annulateur.

Déterminer le reste dans la division euclidienne X^k par P.
Déterminer A^k.

Exemple 15 Soit $p \geq 1$ et soit $n \geq 1$.

1. Déterminer le reste de la division euclidienne de $(1+X)^n$ par $X(X-p)$.
2. On pose $U = \begin{pmatrix} 1 & \cdots & \cdots & 1 \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 1 & \cdots & \cdots & 1 \end{pmatrix} \in \mathcal{M}_p(\mathbb{R})$, et $A = U + I_p = \begin{pmatrix} 2 & 1 & \cdots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 2 \end{pmatrix}$.
   (a) Calculer U^2 et déterminer un polynôme annulateur de U.
   (b) En déduire A^n pour $n \in \mathbb{N}$, ainsi que l'inverse de A, s'il existe.

De la même manière : si u est un endomorphisme de E de polynôme annulateur P qui est de degré d), alors on peut réaliser la division euclidienne de X^n par P :

$$X^n = PQ + R, \text{ avec } \deg(R) < d.$$

Ainsi $u^n = P(u) \circ Q(u) + R(u) = R(u)$ puisque $P(u) = 0$.