Classes préparatoires aux grandes écoles

Filière scientifique • Mathématiques

Compléments d'algèbre linéaire

Mouad El Assadi

Professeur agrégé de mathématiques

Ingénieur d'État en génie civil — École Hassania des Travaux Publics (EHTP)

elassadimouad1@gmail.com

Table des matières

1 Sommes directes et blocs **2**
1.1 Somme directe de n sous-espaces vectoriels 2
1.2 Détermination d'une application linéaire 4
1.3 Calcul matriciel par blocs 6
1.4 Déterminants par blocs 8

2 Algèbres **9**
2.1 Définitions générales 9
2.2 Spécialisation d'un polynôme 12

3 Polynômes d'endomorphismes **13**
3.1 Polynômes annulateurs et polynôme minimal 13
3.2 Lemme de décomposition des noyaux 16

1. Sommes directes et blocs

1.1 Somme directe de n sous-espaces vectoriels

On définit la somme de n espaces vectoriels de façon globale, plutôt qu'itérative :

Définition 1.1 (Somme d'un nombre fini de sous-espaces)**.** *Soit $n \geq 1$, et $F_1, \ldots, F_n$ des sous-espaces vectoriel de E. On définit*

$$\sum_{i=1}^{n} F_i = F_1 + \cdots + F_n = \left\{ \sum_{i=1}^{n} x_i \mid x_1 \in F_1, \ldots, x_n \in F_n \right\}.$$

Théorème 1.2 (Minimalité de la somme)**.**

$\sum_{i=1}^{n} F_i$ *est le plus petit sous-espace vectoriel de E incluant tous les E_i. En d'autres termes,*

$$\sum_{i=1}^{n} F_i = \mathit{Vect}\left(\bigcup_{i=1}^{n} F_i \right).$$

Éléments de preuve.
- C'est un sev, par vérifications simples
- Il inclut tous les F_i
- Par stabilité par somme, si un sev G inclut tous les F_i, il inclut aussi leur somme.

□

Proposition 1.3 (Somme directe)**.** *Soit $F_1, \ldots, F_n$ des sev de E. Les propositions suivantes sont équivalentes:*

(i) 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 $x = x_1 + \cdots + x_n$

(ii) Pour tout $(x_1, \ldots, x_n) \in F_1 \times \cdots \times F_n$, tel que $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$, $x_1 + \cdots + x_n \neq 0$.

(iii) Pour tout $i \in [1, n]$, $F_i \cap \sum_{j \in [1,n] \setminus \{i\}} F_j = \{0\}$

(iv) Pour tout $i \in [2, n]$, $F_i \cap \sum_{j=1}^{i-1} F_j = \{0\}$

(v) Pour tout $i \in [2, n]$, la somme de F_i et de $\sum_{j=1}^{i-1} F_j$ est directe.

Dans ce cas, on dit que la somme $F_1 + \cdots + F_n$ est directe, et pour indiquer cette propriété, on note :

$$F_1 + \cdots + F_n = F_1 \oplus \cdots \oplus F_n = \bigoplus_{i=1}^{n} F_i.$$

Remarque 1.4. *La propriété (v) montre que la somme globale est directe, si et seulement si à chaque étape, le terme qu'on ajoute est en somme directe avec les précédents. Combine aux propriétés d'associativité, cela permet d'écrire :*

$$\bigoplus_{i=1}^{n} F_i = ((F_1 \oplus F_2) \oplus F_3) \oplus \cdots \oplus F_{n-1}) \oplus F_n.$$

Remarque 1.5 (Avertissement)**.** *Attention à l'erreur courante consistant à caractériser la somme directe par le fait que les intersections deux à deux sont réduites à $\{0\}$ (autrement dit les E_i sont 2 à 2 en somme directe. C'est clairement insuffisant, comme le montre l'exemple de 3 droites vectorielles non confondues dans le plan.*

Exercice 1.6 (Une condition d'égalité de deux sommes directes)**.** *Soit E un $\mathbb{K}$-ev, $E_1, \dots, E_n, F_1, \dots, F_n$ des sev de E tels que :*

$$\bigoplus_{i=1}^{n} E_i = \bigoplus_{i=1}^{n} F_i \qquad \text{et} \qquad \forall i \in [\![1, n]\!], \quad E_i \subset F_i.$$

Montrer que pour tout $i \in [\![1, n]\!]$, $E_i = F_i$.

Exercice 1.7 (Caractère direct de la somme des sous-espaces propres)**.** *Soit $u \in \mathcal{L}(E)$ un endomorphisme d'un K-espace vectoriel E. Soit $\lambda_1, \dots, \lambda_n$ des elements de K deux a deux distincts. Montrer de deux manieres (l'une avec, l'autre sans le lemme de decomposition des noyaux), que la somme $\bigoplus_{i=1}^{n} \operatorname{Ker}(u - \lambda_i id)$ est directe.*

Proposition 1.8 (Dimension d'une somme)**.** *Soit $F_1, \dots, F_n$ des sous-espaces de dimension finie de E. Alors :*

1. *$F_1 + \cdots + F_n$ est aussi de dimension finie ;*
2. *$\dim(F_1 + \cdots + F_n) \leq \sum_{i=1}^{n} \dim(F_i)$;*
3. *si la somme est directe, $\dim\left(\bigoplus_{i=1}^{n} F_i\right) = \sum_{i=1}^{n} \dim(F_i)$.*

Définition 1.9 (Concaténation)**.** *Pour $X = (x_1, \dots, x_k) \in E^k$ et $Y = (y_1, \dots, y_\ell) \in E^\ell$, on note*

$$X \sim Y = (x_1, \dots, x_k, y_1, \dots, y_\ell)$$

la concaténation du k-uplet X et du ℓ-uplet Y. Il s'agit donc d'un $k + \ell$-uplet. C'est une notation à redémir si vous l'utilisez.

Proposition 1.10 (Base adaptée à une décomposition en somme directe)**.**

1. *Soit E un espace vectoriel de dimension finie, tel que $E = \bigoplus_{i=1}^{n} E_i$, et tout $i \in [1, n]$, B_i une base de E_i. Alors $B = B_1 \cup \cdots \cup B_n$ est une base de E.*
2. *Une base B de E est dite adaptée à la décomposition en somme directe $E = \bigoplus_{i=1}^{n} E_i$ si elle est obtenue de la sorte, par concaténation de bases des E_i.*

Le point 1 montre qu'il existe toujours une base adaptée à une décomposition en somme directe.

Proposition 1.11 (Projecteurs associés à une décomposition en somme directe)**.** *Soit E un espace vectoriel tel que $E = \bigoplus_{i=1}^{n} E_i$. On définit pour tout $i \in [1, n]$, $\pi_i : E \to E$ par*

$$\pi_i : x_1 + \cdots + x_n \mapsto x_i.$$

1. *Pour tout $i \in [1, n]$, π_i est un projecteur. Plus précisément, c'est le projecteur sur E_i parallèlement à la somme des autres E_k.*

2. *Les π_i vérifient :*

$$\sum_{i=1}^{n} \pi_i = id_E \quad \textit{et} \quad \forall (i,j) \in [1,n]^2 \quad \pi_i \circ \pi_j = \delta_{i,j}.$$

On peut montrer que réciproquement, si $(\pi_1, \dots, \pi_n)$ sont des projecteurs vérifiant le point 2, leurs images forment une décomposition de E en somme directe dont ils sont les projecteurs associés.

1.2 Détermination d'une application linéaire

Vous avez déjà vu l'année dernière qu'une application linéaire se détermine entièrement et sans ambiguïté par l'image des vecteurs d'une base. C'est cette représentation qui donne lieu ensuite aux interprétations matricielles : la matrice d'une application linéaire u détermine entièrement u, justement car elle décrit l'image d'une base.

Nous allons donner une version un peu plus générale de ce résultat, en montrant qu'une application linéaire est déterminée par ses restrictions à des sous-espaces formant une décomposition de E en somme directe. En considérant une décomposition de E en somme directe de droites engendrées par les vecteurs d'une base, on retrouve plus ou moins le théorème de détermination d'une AL sur une base, pouvant ainsi considérer que nous avons généralisé ce résultat.

Proposition 1.12 (Détermination d'une AL sur une décomposition en somme directe)**.** *Soit E et F deux $\mathbb{K}$-ev. Soit $E = \bigoplus_{j=1}^{n} E_j$ une décomposition de E en somme directe, et pour tout $j \in [1,n]$, $u_j \in \mathcal{L}(E_j, F)$. Alors il existe une et une seule application linéaire $u \in \mathcal{L}(E,F)$ telle que pour tout $j \in [1,n]$, $u|_{E_j} = u_j$.*

Éléments de preuve. Une analyse synthèse sans difficulté. □

Proposition 1.13 (Interprétation matricielle de la détermination sur une $\bigoplus$)**.** *Soit $E = \bigoplus_{i=j}^{n} E_j$ et F deux espaces vectoriels de dimension finie. On note, pour $i \in [1,n]$, $p_j = \dim E_j$, $p = \dim E$ et $q = \dim F$. On se donne $B_1, \dots, B_n$ des bases de $E_1, \dots, E_n$, C une base de F, et on définit $B = B_1 \cup \dots \cup B_n$, base adaptée à la décomposition de E en somme directe.*

1. *Soit pour tout $j \in [1,n]$, $u_j \in \mathcal{L}(E_j, F)$, et $A_j = Mat_{B_i,C}(u_j) \in \mathcal{M}_{q,p_j}(\mathbb{K})$. Alors l'unique application linéaire $u \in \mathcal{L}(E,F)$ coïncidant avec chacun des u_j est l'application déterminée par la matrice*

$$Mat_{B,C}(u) = (Mat_{B_1,C}(u_1) \quad Mat_{B_2,C}(u_2) \quad \cdots \quad Mat_{B_n,C}(u_n)) \in \mathcal{M}_{q,p}(\mathbb{K}),$$

   c'est-à-dire la matrice obtenue en juxtaposant dans une même grande matrice les matrices des u_i dans l'ordre.

2. *Réciproquement, pour $u \in \mathcal{L}(E,F)$, et une décomposition en blocs*

$$Mat_{B,C}(u) = (A_1 \quad A_2 \quad \cdots \quad A_n),$$

   où pour tout $j \in [1,n]$, $A_j \in \mathcal{M}_{q,p_j}$, alors

$$A_j = Mat_{B_j,F}(u|_{E_j}).$$

3. *En particulier, pour $u \in \mathcal{L}(E,F)$, avec les notations précédentes,*

$$\mathit{Mat}_{B,C}(u \circ \pi_j) = \begin{pmatrix} 0_{q,p_1} & \cdots & 0_{q,p_{j-1}} & A_j & 0_{q,p_{j+1}} & \cdots & 0_{q,p_n} \end{pmatrix}.$$

On s'intéresse maintenant au problème dual, lorsque $F = \bigoplus_{i=1}^m F_i$ admet une décomposition en somme directe.

Proposition 1.14 (Interprétation matricielle d'une décomposition en $\oplus$ à l'arrivée)**.** *Soit E et F deux espaces vectoriels de dimension finie, et $F = \bigoplus_{i=1}^m F_i$ une décomposition de F en somme directe. Soit pour tout $i \in [1,m]$ une base C_i de F_i, et $C = C_1 \sim \cdots \sim C_m$ la base de F correspondante, adaptée à la décomposition. Soit B une base de E. Alors*

$$\mathit{Mat}_{B,C}(u) = \begin{pmatrix} M_{B,C_1}(u) \\ \vdots \\ M_{B,C_m}(u) \end{pmatrix}.$$

De plus, on a alors, pour tout $i \in [1,m]$

$$\mathit{Mat}_{B,C}(\rho_i \circ u) = \begin{pmatrix} 0_{q_1,p} \\ \vdots \\ 0_{q_{i-1},p} \\ M_{B,C_i}(u) \\ 0_{q_{i+1},p} \\ \vdots \\ 0_{q_m,p} \end{pmatrix}$$

Définition 1.15 (Décomposition en blocs d'une matrice)**.** *On appellera décomposition (ou découpage) par blocs d'une matrice A une représentation de A dans laquelle on a regroupé certaines lignes consécutives ou colonnes consécutives de sorte à former des sous-matrices, vérifiant les conditions du 3 du théorème 8.1.13*

Corollaire 1.16 (Décomposition de E stable par u)**.** *Soit E un espace vectoriel de dimension finie, et une décomposition en somme directe :*

$$E = \bigoplus_{j=1}^n E_j.$$

Soit pour tout $i \in [1,n]$, B_i une base de E_i, et $B = B_1 \sim \cdots \sim B_n$ une base adaptée. Soit $u \in \mathcal{L}(E)$ tel que pour tout $i \in [1,n]$, E_i est stable par u. Alors

$$\mathit{Mat}_B(u) = \begin{pmatrix} \mathit{Mat}_{B_1}(u_{E_1}) & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \mathit{Mat}_{B_n}(u_{E_n}) \end{pmatrix},$$

où $u_{E_i} = iu_i$ est l'endomorphisme de $\mathcal{L}(E_i)$ induit par u.

Une telle matrice est appelée matrice diagonale par blocs.

1.3 Calcul matriciel par blocs

Les descriptions précédentes vont permettre d'établir assez facilement (disons que le plus dur est fait...) les règles de calcul matriciel par blocs.

Définition 1.17 (Découpages par blocs de tailles compatibles)**.** *Soit $A \in \mathcal{M}_{q,r}(\mathbb{K})$ et $B \in \mathcal{M}_{r,s}(\mathbb{K})$ deux matrices, munis de découpages par blocs*

$$A = (A_{i,j})_{(i,j)\in[1,m]\times[1,n]} \quad \textit{et} \quad B = (B_{j,k})_{(j,k)\in[1,n]\times[1,p]}.$$

On dira que les deux découpages par blocs ont des tailles compatibles si pour tout $j \in [1,n]$, le nombre de colonnes des $A_{i,j}$ est égal au nombre de lignes des $B_{j,k}$.

Remarque 1.18.

1. *Attention, on ne peut pas permuter A et B dans cette définition.*
2. *Cette condition permet de considérer, pour tout $j \in [1,n]$, le produit $A_{i,j}B_{j,k}$. De plus, le format de cette matrice ne dépend pas de j. Ainsi, la matrice suivante est bien définie :*
$$\sum_{j=1}^{n} A_{i,j}B_{j,k}.$$
3. *D'un point de vue vectoriel, si A et B sont interprétés comme des matrices d'applications linéaires $u \in L(F,G)$ et $v \in L(E,F)$ respectivement, relativement à des bases B, C et D, les découpages par blocs définissent des décompositions en somme directe de E, F et G. La compatibilité des tailles des blocs dit simplement que les blocs de A et B définissent la même décomposition en somme directe de F.*

Théorème 1.19 (Produit matriciel par blocs)**.** *Soit $A \in M_{q,r}(\mathbb{K})$ et $B \in M_{r,s}(\mathbb{K})$ deux matrices, munis de découpages par blocs*

$$A = (A_{i,j})_{(i,j)\in[1,m]\times[1,n]} \quad \textit{et} \quad B = (B_{j,k})_{(j,k)\in[1,n]\times[1,p]}$$

de tailles compatibles. Alors le produit AB peut se calculer par blocs :

$$AB = \left(\sum_{j=1}^{n} A_{i,j}B_{j,k}\right)_{(i,k)\in[1,m]\times[1,p]}.$$

Éléments de preuve. La démonstration n'est pas exigible.

Considérer $u \in L(F,G)$ et $v \in L(E,F)$ des endomorphismes associés à A et B, avec des décompositions en somme directe associées de E, F et G, de projections respectives π_k, ρ_j et σ_i. Décomposer

$$\pi_k \circ u \circ v \circ \sigma_i = \sum_j \pi_k \circ u \circ \rho_j \circ \rho_j \circ v \circ \sigma_i$$

et utiliser les résultats du paragraphe précédent. □

Ainsi, le produit matriciel par blocs suit les mêmes règles que le produit matriciel sur les coefficients, en remplaçant les coefficients par des blocs matriciels. Il faut juste pour cela que les tailles soient compatibles pour former les produits.

Corollaire 1.20 (Puissances de matrices triangulaires par blocs)**.** *Soit $A \in M_p(\mathbb{K})$ découpée en blocs $A = (A_{i,j})_{1\leq i,j\leq n}$, de tailles compatibles pour former le produit $A \times A$ (autrement dit, les regroupements de lignes ont la même taille que les regroupements de colonnes, ce qui équivaut à dire que les blocs diagonaux sont carrés).*

1. *On dit que A est triangulaire (supérieure) par blocs si pour tout $i > j$, $A_{i,j} = 0$, donc*

$$A = \begin{pmatrix} A_{1,1} & \cdots & \cdots & A_{1,n} \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & A_{q,q} \end{pmatrix}$$

Alors pour tout $n \in \mathbb{N}$, A^n est aussi triangulaire par blocs, avec des blocs de même taille que A, et

$$A^n = \begin{pmatrix} A_{1,1}^n & \cdots & \cdots \\ 0 & \cdots & \cdots \\ \vdots & \ddots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}$$

2. *On dit que A est diagonale par blocs si pour tout $i \neq j$, $A_{i,j} = 0$, donc*

$$A = \begin{pmatrix} A_{1,1} & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots \\ \vdots & \ddots & \cdots & 0 \\ 0 & \cdots & 0 & A_{q,q} \end{pmatrix}$$

Alors pour tout $n \in \mathbb{N}$, A^n est aussi diagonale par blocs, avec des blocs de même taille que A, et

$$A^n = \begin{pmatrix} A_{1,1}^n & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots \\ \vdots & \ddots & \cdots & 0 \\ 0 & \cdots & 0 & A_{q,q}^n \end{pmatrix}$$

Éléments de preuve. Comme pour les matrices exprimées avec des coefficients scalaires. Inutile de refaire. □

Exemple 1.21. *Calcul des puissances successives de*

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Exercice 1.22 (Matrices diagonales par blocs à blocs diagonaux semblables)**.** *Soit A et B deux éléments de $\mathcal{M}_n(\mathbb{C})$ diagonales par blocs. On suppose que les blocs diagonaux de A et de B sont en même nombre. On note (dans l'ordre) $A_1, \ldots, A_k$ les blocs diagonaux de A et $B_1, \ldots, B_k$ ceux de B, et on suppose que pour tout $i \in [1, k]$, A_i est de même taille que B_i, et semblable à cette dernière. Montrer que A et B sont semblables.*

1.4 Déterminants par blocs

Le but de ce paragraphe est de donner quelques outils supplémentaires sur le calcul des déterminants, notamment lorsqu'on dispose d'un découpage par blocs de la matrice. En règle générale, on ne peut pas exploiter un découpage quelconque. Mais certaines manipulations sont permises.

Définition 1.23 (Transvection par blocs)**.** *Soit $A = (A_{i,j})_{(i,j)\in[1,m]\times[1,n]}$ une représentation de A par blocs matriciels $A_{i,j} \in \mathcal{M}_{m_i,n_j}(\mathbb{K})$. Soit $T \in \mathcal{M}_{m_i,m_k}(\mathbb{K})$. Pour $i \neq k$, la transvection $L_i \leftarrow L_i + TL_k$ consiste à remplacer les $A_{i,j}$ de la ligne L_i par $A_{i,j} + TA_{k,j}$.*

La ligne L_i correspond évidemment à la i-lème ligne (matricielle) du découpage par blocs.

Proposition 1.24 (Interprétation matricielle d'une transvection par blocs)**.** *La transvection par blocs $L_i \leftarrow L_i + TL_k$ correspond à la multiplication à gauche par la matrice*

$$E_{i,k,T} = \begin{pmatrix} I & 0 & \cdots & 0 \\ 0 & \ddots & T & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & I \end{pmatrix}$$

les blocs diagonaux étant triangulaires, et les blocs étant de taille compatible avec ceux de A pour effectuer le produit.

Éléments de preuve. C'est la même chose que dans le cas scalaire, à adapter grâce aux règles de produit matriciel par blocs. □

Corollaire 1.25 (Invariance du déterminant par transvection par blocs)**.** *Soit B la matrice obtenue de A par transvection $L_i \leq L_i + TL_k$. Alors det(A) = det(B).*

Éléments de preuve. En effet, la matrice $E_{i,k,T}$ est triangulaire (vraiment, pas seulement par blocs), de coefficients diagonaux tous égaux à 1. □

Lemme 1.26. *1. $\det \begin{pmatrix} I & 0 \\ C & B \end{pmatrix} = \det(B)$*

2. $\det \begin{pmatrix} I & C \\ 0 & B \end{pmatrix} = \det(B)$

Éléments de preuve. 1. Une transvection fait sauter C, puis faire des développements suivant des colonnes pour se débarrasser du I.

2. Transposer.

□

Exercice 1.27 (Déterminants par blocs)**.** *Soit A, B dans $\mathcal{M}_n(\mathbb{C})$. Montrer que*

$$\begin{vmatrix} A & B \\ B & A \end{vmatrix} = \det(A+B)\det(A-B) \quad \textit{et} \quad \begin{vmatrix} A & B \\ -B & A \end{vmatrix} = \det(A+iB)\det(A-iB)$$

Exercice 1.28 (Expression d'un déterminant par blocs)**.** *Soit $n \in \mathbb{N}^*$, A, B, C, D dans $\mathcal{M}_n(\mathbb{R})$ telles que D soit inversible et $CD = DC$. Montrer que*

$$\begin{vmatrix} A & B \\ C & D \end{vmatrix} = \det(AD - BC).$$

Théorème 1.29 (Déterminant d'une matrice triangulaire par blocs)**.** *Soit T une matrice triangulaire par blocs, c'est-à-dire de la forme*

$$T = \begin{pmatrix} A_1 & \cdots & \cdots & \cdots \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & A_k \end{pmatrix}$$

où les A_k sont des matrices carrées. Alors

$$det(T) = det(A_1) \cdots det(A_k).$$

Éléments de preuve. Par récurrence, se ramener au cas $n = 2$, pour lequel on peut décomposer

$$\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \begin{pmatrix} I & C \\ 0 & B \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$$

puis utiliser le lemme 8.1.24. □

Exemple 1.30. *Exprimer $det \begin{pmatrix} A & B \\ B & A \end{pmatrix}$ en fonction de $det(A - B)$ et $det(A + B)$.*

Exercice 1.31 (Formule de Williamson)**.** *Soit $(A_{i,j})_{1 \leq i,j \leq m}$ une famille de matrices de $\mathcal{M}_n(\mathbb{C})$ commutant 2 à 2, et A la matrice de $\mathcal{M}_{mn}(\mathbb{C})$ dont le découpage par blocs de taille $n \times n$ est donné par les $(A_{i,j})$. Soit $B = \sum_{\sigma \in \Theta_m} \epsilon(\sigma) \prod_{i=1}^{m} A_{\sigma(i),i}$. Montrer que $\det(A) = \det(B)$. On pourra construire une récurrence en supposant dans un premier temps que $A_{m,m}$ est inversible.*

2. Algèbres

2.1 Définitions générales

Soit K un corps quelconque.

Définition 2.1 (Algèbre)**.** *Soit $(A, +, \cdot, \times)$ un ensemble muni de 2 l.c.i. $+$ et $\times$ et d'une l.c.e. $\cdot$ sur le corps K. On dit que A est une algèbre sur K si :*

(i) *$(A, +, \cdot)$ est un espace vectoriel sur K*

(ii) *$(A, +, \times)$ est un anneau*

(iii) *Pour tout $(\lambda, x, y) \in \mathbb{K} \times A \times A$, $(\lambda \cdot x) \times y = \lambda \cdot (x \times y) = x \times (\lambda \cdot x)$.*

Remarque 2.2. *1. En particulier, une algèbre est unitaire, dans le sens où elle possède un neutre multiplicatif. Dans certains ouvrages plus généraux, ce n'est pas toujours le cas. Se méfier.*

2. *La définition est redondante, puisque certaines propriétés de $+$ se retrouvent à la fois dans la structure d'anneau et dans la structure d'espace vectoriel*

3. *Pour éviter ces redondances, on peut définir une algèbre comme un K-ev enrichi d'une multiplication $\times$ associative, unitaire, et bilinéaire. La bilinéarité englobe à la fois les propriétés de distributivité et la propriété (iii).*

4. *Les signes opératoires $\times$ et $\cdot$ sont souvent omis. Il n'y a pas de confusion possible entre les deux, puisque l'une des deux lois implique des scalaires et pas l'autre. L'examen de la nature des objets en jeu permet donc de lever toute ambiguïté.*

Exemple 2.3. 1. *$(\mathbb{K}, +, \cdot, \cdot)$ est une K-algèbre (le produit externe et le produit interne sont ici égaux).*

2. *$\mathbb{K}[X]$ est une K-algèbre.*

3. *$\mathbb{K}[X, Y]$ (combinaison linéaire de monômes $X^i Y^j$) aussi.*

4. *$\mathcal{M}_n(\mathbb{K})$ est une K-algèbre*

5. *Si E est un K-ev, $\mathcal{L}(E)$ est une K-algèbre.*

6. *$\mathbb{K}^X = \mathcal{F}(X, \mathbb{K})$ est une K-algèbre.*

7. *C est une R-algèbre.*

8. *Soit $a \in \mathbb{R}$, et $\mathbb{Q}[a] = \{P(a), P \in \mathbb{Q}[X]\}$. Alors $\mathbb{Q}[a]$ est une $\mathbb{Q}$-algèbre.*

Définition 2.4 (Sous-algèbre)**.** *Une sous-algèbre B d'une algèbre A est un sous-ensemble $B \subset A$ tel que :*

(i) *B soit stable par les 3 lois de A*

(ii) *$1_A \in B$*

(iii) *La restriction à B des lois de A définit sur B une structure d'algèbre.*

Proposition 2.5 (Reformulation de la définition des sous-algèbres)**.** *Ainsi, les propositions suivantes sont équivalentes :*

(i) *B est une sous-algèbre de A;*

(ii) *B est un sous-espace vectoriel de A, stable par x et vérifiant $1_A \in B$*

(iii) *B est un sous-anneau de A stable par combinaison linéaire.*

Éléments de preuve. Comme toujours dans ce type de propriété, une fois la stabilité acquise, toutes les propriétés universelles sont préservées par restriction. Il faut juste s'assurer des propriétés existentielles. □

Corollaire 2.6 (Caractérisation des sous-algèbres)**.** *B est une sous-algèbre de A si et seulement si :*

(i) *$B \subset A$*

(ii) $1_A \in B$

(iii) $\forall (x,y) \in \mathbb{K} \times B \times B, \lambda x = y \in B$

(iv) $\forall (x,y) \in B \times B, xy \in B$

Exercice 2.7 (Des sous-algèbres de l'algèbre des fonctions continues)**.** *Déterminer les sous-algèbres de dimension finie de* $C^0(\mathbb{R},\mathbb{R})$.

Exemple 2.8.
1. $\mathbb{K}$ *est une sous-algèbre de* $\mathbb{K}[X]$ *(le corps* $\mathbb{K}$ *étant identifié aux polynômes constants).*
2. *Plus généralement, si* A *est une* $\mathbb{K}$*-algèbre,* $\mathbb{K} \cdot 1_A = Vect(1_A)$ *est une sous-algèbre de* A*.*
3. $\mathbb{K}[X]$ *est une sous-algèbre de* $\mathbb{K}[X,Y]$*.*
4. *L'ensemble* $D_n(\mathbb{K})$ *des matrices diagonales est une sous-algèbre de* $M_n(\mathbb{K})$*.*
5. *De même,* $T_n^+(\mathbb{K})$ *est une sous-algèbre de* $M_n(\mathbb{K})$*.*
6. $T_n^{++}(\mathbb{K})$ *(matrices strictement triangulaires supérieures) est-elle une sous-algèbre de* $M_n(\mathbb{K})$*.*

Exercice 2.9 (Centrale, stabilité d'une sous-algèbre par inversion)**.** *Soient* $n \in \mathbb{N}^*$ *et* A *une sous-algèbre de* $\mathcal{M}_n(\mathbb{K})$*. On suppose que* $M \in \mathcal{A}$ *est une matrice inversible. Montrer que* $M^{-1} \in \mathcal{A}$*.*

Définition 2.10 (Morphisme d'algèbre)**.** *Soit* $(A,+,\cdot,\times)$ *et* $(B,+,\cdot,\times)$ *deux algèbres. Un morphisme d'algèbre est une application* $f \in \mathcal{F}(A,B)$ *telle que :*

(i) f *est une application linéaire de* $(A,+,\cdot)$ *dans* $(B,+,\cdot)$*;*

(ii) f *est un morphisme d'anneaux de* $(A,+,\cdot)$ *dans* $(B,+,\cdot)$*.*

Un isomorphisme d'algèbre est un morphisme d'algèbre bijectif.

Ainsi, en notant 1_A *et* 1_B *les neutres multiplicatifs respectifs de* A *et* B*,* f *est un morphisme d'algèbre si et seulement si :*

- $\forall (\lambda,x,y) \in \mathbb{K} \times A \times A,\ f(\lambda x + y) = \lambda f(x) + f(y)$
- $\forall (x,y) \in A^2,\ f(xy) = f(x)f(y)$
- $f(1_A) = 1_B$*.*

Exemple 2.11.
1. $\mathbb{K} \cdot 1_A$ *est isomorphe à* $\mathbb{K}$*.*
2. $f : \mathbb{R}[X] \to \mathbb{C}$ *définie par* $f(P) = P(i)$ *est un morphisme d'algèbre.*
3. *Plus généralement pour* $a \in \mathbb{K}$*, l'évaluation* $ev_a : \mathbb{K}[X] \to \mathbb{K}$ *définie par* $ev_a(P) = P(a)$ *est un morphisme d'algèbre.*
4. *Si* a *est transcendant (i.e. non racine d'un polynôme de* $\mathbb{Q}[X]$*), alors* $\mathbb{Q}[a]$ *est isomorphe à* $\mathbb{Q}[X]$*.*

Proposition 2.12 (Image d'une sous-algèbre)**.** *Soit* $f : A \to B$ *un morphisme d'algèbre, et* A' *une sous-algèbre de* A*. Alors* $f(A')$ *est une sous-algèbre de* B*.*

2.2 Spécialisation d'un polynôme

Définition 2.13 (Spécialisation d'un polynôme sur une algèbre)**.** *Soit A une $\mathbb{K}$-algèbre, et soit $P \in \mathbb{K}[X]$, décrit par*

$$P = \sum_{k=0}^{d} a_k X^k.$$

La spécialisation de P en $x \in A$ est définie par

$$P(x) = \sum_{k=0}^{d} a_k x^k,$$

Remarque 2.14. 1. *La spécialisation $P(x)$ est bien définie, puisqu'on sait :*

- *faire des produits (donc prendre des puissances) dans A, y compris un produit vide (la puissance d'ordre 0), puisque A est unitaire : pour tout $x \in A$, $x^0 = 1_A$;*
- *multiplier un élément de A par un scalaire $a_i \in \mathbb{K}$;*
- *sommer entre eux des éléments de A.*

2. *Le terme « évaluation » pour désigner $P(x)$ est en général réservé au cas où $x \in \mathbb{K}$. Ainsi, on ne peut évaluer qu'en des éléments du corps de base, mais on peut spécialiser sur des objets plus complexes.*

3. *L'évaluation est un cas particulier de spécialisation, en considérant $A = \mathbb{K}$, qui est bien une algèbre.*

Exemple 2.15. 1. *Spécialisation en une matrice carrée : si $M \in \mathcal{M}_n(\mathbb{K})$, on peut considérer $P(M)$.*

Par exemple, déterminer $P(M)$ lorsque $P = 2X^2 + X + 1$ et $M = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$.

2. *Spécialisation en un endomorphisme : si $u \in \mathcal{L}(E)$, $P(u)$ est bien défini, et est un élément de $\mathcal{L}(E)$, les puissances qui interviennent correspondant à l'itération de la composition.*

Par exemple si $P = 2X^2 + X + 1$, $P(u)$ est l'endomorphisme défini par :

$$P(u)(x) = 2u^2(x) + u(x) + u^0(x) = 2u \circ u(x) + u(x) + x.$$

3. *Attention à ne pas confondre :*

   (a) *$P(u)(x)$ évaluation de l'endomorphisme $P(u)$ en x*

   (b) *$P(u(x))$ spécialisation du polynôme P en $u(x)$ qui nous amène donc à prendre des puissances du vecteur $u(x)$, ce qui n'a de sens que si E est elle-même une algèbre ; ces puissances n'ont alors aucun rapport avec des compositions de u par lui-même.*

Proposition 2.16 (Morphisme de spécialisation)**.** *Pour $x \in A$, l'application $S_x : \mathbb{K}[X] \to A$ définie par $S_x(P) = P(x)$ est un morphisme d'algèbre.*

Éléments de preuve. Le seul point un peu délicat à montrer est le respect du produit qui nécessite une petite manipulation de sommes. □

Proposition 2.17 (Sous-algèbre engendré par un élément). *Soit A une $\mathbb{K}$-algèbre, et $x \in A$. On définit*

$$\mathbb{K}[x] = \{P(x), P \in \mathbb{K}[X]\}$$

Alors $\mathbb{K}[x]$ est une sous-algèbre commutative de A, et est minimale parmi les sous-algèbres de A contenant x. On l'appelle sous-algèbre de A engendrée par x.

Ainsi, $\mathbb{K}[x]$ est l'ensemble des éléments de A s'obtenant polynomialement à partir de x.

Éléments de preuve. C'est l'image par un morphisme d'algèbre d'une algèbre commutative.

En particulier, même si A n'est pas commutative, deux polynômes d'un même élément $x \in A$ commutent. □

Exemple 2.18.

1. *Pour $A = \mathcal{L}(E)$ et $u \in \mathcal{L}(E)$, le produit dans $\mathcal{L}(E)$ étant la composition, le respect du produit par S_u s'écrit :*

$$P(u) \circ Q(u) = (PQ)(u) = (QP)(u) = Q(u) \circ P(u).$$

L'égalité du milieu exploite la commutativité dans $\mathbb{K}[X]$, qui permet donc d'obtenir la commutativité de l'algèbre $(\mathbb{K}[u], +, \cdot, \circ)$.

2. *Décrire $\mathbb{K}[M]$, où $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.*

On remarque que cette propriété de commutation est un cas particulier d'un résultat un peu plus général :

Proposition 2.19 (Polynômes d'endomorphismes qui commutent). *Soit u et v dans $\mathcal{L}(E)$ tels que $u \circ v = v \circ u$. Soit P et Q deux polynômes de $\mathbb{K}[X]$. Alors $P(u) \circ Q(v) = Q(v) \circ P(u)$.*

Éléments de preuve. Par manipulation de sommes, en remarquant que $u^k v^l = v^k u^k$. □

Corollaire 2.20 (Des propriétés de stabilité par commutation). *Soit u et v des endomorphismes qui commutent et P et Q des polynômes. Alors :*

1. *$\mathrm{Im}(u)$ et $\mathrm{Ker}(u)$ sont stables par v;*
2. *$\mathrm{Im}(P(u))$ et $\mathrm{Ker}(P(u))$ sont stables par $Q(v)$*

Éléments de preuve. Le 1 est classique et se démontre indépendamment de ce qui précède. Le 2 consiste à appliquer le 1 aux endomorphismes $P(u)$ et $Q(v)$ qui commutent. □

3. Polynômes d'endomorphismes

3.1 Polynômes annulateurs et polynôme minimal

On rappelle que pour E un K-espace vectoriel et $u \in \mathcal{L}(E)$, l'application $S_u : \mathbb{K}[X] \to \mathcal{L}(E)$ est un morphisme d'algèbre. En particulier, c'est un morphisme d'anneaux. On en déduit la structure de son noyau.

Proposition 3.1 (Idéal des polynômes annulateurs).

- *Le noyau $\mathrm{Ker}(S_u)$ de $S_u : P \mapsto P(u)$ est un idéal, constitué de tous les polynômes $P \in \mathbb{K}[X]$ tels que $P(u) = 0_{\mathcal{L}(E)}$.*

- *Un polynôme vérifiant $P(u) = 0_{\mathcal{L}(E)}$ est appelé polynôme annulateur de u.*

Proposition 3.2 (Existence d'un polynôme annulateur non nul en dimension finie)**.** *Soit E un K-espace vectoriel de dimension finie, et $u \in \mathcal{L}(E)$. Alors u admet au moins un polynôme annulateur non nul.*

Éléments de preuve. Pour $n = \dim(E)$, la famille $(u^0, u^1, \dots, u^{n^2})$ est liée car $\dim(\mathcal{L}(E)) = n^2$. □

Définition 3.3 (Polynôme minimal)**.** *Le polynôme minimal de $u \in \mathcal{L}(E)$ est l'unique polynôme unitaire engendrant l'idéal principal Ker(S_u) des polynômes annulateurs de u. Il est souvent noté μ_u ou π_u.*

Proposition 3.4. *Base et dimension de $\mathbb{K}[u]$. $SoitE$ un espace vectoriel de dimension finie n, et $u \in \mathcal{L}(E)$. Soit $d = \deg(\mu_u)$. Alors*

$$\dim \mathbb{K}[u] = d,$$

et une base en est $(id, u, \dots, u^{d-1})$.

Éléments de preuve. Caractère générateur par division euclidienne. Liberté par minimalité du degré de μ_u. Ainsi, le polynôme minimal μ_u est l'unique polynôme unitaire tel que pour tout polynôme annulateur P de $u, \mu_u | P$. C'est donc aussi, parmi les polynômes annulateurs unitaires non nuls, celui dont le degré est minimal. On peut évidemment traduire ces définitions en termes matriciels. Pour $M \in \mathcal{M}_n(\mathbb{K})$, l'ensemble des polynômes annulateurs de M est l'idéal Ker(S_M), non réduit à 0 car $(M^0, \dots, M^{n^2})$ est liée, et engendrée par un unique polynôme annulateur unitaire μ_M ou π_M, appelé polynôme minimal de M. Avant de voir des exemples de polynômes minimaux, on donne une définition : □

Exercice 3.5 (Une matrice circulante)**.** *Soit $C_n \in \mathcal{M}_n(\mathbb{C})$ définie par*

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

.

Déterminer un polynôme annulateur de C_n, puis son polynôme minimal.

Définition 3.6 (Endomorphisme nilpotent)**.** *Un endomorphisme $u \in \mathcal{L}(E)$ est nilpotent s'il existe $k \in \mathbb{N}$ tel que $u^k = 0_{\mathcal{L}(E)}$. Dans ce cas, l'entier $d = \min\{k \in \mathbb{N}, u^k = 0_{\mathcal{L}(E)}\}$ est appelé indice de nilpotence de u. C'est donc le plus petit entier positif tel que $u^d = 0$.*

L'indice de nilpotence d'un endomorphisme nilpotent est toujours au moins égal à 1 (car $u^d = id$, et même à 2, sauf si $u = 0$. Cette définition s'adapte bien entendu aux matrices.

Exemple 3.7. *Les exemples suivants doivent être pris comme des exemples du cours.*

1. *Polynôme minimal de $0_{\mathcal{L}(E)}$.*
2. *Polynôme minimal d'une matrice scalaire λI_n, $\lambda \neq 0$.*

3.

$$J_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{C})$$

4. *Les projecteurs sont définis algébriquement par un polynôme annulateur $X^2 - X$. À quelle condition est-ce le polynôme annulateur ?*

5. *De même, $X^2 - 1$ est un polynôme annulateur de toute symétrie. À quelle condition est-ce le polynôme minimal ?*

L'exemple de la matrice J_n se généralise de la sorte.

Proposition 3.8 (Caractérisation d'un endomorphisme nilpotent par son pol. min.)**.** *Soit $u \in \mathcal{L}(E)$. Les propositions suivantes sont équivalentes:*

(i) *u est nilpotente d'indice de nilpotence d;*

(ii) *$\mu_u = X^d$.*

Par ailleurs, on sait comparer le degré de μ_d à $n = \dim(E)$, dans ce cas particulier, grâce au lemme suivant.

Lemme 3.9 (Majoration de l'indice de nilpotence)**.** *Soit E un espace vectoriel de dimension finie n, et soit u un endomorphisme nilpotent de E, d'indice de nilpotence d. Alors $d \leq n$.*

Éléments de preuve. Montrer qu'il existe $x \in E$ tel que $(x, u(x), \ldots, u^{d-1}(x))$ soit libre. □

Ainsi, le polynôme minimal d'un endomorphisme minimal est toujours de degré inférieur à $\dim(E)$. Ce résultat se généralisera à tout polynôme minimal plus tard, grâce au théorème de Cayley-Hamilton, qui fournit un polynôme annulateur de degré $n = \dim(E)$ (ce qui assure de facto que le polynôme minimal est de degré plus petit).

Exercice 3.10 (Sous-espaces caractéristiques)**.** *Soit E un $\mathbb{R}$-ev de dimension quelconque, et soit $u \in \mathcal{L}(E)$.*

1. *Montrer que la suite de sous-espaces vectoriels $(\mathit{Ker}\ u^k)_{k\in\mathbb{N}}$ est croissante pour l'inclusion, et la suite $(\mathit{Im}\ u^k)_{k\in\mathbb{N}}$ est decroissante.*

2. *Soit $p \in \mathbb{N}$. Montrer que si $\mathit{Ker}(u^p) = \mathit{Ker}(u^{p+1})$, alors $\mathit{Ker}(u^k) = \mathit{Ker}(u^p)$ pour tout $k \geqslant p$. Qu'en est-il de $\mathit{Im}(u^k)$?*

   L'espace $\mathit{Ker}(u^p)$ est appele sous-espace caracteristique de u associe a la valeur (propre) 0. On peut considerer plus generalement l'espace obtenu de la sorte avec l'endomorphisme $u-\lambda\mathrm{id}$, appele, s'il est non trivial, sous-espace caracteristique associe a la valeur propre λ.

Exercice 3.11 (Théorème des noyaux itérés)**.** *Soit E un espace vectoriel de dimension finie sur $\mathbb{K}$, et $u \in \mathcal{L}(E)$.*

1. *Montrer que pour tout $k \in \mathbb{N}$, $\mathrm{rg}(u^k) - \mathrm{rg}(u^{k+1}) = \dim(\mathit{Ker}(u) \cap \mathit{Im}(u^k))$.*

2. *En deduire que la suite $(\dim \mathit{Ker}(u^{k+1}) - \dim \mathit{Ker}(u^k))_{k\in\mathbb{N}}$ est decroissante.*

3.2 Lemme de décomposition des noyaux

On termine cette section dédiée aux polynômes d'endomorphismes et de matrices par un résultat qui sera d'une importance capitale pour les problèmes de diagonalisation, et plus généralement de réduction. Je lui donne un statut de théorème, même s'il est communément appelé lemme.

Théorème 3.12 (Lemme de décomposition des noyaux)**.** *Soit $r \in \mathbb{N}^*$, et $P_1, \dots, P_r$ des éléments de $\mathbb{K}[X]$ deux à deux premiers entre eux. Alors*

$$Ker(P(u)) = \bigoplus_{i=1}^{r} Ker(P_i(u)).$$

Éléments de preuve. Par récurrence immédiate, la primalité 2 à 2 impliquant en particulier que P_k est premier avec $P_1 \dots P_{k-1}$, il suffit de le montrer lorsque $r = 2$. Pour $r = 2$, se servir d'une relation de Bézout, à la fois pour montrer l'inclusion directe, et pour montrer le caractère directe de la somme. □

Corollaire 3.13 (Décomposition de E issue d'un polynôme annulateur)**.** *Soit P un polynôme annulateur de u, tel que $P = P_1 \dots P_r$, où les P_i sont 2 à 2 premiers entre eux. Alors*

$$E = \bigoplus_{i=1}^{r} Ker(P_i(u)).$$

Exemple 3.14.

1. *Si p est un projecteur, on retrouve $E = Ker(p) \oplus Ker(p - id)$*
2. *Si s est une symétrie, on retrouve $E = Ker(s - id) \oplus Ker(s + id)$*
3. *Dans les deux exemples précédents, trouver une base B de E telle que $Mat_B(p)$ (resp. $Mat_B(s)$) soit diagonale.*

Le dernier point nous fait bien comprendre l'utilité de ce résultat dans des études de diagonalisabilité. Ainsi, on obtient par exemple le résultat important suivant (qui sera repris et complété dans le chapitre suivant) :

Théorème 3.15 (Caractérisation de la diagonalisabilité par polynômes annulateurs)**.** *Soit E de dimension finie, et $u \in \mathcal{L}(E)$ admettant un polynôme annulateur scindé à racines simples. Alors P est diagonalisable.*

Éléments de preuve. Par le lemme de décomposition des noyaux, puis prendre une base de chaque terme de la somme directe. C'est même une équivalence, comme on le justifiera plus tard. D'où la terminologie « caractérisation ». □