

Agrégation Interne

Décomposition de Dunford (ou Jordan-Chevalley)

Ce problème est l'occasion de revoir quelques résultats de base d'algèbre linéaire.

Les notions qu'il peut être utile de réviser sont les suivantes :

- polynômes d'endomorphismes ;
- valeurs et vecteurs propres, polynôme caractéristique, trigonalisation des matrices ;
- le théorème de décomposition des noyaux ;
- polynôme minimal ;
- extensions de corps ;
- endomorphismes nilpotents ;
- l'exponentielle d'endomorphisme ;
- normes matricielles, rayon spectral.

Sur ces questions d'analyse matricielle, on peut consulter les ouvrages suivants :

- P. G. CIARLET — *Introduction à l'analyse numérique matricielle et à l'optimisation*. Masson (1982).
- F. R. GANTMACHER — *Théorie des matrices (Vol. 1 et 2)*. Dunod (1966).
- X. GOURDON — *Les maths en tête. Algèbre*. Ellipses. (1994).
- R. A. HORN, C. A. JOHNSON — *Matrix analysis*. Cambridge University Press (1985).
- J. E. ROMBALDI — *Analyse matricielle*. EDP Sciences (2000).
- P. TAUVEL — *Mathématiques générales pour l'agrégation*. Masson (1993).

1 Énoncé

Pour ce problème, E est un espace vectoriel de dimension $n \geq 1$ sur un corps commutatif \mathbb{K} et $\mathcal{L}(E)$ est l'algèbre des endomorphismes de E .

On se donne $u \in \mathcal{L}(E)$ et $P_u(X) = \det(u - XId)$ désigne le polynôme caractéristique de u .

On rappelle que pour tout polynôme $P(X) = \sum_{k=0}^p a_k X^k$, $P(u)$ est l'endomorphisme de E défini par :

$$P(u) = a_0 Id + a_1 u + \cdots + a_p u^p$$

où $u^k = u \circ \cdots \circ u$, cette composition étant effectuée k fois pour $k \geq 1$ et $u^0 = Id$. On vérifie alors que $\mathbb{K}[u] = \{P(u) \mid P \in \mathbb{K}[X]\}$ est une algèbre unitaire commutative.

$\mathcal{M}_n(\mathbb{K})$ désigne l'algèbre des matrices carrées d'ordre n à coefficients dans \mathbb{K} .

– I – Généralités

- Soient p un entier supérieur ou égal à 2, P_1, \dots, P_p des polynômes non nuls dans $\mathbb{K}[X]$ et Q_1, \dots, Q_p les polynômes définis par $Q_k = \prod_{\substack{j=1 \\ j \neq k}}^p P_j$ pour tout k compris entre 1 et p . Montrer que

si les polynômes P_k sont deux à deux premiers entre eux dans $\mathbb{K}[X]$, alors les polynômes Q_k sont premiers entre eux dans leur ensemble et pour tout k compris entre 1 et p , les polynômes P_k et Q_k sont premiers entre eux.

- Soient p un entier supérieur ou égal à 2, P_1, \dots, P_p des polynômes non nuls dans $\mathbb{K}[X]$ deux à deux premiers entre eux et $P = \prod_{k=1}^p P_k$.

Montrer que :

$$\ker(P(u)) = \bigoplus_{k=1}^p \ker(P_k(u))$$

les projecteurs $\pi_k : \ker(P(u)) \rightarrow \ker(P_k(u))$, pour k compris entre 1 et p , étant des éléments de $\mathbb{K}[u]$ (théorème de décomposition des noyaux).

- Soient p un entier supérieur ou égal à 2 et :

$$P(X) = \prod_{k=1}^p (X - \lambda_k)^{\alpha_k}$$

un polynôme scindé sur \mathbb{K} , où les α_k sont des entiers naturels non nuls et les λ_k des scalaires deux à deux distincts. En utilisant la décomposition en éléments simples de la fraction rationnelle $\frac{1}{P}$, donner une expression des projecteurs π_k de $\ker(P(u))$ sur $\ker(P_k(u))$ pour tout k compris entre 1 et p .

- Justifier l'existence et l'unicité d'un polynôme unitaire de plus petit degré qui annule u . Ce polynôme est noté π_u et on dit que c'est le polynôme minimal de u . On définit de manière analogue le polynôme minimal π_A d'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ et on vérifie que si A est la matrice de u dans une base de E , alors $\pi_u = \pi_A$.
- Montrer que si F est un sous espace vectoriel de E stable par u , alors le polynôme caractéristique de la restriction de u à F divise celui de u .

6. On propose ici une démonstration du théorème de Cayley-Hamilton qui nous dit que $P_u(u) = 0$, ce qui est encore équivalent à dire que π_u divise P_u .

En désignant par A la matrice de u , dans une base de E , il est équivalent de montrer que $P_A(A) = 0$.

On considère la matrice $A - XI_n$ comme un élément de $\mathcal{M}_n(\mathbb{K}(X))$ où $\mathbb{K}(X)$ est le corps des fractions rationnelles à coefficients dans \mathbb{K} .

- (a) Justifier le fait que la transposée $C(X)$ de la matrice des cofacteurs de $A - XI_n$ s'écrit :

$$C(X) = \sum_{k=0}^{n-1} C_k X^k$$

où les C_k sont des éléments de $\mathcal{M}_n(\mathbb{K})$.

- (b) En notant $P_u(X) = \sum_{k=0}^n a_k X^k$, montrer que :

$$\begin{cases} AC_0 = a_0 I_n \\ AC_k - C_{k-1} = a_k I_n \quad (1 \leq k \leq n-1) \\ -C_{n-1} = a_n I_n \end{cases}$$

- (c) En déduire que $P_A(A) = \sum_{k=0}^n a_k A^k = 0$ et $P_u(u) = 0$.

7. On propose ici une deuxième démonstration du théorème de Cayley-Hamilton pour u non nul (pour $u = 0$ c'est clair).

On se donne un vecteur non nul $x \in E$ et on désigne par E_x le sous espace vectoriel de E engendré par $\{u^k(x) \mid k \in \mathbb{N}\}$ (sous espace cyclique engendré par x).

- (a) Soit p_x le plus petit entier strictement positif tel que le système :

$$\mathcal{B}_x = \{u^k(x) \mid 0 \leq k \leq p_x - 1\}$$

soit libre. Montrer que \mathcal{B}_x est une base de E_x .

- (b) Justifier l'existence d'un polynôme :

$$\pi_x(X) = X^{p_x} - \sum_{k=0}^{p_x-1} a_k X^k$$

tel que $u^{p_x}(x) = \sum_{k=0}^{p_x-1} a_k u^k(x)$, puis montrer que π_x est le polynôme minimal et $(-1)^{p_x} \pi_x$ le polynôme caractéristique de la restriction de u à E_x .

- (c) En déduire que $P_u(u) = 0$.

8. Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice réelle. Cette matrice est aussi une matrice complexe. En désignant respectivement par $\pi_{A,\mathbb{R}}$ et $\pi_{A,\mathbb{C}}$ le polynôme minimal de A dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$, montrer que $\pi_{A,\mathbb{R}} = \pi_{A,\mathbb{C}}$

9. Montrer que si \mathbb{L} est une extension du corps \mathbb{K} , A une matrice dans $\mathcal{M}_n(\mathbb{K})$, $\pi_{A,\mathbb{K}}$ et $\pi_{A,\mathbb{L}}$ le polynôme minimal de A dans $\mathbb{K}[X]$ et $\mathbb{L}[X]$ respectivement, alors $\pi_{A,\mathbb{K}} = \pi_{A,\mathbb{L}}$.

10. Montrer que les valeurs propres de u sont les racines de π_u .

11. Montrer que si P_u est scindé sur \mathbb{K} avec :

$$P_u(X) = (-1)^n \prod_{k=1}^p (X - \lambda_k)^{\alpha_k}$$

où les α_k sont des entiers naturels non nuls et les λ_k des scalaires deux à deux distincts, alors :

$$\pi_u(X) = \prod_{k=1}^p (X - \lambda_k)^{\beta_k}$$

avec $1 \leq \beta_k \leq \alpha_k$.

12. Montrer que si F est un sous-espace vectoriel de E stable par u , alors le polynôme minimal de la restriction de u à F divise celui de u .

13.

(a) Montrer que u est diagonalisable si, et seulement si, il est annulé par un polynôme scindé à racine simple.

(b) En déduire que si u est diagonalisable et F un sous-espace vectoriel de E stable par u , alors la restriction de u à F est un endomorphisme de F diagonalisable.

14. Montrer que si u, v sont deux endomorphismes de E qui sont diagonalisables et qui commutent, il existe alors une base commune de diagonalisation.

– II – Endomorphismes nilpotents

On dit qu'un endomorphisme v est nilpotent s'il existe un entier q strictement positif tel que $v^{q-1} \neq 0$ et $v^q = 0$. On dit que q est l'indice de nilpotence de v .

1. Montrer que si $v \in \mathcal{L}(E)$ est nilpotent, alors 0 est valeur propre de v et $\text{Tr}(v) = 0$.
2. Montrer que, pour \mathbb{K} algébriquement clos, v est nilpotent si, et seulement si, 0 est la seule valeur propre de v . Que se passe-t-il pour \mathbb{K} non algébriquement clos ?
3. On suppose le corps \mathbb{K} de caractéristique nulle (ce qui signifie que le morphisme d'anneaux $k \mapsto k \cdot 1$ de \mathbb{Z} dans \mathbb{K} est injectif, ce qui est encore équivalent à dire que l'égalité $k\lambda = 0$ dans \mathbb{K} avec $k \in \mathbb{Z}$ et $\lambda \in \mathbb{K}^*$ équivaut à $k = 0$).
Montrer qu'un endomorphisme v est nilpotent si, et seulement si, $\text{Tr}(v^k) = 0$ pour tout k compris entre 1 et n .
4. On suppose le corps \mathbb{K} de caractéristique nulle et algébriquement clos.
Montrer que si v est tel que $\text{Tr}(v^k) = 0$ pour tout k compris entre 1 et $n - 1$, il est alors nilpotent ou diagonalisable inversible.
5. Montrer que si $(v_i)_{1 \leq i \leq n}$ est une famille d'endomorphismes nilpotents qui commutent deux à deux ($n = \dim(E)$), alors $\prod_{i=1}^n v_i = 0$.
6. Montrer que si v, w sont deux endomorphismes nilpotents qui commutent, alors $v + w$ est nilpotent.

– III – Décomposition de Dunford (ou Jordan-Chevalley)

En utilisant les notations de **I.11** les sous espaces vectoriels $N_k = \ker(u - \lambda_k Id)^{\alpha_k}$ sont les sous-espaces caractéristiques de u (comme N_k contient l'espace propre $\ker(u - \lambda_k Id)$, il n'est pas réduit à $\{0\}$).

1. En supposant que P_u est scindé sur \mathbb{K} , montrer que :

(a) $E = \bigoplus_{k=1}^p N_k$.

(b) $N_k = \ker (u - \lambda_k Id)^{\beta_k}$, pour tout $k \in \{1, 2, \dots, p\}$.

(c) λ_k est la seule valeur propre de la restriction de u à N_k .

(d) $\dim(N_k) = \alpha_k$.

(e) La restriction de $u - \lambda_k Id$ à N_k est nilpotente d'indice β_k .

2. On suppose que le polynôme caractéristique de u est scindé sur \mathbb{K} . Montrer qu'il existe un unique couple (d, v) d'endomorphismes de E tel que d soit diagonalisable, v soit nilpotent, d et v commutent et $u = d + v$ (théorème de Dunford). On vérifiera que d et v sont des polynômes en u et que les valeurs propres de d sont celles de u .

3. Soit u l'endomorphisme de \mathbb{K}^4 de matrice :

$$A = \begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

dans la base canonique.

(a) Ecrire la décomposition de Dunford de u .

(b) En déduire un calcul de u^r pour tout entier r strictement positif.

4. On suppose que $\mathbb{K} = \mathbb{C}$ et $\lambda_1, \dots, \lambda_p$ sont les valeurs propres deux à deux distinctes de u dans \mathbb{C} .

On note $\rho(u) = \max_{1 \leq k \leq p} |\lambda_k|$ le rayon spectral de u .

Dans un premier temps, on se donne une norme $x \mapsto \|x\|$ sur E et on lui associe la norme sur $\mathcal{L}(E)$ définie par :

$$\forall v \in \mathcal{L}(E), \|v\| = \sup_{x \in E \setminus \{0\}} \frac{\|v(x)\|}{\|x\|}$$

On rappelle qu'une telle norme est sous-multiplicative dans le sens où $\|v \circ w\| \leq \|v\| \|w\|$ pour tous v, w dans $\mathcal{L}(E)$.

(a) Montrer que :

$$\forall k \geq 1, \rho(u) \leq \|u^k\|^{\frac{1}{k}}$$

(b) On suppose que u est diagonalisable. Montrer qu'il existe une constante réelle $\alpha > 0$ telle que :

$$\forall k \geq 1, \|u^k\|^{\frac{1}{k}} \leq \alpha^{\frac{1}{k}} \rho(u)$$

et en déduire que :

$$\rho(u) = \lim_{k \rightarrow +\infty} \left(\|u^k\|^{\frac{1}{k}} \right).$$

(c) En utilisant la décomposition de Dunford $u = d + v$, montrer qu'il existe une constante réelle $\beta > 0$ telle que :

$$\forall k \geq n, \|u^k\| \leq \beta k^n \|d^{k-n}\|$$

et en déduire que :

$$\rho(u) = \lim_{k \rightarrow +\infty} \left(\|u^k\|^{\frac{1}{k}} \right).$$

(d) Montrer que $\rho(u) = \lim_{k \rightarrow +\infty} \left(\|u^k\|^{\frac{1}{k}} \right)$ où $v \mapsto \|v\|$ est une norme quelconque sur $\mathcal{L}(E)$.

5. Montrer que la série $\sum u^k$ est convergente dans $\mathcal{L}(E)$ si, et seulement si, $\rho(u) < 1$. En cas de convergence de $\sum u^k$, montrer que $Id - u$ est inversible d'inverse $\sum_{k=0}^{+\infty} u^k$.

– IV – Exponentielle d'un endomorphisme (pour $\mathbb{K} = \mathbb{C}$)

On suppose que $\mathbb{K} = \mathbb{C}$ et $v \mapsto \|v\|$ est une norme sur $\mathcal{L}(E)$.

1. Justifier, pour tout $v \in \mathcal{L}(E)$, la définition de l'endomorphisme e^v par :

$$e^v = \sum_{k=0}^{+\infty} \frac{1}{k!} v^k.$$

On définit de manière analogue l'exponentielle d'une matrice $A \in \mathcal{M}_n(\mathbb{C})$ par :

$$e^A = \sum_{k=0}^{+\infty} \frac{1}{k!} A^k$$

et on vérifie facilement que si A est la matrice de v dans une base \mathcal{B} de E , alors e^A est la matrice de e^v dans cette base.

2. Montrer que, pour tout $v \in \mathcal{L}(E)$, on $\det(e^v) = e^{\text{Tr}(v)}$ et e^v est inversible.
3. Calculer, pour tout réel θ l'exponentielle de la matrice $A_\theta = \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}$.
4. Montrer que si v est diagonalisable, il en est alors de même de e^v et exprimer les valeurs propres de e^v en fonctions de celles de v .
5. Montrer que, pour tout $v \in \mathcal{L}(E)$, la fonction $\varphi : t \mapsto e^{tv}$ est de classe \mathcal{C}^1 de \mathbb{R} dans $\mathcal{L}(E)$ et calculer sa dérivée.
6. Montrer que, pour tout $v \in \mathcal{L}(E)$, e^v est inversible d'inverse e^{-v} .
7. Soient v, w dans $\mathcal{L}(E)$. Montrer que $e^{t(v+w)} = e^{tv}e^{tw}$ pour tout réel t si, et seulement si v et w commutent.
8. En utilisant la décomposition de Dunford $u = d + v$, montrer que :

$$e^u = e^d e^v = e^d \sum_{k=0}^{q-1} \frac{1}{k!} v^k$$

où $q \geq 1$ est l'indice de nilpotence de v .

9. Montrer que si $u = d + v$ est la décomposition de Dunford de u , alors celle de e^u est donnée par :

$$e^u = e^d + e^d (e^v - Id),$$

avec e^d diagonalisable et $e^d (e^v - Id)$ nilpotente.

10. Montrer que u est diagonalisable si, et seulement si, e^u est diagonalisable.
11. Déterminer toutes les solutions dans $\mathcal{L}(E)$ de l'équation $e^u = Id$.

– V – Endomorphismes semi-simples

On dit que $u \in \mathcal{L}(E)$ est semi-simple si tout sous-espace vectoriel de E stable par u admet un supplémentaire stable par u .

1. On suppose que le corps \mathbb{K} est algébriquement clos.
Montrer que $u \in \mathcal{L}(E)$ est semi-simple si, et seulement si, il est diagonalisable.
2. Montrer que si u est semi-simple, son polynôme minimal est alors sans facteurs carrés dans sa décomposition en facteurs irréductibles dans $\mathbb{K}[x]$ (i. e. $\pi_u = \prod_{k=1}^p P_k$, où les P_k sont des polynômes irréductibles deux à deux distincts dans $\mathbb{K}[x]$).
3. On suppose que π_u est irréductible dans $\mathbb{K}[x]$. On sait alors que $\mathbb{L} = \frac{\mathbb{K}[x]}{(\pi_u)}$ est un corps.

(a) Montrer que l'espace vectoriel E peut être muni d'une structure de \mathbb{L} -espace vectoriel avec la multiplication externe définie par :

$$\bar{P} \cdot x = P(u)(x)$$

pour tout $\bar{P} \in \mathbb{L}$ et tout $x \in E$.

- (b) Montrer que F est un \mathbb{K} -sous-espace vectoriel de E stable par u si, et seulement si, F est un \mathbb{L} -sous-espace vectoriel de E .
- (c) En déduire que u est semi-simple.
4. Montrer que si le polynôme minimal de u est sans facteurs carrés dans sa décomposition en facteurs irréductibles dans $\mathbb{K}[x]$, alors u est semi-simple.
5. Montrer que si u est semi-simple, alors pour tout sous-espace F de E stable par u , la restriction de u à F est semi-simple.
6. Quels sont les endomorphismes nilpotents de u qui sont semi-simples ?
7. On suppose que $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} . Montrer qu'il existe un unique couple (s, v) d'endomorphismes de E tel que s soit semi-simple, v soit nilpotent, d et s commutent et $u = s + v$ (théorème de Dunford).

2 Solution

– I – Généralités

1. Si le pgcd Δ de (Q_1, \dots, Q_p) est non constant, il admet un diviseur premier R qui divise $Q_1 = \prod_{j=2}^p P_j$, donc l'un des P_j avec $j \neq 1$ et comme R divise aussi Q_j , il divise l'un des P_k avec $k \neq j$, ce qui contredit le fait que P_j et P_k sont premiers entre eux.

Si le pgcd Δ_k de P_k et Q_k est non constant, il admet un diviseur irréductible R_k qui divise P_k et le produit Q_k , il divise donc l'un des P_j avec $j \neq k$, ce qui contredit P_j et P_k premiers entre eux pour $k \neq j$.

2. En utilisant les notations de la question précédente, le théorème de Bézout nous dit qu'il existe des polynômes R_1, \dots, R_p tels que $\sum_{k=1}^p R_k Q_k = 1$ et dans $\mathcal{L}(E)$, on a $Id = \sum_{k=1}^p R_k(u) \circ Q_k(u)$, soit

$$\forall x \in E, x = \sum_{k=1}^p R_k(u) \circ Q_k(u)(x)$$

Pour tout $x \in \ker(P(u))$ et k compris entre 1 et p , on a :

$$P_k(u)(R_k(u) \circ Q_k(u)(x)) = R_k(u) \circ P(u)(x) = 0$$

(commutativité de $\mathbb{K}[u]$), soit :

$$x_k = R_k(u) \circ Q_k(u)(x) \in \ker(P_k(u)).$$

On a donc $\ker(P(u)) \subset \sum_{k=1}^p \ker(P_k(u))$ et comme $\ker(P_k(u)) \subset \ker(P(u))$ pour tout k compris

entre 1 et p , on a l'égalité $\ker(P(u)) = \sum_{k=1}^p \ker(P_k(u))$.

Soit (x_1, \dots, x_p) dans $\prod_{k=1}^p \ker(P_k(u))$ tel que $\sum_{j=1}^p x_j = 0$. Pour k compris entre 1 et p , on a

$0 = Q_k(u) \left(\sum_{j=1}^p x_j \right) = Q_k(u)(x_k)$ et $P_k(u)(x_k) = 0$. Comme P_k et Q_k sont premiers entre eux, il existe deux polynômes A et B tels que $AP_k + BQ_k = 1$ et :

$$A(u) \circ P_k(u) + B(u) \circ Q_k(u) = Id$$

dans $\mathcal{L}(E)$, ce qui donne :

$$x_k = (A(u) \circ P_k(u))(x_k) + (B(u) \circ Q_k(u))(x) = 0$$

On a donc $\ker(P(u)) = \bigoplus_{k=1}^p \ker(P_k(u))$ et les projecteurs de $\ker(P(u))$ sur $\ker(P_k(u))$ sont les $\pi_k = R_k(u) \circ Q_k(u) \in \mathbb{K}[u]$.

3. On a la décomposition en éléments simples :

$$\frac{1}{P(X)} = \sum_{k=1}^p \sum_{i=1}^{\alpha_k} \frac{a_{ik}}{(X - \lambda_k)^i},$$

et en posant, pour tout k compris entre 1 et p :

$$\begin{cases} R_k(X) = (X - \lambda_k)^{\alpha_k} \sum_{i=1}^{\alpha_k} \frac{a_{ik}}{(X - \lambda_k)^i} = \sum_{i=1}^{\alpha_k} a_{ik} (X - \lambda_k)^{\alpha_k - i} \in \mathbb{K}[X] \\ Q_k(X) = \frac{P(X)}{(X - \lambda_k)^{\alpha_k}} = \prod_{\substack{j=1 \\ j \neq k}}^p (X - \lambda_j)^{\alpha_j}, \end{cases}$$

on obtient :

$$\frac{1}{P(X)} = \sum_{k=1}^p \frac{R_k(X)}{(X - \lambda_k)^{\alpha_k}}$$

et la décomposition de Bézout :

$$1 = \sum_{k=1}^p \frac{P(X)}{(X - \lambda_k)^{\alpha_k}} R_k(X) = \sum_{k=1}^p R_k(X) Q_k(X)$$

(on retrouve en fait que les Q_k sont premiers entre eux dans leur ensemble), qui permet d'obtenir les projecteurs :

$$\pi_k = (R_k Q_k)(u).$$

4. Pour E de dimension n , l'espace vectoriel $\mathcal{L}(E)$ est de dimension n^2 et la famille $\{u^k \mid 0 \leq k \leq n^2\}$ est nécessairement liée, ce qui se traduit par l'existence d'un polynôme non nul P tel que $P(u) = 0$. Donc, l'ensemble :

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

n'est pas réduit au polynôme nul et comme I_u est un idéal de l'anneau principal $\mathbb{K}[X]$ (c'est le noyau du morphisme d'algèbres $\varphi : P \mapsto P(u)$, donc $I_u = \ker(\varphi)$ est un sous groupe additif de $\mathbb{K}[X]$ et pour $P \in I_u$ et $Q \in \mathbb{K}[X]$, on a $\varphi(PQ) = \varphi(P) \circ \varphi(Q) = 0$ et $PQ \in I_u$) il existe un unique polynôme unitaire $\pi_u \in \mathbb{K}[X]$ tel que $I_u = \mathbb{K}[X] \pi_u$ (c'est une conséquence du théorème de division euclidienne dans $\mathbb{K}[X]$). π_u est le polynôme unitaire (donc non nul) de plus petit degré annulant u .

Dans $\mathcal{M}_n(\mathbb{K})$ les arguments sont analogues pour définir le polynôme minimal.

Si A est la matrice de u dans une base \mathcal{B} , alors pour tout polynôme $P \in \mathbb{K}[X]$, $P(A)$ est la matrice de $P(u)$ dans \mathcal{B} et en conséquence $I_u = I_A$, $\pi_u = \pi_A$.

5. On désigne par \mathcal{B}_1 une base de F complétée en une base de E , $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Dans cette base la matrice de u est $A = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix}$ où A_1 est la matrice, dans la base \mathcal{B}_1 , de la restriction de u à F (F est stable par u) et le polynôme caractéristique de u s'écrit :

$$P_u(X) = \det(A_1 - XI_{n_1}) \det(A_3 - XI_{n_3}).$$

On en déduit alors que P_u est un multiple du polynôme caractéristique de la restriction de u à F .

6.

- (a) On a $C(X) = \sum_{1 \leq i, j \leq n} \left((-1)^{i+j} \det(C_{i,j}(X)) \right) X^{i+j-1}$, où on a noté $C_{i,j}(x)$ la matrice d'ordre $n-1$ extraite de $A - XI_n$ en supprimant la ligne numéro i et la colonne numéro j . Les coefficients de $C_{i,j}(X)$ étant des polynômes de degré au plus égal à 1, $\det(C_{i,j}(X))$ est un polynôme de degré au plus égal à $n-1$ et $C(X)$ s'écrit :

$$C(X) = \sum_{k=0}^{n-1} C_k X^k$$

où les C_k sont des éléments de $\mathcal{M}_n(\mathbb{K})$.

(b) On a dans $\mathcal{M}_n(\mathbb{K}(X))$:

$$(A - XI_n)C(X) = \det(A - XI_n)I_n$$

soit :

$$(A - XI_n) \sum_{k=0}^{n-1} C_k X^k = \sum_{k=0}^n a_k X^k I_n$$

dans $\mathcal{M}_n(\mathbb{K})[X]$, ce qui s'écrit :

$$AC_0 + \sum_{k=0}^{n-1} (AC_k - C_{k-1})X^k - C_{n-1}X^n = \sum_{k=0}^n a_k X^k I_n$$

et en identifiant les coefficients dans l'anneau $\mathcal{M}_n(\mathbb{K})$, on obtient :

$$\begin{cases} AC_0 = a_0 I_n \\ AC_k - C_{k-1} = a_k I_n \quad (1 \leq k \leq n-1) \\ -C_{n-1} = a_n I_n \end{cases}$$

(c) Des identifications précédentes, on déduit que :

$$\begin{cases} AC_0 = a_0 I_n \\ A^{k+1}C_k - A^k C_{k-1} = a_k A^k \quad (1 \leq k \leq n-1) \\ -A^n C_{n-1} = a_n A^n \end{cases}$$

et en additionnant :

$$AC_0 + \sum_{k=1}^{n-1} (A^{k+1}C_k - A^k C_{k-1}) - A^n C_{n-1} = \sum_{k=0}^n a_k A^k$$

soit :

$$\sum_{k=0}^n a_k A^k = \sum_{k=0}^{n-1} A^{k+1}C_k - \sum_{k=1}^n A^k C_{k-1} = 0$$

On a donc $P_A(A) = 0$ et $P_u(u) = 0$ puisque sa matrice dans la base choisie est $P_A(A)$.

7.

(a) On a $F_x = \text{Vect}(\mathcal{B}_x) \subset E_x$.

Par définition de l'entier p_x , le système \mathcal{B}_x est une base de F_x et $u^{p_x}(x) \in F_x$ (le système $\{u^k(x) \mid 0 \leq k \leq p_x - 1\}$ est libre et $\{u^k(x) \mid 0 \leq k \leq p_x\}$ est lié). On déduit alors, par récurrence sur $k \geq 0$, que $u^{p_x+k}(x) \in F_x$ pour tout entier naturel k . On a donc $F_x = E_x$.

(b) Comme $u^{p_x}(x) \in E_x = \text{Vect}(\mathcal{B}_x)$, il existe des coefficients a_k tels que $u^{p_x}(x) = \sum_{k=0}^{p_x-1} a_k u^k(x)$.

On note $\pi_x(X) = X^{p_x} - \sum_{k=0}^{p_x-1} a_k X^k$.

On a $\pi_x(u)(x) = u^{p_x}(x) - \sum_{k=0}^{p_x-1} a_k u^k(x) = 0$ et avec la commutativité de $\mathbb{K}[u]$, on déduit que :

$$\pi_x(u)(u^k(x)) = u^k(\pi_x(u)(x)) = 0$$

pour tout entier k , ce qui signifie que $\pi_x(u|_{E_x}) = 0$.

Si $Q \in \mathbb{K}_{p_x-1}[t] - \{0\}$ annule u , on a alors $Q(u)(x) = 0$ et le système \mathcal{B}_x est lié, ce qui

contredit la définition de p_x . En conclusion π_x est le polynôme minimal de $u|_{E_x}$.
En écrivant que la matrice de $u|_{E_x}$ dans la base \mathcal{B}_x est :

$$A_x = \begin{pmatrix} 0 & \cdots & 0 & a_0 \\ 1 & \ddots & \vdots & a_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & a_{p_x-1} \end{pmatrix},$$

on déduit que $(-1)^{p_x} \pi_x$ est le polynôme caractéristique de $u|_{E_x}$. En effet en notant $P_{A_x} = P_{(a_0, \dots, a_{p_x-1})}$ ce polynôme caractéristique et en le développant par rapport à la première ligne, on a :

$$P_{(a_0, \dots, a_{p_x-1})}(t) = -t P_{(a_1, \dots, a_{p_x-1})}(t) + (-1)^{p_x+1} a_0$$

et par récurrence $P_{A_x}(t) = (-1)^{p_x} \left(t^{p_x} - \sum_{k=0}^{p_x-1} a_k t^k \right)$.

- (c) Pour tout $x \in E$ le sous espace cyclique E_x étant stable par u , le polynôme caractéristique π_x de $u|_{E_x}$ divise celui de u . C'est-à-dire que $P_u = Q \cdot \pi_x$ et $P_u(u)(x) = Q(u) \circ \pi_x(u)(x) = 0$.

On a donc ainsi montré que pour tout $x \in E$, on a $P_u(u)(x) = 0$ (pour $x = 0$ c'est clair) et donc que $P_u(u) = 0$.

8. Soit $A \in \mathcal{M}_n(\mathbb{R}) \subset \mathcal{M}_n(\mathbb{C})$. Comme $\pi_{A, \mathbb{R}}(A) = 0$ dans $\mathcal{M}_n(\mathbb{C})$, le polynôme $\pi_{A, \mathbb{R}}$ est multiple de $\pi_{A, \mathbb{C}}$ et $d' = \deg(\pi_{A, \mathbb{C}}) \leq d = \deg(\pi_{A, \mathbb{R}})$.

Comme d est le degré du polynôme minimal dans $\mathbb{R}[X]$ de $A \in \mathcal{M}_n(\mathbb{R})$, le système $(A^k)_{0 \leq k \leq d-1}$ est nécessairement \mathbb{R} -libre dans $\mathcal{M}_n(\mathbb{R})$, ce qui entraîne qu'il est \mathbb{C} -libre dans $\mathcal{M}_n(\mathbb{C})$. En effet s'il existe des nombres complexes $\lambda_0, \dots, \lambda_{d-1}$ tels que $\sum_{k=0}^{d-1} \lambda_k A^k = 0$, en notant $\lambda_k = \alpha_k + i\beta_k$

avec α_k et β_k réels, on a $\sum_{k=0}^{d-1} \alpha_k A^k = 0$ et $\sum_{k=0}^{d-1} \beta_k A^k = 0$ dans $\mathcal{M}_n(\mathbb{R})$ (A est réelle) et $\alpha_k = \beta_k$ pour tout k .

Comme d' est le degré du polynôme minimal dans $\mathbb{C}[X]$ de $A \in \mathcal{M}_n(\mathbb{C})$, le système $(A^k)_{0 \leq k \leq d'}$ est \mathbb{C} -lié dans $\mathcal{M}_n(\mathbb{C})$ et $d' \leq d-1$ entraînerait $(A^k)_{0 \leq k \leq d-1}$ lié dans $\mathcal{M}_n(\mathbb{C})$, ce qui n'est pas. On a donc $d' > d-1$, soit $d' \geq d$ et $d = d'$. Comme les polynômes $\pi_{A, \mathbb{R}}$ et $\pi_{A, \mathbb{C}}$ sont unitaires, on en déduit l'égalité $\pi_{A, \mathbb{R}} = \pi_{A, \mathbb{C}}$.

9. Dans le cas plus général d'une extension de corps $\mathbb{K} \subset \mathbb{L}$, on a encore $d' = \deg(\pi_{A, \mathbb{L}}) \leq d = \deg(\pi_{A, \mathbb{K}})$, le système $(A^k)_{0 \leq k \leq d-1}$ est \mathbb{K} -libre dans $\mathcal{M}_n(\mathbb{K})$ et on en déduit qu'il est \mathbb{L} -libre dans $\mathcal{M}_n(\mathbb{L})$. Supposons qu'il existe des scalaires $\lambda_0, \dots, \lambda_{d-1}$ dans \mathbb{L} , tels que $\sum_{k=0}^{d-1} \lambda_k A^k = 0$. Le \mathbb{K} -sous-espace vectoriel V de \mathbb{L} engendré par $\lambda_0, \dots, \lambda_{d-1}$ étant de dimension finie, il admet une base e_1, \dots, e_r et chaque λ_k s'écrit $\lambda_k = \sum_{j=1}^r \alpha_{k,j} e_j$, ce qui donne :

$$0 = \sum_{k=0}^{d-1} \lambda_k A^k = \sum_{k=0}^{d-1} \left(\sum_{j=1}^r \alpha_{k,j} e_j \right) A^k = \sum_{j=1}^r \left(\sum_{k=0}^{d-1} \alpha_{k,j} A^k \right) e_j$$

et $\sum_{k=0}^{d-1} \alpha_{k,j} A^k = 0$ dans $\mathcal{M}_n(\mathbb{K})$ pour tout j compris entre 1 et r , ce qui entraîne la nullité de tous les $\alpha_{k,j}$ et tous les λ_k . On conclut alors comme pour l'extension $\mathbb{R} \subset \mathbb{C}$.

10. Si $\lambda \in \mathbb{K}$ est une valeur propre de u et x un vecteur propre (non nul) associé, de l'égalité :

$$0 = \pi_u(u)(x) = \pi_u(\lambda)x$$

avec $x \neq 0$ on déduit que $\pi_u(\lambda) = 0$, c'est-à-dire que λ est racine de π_u .

Réciproquement si λ est racine de π_u alors π_u s'écrit $\pi_u(X) = (X - \lambda)Q(X)$ et avec $\pi_u(u) = (u - \lambda Id) \circ Q(u) = 0$ et le caractère minimal de π_u , on déduit que $u - \lambda Id$ est non inversible ce qui équivaut à dire que λ est une valeur propre de u .

11. Le théorème de Cayley-Hamilton nous dit que $P_u(u) = 0$, donc π_u divise P_u et comme ces polynômes ont les mêmes racines, le polynôme π_u étant unitaire, le résultat en découle.
12. Notons v la restriction de u à F . C'est un endomorphisme de F si F est stable par u . De $\pi_u(u) = 0$ dans $\mathcal{L}(E)$, on déduit que $\pi_u(v) = 0$ dans $\mathcal{L}(F)$, donc π_u est dans l'idéal annulateur de v et c'est un multiple du polynôme minimal de v .
- 13.

(a) Si u est diagonalisable, on a alors $E = \bigoplus_{k=1}^p \ker(u - \lambda_k Id)$ où $\lambda_1, \dots, \lambda_p$ sont les valeurs propres deux à deux distinctes de u dans \mathbb{K} et u est annulé par le polynôme scindé à racines simples $\pi_u(X) = \prod_{k=1}^p (X - \lambda_k)$ (ce polynôme est le polynôme minimal de u).

Si u est annulé par un polynôme $Q(X) = \prod_{k=1}^q (X - \lambda_k)$ scindé à racines simples, le théorème de décomposition des noyaux nous dit que $E = \ker(Q(u)) = \bigoplus_{k=1}^q \ker(u - \lambda_k Id)$ et u est diagonalisable (le polynôme minimal est alors un diviseur de Q).

(b) Si F est un sous-espace vectoriel de E stable par u , la restriction v de u à F est un endomorphisme de F . Comme u est diagonalisable, il est annulé par un polynôme scindé à racines simples et ce polynôme annule v qui est alors diagonalisable.

14. Comme u est diagonalisable, on a la décomposition en sous espaces propres :

$$E = \bigoplus_{k=1}^p \ker(u - \lambda_k Id).$$

chaque sous espace propre $F_k = \ker(u - \lambda_k Id)$ étant stable par v puisque u et v commutent (pour $x \in F_k$, on a $u(v(x)) = v(u(x)) = v(\lambda_k x) = \lambda_k v(x)$ et $v(x) \in F_k$) et la restriction de v à chaque F_k est diagonalisable (le polynôme minimal de cette restriction divise celui de v qui est scindé à racines simples puisque v est diagonalisable). Il existe donc, pour tout k compris entre 1 et p , une base de F_k formée de vecteurs propres de u et v et la réunion de ces bases nous donne une base de diagonalisation commune à u et v .

– II – Endomorphismes nilpotents

1. Supposons v nilpotent d'ordre $q \geq 1$, soit que $v^{q-1} \neq 0$ et $v^q = 0$.
Avec $\det(v^q) = (\det(v))^q = 0$, on déduit que $\det(v) = 0$ et 0 est valeur propre de v .
On peut aussi dire si $x \in E$ est tel que $v^{q-1}(x) \neq 0$, on a alors $v(v^{q-1}(x)) = v^q(x) = 0$ et 0 est valeur propre de v (la dimension de E n'intervient pas ici).
Pour montrer que la trace d'un endomorphisme nilpotent est nulle, on procède par récurrence sur la dimension $n \geq 1$ de E .
Pour $n = 1$, l'unique endomorphisme nilpotent est l'endomorphisme nul et sa trace est nulle.
Supposons le résultat acquis pour les espaces de dimension au plus égale à $n - 1 \geq 1$ et soit $v \in \mathcal{L}(E)$ nilpotent d'ordre $q \geq 1$ avec E de dimension $n \geq 2$. Comme 0 est valeur propre de v , il existe un vecteur non nul e_1 dans le noyau de v et en complétant ce vecteur en une base

\mathcal{B} de E , la matrice de v dans cette base est de la forme $A = \begin{pmatrix} 0 & \alpha \\ 0 & B \end{pmatrix}$ où $\alpha \in \mathcal{M}_{1,n-1}(\mathbb{K})$

et $B \in \mathcal{M}_{n-1}(\mathbb{K})$. Avec $A^{q+1} = \begin{pmatrix} 0 & \alpha B^q \\ 0 & B^{q+1} \end{pmatrix} = 0$, on déduit que B est nilpotente et en conséquence $\text{Tr}(B) = 0$ (l'hypothèse de récurrence nous donne le résultat sur $\mathcal{M}_{n-1}(\mathbb{K})$), ce qui entraîne $\text{Tr}(v) = \text{Tr}(A) = \text{Tr}(B) = 0$.

2. On a déjà vu que si v est nilpotent d'ordre q , alors 0 est valeur propre de v . S'il existe une autre valeur propre $\lambda \in \mathbb{K}$ de v , on a alors pour tout vecteur propre non nul associé x , $v^q(x) = \lambda^q x = 0$ et $\lambda = 0$. On peut aussi dire que si v est nilpotent d'indice q , son polynôme minimal est X^q et 0 est l'unique valeur propre de v (le fait que \mathbb{K} soit algébriquement clos n'intervient pas ici).

Réciproquement si 0 est la seule valeur propre de v avec \mathbb{K} algébriquement clos, alors le polynôme minimal de v est X^q avec $1 \leq q \leq n$ et v est nilpotent.

Pour \mathbb{K} non algébriquement clos, un endomorphisme v peut avoir 0 pour seule valeur propre dans \mathbb{K} sans être nilpotent comme le montre l'exemple de l'endomorphisme v de \mathbb{R}^3 de matrice :

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ & \sin(\theta) & \cos(\theta) \end{pmatrix}$$

dans la base canonique avec $\theta \notin \pi\mathbb{Z}$. Le polynôme caractéristique de v est :

$$P_v(X) = -X((\cos(\theta) - X)^2 + \sin^2(\theta)),$$

la seule valeur propre réelle est 0 et pour tout entier $q \geq 1$, on a :

$$A^q = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \cos(q\theta) & -\sin(q\theta) \\ & \sin(q\theta) & \cos(q\theta) \end{pmatrix} \neq 0.$$

3. Si v est nilpotent, il en est de même de v^k pour tout entier $k \geq 1$ et $\text{Tr}(v^k) = 0$.

Pour la réciproque, on procède par récurrence sur la dimension $n \geq 1$ de E .

Pour $n = 1$, on a $v(x) = \lambda x$, $\text{tr}(v) = \lambda$ et le résultat est trivial.

Supposons le résultat acquis pour les espaces de dimension au plus égale à $n - 1 \geq 1$ et soit $v \in \mathcal{L}(E)$ tel que $\text{Tr}(v^k) = 0$ pour tout k compris entre 1 et $n = \dim(E) \geq 2$. Si $P_v(X) = \sum_{k=0}^n a_k X^k$ est le polynôme caractéristique de v , en tenant compte de $P_v(v) = \sum_{k=0}^n a_k v^k = 0$ et

$\text{tr}(v^k) = 0$ pour $k = 1, \dots, n$, on déduit que $\text{tr}(P(v)) = na_0 = 0$ et $a_0 = \det(v) = 0$ puisque \mathbb{K} de caractéristique nulle. Donc 0 est valeur propre de v et il existe une base \mathcal{B} de E , dans laquelle

la matrice de v est de la forme $A = \begin{pmatrix} 0 & \alpha \\ 0 & B \end{pmatrix}$ où $\alpha \in \mathcal{M}_{1,n-1}(\mathbb{K})$ et $B \in \mathcal{M}_{n-1}(\mathbb{K})$. Avec

$A^k = \begin{pmatrix} 0 & \alpha B^{k-1} \\ 0 & B^k \end{pmatrix}$, on déduit que $\text{tr}(B^k) = \text{tr}(A^k) = \text{tr}(v^k) = 0$ pour tout $k = 1, \dots, n$ et

l'hypothèse de récurrence nous dit que B est nilpotente. Enfin, en notant p l'indice de nilpotence de B , avec $A^{p+1} = \begin{pmatrix} 0 & \alpha B^p \\ 0 & B^{p+1} \end{pmatrix} = 0$, on déduit que A est nilpotente et il en est de même de v .

Pour \mathbb{K} algébriquement clos et de caractéristique nulle, on peut donner la démonstration directe suivante.

Supposons que $\text{Tr}(v^k) = 0$ pour tout k compris entre 1 et $n = \dim(E)$. S'il existe des valeurs propres non nulles $\lambda_1, \dots, \lambda_p$ d'ordres respectifs $\alpha_1, \dots, \alpha_p$ avec p compris entre 1 et n , on a :

$$\text{Tr}(v^k) = \sum_{j=1}^p \alpha_j \lambda_j^k = 0 \quad (1 \leq k \leq p)$$

(comme \mathbb{K} est algébriquement clos, il existe une base de E dans laquelle la matrice de v est triangulaire de diagonale $(0, \lambda_1, \dots, \lambda_1, \dots, \lambda_p, \dots, \lambda_p)$ et dans cette base, la matrice de v^k est aussi triangulaire de diagonale $(0, \lambda_1^k, \dots, \lambda_1^k, \dots, \lambda_p^k, \dots, \lambda_p^k)$. Mais la matrice de ce système d'équations aux inconnues α_j est une matrice de type Vandermonde de déterminant :

$$\begin{vmatrix} \lambda_1 & \cdots & \lambda_p \\ \vdots & \ddots & \vdots \\ \lambda_1^p & \cdots & \lambda_p^p \end{vmatrix} = \prod_{j=1}^p \lambda_j \begin{vmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ \lambda_1^{p-1} & \cdots & \lambda_p^{p-1} \end{vmatrix} = \prod_{j=1}^p \lambda_j \prod_{1 \leq i < j \leq p-1} (\lambda_j - \lambda_i) \neq 0$$

ce qui entraîne que tous les α_j sont nuls puisque \mathbb{K} de caractéristique nulle. Mais on a alors une contradiction avec $\alpha_j \geq 1$.

En définitive 0 est la seule valeur propre de v et v est nilpotent.

4. Si $\text{Tr}(v^n) = 0$, ce qui précède nous dit que v est nilpotent.

Supposons $\text{Tr}(v^n) \neq 0$. Il existe alors au moins une valeur propre de v non nulle. Notons $\lambda_1, \dots, \lambda_p$ ces valeurs propres non nulles avec $\alpha_1, \dots, \alpha_p$ pour ordres respectifs, où p est compris entre 1 et n . Si $p \leq n - 1$, on a alors :

$$\text{Tr}(v^k) = \sum_{j=1}^p \alpha_j \lambda_j^k = 0 \quad (1 \leq k \leq p)$$

ce qui est en contradiction avec $\alpha_j \geq 1$ pour tout j et le fait que le déterminant de ce système est non nul (\mathbb{K} de caractéristique nulle). On a donc $p = n$ et v est diagonalisable inversible du fait qu'il a n valeurs propres distinctes non nulles.

5. On raisonne par récurrence sur la dimension $n \geq 1$ de E . Pour $n = 1$, il n'y a rien à montrer. Supposons le résultat acquis pour les espaces de dimension comprise entre 1 et $n - 1 \geq 1$. Si $v_1 = 0$, alors $v = 0$. Sinon l'espace $E_1 = \text{Im}(v_1)$ est de dimension comprise entre 1 et $n - 1$ (v_1 est nilpotent, donc non bijectif), stable par tous les v_i pour i compris entre 2 et n puisque v_1 commute à ces v_i et la restriction w_i de chaque v_i à E_1 est aussi nilpotent. Comme les w_i , pour i compris entre 2 et n commutent, l'hypothèse de récurrence nous dit que $\prod_{i=2}^n w_i = 0$ sur E_1 . Pour tout $x \in E$, on a alors :

$$\left(\prod_{i=1}^n v_i \right) (x) = \left(\prod_{i=2}^n v_i \right) (v_1(x)) = \left(\prod_{i=2}^n w_i \right) (v_1(x)) = 0$$

On peut aussi procéder comme suit.

On note $E_k = \text{Im} \left(\prod_{i=k}^n v_i \right)$ pour k compris entre 1 et $n \geq 2$. Comme les v_i commutent deux à deux, l'espace E_k est stable par v_{k-1} pour k compris entre 2 et n et la restriction w_{k-1} de v_{k-1} à E_k est aussi nilpotent, donc non injectif et le théorème du rang nous dit que $\dim(E_k) > \dim(\text{Im}(w_{k-1})) = \dim(E_{k-1})$. On a donc :

$$0 \leq \dim(E_1) < \dim(E_2) < \cdots < \dim(E_n) = \dim(\text{Im}(v_n)) < n = \dim(E)$$

(v_n est nilpotent, donc non injectif et $\dim(\text{Im}(v_n)) < n$) et nécessairement $\dim(E_1) = 0$, ce qui revient à dire que $\prod_{i=1}^n v_i$.

Dans le cas particulier où tous v_i sont égaux à un même endomorphisme nilpotent v , on obtient $v^n = 0$ et on en déduit que l'indice de nilpotence de v est au plus égal à n (ce que l'on peut aussi voir en disant que le polynôme minimal de v est X^q et le théorème de Cayley-Hamilton nous dit que nécessairement $q \leq n$).

6. Comme v et w commutent, on a :

$$(v + w)^n = \sum_{j=0}^n C_n^j v^j w^{n-j} = 0$$

puisque chaque $v^j w^{n-j}$ est un produit de n endomorphismes nilpotents qui commutent deux à deux.

– III – Décomposition de Dunford

1.

(a) De $P_u(u) = 0$ (Cayley-Hamilton) et du théorème de décomposition des noyaux, on déduit que $E = \bigoplus_{k=1}^p N_k$.

(b) On note, pour tout k compris entre 1 et p , $M_k = \ker(u - \lambda_k Id)^{\beta_k}$ et on a :

$$M_k \subset N_k, \quad E = \bigoplus_{k=1}^p N_k = \bigoplus_{k=1}^p M_k,$$

(l'égalité $E = \bigoplus_{k=1}^p M_k$ est encore une conséquence du théorème de décomposition des noyaux), donc :

$$\begin{cases} 1 \leq \dim(M_k) \leq \dim(N_k) \\ n = \sum_{k=1}^p \dim(N_k) = \sum_{k=1}^p \dim(M_k) \end{cases}$$

dans \mathbb{N}^* et nécessairement $\dim(M_k) = \dim(N_k)$, ce qui entraîne $M_k = N_k$.

(c) Comme $\mathbb{K}[u]$ est commutatif, N_k est stable par u et $u|_{N_k}$ est un endomorphisme de N_k . Si λ est une valeur propre de $u|_{N_k}$, c'est aussi une valeur propre de u et il existe alors un indice $j \in \{1, 2, \dots, p\}$ tel que $\lambda = \lambda_j$ et un vecteur $x \in N_k - \{0\}$ tel que $(u - \lambda_j Id)(x) = 0$. On a alors $x \in N_k \cap N_j - \{0\}$ et nécessairement $j = k$ puisque $N_k \cap N_j = \{0\}$ si $j \neq k$.

(d) Soit $d_k = \dim(N_k)$, pour k compris entre 1 et p . De ce qui précède on déduit que le polynôme caractéristique de $u|_{N_k} \in \mathcal{L}(N_k)$ est $P_k(X) = (\lambda_k - X)^{d_k}$. De $E = \bigoplus_{k=1}^p N_k$, les

N_k étant stables par u , on déduit que $P_u = \prod_{k=1}^p P_k$ et $d_k = \alpha_k$.

(e) Pour tout $k \in \{1, 2, \dots, p\}$, on note :

$$v_k = (u - \lambda_k Id)|_{N_k} \in \mathcal{L}(N_k)$$

et on a $v_k^{\beta_k} = 0$ ($N_k = \ker(u - \lambda_k Id)^{\beta_k}$). Si, pour un $k \in \{1, 2, \dots, p\}$, $v_k^{\beta_k-1} = 0$, alors le polynôme $(X - \lambda_k)^{\beta_k-1} \prod_{\substack{j=1 \\ j \neq k}}^p (X - \lambda_j)^{\beta_j}$ annule u puisqu'il annule tous les $u|_{N_j}$ et on a

$E = \bigoplus_{j=1}^p N_j$, ce qui contredit le fait que $\prod_{k=1}^p (X - \lambda_k)^{\beta_k}$ est le polynôme minimal de u . On a donc $v_k^{\beta_k-1} \neq 0$ et v_k est nilpotent d'indice β_k .

2. Sur chaque sous espace vectoriel N_k , on a vu que l'endomorphisme $v_k = (u - \lambda_k Id)|_{N_k}$ est nilpotent et en notant $d_k = \lambda_k Id|_{N_k}$, on a $u|_{N_k} = d_k + v_k$ avec d_k diagonalisable, v_k nilpotent et $d_k v_k = v_k d_k$.

On définit alors les endomorphismes d et v par $d = \sum_{k=1}^p \lambda_k \pi_k$, où on a noté pour tout k compris

entre 1 et p , π_k le projecteur de E sur N_k (les π_k sont les projecteurs spectraux), et $v = u - d$. Les π_k étant des polynômes en u (question **I.2.**), il en est de même de d et de $v = u - d$.

L'endomorphisme d est diagonalisable de mêmes valeurs propres que u ($d = d_k = \lambda_k Id|_{N_k}$ sur N_k), l'endomorphisme v est nilpotent ($v = v_k$ sur N_k), d et v commutent puisqu'ils sont dans l'algèbre commutative $\mathbb{K}[u]$ et $u = d + v$.

Il reste à montrer l'unicité d'un tel couple (d, v) .

Soit (d', v') un autre couple d'endomorphismes vérifiant les mêmes conditions que (d, v) . Comme $u = d' + v'$ et d' et v' commutent, ils commutent avec u donc avec d et v qui sont des polynômes en u . On a alors $d - d' = v' - v$, avec $d - d'$ diagonalisable comme somme de deux endomorphismes diagonalisables qui commutent et $v' - v$ nilpotent comme somme de deux endomorphismes nilpotents qui commutent. Et nécessairement $d - d' = v' - v = 0$. D'où l'unicité de la décomposition.

3.

- (a) Pratiquement la décomposition de Dunford de u passe par le calcul des projecteurs spectraux π_k qui peut se faire en utilisant **I.3.** où P est un polynôme annulateur de u .

Le polynôme caractéristique de u est $P_u(X) = X(X-1)^3$ et son polynôme minimal est $\pi_u(X) = X(X-1)^2$. On a la décomposition en éléments simples :

$$\frac{1}{\pi_u(X)} = \frac{1}{X} + \left(\frac{1}{(X-1)^2} - \frac{1}{X-1} \right)$$

qui donne la décomposition de Bézout :

$$1 = (X-1)^2 + (2-X)X$$

et les projecteurs spectraux :

$$\pi_1 = (u - Id)^2, \quad \pi_2 = 2u - u^2$$

(on a $\pi_1 + \pi_2 = Id$). On obtient alors la décomposition $u = d + v$ avec $d = 0 \cdot \pi_1 + 1 \cdot \pi_2 = \pi_2$ et $v = u - d = u^2 - u$ de matrices respectives dans la base canonique de \mathbb{K}^4 :

$$D = \begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad V = A - D = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

- (b) Comme d et v commutent, on peut utiliser la formule du binôme de Newton pour écrire :

$$\forall r \geq 1, u^r = (d + v)^r = \sum_{k=0}^r C_r^k d^k \circ v^{r-k}.$$

Le calcul des puissances successives de l'endomorphisme d peut se faire dans une base de diagonalisation ou en utilisant les propriétés des projecteurs pour écrire que :

$$\forall r \geq 1, d^r = \left(\sum_{k=1}^p \lambda_k \pi_k \right)^r = \sum_{k=1}^p \lambda_k^r \pi_k$$

(puisque $\pi_k^2 = \pi_k$ et $\pi_k \circ \pi_j$ pour $k \neq j$) et le calcul des puissances successives de l'endomorphisme nilpotent v s'arrête à v^{q-1} où q est son indice de nilpotence.

Pour notre exemple, on a pour $r > 0$:

$$u^r = d^r + rd^{r-1}v$$

($v^2 = 0$) avec $d^r = \pi_2^r = \pi_2 = d$. Soit, dans la base canonique de \mathbb{K}^4 :

$$\forall r \geq 2, A^r = D(I_4 + rV) = \begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & r & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

4.

- (a) Il existe un entier j compris entre 1 et p tel que $\rho(u) = |\lambda_j|$ et en désignant par $x \in E$ un vecteur propre de u de norme 1 associé à cette valeur propre λ_j , on a pour tout entier $k \geq 1$, $u^k(x) = \lambda_j^k x$, ce qui donne :

$$\rho(u)^k = |\lambda_j|^k = \|\lambda_j^k x\| = \|u^k(x)\| \leq \|u^k\|$$

et $\rho(u) \leq \|u^k\|^{\frac{1}{k}}$.

- (b) Si u est diagonalisable, il existe alors une base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E formée de vecteurs propres de u avec $u(e_i) = \mu_i e_i$ pour tout i compris entre 1 et n , où les μ_i sont les valeurs propres de u distinctes ou confondues. On a alors, pour tout vecteur $x \in E$ et tout entier $k \geq 1$:

$$u^k(x) = u^k \left(\sum_{j=1}^n x_j e_j \right) = \sum_{j=1}^n x_j u^k(e_j) = \sum_{j=1}^n x_j \mu_j^k e_j$$

et :

$$\|u^k(x)\| \leq \sum_{j=1}^n |x_j| |\mu_j^k| \|e_j\| \leq \rho(u)^k \sum_{j=1}^n |x_j| \|e_j\|,$$

soit en posant $\beta = \max_{1 \leq i \leq n} \|e_i\|$:

$$\|u^k(x)\| \leq \beta \rho(u)^k \sum_{j=1}^n |x_j|$$

L'application $x \mapsto \|x\|_1 = \sum_{j=1}^n |x_j|$ définissant une norme sur E qui est équivalente à $x \mapsto \|x\|$ (en dimension finie toutes les normes sont équivalentes), il existe une constante $\gamma > 0$ telle $\|x\|_1 \leq \gamma \|x\|$ pour tout $x \in E$ et on a :

$$\|u^k(x)\| \leq \beta \gamma \rho(u)^k \|x\|$$

pour tout $x \in E$ et tout $k \geq 1$, ce qui entraîne $\|u^k\| \leq \beta \gamma \rho(u)^k = \alpha \rho(u)^k$ et $\|u^k\|^{\frac{1}{k}} \leq \alpha^{\frac{1}{k}} \rho(u)$.

On a donc, pour tout entier $k \geq 1$:

$$\rho(u) \leq \|u^k\|^{\frac{1}{k}} \leq \alpha^{\frac{1}{k}} \rho(u)$$

et avec $\lim_{k \rightarrow +\infty} \alpha^{\frac{1}{k}} = 1$ pour $\alpha > 0$, on déduit que $\lim_{k \rightarrow +\infty} \|u^k\|^{\frac{1}{k}} = \rho(u)$.

- (c) On a la décomposition de Dunford $u = d + v$ avec d diagonalisable de mêmes valeurs propres que u , v nilpotente et $dv = vd$. Pour tout entier $j \geq n$, on a $v^j = 0$ (le polynôme minimal de v est X^p avec p compris entre 1 et n) et pour $k \geq n$:

$$u^k = (d + v)^k = \sum_{j=0}^k C_k^j d^{k-j} v^j = \sum_{j=0}^n C_k^j d^{k-j} v^j = d^{k-n} \sum_{j=0}^n C_k^j d^{n-j} v^j.$$

ce qui entraîne :

$$\|u^k\| \leq \|d^{k-n}\| \sum_{j=0}^n C_k^j \|d\|^{n-j} \|v\|^j.$$

(la norme choisie sur $\mathcal{L}(E)$ est sous-multiplicative).

Pour tout j compris entre 0 et n , on a :

$$C_k^j = \frac{k!}{j!(k-j)!} = \frac{k(k-1)\cdots(k-j+1)}{j!} \leq \frac{k^j}{j!} \leq k^n,$$

ce qui donne :

$$\|u^k\| \leq \|d^{k-n}\| k^n \sum_{j=0}^n \|d\|^{n-j} \|v\|^j = \beta k^n \|d^{k-n}\|$$

avec $\beta = \sum_{j=0}^n \|d\|^{n-j} \|v\|^j > 0$ ($u \neq 0$).

On a donc :

$$\forall k \geq n, \rho(u) \leq \|u^k\|^{\frac{1}{k}} \leq \beta^{\frac{1}{k}} k^{\frac{n}{k}} \|d^{k-n}\|^{\frac{1}{k}},$$

avec $\lim_{k \rightarrow +\infty} \beta^{\frac{1}{k}} k^{\frac{n}{k}} \lim_{k \rightarrow +\infty} \exp\left(\frac{\ln(\beta)}{k} + n \frac{\ln(k)}{k}\right) = 1$ et :

$$\lim_{k \rightarrow +\infty} \|d^{k-n}\|^{\frac{1}{k}} = \lim_{k \rightarrow +\infty} \left(\|d^{k-n}\|^{\frac{1}{k-n}} \right)^{\frac{k-n}{k}} = \rho(d)$$

puisque $\lim_{k \rightarrow +\infty} \left(\|d^{k-n}\|^{\frac{1}{k-n}} \right) = \rho(d)$ (d est diagonalisable) et :

$$\lim_{k \rightarrow +\infty} t^{\frac{k-n}{k}} = \lim_{k \rightarrow +\infty} \exp\left(\left(1 - \frac{n}{k}\right) \ln(t)\right) = t$$

pour tout $t > 0$ (pour $t = 0$, c'est évident). Enfin comme d et u ont les mêmes valeurs propres, on a $\rho(d) = \rho(u)$ et $\lim_{k \rightarrow +\infty} \left(\|u^k\|^{\frac{1}{k}} \right) = \rho(u)$.

- (d) Se déduit du fait que toutes les normes sur $\mathcal{L}(E)$ sont équivalentes (cet espace est de dimension finie).

5. Si $\rho(u) < 1$, on a alors $\lim_{k \rightarrow +\infty} \left(\|u^k\|^{\frac{1}{k}} \right) = \rho(u) < 1$ et le critère de Cauchy pour les séries réelles nous dit que la série $\sum \|u^k\|$ est convergente, ce qui signifie que la série $\sum u^k$ est normalement convergente dans $\mathcal{L}(E)$, donc convergente puisque ce espace est complet. Réciproquement si la série $\sum u^k$ converge, son terme général tend vers 0 et avec $\rho(u)^k \leq \|u^k\|$ pour une norme sur $\mathcal{L}(E)$ qui est sous-multiplicative, on déduit que $\lim_{k \rightarrow +\infty} \rho(u)^k = 0$ et nécessairement $\rho(u) < 1$.

On peut aussi dire que si $\rho(u) > 1$, on a alors $\lim_{k \rightarrow +\infty} \left(\|u^k\|^{\frac{1}{k}} \right) = \rho(u) > 1$, donc $\|u^k\|^{\frac{1}{k}} \geq$

$\rho(u) - \varepsilon$ pour k assez grand où $\varepsilon > 0$ est choisi assez petit pour que $\rho(u) - \varepsilon > 1$, ce qui entraîne :

$$\|u^k\| \geq (\rho(u) - \varepsilon)^k \xrightarrow{k \rightarrow +\infty} +\infty$$

et la série $\sum u^k$ diverge.

Pour $\rho(u) < 1$, on a pour tout $k \geq 1$:

$$(Id - u) \sum_{j=0}^k u^j = Id - u^{k+1}$$

et avec la continuité de l'application $w \mapsto (Id - u) \circ w$ sur $\mathcal{L}(E)$, on déduit que :

$$Id = \lim_{k \rightarrow +\infty} (Id - u^{k+1}) = (Id - u) \lim_{k \rightarrow +\infty} \left(\sum_{j=0}^k u^j \right) = (Id - u) \sum_{k=0}^{+\infty} u^k$$

ce qui signifie que $Id - u$ est inversible d'inverse $\sum_{k=0}^{+\infty} u^k$.

– IV – Exponentielle d'un endomorphisme (pour $\mathbb{K} = \mathbb{C}$)

1. Toutes les normes sur $\mathcal{L}(E)$ étant équivalentes, on peut supposer que la norme choisie sur $\mathcal{L}(E)$ est déduite d'une norme sur E , donc sous-multiplicative.

Pour tout entier $k \geq 0$, on a :

$$\left\| \frac{v^k}{k!} \right\| \leq \frac{\|v\|^k}{k!}$$

avec $\sum_{k=0}^{+\infty} \frac{\|v\|^k}{k!} = e^{\|v\|} < +\infty$ et en conséquence la série $\sum \frac{v^k}{k!}$ est normalement convergence dans $\mathcal{L}(E)$, donc convergente puisque cet espace est complet (il est de dimension finie). De plus, on a :

$$\|e^v\| = \left\| \sum_{k=0}^{+\infty} \frac{v^k}{k!} \right\| \leq \sum_{k=0}^{+\infty} \frac{\|v\|^k}{k!} = e^{\|v\|}.$$

Si $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une base de E et A la matrice de v dans cette base, on a alors du fait de la continuité du produit matriciel, pour tout entier i compris entre 1 et n :

$$e^v \cdot e_i = \lim_{k \rightarrow +\infty} \sum_{j=0}^k \frac{1}{k!} v^j \cdot e_i$$

ce qui se traduit en disant que la matrice de e^v dans \mathcal{B} est $\lim_{k \rightarrow +\infty} \sum_{j=0}^k \frac{1}{k!} A^j = e^A$.

2. Sur \mathbb{C} l'endomorphisme v est trigonalisable, ce qui signifie qu'il existe une base de E dans laquelle la matrice A de v est triangulaire supérieure, les termes diagonaux de cette matrice étant les valeurs propres μ_1, \dots, μ_n de v . Comme, pour tout entier $k \geq 0$, la matrice A^k est aussi triangulaire supérieure de termes diagonaux μ_1^k, \dots, μ_n^k , on déduit que e^A est triangulaire supérieure de termes diagonaux $e^{\mu_1}, \dots, e^{\mu_n}$ et :

$$\det(e^v) = \det(e^A) = \prod_{j=1}^n e^{\mu_j} = \exp\left(\sum_{j=1}^n \mu_j\right) = e^{\text{Tr}(A)} = e^{\text{Tr}(v)} \neq 0$$

et e^v est inversible.

3. Pour tout réel θ , on a :

$$A_\theta^2 = \begin{pmatrix} -\theta^2 & 0 \\ 0 & -\theta^2 \end{pmatrix} = -\theta^2 I_2$$

et en conséquence, pour tout entier $k \geq 0$, on a :

$$A_\theta^{2k} = \begin{pmatrix} (-1)^k \theta^{2k} & 0 \\ 0 & (-1)^k \theta^{2k} \end{pmatrix} = (-1)^k \theta^{2k} I_n$$

et :

$$A_\theta^{2k+1} = A_\theta^{2k} A_\theta = (-1)^k \theta^{2k} A_\theta = \begin{pmatrix} 0 & -(-1)^k \theta^{2k+1} \\ (-1)^k \theta^{2k+1} & 0 \end{pmatrix}$$

ce qui donne :

$$\begin{aligned} e^{A_\theta} &= \sum_{k=0}^{+\infty} \frac{A_\theta^{2k}}{(2k)!} + \sum_{k=0}^{+\infty} \frac{A_\theta^{2k+1}}{(2k+1)!} \\ &= \begin{pmatrix} \cos(\theta) & 0 \\ 0 & \cos(\theta) \end{pmatrix} + \begin{pmatrix} 0 & -\sin(\theta) \\ \sin(\theta) & 0 \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \end{aligned}$$

soit la matrice de la rotation d'angle θ (la série $\sum \frac{A_\theta^k}{k!}$ étant normalement convergence est commutativement convergente).

En fait A_θ est la représentation matricielle du nombre complexe $i\theta$ et e^{A_θ} est la représentation de $e^{i\theta}$ (la multiplication par $e^{i\theta}$ est bien la rotation d'angle θ).

4. Si $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une base de E formée de vecteurs propres de v , avec $v(e_i) = \mu_i e_i$ pour tout i compris entre 1 et n , en utilisant la continuité des applications $\varphi_i : v \mapsto v(e_i)$ (φ_i est linéaire et $\|\varphi_i(v)\| = \|v(e_i)\| \leq \|v\| \|e_i\|$ pour tout $v \in \mathcal{L}(E)$), on déduit que :

$$\begin{aligned} e^v e_i &= \left(\lim_{k \rightarrow +\infty} \sum_{j=0}^k \frac{1}{j!} v^j \right) (e_i) = \varphi_i \left(\lim_{k \rightarrow +\infty} \sum_{j=0}^k \frac{1}{j!} v^j \right) = \lim_{k \rightarrow +\infty} \sum_{j=0}^k \frac{1}{j!} \varphi_i(v^j) \\ &= \lim_{k \rightarrow +\infty} \sum_{j=0}^k \frac{1}{j!} v^j(e_i) = \lim_{k \rightarrow +\infty} \sum_{j=0}^k \frac{1}{j!} \mu_i^j e_i = \left(\lim_{k \rightarrow +\infty} \sum_{j=0}^k \frac{1}{j!} \mu_i^j \right) e_i = e^{\mu_i} e_i \end{aligned}$$

ce qui signifie que e^v est diagonalisable de valeurs propres e^{μ_i} , les vecteurs propres associées étant ceux de v .

On peut aussi dire que la matrice de v dans \mathcal{B} est une matrice diagonale A de termes diagonaux μ_1, \dots, μ_n et celle de e^v dans cette même base est la matrice diagonale e^A de termes diagonaux $e^{\mu_1}, \dots, e^{\mu_n}$, donc e^v est diagonalisable.

5. Pour tout segment réel $[a, b]$, tout entier $k \geq 1$ et tout $t \in [a, b]$, on a :

$$\left\| \frac{t^{k-1} v^k}{(k-1)!} \right\| \leq \alpha^{k-1} \frac{\|v\|^k}{(k-1)!}$$

où $\alpha = \max(|a|, |b|)$. Il en résulte que la série dérivée $\sum \frac{t^{k-1} v^k}{(k-1)!}$ de la série simplement

convergente $\sum \frac{t^k v^k}{k!}$ est uniformément convergente sur $[a, b]$. Comme chaque fonction $t \mapsto \frac{t^k v^k}{k!}$

est de classe \mathcal{C}^1 sur \mathbb{R} , on en déduit que la fonction φ est de classe \mathcal{C}^1 sur tout segment de \mathbb{R} , donc sur \mathbb{R} , et sa dérivée est donnée par :

$$\varphi'(t) = \sum_{k=1}^{+\infty} \frac{t^{k-1} v^k}{(k-1)!} = v \sum_{k=0}^{+\infty} \frac{t^k v^k}{k!} = v e^{tv}$$

Comme v et e^{tv} commutent, on a aussi $\varphi'(t) = e^{tv} v$.

6. La fonction $\psi : t \mapsto e^{tv} e^{-tv}$ est dérivable sur \mathbb{R} de dérivée :

$$\psi'(t) = v e^{tv} e^{-tv} + e^{tv} (-v) e^{-tv} = (v - v) e^{tv} e^{-tv} = 0$$

ce qui entraîne que ψ est constante, soit $\psi(t) = \psi(0) = Id$ pour tout réel t , ce qui signifie que e^{tv} est inversible d'inverse e^{-tv} .

7. Pour la condition suffisante, on peut procéder comme suit.

Supposons que v et w commutent. La fonction $\psi : t \mapsto e^{t(v+w)} e^{-tv} e^{-tw}$ est dérivable sur \mathbb{R} de dérivée :

$$\begin{aligned} \psi'(t) &= (v+w) e^{t(v+w)} e^{-tv} e^{-tw} + e^{t(v+w)} (-v) e^{-tv} e^{-tw} + e^{t(v+w)} e^{-tv} (-w) e^{-tw} \\ &= (v+w - v - w) e^{t(v+w)} e^{-tv} e^{-tw} = 0 \end{aligned}$$

puisque tous les endomorphismes considérés commutent, ce qui entraîne que ψ est constante, soit $\psi(t) = \psi(0) = Id$ pour tout réel t . Comme e^{-tv} est l'inverse de e^{tv} pour tout endomorphisme v , on en déduit que $e^{t(v+w)} = e^{tv} e^{tw}$ et $t = 1$ donne le résultat attendu.

L'unicité du développement en série entière au voisinage de 0 d'une fonction développable en série entière de $] -r, r[$ dans l'algèbre de Banach $\mathcal{L}(E)$ (identifiée à $\mathcal{M}_n(\mathbb{C})$), nous donne une démonstration de la condition nécessaire. Pour v, w fixés dans $\mathcal{L}(E)$ et tout réel t on a :

$$e^{t(v+w)} = \sum_{k=0}^{+\infty} \frac{t^k (v+w)^k}{k!}$$

et :

$$e^{tv} e^{tw} = \sum_{k=0}^{+\infty} \frac{t^k v^k}{k!} \sum_{k=0}^{+\infty} \frac{t^k w^k}{k!} = Id + t(v+w) + \frac{t^2}{2} (v^2 + 2vw + w^2) + \sum_{k=3}^{+\infty} t^k u_k$$

et l'égalité $e^{t(v+w)} = e^{tv} e^{tw}$ est réalisée si et seulement si tous les coefficients de ces deux développements en séries entières coïncident, ce qui entraîne en particulier $(v+w)^2 = v^2 + 2vw + w^2$ ce qui équivaut à $vw = wv$.

8. Comme d et v commutent, on a $e^u = e^d e^v$ avec :

$$e^v = \sum_{k=0}^{q-1} \frac{1}{k!} v^k$$

puisque $v^k = 0$ pour $k \geq q$.

9. On a :

$$\begin{aligned} e^u &= e^d e^v = e^d \sum_{k=0}^{q-1} \frac{1}{k!} v^k = e^d \left(Id + v \sum_{k=1}^{q-1} \frac{1}{k!} v^{k-1} \right) \\ &= e^d + v e^d \sum_{k=1}^{q-1} \frac{1}{k!} v^{k-1} = e^d + v \cdot w \end{aligned}$$

(v et e^d commutent puisque v et d commutent).

Comme v est nilpotent d'indice q et commute à w , on a $(v \cdot w)^q = v^q w^q = 0$, c'est-à-dire que $v \cdot w$ est nilpotent.

L'endomorphisme e^d est diagonalisable comme d . On a donc obtenu ainsi la décomposition de Dunford de e^v puisque cette décomposition est unique.

La partie nilpotente de cette décomposition s'écrit aussi :

$$v \cdot w = e^d \sum_{k=1}^{q-1} \frac{1}{k!} v^k = e^d (e^v - Id).$$

10. En désignant par $u = d + v$ la décomposition de Dunford de u , on déduit de l'unicité de cette décomposition que u est diagonalisable si, et seulement si, $v = 0$.

Il en résulte que si u est diagonalisable alors la partie nilpotente de la décomposition de Dunford de e^u est $e^d (e^v - Id) = 0$ et e^u est diagonalisable.

Réciproquement dire que e^u est diagonalisable équivaut à dire que $e^d (e^v - Id) = 0$, soit à $e^v = Id$ puisque e^d est inversible. On a donc $\sum_{k=0}^q \frac{1}{k!} v^k = Id$, où $q \geq 1$ est l'indice de nilpotence

de v , soit $\sum_{k=1}^q \frac{1}{k!} v^k = 0$, c'est-à-dire que $P(X) = \sum_{k=1}^q \frac{1}{k!} X^k$ est un polynôme annulateur de v

et X^q qui est le polynôme minimal de v va diviser P , ce qui impose $q = 1$ (on a $\frac{1}{q!} = 1$ en identifiant les termes de degré q), soit $v = 0$ et u est diagonalisable.

Pour montrer que $q = 1$, on peut aussi écrire que si $q \geq 2$, alors $v^{q-1} = v^{q-2} \sum_{k=1}^q \frac{1}{k!} v^k = 0$, ce qui est incompatible avec le fait que q est l'indice de nilpotence de v . On a donc $q = 1$.

11. Pour $E = \mathbb{C}$, on a $\mathcal{L}(E) = \mathbb{C}$ et les solutions de $e^z = 1$ dans \mathbb{C} sont les $e^{2in\pi}$ où n décrit \mathbb{Z} . De manière générale soit $u \in \mathcal{L}(E)$ telle que $e^u = Id$. La décomposition de Dunford $u = d + v$ de u donne celle de e^u :

$$e^u = e^d + e^d (e^v - Id)$$

et avec l'unicité de cette décomposition, on déduit que l'équation $e^u = Id$ équivaut à $e^d = Id$ et $e^v = Id$. On a vu que $e^v = Id$ avec v nilpotent équivaut à $v = 0$. De plus e^d est diagonalisable de valeurs propres e^{μ_k} où les μ_k , pour k compris entre 1 et n , sont les valeurs propres de d , donc celles de u et $e^d = Id$ impose $e^{\mu_k} = 1$, soit $\mu_k \in 2i\pi\mathbb{Z}$ pour tout k compris entre 1 et n . En définitive, u est diagonalisable de valeurs propres dans $2i\pi\mathbb{Z}$. La réciproque étant évidente.

– V – Endomorphismes semi-simples

1. Supposons u semi-simple. On désigne par $\lambda_1, \dots, \lambda_p$ les valeurs propres deux à deux distinctes de u dans \mathbb{K} algébriquement clos et on note $F = \bigoplus_{k=1}^p \ker(u - \lambda_k Id)$. Il s'agit alors de montrer que $F = E$. Comme les sous-espaces propres $\ker(u - \lambda_k Id)$ sont tous stables par u , il en est de même de F et ce sous-espace vectoriel admet un supplémentaire G dans E qui est stable par u . Si $G \neq \{0\}$, la restriction v de u à G est un endomorphisme de G qui admet des valeurs propres puisque \mathbb{K} est algébriquement clos. Mais si λ est une telle valeur propre et $x \in G \setminus \{0\}$ un vecteur propre associé, il existe un entier k compris entre 1 et p tel que $\lambda = \lambda_k$ et $x \in \ker(u - \lambda_k Id)$, ce qui entraîne $x \in F \cap G$ avec $x \neq 0$, en contradiction avec $F \cap G = \{0\}$. On a donc $G = \{0\}$ et $E = F$, ce qui signifie que u est diagonalisable.

Supposons u diagonalisable. On a donc $E = \bigoplus_{k=1}^p \ker(u - \lambda_k Id)$ avec les notations qui précèdent.

Si F est un sous-espace vectoriel de E stable par u , la restriction v de u à F est un endomorphisme de F diagonalisable. On a alors $F = \bigoplus_{k=1}^p \ker(v - \lambda_k Id)$, certains des $\ker(v - \lambda_k Id) \subset \ker(u - \lambda_k Id)$ pouvant être réduits à $\{0\}$ (le polynôme minimal de v divise π_u , donc les valeurs propres de v sont dans $\{\lambda_1, \dots, \lambda_p\}$). En désignant, pour tout k compris entre 1 et p , par G_k un supplémentaire de $\ker(v - \lambda_k Id)$ dans $\ker(u - \lambda_k Id)$, G_k est stable par u (puisque $u(x) = \lambda_k x$ pour tout $x \in G_k \subset \ker(u - \lambda_k Id)$), donc aussi $G = \bigoplus_{k=1}^p G_k$ et avec :

$$E = \bigoplus_{k=1}^p \ker(u - \lambda_k Id) = \bigoplus_{k=1}^p \ker(v - \lambda_k Id) \oplus G_k = F \oplus G$$

En définitive, tout sous-espace vectoriel de E stable par u admet un supplémentaire dans E stable par u , ce qui signifie que u est semi-simple.

On peut aussi utiliser le théorème de la base incomplète pour les espaces vectoriels de dimension finie.

Rappelons ce théorème : Si \mathcal{G} est une famille génératrice de E et \mathcal{L} une famille libre contenue dans \mathcal{G} , on peut alors compléter \mathcal{L} en une base de E avec des éléments de \mathcal{G} . On déduit de ce théorème le corollaire suivant : Si \mathcal{G} est une famille génératrice de E et \mathcal{L} une famille libre de E , on peut alors compléter \mathcal{L} en une base de E avec des éléments de \mathcal{G} (il suffit de remarquer que $\mathcal{G}' = \mathcal{G} \cup \mathcal{L}$ est génératrice et contient \mathcal{L}).

En supposant u diagonalisable, il existe une base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E formée de vecteurs propres de u et pour tout sous-espace vectoriel strict F de E stable par u (pour $F = E$, il n'y a rien à montrer), une base $(f_i)_{1 \leq i \leq p}$ de F peut se compléter en une base de E avec des éléments de \mathcal{B} et en notant $(f_1, \dots, f_p, e_{i_{p+1}}, \dots, e_{i_n})$ une telle base, l'espace vectoriel G engendré par $(e_{i_{p+1}}, \dots, e_{i_n})$ est un supplémentaire de F stable par u .

On peut remarquer que l'implication u diagonalisable entraîne u semi-simple est valable pour tout corps commutatif \mathbb{K} (non nécessairement algébriquement clos).

2. Il est équivalent de montrer que s'il existe deux polynômes non constants P et Q tels que $\pi_u = P^2Q$, alors u ne peut être semi-simple. Pour ce faire on considère le sous-espace vectoriel de E , $F = \ker(P(u))$. Pour tout $x \in F$, on a $P(u)(u(x)) = u(P(u)(x)) = u(0) = 0$ ($\mathbb{K}[u]$ est une algèbre commutative), donc F est stable par u et il admet un supplémentaire G dans E qui est stable par u si u est semi-simple.

Comme $\mathbb{K}[u]$ est une algèbre commutative, on a $(PQ)(u)(x) = Q(u)(P(u)(x)) = 0$ pour tout $x \in F$ et $P(u)((PQ)(u)(x)) = \pi_u(u)(x) = 0$ pour tout $x \in G$, donc $(PQ)(u)(x) \in F$ pour tout $x \in G$ et comme $(PQ)(u)(x)$ est aussi dans G puisque cet espace est stable par u , on a aussi $(PQ)(u)(x) \in G$, ce qui donne $(PQ)(u)(x) \in F \cap G = \{0\}$. L'endomorphisme $(PQ)(u)$ est donc nul sur E puisqu'il est nul sur F et G , ce qui contredit le caractère minimal de π_u .

En définitive π_u est sans facteurs carrés dans $\mathbb{K}[x]$ si u est semi-simple.

3. On suppose que π_u est irréductible dans $\mathbb{K}[x]$. On sait alors que $\mathbb{L} = \frac{\mathbb{K}[x]}{(\pi_u)}$ est un corps (pour $P \in \mathbb{K}[x]$, la classe de P modulo π_u est $\overline{P} = \{Q \in \mathbb{K}[x] \mid \pi_u \text{ divise } P - Q\}$, on vérifie facilement que \mathbb{L} muni des lois définies par $\overline{P} + \overline{Q} = \overline{P+Q}$ et $\overline{PQ} = \overline{P}\overline{Q}$ est un anneau commutatif unitaire et dire que $\overline{P} \neq \overline{0}$ équivaut à dire que P n'est pas divisible par π_u , il est donc premier avec π_u puisque π_u est irréductible et le théorème de Bézout nous dit qu'il existe deux polynômes U et V tels que $UP + V\pi_u = 1$, ce qui entraîne $\overline{UP} = \overline{1}$ et \overline{P} est inversible d'inverse \overline{U}).

- (a) L'espace vectoriel E peut alors être muni d'une structure de \mathbb{L} -espace vectoriel avec la multiplication externe définie par :

$$\overline{P} \cdot x = P(u)(x)$$

pour tout $\bar{P} \in \mathbb{L}$ et tout $x \in u$. Vérifions que cette multiplication est bien définie, c'est-à-dire que $\bar{P} \cdot x$ ne dépend du choix d'un représentant de la classe de P . Si $P \equiv Q$ modulo π_u , on a $P - Q = R\pi_u$ et $P(u) - Q(u) = R(u) \circ \pi_u(u) = 0$, donc $P(u)(x) = Q(u)(x)$ pour tout $x \in E$.

On vérifie ensuite facilement qu'avec cette multiplication externe E est un \mathbb{L} -espace vectoriel. On sait déjà que $(E, +)$ est un groupe commutatif et pour \bar{P}, \bar{Q} dans \mathbb{L} , x, y dans E , on a :

$$\left\{ \begin{array}{l} \bar{P} \cdot (x + y) = P(u)(x + y) = P(u)(x) + P(u)(y) = \bar{P} \cdot x + \bar{P} \cdot y \\ (\bar{P} + \bar{Q}) \cdot x = (P + Q)(u)(x) = P(u)(x) + Q(u)(x) = \bar{P} \cdot x + \bar{Q} \cdot x \\ (\bar{P}\bar{Q}) \cdot x = (PQ)(u)(x) = P(u) \circ Q(u)(x) = \bar{P} \cdot (Q(u)(x)) = \bar{P}(\bar{Q} \cdot x) \\ \bar{1} \cdot x = Id(x) = x \end{array} \right.$$

(b) Si F est un \mathbb{K} -sous-espace vectoriel de E stable par u , alors F est un \mathbb{L} -sous-espace vectoriel de E . En effet pour x, y dans F on a déjà $x + y \in F$ et pour tout $\bar{P} \in \mathbb{L}$, on a $\bar{P} \cdot x = P(u)(x) \in F$ puisque F est stable par u .

Réciproquement, si F est un \mathbb{L} -sous-espace vectoriel de E , on a alors $\bar{P} \cdot x \in F$ pour tout $x \in F$ et $\bar{P} \in \mathbb{L}$, ce qui donne pour $\bar{P} = \bar{X}$, $\bar{X} \cdot x = u(x) \in F$ pour tout $x \in F$, ce qui signifie que F est stable par u .

(c) Comme F est un \mathbb{L} -sous-espace vectoriel de E , il admet un \mathbb{L} -supplémentaire G dans E et ce supplémentaire est également un \mathbb{K} -supplémentaire de F dans E qui est stable par u . En définitive, u est semi-simple.

4. Supposons π_u sans facteurs carrés, soit $\pi_u = \prod_{k=1}^p P_k$, les P_k étant irréductibles deux à deux distincts dans $\mathbb{K}[x]$. Le théorème de décomposition des noyaux nous dit alors que $E = \ker(\pi_u(u)) = \bigoplus_{k=1}^p \ker(P_k(u))$. Chacun des sous-espaces $\ker(P_k(u))$ est stable par u (puisque u et $P_k(u)$ commutent) et le polynôme minimal de la restriction v_k de u à $\ker(P_k(u))$ est égal à P_k et comme ce polynôme est irréductible, v_k est semi-simple. Si F est un sous-espace vectoriel de E stable par u , on a alors $F = \bigoplus_{k=1}^p \ker(P_k(u)) \cap F$. En effet, la restriction v de u à F étant annulée par $\pi_u = \prod_{k=1}^p P_k$, le théorème de décomposition des noyaux nous dit que $F = \bigoplus_{k=1}^p \ker(P_k(v)) = \bigoplus_{k=1}^p \ker(P_k(u)) \cap F$. En désignant, pour tout k compris entre 1 et p , par G_k un supplémentaire de $\ker(P_k(v))$ dans $\ker(P_k(u))$, G_k est stable par u puisque v_k est semi-simple, donc aussi $G = \bigoplus_{k=1}^p G_k$ et avec :

$$E = \bigoplus_{k=1}^p \ker(P_k(u)) = \bigoplus_{k=1}^p (\ker(P_k(u)) \cap F) \oplus G_k = F \oplus G$$

on déduit que F admet un supplémentaire stable par u .

L'endomorphisme u donc est semi-simple.

Dans le cas où le corps \mathbb{K} est algébriquement clos, les polynômes irréductibles sont de degré 1 et dire que π_u est sans facteurs carrés équivaut à dire qu'il est scindé à racines simples, ce qui équivaut à dire que u est diagonalisable, soit semi-simple.

5. Si u est semi-simple et F est un sous-espace vectoriel de E stable par u , alors la restriction v de u à F est un endomorphisme de F dont le polynôme minimal π_v divise celui de u , ce polynôme π_v est donc sans facteurs carrés comme π_u et v est semi-simple.

6. Le polynôme minimal d'un endomorphisme nilpotent v est X^q avec $q \geq 1$ et ce endomorphisme est semi-simple si, et seulement si, $q = 1$, ce qui revient à dire que v est nul.
7. Pour $\mathbb{K} = \mathbb{C}$, le résultat annoncé est le théorème de Dunford classique puisque diagonalisable et semi-simple sont équivalents dans ce cas.

On suppose que $\mathbb{K} = \mathbb{R}$. On se donne une base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E et on désigne par $A \in \mathcal{M}_n(\mathbb{R})$ la matrice de u dans cette base. Cette matrice A est la matrice dans la base canonique d'un endomorphisme $\tilde{u} \in \mathcal{L}(\mathbb{C}^n)$ et la décomposition de Dunford $\tilde{u} = \tilde{d} + \tilde{v}$ dans $\mathcal{L}(\mathbb{C}^n)$ nous donne la décomposition $A = D + V$ dans $\mathcal{M}_n(\mathbb{C})$ avec D diagonalisable, V nilpotente, $DV = VD$, les matrices D et V étant des polynômes en A . Avec $A = \overline{A} = \overline{D} + \overline{V}$ et l'unicité de la décomposition, on déduit que $D = \overline{D}$ et $V = \overline{V}$, c'est-à-dire que D et V sont réelles. L'égalité $A = D + V$ dans $\mathcal{M}_n(\mathbb{R})$ se traduit alors par $u = d + v$ avec v nilpotent. Le polynôme minimal de d (ou D) sur \mathbb{R} étant égal à son polynôme minimal sur \mathbb{C} , on déduit que π_d est scindé à racine simple dans $\mathbb{C}[X]$, donc sans facteurs carrés dans $\mathbb{R}[X]$, ce qui revient à dire que D est semi-simple.