

Réduction des endomorphismes et des matrices 2

- 1. Polynômes d'un endomorphisme, d'une matrice carrée 1
 - 1.1. Définition d'un polynôme d'endomorphisme, d'un polynôme de matrice 1
 - 1.2. Les morphismes de \mathbf{K} -algèbres $P \mapsto P(u)$ de $\mathbf{K}[X]$ dans $\mathcal{L}(E)$, $P \mapsto P(M)$ de $\mathbf{K}[X]$ dans $\mathcal{M}_n(\mathbf{K})$ 2
 - 1.3. Deux polynômes d'un même endomorphisme, d'une même matrice, commutent 3
 - 1.4. \mathbf{K} -algèbre engendrée par un endomorphisme, par une matrice 4
 - 1.5. Idéal annulateur d'un endomorphisme, d'une matrice 5
 - 1.6. Polynôme minimal d'un endomorphisme d'un espace de dimension finie, d'une matrice 6
 - 1.7. Valeurs propres et polynômes annulateurs d'un endomorphisme, d'une matrice 7
 - 1.8. Les racines du polynôme minimal sont les valeurs propres pour un endomorphisme, pour une matrice 8
- 2. Lemme des noyaux 8
- 3. Endomorphismes cycliques et matrices compagnons (HP) 12
 - 3.1. Matrices compagnons 12
 - 3.2. Endomorphismes cycliques 13
- 4. Théorème de Cayley-Hamilton 14
- 5. Polynômes annulateurs et réduction 16
 - 5.1. Caractérisations algébriques de la diagonalisabilité 16
 - 5.2. Polynôme minimal et diagonalisabilité d'un endomorphisme induit 17
 - 5.3. Codiagonalisation (HP) 17
 - 5.4. Caractérisations algébriques de la trigonalisabilité 17
 - 5.5. Cotrigonalisation (HP) 18
- 6. Sous-espaces caractéristiques d'un endomorphisme à polynôme caractéristique scindé 19
 - 6.1. Décomposition de l'espace en somme directe de sous-espaces caractéristiques, si χ_u est scindé sur \mathbf{K} ... 19
 - 6.2. De la classe de similitude d'une matrice à polynôme caractéristique scindé sur \mathbf{K} 19

Notation. — La lettre \mathbf{K} désigne le corps \mathbf{R} ou \mathbf{C} .

1. Polynômes d'un endomorphisme, d'une matrice carrée

Notation. — Dans cette partie, E est un \mathbf{K} -espace vectoriel et n un entier naturel non nul.

1.1. Définition d'un polynôme d'endomorphisme, d'un polynôme de matrice

Définition 1. — Soient $P \in \mathbf{K}[X]$, $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbf{K})$.

L'endomorphisme de E :

$$P(u) := \sum_{k=0}^{+\infty} [P]_k u^k$$

est appelé polynôme de l'endomorphisme u .

La matrice :

$$P(M) := \sum_{k=0}^{+\infty} [P]_k M^k$$

est appelée polynôme de matrices en M .

Exemple 2. — Soient $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbf{K})$. Si $P = X^3 - 2X^2 + 7X + 4$, alors :

$$P(u) = u^3 - 2u^2 + 7u + 4 \operatorname{id}_E \quad \text{et} \quad P(M) = M^3 - 2M^2 + 7M + 4I_n.$$

Remarque 3. — Supposons E de dimension finie $n \geq 1$ et considérons une base \mathcal{B} de E . Comme :

$$\operatorname{Mat}_{\mathcal{B}}(\cdot) \left| \begin{array}{l} (\mathcal{L}(E), +, \circ, \cdot) \longrightarrow (\mathcal{M}_n(\mathbf{K}), +, \circ, \cdot) \\ v \longmapsto \operatorname{Mat}_{\mathcal{B}}(v) \end{array} \right.$$

est un morphisme de \mathbf{K} -algèbres, pour tout $(P, u) \in \mathbf{K}[X] \times \mathcal{L}(E)$:

$$\text{Mat}_{\mathcal{B}}(P(u)) = \text{Mat}_{\mathcal{B}}\left(\sum_{k=0}^{+\infty} [P]_k u^k\right) = \sum_{k=0}^{+\infty} [P]_k \text{Mat}_{\mathcal{B}}(u)^k = P(\text{Mat}_{\mathcal{B}}(u)) .$$

- Si $P \in \mathbf{K}[X]$, $u \in \mathcal{L}(E)$ et $x \in E$ alors

$P(u)(x)$ est l'image du vecteur x par l'endomorphisme $P(u)$ de E

et est donc bien défini. En revanche

$P(u(x))$ n'a aucun sens

puisqu'on ne peut considérer les puissances du vecteur $u(x)$ de E .

- Si $P \in \mathbf{K}[X]$, $M \in \mathcal{M}_n(\mathbf{K})$ et $X \in \mathcal{M}_{n,1}(\mathbf{K})$ alors

$P(M)X$ est le produit du vecteur X par la matrice $P(M)$

et est donc bien défini. En revanche

$P(MX)$ n'a aucun sens

puisqu'on ne peut considérer les puissances du vecteur colonne MX .



1.2. Les morphismes de \mathbf{K} -algèbres $P \mapsto P(u)$ de $\mathbf{K}[X]$ dans $\mathcal{L}(E)$, $P \mapsto P(M)$ de $\mathbf{K}[X]$ dans $\mathcal{M}_n(\mathbf{K})$

Théorème 4. — Soient $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbf{K})$. Les applications :

$$\varphi \left| \begin{array}{l} (\mathbf{K}[X], +, \times, \cdot) \longrightarrow (\mathcal{L}(E), +, \circ, \cdot) \\ P \longmapsto P(u) := \sum_{k=0}^{+\infty} [P]_k u^k \end{array} \right. \quad \text{et} \quad \psi \left| \begin{array}{l} (\mathbf{K}[X], +, \times, \cdot) \longrightarrow (\mathcal{M}_n(\mathbf{K}), +, \times, \cdot) \\ P \longmapsto P(M) := \sum_{k=0}^{+\infty} [P]_k M^k \end{array} \right.$$

sont des morphismes de \mathbf{K} -algèbres.

Démonstration. On ne considère que l'application φ .

N.B. | Il nous faut connaître les coefficients du polynôme $P \in \mathbf{K}[X]$, pour être en mesure d'explicitier l'endomorphisme $P(u)$ de E , cf. définition 1.

(a) L'application φ est \mathbf{K} -linéaire. — Soient $(\lambda, \mu) \in \mathbf{K}^2$ et $(P, Q) \in \mathbf{K}[X]^2$. Posons $P = \sum_{i=0}^{+\infty} a_i X^i$ et $Q = \sum_{i=0}^{+\infty} b_i X^i$, où $(a_i)_{i \in \mathbf{N}}$ et $(b_i)_{i \in \mathbf{N}}$ sont des familles de scalaires presque nulles.

$$\begin{aligned} \varphi(\lambda P + \mu Q) &= \sum_{i=0}^{+\infty} (\lambda a_i + \mu b_i) u^i \quad [\text{le coefficient de degré } i \text{ de } \lambda P + \mu Q \text{ est } \lambda a_i + \mu b_i] \\ &= \sum_{i=0}^{+\infty} (\lambda a_i u^i + \mu b_i u^i) \\ &= \lambda \left(\sum_{i=0}^{+\infty} a_i u^i \right) + \mu \left(\sum_{i=0}^{+\infty} b_i u^i \right) \\ &= \lambda \varphi(P) + \mu \varphi(Q) \end{aligned}$$

(b) L'application φ respecte les multiplications internes. — Soit $(P, Q) \in \mathbf{K}[X]^2$. Posons $P = \sum_{i=0}^{+\infty} a_i X^i$ et $Q = \sum_{i=0}^{+\infty} b_i X^i$, où $(a_i)_{i \in \mathbf{N}}$ et $(b_i)_{i \in \mathbf{N}}$ sont des familles de scalaires presque nulles. En considérant plusieurs manières de sommer sur l'ensemble des couples (i, j) d'entiers tels que :

$$0 \leq j \leq i$$

il vient :

$$\begin{aligned} \varphi(P \times Q) &= \sum_{i=0}^{+\infty} \left(\sum_{j=0}^i a_j b_{i-j} \right) u^i && \left[\text{le coefficient de degré } i \text{ de } P \times Q \text{ est } \sum_{j=0}^i a_j b_{i-j} \right] \\ &= \sum_{0 \leq j \leq i} a_j b_{i-j} u^i \\ &= \sum_{j=0}^{+\infty} \sum_{i=j}^{+\infty} a_j b_{i-j} u^j && [\text{autre écriture de la somme triangulaire}] \\ &= \sum_{j=0}^{+\infty} a_j \left(\sum_{i=j}^{+\infty} b_{i-j} u^j \circ u^{i-j} \right) && [u^i = u^j \circ u^{i-j}] \\ &= \sum_{j=0}^{+\infty} a_j u^j \circ \left(\sum_{i=j}^{+\infty} b_{i-j} u^{i-j} \right) && [\text{linéarité de } u^j] \\ &= \sum_{j=0}^{+\infty} a_j u^j \circ \left(\sum_{k=0}^{+\infty} b_k u^k \right) && [k = i - j, \text{ avec } j \text{ fixé, dans la deuxième somme}] \\ &= \underbrace{\left(\sum_{j=0}^{+\infty} a_j u^j \right)}_{P(u)} \circ \underbrace{\left(\sum_{k=0}^{+\infty} b_k u^k \right)}_{Q(u)} \end{aligned}$$

(c) L'application φ respecte les éléments neutres des multiplications internes. — $\varphi(1) = \varphi(X^0) = u^0 = \text{id}_E$

□

1.3. Deux polynômes d'un même endomorphisme, d'une même matrice, commutent

Corollaire 5. — Soient $P, Q \in \mathbf{K}[X]$, $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbf{K})$.

Nous disposons de l'identité :

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

fort utile pour calculer des polynômes d'endomorphisme en u .

Nous disposons de l'identité :

$$P(M) \times Q(M) = (PQ)(M) = (QP)(M) = Q(M) \times P(M)$$

fort utile pour calculer des polynômes de matrice en M .

💡 | Deux polynômes d'un même endomorphisme (resp. d'une même matrice) commutent.

Exemple 6. — Soient $\lambda_1, \dots, \lambda_r$ des scalaires, m_1, \dots, m_r des entiers naturels non nuls et $P = \prod_{k=1}^r (X - \lambda_k)^{m_k} \in \mathbf{K}[X]$.

1. Si $u \in \mathcal{L}(E)$ alors $P(u) = (u - \lambda_1 \text{id}_E)^{m_1} \circ \dots \circ (u - \lambda_r \text{id}_E)^{m_r}$ et les r facteurs commutent.
2. Si $M \in \mathcal{M}_n(\mathbf{K})$ alors $P(M) = (M - \lambda_1 I_n)^{m_1} \times \dots \times (M - \lambda_r I_n)^{m_r}$ et les r facteurs commutent.

1.4. **K**-algèbre engendrée par un endomorphisme, par une matrice

Corollaire 7. — Soient $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbf{K})$.

(a) L'ensemble :

$$\mathbf{K}[u] := \text{Vect}_{\mathbf{K}}\left(\left(u^k\right)_{k \in \mathbf{N}}\right)$$

est une sous-algèbre commutative de $(\mathcal{L}(E), +, \circ, \cdot)$.

(b) $\mathbf{K}[u]$ est la plus petite sous-algèbre de $(\mathcal{L}(E), +, \circ, \cdot)$ qui contient u , aussi est-elle appelée « sous-algèbre engendrée par u ».

(a) L'ensemble :

$$\mathbf{K}[M] := \text{Vect}_{\mathbf{K}}\left(\left(M^k\right)_{k \in \mathbf{N}}\right)$$

est une sous-algèbre commutative de $(\mathcal{M}_n(\mathbf{K}), +, \times, \cdot)$.

(b) $\mathbf{K}[M]$ est la plus petite sous-algèbre de $(\mathcal{M}_n(\mathbf{K}), +, \times, \cdot)$ qui contient M , aussi est-elle appelée « sous-algèbre engendrée par M ».

Démonstration. Nous ne considérons que le cas d'un endomorphisme u .

(a) Rappelons qu'un endomorphisme de E est combinaison linéaire des endomorphismes de la famille $(u^k)_{k \in \mathbf{N}}$ si et seulement s'il s'écrit :

$$\sum_{k=0}^{+\infty} a_k u^k$$

où $(a_k)_{k \in \mathbf{N}}$ est une famille presque nulle de scalaires dans \mathbf{K} , i.e. :

$$\mathbf{K}[u] := \text{Vect}_{\mathbf{K}}\left(\left(u^k\right)_{k \in \mathbf{N}}\right) = \left\{ \sum_{k=0}^{+\infty} a_k u^k : (a_k)_{k \in \mathbf{N}} \in \mathbf{K}^{(\mathbf{N})} \right\}.$$

Nous observons que, d'après la définition 1 :

$$\left\{ \sum_{k=0}^{+\infty} a_k u^k : (a_k)_{k \in \mathbf{N}} \in \mathbf{K}^{(\mathbf{N})} \right\} = \{P(u) : P \in \mathbf{K}[X]\}$$

et donc :

$$\mathbf{K}[u] = \varphi(\mathbf{K}[X])$$

où φ est le morphisme de **K**-algèbres :

$$\varphi \left| \begin{array}{ll} (\mathbf{K}[X], +, \times, \cdot) & \longrightarrow (\mathcal{L}(E), +, \circ, \cdot) \\ P & \longmapsto P(u) := \sum_{k=0}^{+\infty} [P]_k u^k. \end{array} \right.$$

Nous en déduisons que $\mathbf{K}[u]$ est une sous-**K**-algèbre commutative de $\mathcal{L}(E)$, comme image de la **K**-algèbre commutative $\mathbf{K}[X]$ par le morphisme de **K**-algèbres φ .

(b) Nous savons déjà que $\mathbf{K}[u]$ est une sous-**K**-algèbre de $\mathcal{L}(E)$ qui contient u . Démontrons qu'il s'agit de la plus petite, au sens de l'inclusion, qui vérifie ces propriétés.

Soit A une sous-**K**-algèbre de $\mathcal{L}(E)$ contenant u . Alors :

- id_E appartient à A (A contient le neutre pour la multiplication interne de $\mathcal{L}(E)$, en tant que sous-anneau) ;
- pour tout $k \in \mathbf{N}^*$, $u^k \in A$ (A est stable pour la multiplication interne de $\mathcal{L}(E)$, en tant que sous-anneau) ;

et donc :

$$\{u^k : k \in \mathbf{N}\} \subset A.$$

Or A est un sous-**K**-espace vectoriel de $\mathcal{L}(E)$. Par minimalité d'un sous-espace vectoriel engendré :

$$\mathbf{K}[u] := \text{Vect}_{\mathbf{K}}\left(\left(u^k\right)_{k \in \mathbf{N}}\right) \subset A.$$

□

Exemple 8. — Si u un projecteur ($u^2 = u$) ou une symétrie ($u^2 = \text{id}_E$) de E , alors $\mathbf{K}[u] = \text{Vect}_{\mathbf{K}}(\text{id}_E, u)$.

Exemple 9. — Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbf{K})$. On calcule :

$$\chi_M(M) = M^2 - \text{tr}(M) M + \det(M) I_2 = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & bc + d^2 \end{pmatrix} - (a+d) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad - bc) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

De l'identité :

$$\chi_M(M) = M^2 - \text{tr}(M) M + \det(M) I_2 = 0_{\mathcal{M}_2(\mathbf{K})} \quad [\text{théorème de Cayley-Hamilton pour une matrice } (2, 2)]$$

nous déduisons que :

$$\mathbf{K}[M] = \text{Vect}_{\mathbf{K}}(I_2, M)$$

en prouvant l'inclusion non triviale à l'aide de la division euclidienne d'un polynôme de $\mathbf{K}[X]$ par χ_M .

Exercice 10. — Soit $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbf{K})$. Démontrer que (I_3, M, M^2) est une base de $\mathbf{K}[M]$.

Exercice 11. — Soit $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & j & 0 \\ 0 & 0 & j^2 \end{pmatrix} \in \mathcal{M}_3(\mathbf{C})$. Démontrer que (I_3, D, D^2) est une base de $\mathbf{C}[D]$.

1.5. Idéal annulateur d'un endomorphisme, d'une matrice

Corollaire 12. — Soient $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbf{K})$.

L'ensemble :

$$\text{Ann}(u) := \{P \in \mathbf{K}[X] : P(u) = 0_{\mathcal{L}(E)}\}$$

est un idéal de $\mathbf{K}[X]$, appelé idéal annulateur de u .

L'ensemble :

$$\text{Ann}(M) := \{P \in \mathbf{K}[X] : P(M) = 0_{\mathcal{M}_n(\mathbf{K})}\}$$

est un idéal de $\mathbf{K}[X]$, appelé idéal annulateur de M .

Remarque 13. — Supposons E de dimension finie $n \geq 1$. Considérons une base \mathcal{B} de E et $u \in \mathcal{L}(E)$. Comme, pour tout $P \in \mathbf{K}[X]$:

$$\begin{aligned} P(u) = 0_{\mathcal{L}(E)} &\iff \text{Mat}_{\mathcal{B}}(P(u)) = 0_{\mathcal{M}_n(\mathbf{K})} && [\text{Mat}_{\mathcal{B}}(\cdot) \text{ est linéaire et injective}] \\ &\iff P(\text{Mat}_{\mathcal{B}}(u)) = 0_{\mathcal{M}_n(\mathbf{K})} && [\text{remarque 3}] \end{aligned}$$

il vient $\text{Ann}(u) = \text{Ann}(\text{Mat}_{\mathcal{B}}(u))$.

Exercice 14. — Soit M_1 et M_2 deux matrices de $\mathcal{M}_n(\mathbf{K})$, semblables sur \mathbf{K} . Démontrer que $\text{Ann}(M_1) = \text{Ann}(M_2)$.

Exercice 15. — Déterminer l'idéal annulateur $\text{Ann}(V)$ de l'endomorphisme :

$$V \left| \begin{array}{ccc} \mathbf{R}^{\mathbb{N}} & \longrightarrow & \mathbf{R}^{\mathbb{N}} \\ u = (u_n)_{n \in \mathbb{N}} & \longmapsto & V(u) = (u_{n+1})_{n \in \mathbb{N}} \end{array} \right.$$

de $\mathbf{R}^{\mathbb{N}}$.

Exercice 16. — Déterminer l'idéal annulateur $\text{Ann}(\Delta_n)$ de l'endomorphisme :

$$\Delta_n \left| \begin{array}{ccc} \mathbf{C}_n[X] & \longrightarrow & \mathbf{C}_n[X] \\ P & \longmapsto & \Delta_n(P) = P' \end{array} \right.$$

de $\mathbf{C}_n[X]$.

Exercice 17. — Déterminer l'idéal annulateur $\text{Ann}(\Delta)$ de l'endomorphisme :

$$\Delta \left\{ \begin{array}{l} \mathbf{C}[X] \longrightarrow \mathbf{C}[X] \\ P \longmapsto \Delta(P) = P' \end{array} \right.$$

de $\mathbf{C}[X]$.

Exercice 18. — Soit $M = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbf{C})$. Démontrer que :

$$\text{Ann}(M) = (X^3 - 1) \mathbf{C}[X]$$

puis que $(1, X, X^2)$ est une base de $\mathbf{C}[M]$.

1.6. Polynôme minimal d'un endomorphisme d'un espace de dimension finie, d'une matrice

Corollaire 19. — Soient $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbf{K})$.

(a) Si E est de dimension finie, alors l'ensemble :

$$\text{Ann}(u) := \{P \in \mathbf{K}[X] : P(u) = 0_{\mathcal{L}(E)}\}$$

est un idéal de $\mathbf{K}[X]$ distinct de $\{0_{\mathbf{K}[X]}\}$.

(b) Le générateur unitaire de $\text{Ann}(u)$ est noté μ_u (ou π_u), d'où :

$$\mu_u \text{ est unitaire et } \text{Ann}(u) = \mu_u \mathbf{K}[X].$$

(c) Le polynôme μ_u est le polynôme unitaire de plus petit degré qui annule u . Il est appelé polynôme minimal de u .

(d) Si on note $d := \deg \mu_u \geq 1$, alors :

$$(\text{id}_E, u, \dots, u^{d-1})$$

est une base de $\mathbf{K}[u]$.

(a) L'ensemble :

$$\text{Ann}(M) := \{P \in \mathbf{K}[X] : P(M) = 0_{\mathcal{M}_n(\mathbf{K})}\}$$

est un idéal de $\mathbf{K}[X]$ distinct de $\{0_{\mathbf{K}[X]}\}$.

(b) Le générateur unitaire de $\text{Ann}(M)$ est noté μ_M (ou π_M), d'où :

$$\mu_M \text{ est unitaire et } \text{Ann}(M) = \mu_M \mathbf{K}[X].$$

(c) Le polynôme μ_M est le polynôme unitaire de plus petit degré qui annule M . Il est appelé polynôme minimal de M .

(d) Si on note $d := \deg \mu_M \geq 1$, alors :

$$(I_n, M, \dots, M^{d-1})$$

est une base de $\mathbf{K}[M]$.

Exercice 20. — Soit $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \mathcal{M}_2(\mathbf{R})$.

1. Donner un polynôme non nul de $\mathbf{R}[X]$ qui annule A (cf. exemple 9).
2. En déduire le polynôme minimal μ_A de A .
3. Donner une base la \mathbf{K} -algèbre $\mathbf{K}[A]$.
4. Soit $n \in \mathbf{N}$. Calculer A^n en divisant euclidiennement le polynôme X^n par μ_A .

Exercice 21. — Soient $D \in \mathcal{M}_n(\mathbf{K})$ une matrice diagonalisable sur \mathbf{K} et $\lambda_1, \dots, \lambda_r$ ses valeurs propres deux à deux distinctes.

1. Démontrer que $\pi_D = \prod_{i=1}^r (X - \lambda_i)$.
2. Donner une base de $\mathbf{K}[D]$.

Exercice 22. — Soient $N \in \mathcal{M}_n(\mathbf{K})$ une matrice nilpotente de nilindice $\nu \geq 1$. Ainsi $N^\nu = 0_{\mathcal{M}_n(\mathbf{K})}$ et $N^{\nu-1} \neq 0_{\mathcal{M}_n(\mathbf{K})}$.

1. Démontrer que $\pi_N = X^\nu$.
2. Donner une base de $\mathbf{K}[N]$.

Exercice 23. — Supposons E de dimension finie $n \geq 1$. Soit u un endomorphisme cyclique de E , i.e. tel que :

$$\exists x \in E \quad (x, u(x), \dots, u^{n-1}(x)) \text{ est une base de } E.$$

1. Démontrer que $\pi_u = \chi_u$.
2. Démontrer que $\{v \in \mathcal{L}(E) : v \circ u = u \circ v\} =: \text{Com}(u) = \mathbf{K}[u]$.

1.7. Valeurs propres et polynômes annulateurs d'un endomorphisme, d'une matrice

Proposition 24. — Soient $P \in \mathbf{K}[X]$, $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbf{K})$.

(a) Pour tout $(\lambda, x) \in \mathbf{K} \times E$:

$$u(x) = \lambda x \implies P(u)(x) = P(\lambda)x.$$

(b) Si P annule u , alors toute valeur propre de u est racine de P .

(a) Pour tout $(\lambda, X) \in \mathbf{K} \times \mathcal{M}_{n,1}(\mathbf{K})$:

$$MX = \lambda X \implies P(M)X = P(\lambda)X.$$

(b) Si P annule M , alors toute valeur propre de M est racine de P .

- Soient $u \in \mathcal{L}(E)$, P un polynôme annulateur de u et $\lambda \in \mathbf{K}$. Alors :

$$\lambda \in \text{Spec}(u) \implies P(\lambda) = 0_{\mathbf{K}}$$

mais la réciproque est fautive. En effet le polynôme $(X - 1)(X - 2026)$ annule $u = \text{id}_E$ mais 2026 n'est pas valeur propre de id_E .

- Soient $M \in \mathcal{M}_n(\mathbf{K})$, P un polynôme annulateur de M et $\lambda \in \mathbf{K}$. Alors :

$$\lambda \in \text{Spec}_{\mathbf{K}}(M) \implies P(\lambda) = 0_{\mathbf{K}}$$

mais la réciproque est fautive. En effet le polynôme $(X - 1)(X - 2026)$ annule $M = I_n$ mais 2026 n'est pas valeur propre de I_n .

Remarque 25. — Comme la conjugaison complexe est un automorphisme du corps \mathbf{C} , l'application :

$$\sigma \left| \begin{array}{l} \mathbf{C}[X] \longrightarrow \mathbf{C}[X] \\ P \longmapsto \bar{P} := \sum_{k=0}^{+\infty} \bar{a}_k X^k \end{array} \right.$$

est un automorphisme de l'anneau $\mathbf{C}[X]$. Nous en déduisons que, pour tout $P \in \mathbf{R}[X]$, pour toute racine complexe λ de P :

1. $\bar{\lambda}$ est une racine de P ;
2. $\text{mult}(\lambda, P) = \text{mult}(\bar{\lambda}, P)$ (cf. caractérisation de la multiplicité d'une racine à l'aide des dérivées itérées de P).

Exercice 26. — Soit $A \in \mathcal{M}_n(\mathbf{R})$ telle que $A^3 - 3A + 4I_n = 0_{\mathcal{M}_n(\mathbf{R})}$. Démontrer que $\det(A) > 0$.

Exercice 27. — Soit $A \in \mathcal{M}_n(\mathbf{R})$ telle que $A^2 + I_n = 0_{\mathcal{M}_n(\mathbf{R})}$. Démontrer que n est pair.

1.8. Les racines du polynôme minimal sont les valeurs propres pour un endomorphisme, pour une matrice


Théorème 28. — Soient $\lambda \in \mathbf{K}$, $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbf{K})$.

Supposons E de dimension finie. Les trois assertions suivantes sont équivalentes.

- (a) $\lambda \in \text{Spec}(u)$
- (b) $\chi_u(\lambda) = 0_{\mathbf{K}}$
- (c) $\pi_u(\lambda) = 0_{\mathbf{K}}$

Les trois assertions suivantes sont équivalentes.

- (a) $\lambda \in \text{Spec}_{\mathbf{K}}(M)$
- (b) $\chi_M(\lambda) = 0_{\mathbf{K}}$
- (c) $\pi_M(\lambda) = 0_{\mathbf{K}}$

 | Le polynôme minimal et le polynôme caractéristique ont les mêmes racines, qui sont les valeurs propres.

Exemple 29. — On considère la matrice $A = \begin{pmatrix} 0 & 2 & -1 \\ -1 & 3 & -1 \\ -1 & 2 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbf{R})$.

1. Montrer que A n'admet qu'une seule valeur propre que l'on déterminera.
2. La matrice A est-elle inversible ? Est-elle diagonalisable ?
3. On admet que $\chi_A(A) = 0_{\mathcal{M}_3(\mathbf{R})}$ (théorème de Cayley-Hamilton). Déterminer, en justifiant, le polynôme minimal de A .
4. Soit $n \in \mathbf{N}$. Déterminer le reste de la division euclidienne de X^n par $(X - 1)^2$ et en déduire la valeur de A^n .

2. Lemme des noyaux

Remarque 30. — Soient $P \in \mathbf{K}[X]$ et $u \in \mathcal{L}(E)$. Alors les sous-espaces :

$$\text{Ker}(P(u)) = \{x \in E : P(u)(x) = 0_E\} \quad \text{et} \quad \text{Im}(P(u)) = \{P(u)(x) : x \in E\}$$

sont stables par u .

Lemme 31. — Soient P_1, \dots, P_r des polynômes de $\mathbf{K}[X]$ deux-à-deux premiers entre eux. Pour tout $i \in \llbracket 1, r \rrbracket$, posons :

$$Q_i = \prod_{\substack{j=1 \\ j \neq i}}^r P_j.$$

- (a) Le PGCD des polynômes Q_1, \dots, Q_r est 1.
- (b) Pour tout $i \in \llbracket 1, r \rrbracket$, $P_i \wedge Q_i = 1$.

Démonstration. Nous prenons appui sur le théorème fondamental de l'arithmétique polynomiale, qui stipule que tout polynôme non nul de $\mathbf{K}[X]$ s'écrit d'une unique manière (à l'ordre des facteurs près) comme produit d'un scalaire non nul et de polynômes unitaires irréductibles sur \mathbf{K} .

(a) Raisonnons par l'absurde et supposons que $\bigwedge_{i=1}^r Q_i \neq 1$.

Il existe alors un polynôme $A \in \mathbf{K}[X]$ irréductible qui divise chacun des polynômes Q_1, Q_2, \dots, Q_r .

Comme A est un diviseur irréductible de $Q_1 = P_2 P_3 \dots P_r$ et les polynômes P_2, P_3, \dots, P_r sont deux-à-deux premiers entre eux, il existe $i \in \llbracket 2, r \rrbracket$ tel que A divise P_i .

Or A est également un diviseur irréductible de $Q_i = P_1 \dots P_{i-1} P_{i+1} \dots P_r$ et les polynômes $P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_r$ sont deux-à-deux premiers entre eux. Il existe donc $j \in \llbracket 1, r \rrbracket \setminus \{i\}$ tel que A divise P_j .

Le polynôme irréductible A divise à la fois P_i et P_j , ce qui contredit $P_i \wedge P_j = 1$.

(b) Soit $i \in \llbracket 1, r \rrbracket$.

Raisonnons par l'absurde et supposons que $P_i \wedge Q_i \neq 1$.

Il existe alors un polynôme $A \in \mathbf{K}[X]$ irréductible qui divise les polynômes P_i et Q_i .

Comme A est un diviseur irréductible de $Q_i = P_1 \dots P_{i-1} P_{i+1} \dots P_r$ et les polynômes $P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_r$ sont deux-à-deux premiers entre eux, Il existe donc $j \in \llbracket 1, r \rrbracket \setminus \{i\}$ tel que A divise P_j .

Le polynôme irréductible A divise à la fois P_i et P_j , ce qui contredit $P_i \wedge P_j = 1$.

□

Proposition 32. — Soient $u \in \mathcal{L}(E)$, P_1, \dots, P_r des polynômes de $\mathbf{K}[X]$ deux-à-deux premiers entre eux et $P = P_1 P_2 \dots P_r$.

(a) Le sous-espace $\text{Ker}(P(u))$, qui est stable par u , se décompose en :

$$\text{Ker}(P(u)) = \bigoplus_{i=1}^r \text{Ker}(P_i(u)) \quad [\text{lemme des noyaux}] .$$

(b) Soit $j \in \llbracket 1, r \rrbracket$. La projection π_j de $\text{Ker}(P(u))$ sur $\text{Ker}(P_j(u))$ parallèlement à $\bigoplus_{\substack{i=1 \\ i \neq j}}^r \text{Ker}(P_i(u))$ i.e. :

$$\pi_j \left| \begin{array}{l} \text{Ker}(P(u)) \quad \longrightarrow \quad \text{Ker}(P(u)) \\ x = \sum_{i=1}^r \underbrace{x_i}_{\in \text{Ker}(P_i(u))} \quad \longmapsto \quad x_j \end{array} \right.$$

est un polynôme en u , i.e. $\pi_j \in \mathbf{K}[u]$.

Démonstration. Pour tout $i \in \llbracket 1, r \rrbracket$, posons :

$$Q_i = \prod_{\substack{j=1 \\ j \neq i}}^r P_j$$

de sorte que $P = Q_i P_i = P_i Q_i$.

(a) L'inclusion $\sum_{i=1}^r \text{Ker}((P_i)(u)) \subset \text{Ker}(P(u))$. — Pour la démontrer, comme $\text{Ker}(P(u))$ est un sous-espace vectoriel de E , il suffit de démontrer que :

$$\forall j \in \llbracket 1, r \rrbracket \quad \text{Ker}((P_j)(u)) \subset \text{Ker}(P(u)) .$$

Soit $j \in \llbracket 1, r \rrbracket$. Comme :

$$P(u) = (Q_j P_j)(u) = Q_j(u) \circ P_j(u) \quad [\text{corollaire 5}]$$

l'inclusion :

$$\text{Ker}((P_j)(u)) \subset \text{Ker}(P(u))$$

est claire.

(b) Décomposition de id_E issue d'une relation de Bézout entre Q_1, \dots, Q_r . — D'après le lemme 31 :

$$Q_1 \mathbf{K}[X] + Q_2 \mathbf{K}[X] + \dots + Q_r \mathbf{K}[X] = \mathbf{K}[X] .$$

Il existe donc des polynômes $V_1, \dots, V_r \in \mathbf{K}[X]$ tels que :

$$Q_1 V_1 + Q_2 V_2 + \dots + Q_r V_r = 1$$

ce qui livre :

$$(*) \quad Q_1(u) \circ V_1(u) + Q_2(u) \circ V_2(u) + \dots + Q_r(u) \circ V_r(u) = \text{id}_E \quad [\text{corollaire 5}] .$$

(c) L'inclusion $\text{Ker}(P(u)) \subset \sum_{i=1}^r \text{Ker}((P_i)(u))$. — Soit $x \in \text{Ker}(P(u))$. D'après (\star) :

$$\underbrace{Q_1(u) \circ V_1(u)(x)}_{=:x_1} + \underbrace{Q_2(u) \circ V_2(u)(x)}_{=:x_2} + \dots + \underbrace{Q_r(u) \circ V_r(u)(x)}_{=:x_r} = x .$$

Soit $j \in \llbracket 1, r \rrbracket$. Le vecteur x_j appartient à $\text{Ker}(P_j(u))$. En effet :

$$\begin{aligned} P_j(u)(x_j) &= P_j(u) \circ (Q_j(u) \circ V_j(u)(x)) && \text{[définition de } x_j] \\ &= P_j(u) \circ Q_j(u) \circ V_j(u)(x) \\ &= V_j(u) \circ (P_j Q_j)(u)(x) && \text{[corollaire 5]} \\ &= V_j(u) \circ (P(u))(x) && [P = P_j Q_j] \\ &= 0_E && [x \in \text{Ker}(P(u))] . \end{aligned}$$

L'inclusion annoncée est donc établie.

(d) Les sous-espaces propres $\text{Ker}((P_1)(u)), \text{Ker}((P_2)(u)), \dots, \text{Ker}((P_r)(u))$ sont en somme directe. — Soient :

$$x_1 \in \text{Ker}((P_1)(u)) , x_2 \in \text{Ker}((P_2)(u)) , \dots , x_r \in \text{Ker}((P_r)(u))$$

tels que $x_1 + x_2 + \dots + x_r = 0_E$. Nous allons démontrer que $x_1 = x_2 = \dots = x_r = 0_E$.

- Pour tout $(i, j) \in \llbracket 1, r \rrbracket^2$ tel que $i \neq j$:

$$\begin{aligned} Q_i(u)(x_j) &= \left(\prod_{\substack{k=1 \\ k \neq i}}^r P_k \right)(u)(x_j) && \text{[définition de } Q_i] \\ &= \left(\left(\prod_{\substack{k=1 \\ k \neq i, j}}^r P_k \right) P_j \right)(u)(x_j) \\ &= \left(\prod_{\substack{k=1 \\ k \neq i, j}}^r P_k \right)(u) \circ P_j(u)(x_j) && \text{[corollaire 5]} \\ &= 0_E && [x_j \in \text{Ker}(P_j(u))] . \end{aligned}$$

- Nous en déduisons que, pour tout $i \in \llbracket 1, r \rrbracket$:

$$0_E = Q_i(u)(0_E) = Q_i(u)(x_1) + Q_i(u)(x_2) + \dots + Q_i(u)(x_r) = Q_i(u)(x_i) .$$

- Des deux points précédents, nous déduisons que :

$$(\star\star) \quad \forall (i, j) \in \llbracket 1, r \rrbracket^2 \quad Q_i(x_j) = 0_E .$$

Fixons $j \in \llbracket 1, r \rrbracket$. Comme des polynômes en u commutent, nous déduisons de (\star) que :

$$\sum_{i=1}^r V_i(u) \circ Q_i(u) = \text{id}_E .$$

En évaluant en x_j , nous obtenons :

$$x_j = \sum_{i=1}^r V_i(u) \circ Q_i(u)(x_j)$$

puis, grâce à $(\star\star)$:

$$x_j = \sum_{i=1}^r V_i(u)(0_E) = 0_E .$$

(e) *Étude des projecteurs associés à la décomposition en somme directe.* — Soit $j \in \llbracket 1, r \rrbracket$. D'après le lemme 31 et le théorème de Bézout, il existe des polynômes $A_j, B_j \in \mathbb{K}[X]$ tels que :

$$A_j P_j + B_j Q_j = 1$$

ce qui livre :

$$A_j(u) \circ P_j(u) + B_j(u) \circ Q_j(u) = \text{id}_E \quad [\text{corollaire 5}] .$$

Fixons $x \in \text{Ker}(P(u))$.

- L'identité précédente livre :

$$x = \underbrace{A_j(u) \circ P_j(u)(x)}_{y_j} + \underbrace{B_j(u) \circ Q_j(u)(x)}_{x_j} .$$

- Nous calculons :

$$\begin{aligned} Q_j(u)(y_j) &= Q_j(u)(A_j(u) \circ P_j(u)(x)) \quad [\text{définition de } y_j] \\ &= Q_j(u) \circ A_j(u) \circ P_j(u)(x) \\ &= A_j(u) \circ (P_j Q_j)(u)(x) \quad [\text{corollaire 5}] \\ &= A_j(u) \circ P(u)(x) \quad [P = P_j Q_j] \\ &= 0_E \quad [x \in \text{Ker}(P(u))] . \end{aligned}$$

Ainsi :

$$y_j \in \text{Ker}(Q_j(u)) = \text{Ker}((P_1 \dots P_{j-1} P_{j+1} \dots P_r)(u)) = \bigoplus_{\substack{i=1 \\ i \neq j}} \text{Ker}(P_i(u))$$

la dernière identité résultant de l'application du lemme des noyaux à la famille de polynômes deux-à-deux premiers entre eux :

$$P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_r .$$

- Nous calculons :

$$\begin{aligned} P_j(u)(x_j) &= P_j(u)(B_j(u) \circ Q_j(u)(x)) \quad [\text{définition de } x_j] \\ &= P_j(u) \circ B_j(u) \circ Q_j(u)(x) \\ &= B_j(u) \circ (P_j Q_j)(u)(x) \quad [\text{corollaire 5}] \\ &= B_j(u) \circ P(u)(x) \quad [P = P_j Q_j] \\ &= 0_E \quad [x \in \text{Ker}(P(u))] . \end{aligned}$$

Ainsi :

$$x_j \in \text{Ker}(P_j) .$$

Des trois points précédents, nous déduisons que la projection π_j de $\text{Ker}(P(u))$ sur $\text{Ker}(P_j(u))$ parallèlement à

$\bigoplus_{\substack{i=1 \\ i \neq j}}^r \text{Ker}(P_i(u))$ vérifie :

$$\pi_j = B_j(u) \circ Q_j(u) = (B_j Q_j)(u) \in \mathbb{K}[u] \quad [\text{corollaire 5}] .$$

□

Exemple 33. — Soit p un projecteur de E . Comme $X^2 - X = X(X - 1)$ annule p et $X \wedge (X - 1) = 1$, le lemme des noyaux nous livre $E = \text{Ker}(p) \oplus \text{Ker}(p - \text{id}_E)$ (décomposition d'un espace sous un projecteur). On rappelle que :

$$\forall x \in E \quad x = \underbrace{p(x)}_{\in \text{Ker}(p - \text{id}_E)} + \underbrace{x - p(x)}_{\in \text{Ker}(p)}$$

et que $\text{Im}(p) = \text{Ker}(p - \text{id}_E)$.

Exemple 34. — Soit s une symétrie de E . Comme $X^2 - 1 = (X + 1)(X - 1)$ annule s et $(X + 1) \wedge (X - 1) = 1$, le lemme des noyaux nous livre $E = \text{Ker}(s + \text{id}_E) \oplus \text{Ker}(s - \text{id}_E)$ (décomposition d'un espace sous une symétrie). On rappelle que :

$$\forall x \in E \quad x = \underbrace{\frac{1}{2}(x + s(x))}_{\in \text{Ker}(s - \text{id}_E)} + \underbrace{\frac{1}{2}(x - s(x))}_{\in \text{Ker}(s + \text{id}_E)}.$$

Exercice 35. — Soit $f \in \mathcal{L}(E)$ tel que $f^2 - f - 2 \text{id}_E = 0_{\mathcal{L}(E)}$.

1. Prouver que f est bijectif et exprimer f^{-1} en fonction de f .
2. Prouver que $E = \text{Ker}(f + \text{id}_E) \oplus \text{Ker}(f - 2 \text{id}_E)$.
3. Dans cette question, on suppose que E est de dimension finie. Prouver que $\text{Im}(f + \text{id}_E) = \text{Ker}(f - 2 \text{id}_E)$.

Exercice 36. — On suppose que E est un \mathbf{R} -espace vectoriel de dimension finie $n \geq 1$ et on considère $u \in \mathcal{L}(E)$ tel que $u^3 + u^2 + u = 0_{\mathcal{L}(E)}$.

1. Démontrer que $\text{Im}(u) \oplus \text{Ker}(u) = E$.
2. En déduire, grâce au lemme des noyaux, que $\text{Im}(u) = \text{Ker}(u^2 + u + \text{Id})$.
3. On suppose que u est non bijectif. Déterminer les valeurs propres de u .

Exercice 37. — Trouver tous les endomorphismes u de \mathbf{R}^n tels que $u^3 - 4u^2 + 4u = 0$ et $\text{tr}(u) = 0$.

3. Endomorphismes cycliques et matrices compagnons (HP)

3.1. Matrices compagnons

Proposition 38. — Soient $a_0, \dots, a_{n-1} \in \mathbf{K}$, $P = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + X^n$ et :

$$C(P) := \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix} \in \mathcal{M}_n(\mathbf{K}) \quad [\text{matrice compagnon du polynôme } P].$$

Le polynôme caractéristique $\chi_{C(P)} := \det(X I_n - C(P))$ de la matrice $C(P)$ est égale à P .

Démonstration. Soit $\lambda \in \mathbf{K}$. En appliquant l'opération élémentaire $L_{n-1} \leftarrow L_{n-1} + \lambda L_n$, nous obtenons :

$$\chi_{C(P)}(\lambda) := \begin{vmatrix} \lambda & \dots & \dots & 0 & a_0 \\ -1 & \ddots & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \lambda & a_{n-2} \\ 0 & \dots & 0 & -1 & \lambda + a_{n-1} \end{vmatrix}_{[n]} = \begin{vmatrix} \lambda & \dots & \dots & \dots & 0 & a_0 \\ -1 & \ddots & & \vdots & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \lambda & 0 & a_{n-3} \\ \vdots & & \ddots & -1 & 0 & \lambda^2 + a_{n-1} \lambda + a_{n-2} \\ 0 & \dots & \dots & 0 & -1 & \lambda + a_{n-1} \end{vmatrix}_{[n]}.$$

En appliquant ensuite l'opération élémentaire $L_{n-2} \leftarrow L_{n-2} + \lambda L_{n-1}$, nous obtenons :

$$\chi_{C(P)}(\lambda) = \begin{vmatrix} \lambda & \dots & \dots & \dots & \dots & 0 & a_0 \\ -1 & \ddots & & & & \vdots & a_1 \\ 0 & \ddots & \ddots & & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \lambda & 0 & 0 & a_{n-4} \\ \vdots & & \ddots & -1 & 0 & 0 & \lambda^3 + a_{n-1}\lambda^2 + a_{n-2}\lambda + a_{n-3} \\ \vdots & & & \ddots & -1 & 0 & \lambda^2 + a_{n-1}\lambda + a_{n-2} \\ 0 & \dots & \dots & \dots & 0 & -1 & \lambda + a_{n-1} \end{vmatrix}_{[n]} .$$

En appliquant successivement les opérations élémentaires :

$$L_{n-3} \leftarrow L_{n-3} + \lambda L_{n-2} \quad , \quad \dots \quad , \quad L_1 \leftarrow L_1 + \lambda L_2$$

nous obtenons :

$$\chi_{C(P)}(\lambda) = \begin{vmatrix} 0 & \dots & \dots & \dots & \dots & 0 & \lambda^n + a_{n-1}\lambda^{n-1} + a_{n-2}\lambda^{n-2} + \dots + a_1\lambda + a_0 \\ -1 & \ddots & & & & \vdots & \lambda^{n-1} + a_{n-1}\lambda^{n-2} + a_{n-2}\lambda^{n-3} + \dots + a_2\lambda + a_1 \\ 0 & \ddots & \ddots & & & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 & 0 & \lambda^4 + a_{n-1}\lambda^3 + a_{n-2}\lambda^2 + a_{n-3}\lambda + a_{n-4} \\ \vdots & & \ddots & -1 & 0 & 0 & \lambda^3 + a_{n-1}\lambda^2 + a_{n-2}\lambda + a_{n-3} \\ \vdots & & & \ddots & -1 & 0 & \lambda^2 + a_{n-1}\lambda + a_{n-2} \\ 0 & \dots & \dots & \dots & 0 & -1 & \lambda + a_{n-1} \end{vmatrix}_{[n]} .$$

En développant par rapport à la première ligne, il vient finalement :

$$\chi_{C(P)}(\lambda) = (-1)^{n+1} (\lambda^n + a_{n-1}\lambda^{n-1} + a_{n-2}\lambda^{n-2} + \dots + a_1\lambda + a_0) |-I_{n-1}| = P(\lambda) .$$

□

3.2. Endomorphismes cycliques

Définition 39. — Supposons E de dimension finie $n \geq 1$. Un endomorphisme u de E est dit cyclique si :

$$\exists x \in E \quad (x, u(x), \dots, u^{n-1}(x))$$

est une base de E .

Théorème 40. — Supposons E de dimension finie $n \geq 1$ et considérons un endomorphisme u de E qui est cyclique. Alors :

$$\chi_u(u) = 0_{\mathcal{L}(E)} \quad [\text{théorème de Cayley-Hamilton pour un endomorphisme cyclique}] .$$

Démonstration.

(a) Matrice de u dans une base reflétant le caractère cyclique de u . — Soit $x \in E$ tel que :

$$\mathcal{B}_x := (x, u(x), \dots, u^{n-1}(x))$$

est une base de E . Comme le vecteur $u^n(x) \in E$:

$$\exists ! (a_0, \dots, a_{n-1}) \in \mathbf{K}^n \quad u^n(x) = a_0 x + a_1 u(x) + \dots + a_{n-1} u^{n-1}(x) .$$

Nous calculons :

$$\text{Mat}_{\mathcal{B}_x}(u) := \begin{pmatrix} 0 & \dots & \dots & 0 & a_0 \\ 1 & \ddots & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \dots & 0 & 1 & a_{n-1} \end{pmatrix} = C(P)$$

où $P = -a_0 - a_1 X + \dots - a_{n-1} X^{n-1} + X^n$. D'après la proposition 38 :

$$(*) \quad \chi_u = \chi_{\text{Mat}_{\mathcal{B}_x}(u)} = -a_0 - a_1 X + \dots - a_{n-1} X^{n-1} + X^n .$$

(b) Réduction du problème au calcul de $\chi_u(u)(u^i(x))$, où $i \in \llbracket 0, n-1 \rrbracket$. — De (*), nous déduisons qu'il nous faut démontrer :

$$-a_0 \text{id}_E - a_1 u + \dots - a_{n-1} u^{n-1} + u^n = 0_{\mathcal{L}(E)}$$

ou, de manière équivalente (\mathcal{B}_x est une base de E), que :

$$\forall i \in \llbracket 0, n-1 \rrbracket \quad -a_0 u^i(x) - a_1 u^{i+1}(x) + \dots - a_{n-1} u^{n-1+i}(x) + u^{n+i}(x) = 0_E .$$

(c) Conclusion. — Soit $i \in \llbracket 0, n-1 \rrbracket$. Le vecteur $-a_0 u^i(x) - a_1 u^{i+1}(x) - \dots + a_{n-1} u^{n-1+i}(x) + u^{n+i}(x)$ égale le vecteur :

$$u^i \left(\underbrace{-a_0 x - a_1 u^1(x) + \dots - a_{n-1} u^{n-1}(x) + u^n(x)}_{=0_E} \right)$$

qui est nul.

□

4. Théorème de Cayley-Hamilton

Théorème 41. — Supposons que E est de dimension finie.

Pour tout $u \in \mathcal{L}(E)$:

$$\chi_u(u) = 0_{\mathcal{L}(E)}$$

ou de manière équivalente :

$$\pi_u \text{ divise } \chi_u \text{ dans } \mathbf{K}[X] .$$

Pour tout $M \in \mathcal{M}_n(\mathbf{K})$:

$$\chi_M(M) = 0_{\mathcal{M}_n(\mathbf{K})}$$

ou de manière équivalente :

$$\pi_M \text{ divise } \chi_M \text{ dans } \mathbf{K}[X] .$$

Démonstration.

(a) Il nous faut démontrer que :

$$\forall x \in E \quad \chi_u(u)(x) = 0_E .$$

L'assertion est claire pour $x = 0_E$. Considérons un vecteur non nul x de E .

(b) L'ensemble :

$$\{k \in \mathbf{N} : \text{la famille } (x, u(x), \dots, u^k(x)) \text{ est libre}\}$$

contient 0 ($x \neq 0_E$) et est majoré par $\dim(E)$. Ainsi

$$d_x := \max \{k \in \mathbf{N} : \text{la famille } (x, u(x), \dots, u^k(x)) \text{ est libre}\}$$

est bien définie.

(c) Comme la famille $(x, u(x), \dots, u^{d_x}(x))$ est libre et la famille $(x, u(x), \dots, u^{d_x}(x), u^{d_x+1}(x))$ est liée :

$$u^{d_x+1}(x) \in \text{Vect}(x, u(x), \dots, u^{d_x}(x))$$

On en déduit que le sous-espace vectoriel :

$$F_x := \text{Vect}((x, u(x), \dots, u^{d_x}(x)))$$

est stable par u .

(d) Notons u_{F_x} l'endomorphisme de F_x induit par u , i.e. :

$$u_{F_x} \left| \begin{array}{l} F_x \longrightarrow F_x \\ y \longmapsto u(y) . \end{array} \right.$$

Comme :

$$(x, u_{F_x}(x), \dots, u_{F_x}^{d_x}(x)) = (x, u(x), \dots, u^{d_x}(x))$$

est une base de F_x , l'endomorphisme u_{F_x} de F_x est cyclique (par construction).

(e) Nous savons que $\chi_{u_{F_x}}$ divise χ_u dans $\mathbb{K}[X]$. Il existe donc $Q \in \mathbb{K}[X]$ tel que $\chi_u = Q \chi_{u_{F_x}}$. Nous calculons :

$$\begin{aligned} \chi_u(u)(x) &= Q(u)(\chi_{u_{F_x}}(u)(x)) \\ &= Q(u)\left(\sum_{i=0}^{d_x} [\chi_{u_{F_x}}]_i u^i(x)\right) \\ &= Q(u)\left(\sum_{i=0}^{d_x} [\chi_{u_{F_x}}]_i u_{F_x}^i(x)\right) \quad [\text{si } i \in \llbracket 0, d_x \rrbracket, \text{ alors } u^i(x) = u_{F_x}^i(x)] \\ &= Q(u)(\chi_{u_{F_x}}(u_{F_x})(x)) \\ &= 0_E \quad [\text{d'après le théorème 40}] . \end{aligned}$$

□

Exercice 42. — Déterminer les polynômes minimaux des matrices suivantes.

$$A_1 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A_2 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A_3 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A_4 := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$B_1 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$B_2 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

$$B_3 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

$$B_4 := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

Exercice 43. — Soit $A = \begin{pmatrix} 1 & -2 \\ 1 & 4 \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$.

1. Calculer le polynôme minimal de A .
2. En déduire A^n , pour tout $n \in \mathbb{N}$.
3. Calculer $\exp(A)$.

Exercice 44. — Soit $A = \begin{pmatrix} 3 & 1 & -1 \\ 1 & 3 & -1 \\ 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{K})$.

1. Calculer le polynôme minimal de A .
2. En déduire A^n , pour tout $n \in \mathbb{N}$.

5. Polynômes annulateurs et réduction

5.1. Caractérisations algébriques de la diagonalisabilité

Théorème 45. — Soient u un endomorphisme d'un \mathbf{K} -espace vectoriel E de dimension finie et $M \in \mathcal{M}_n(\mathbf{K})$.

Les trois assertions suivantes sont équivalentes.

- (a) L'endomorphisme u est diagonalisable.
- (b) Il existe un polynôme $P \in \mathbf{K}[X]$ scindé à racines simples sur \mathbf{K} tel que $P(u) = 0_{\mathcal{L}(E)}$.
- (c) Le polynôme minimal π_u de u est scindé à racines simples sur \mathbf{K} .

Les trois assertions suivantes sont équivalentes.

- (a) La matrice M est diagonalisable sur \mathbf{K} .
- (b) Il existe un polynôme $P \in \mathbf{K}[X]$ scindé à racines simples sur \mathbf{K} tel que $P(M) = 0_{\mathcal{M}_n(\mathbf{K})}$.
- (c) Le polynôme minimal π_M de M est scindé à racines simples sur \mathbf{K} .

Démonstration. Nous ne considérons que le cas des endomorphismes.

- (a) \implies (b) — Supposons l'endomorphisme u diagonalisable. Alors :

$$(*) \quad E = \bigoplus_{i=1}^r E_{\lambda_i}(u)$$

où $\lambda_1, \dots, \lambda_r$ sont les valeurs propres deux à deux distinctes de u .

Nous vérifions que le polynôme :

$$P = \prod_{i=1}^r (X - \lambda_i) \quad [\text{scindé à racines simples sur } \mathbf{K}]$$

annule u , i.e. que :

$$P(u) = (u - \lambda_1 \text{id}_E) \circ \dots \circ (u - \lambda_r \text{id}_E) = 0_{\mathcal{L}(E)}.$$

Soit $i \in \llbracket 1, n \rrbracket$ Comme des polynômes d'endomorphismes en u commutent :

$$P(u) = (u - \lambda_1 \text{id}_E) \circ \dots \circ (u - \lambda_{i-1} \text{id}_E) \circ (u - \lambda_{i+1} \text{id}_E) \circ \dots \circ (u - \lambda_r \text{id}_E) \circ (u - \lambda_i \text{id}_E)$$

donc $P(u)$ est nul sur $\text{Ker}(u - \lambda_i \text{id}_E) = E_{\lambda_i}(u)$. Grâce à (*), nous en déduisons que $P(u)$ est nul sur E tout entier.

- (b) \implies (c) — Supposons qu'il existe $\alpha_1, \dots, \alpha_r$ des éléments de \mathbf{K} deux à deux distincts tel que le polynôme :

$$P = \prod_{i=1}^r (X - \alpha_i)$$

annule u . Ainsi :

$$P \in \text{Ann}(u) = \pi_u \mathbf{K}[X]$$

et π_u divise P dans $\mathbf{K}[X]$. D'après le théorème fondamental de l'arithmétique dans $\mathbf{K}[X]$

$$\exists (m_1, \dots, m_r) \in \{0, 1\}^r \quad \pi_u = \prod_{i=1}^r (X - \alpha_i)^{m_i}$$

et π_u est scindé à racines simples sur \mathbf{K} .

- (c) \implies (a) — Supposons qu'il existe $\alpha_1, \dots, \alpha_r$ des éléments de \mathbf{K} deux à deux distincts tel que :

$$\pi_u = \prod_{i=1}^r (X - \alpha_i).$$

Comme les polynômes $X - \alpha_1, \dots, X - \alpha_r$ sont irréductibles, unitaires et deux à deux distincts, ils sont deux à deux premiers entre eux.

D'après le lemme des noyaux :

$$(\star\star) \quad \text{Ker}(\pi_u(u)) = \bigoplus_{i=1}^r \text{Ker}(u - \alpha_i \text{id}_E).$$

Comme $\pi_u(u) = 0_{\mathcal{L}(E)}$ et les racines de π_u sont les valeurs propres de u , l'identité $(\star\star)$ s'écrit encore :

$$E = \bigoplus_{\lambda \in \text{Spec}(u)} E_\lambda(u).$$

L'endomorphisme u est donc diagonalisable. □

Exercice 46. — Soit $u \in \mathcal{L}(\mathbb{C}^n)$ tel que $u^p = \text{id}_E$, où $p \in \mathbb{N}^*$. Démontrer que u est diagonalisable et que ses valeurs propres sont des racines de l'unité.

Exercice 47. — Soit $A \in \mathcal{M}_n(\mathbb{C})$.

1. Si la matrice A^2 est diagonalisable sur \mathbb{C} , la matrice A est-elle nécessairement diagonalisable sur \mathbb{C} ?
2. On suppose la matrice A^2 inversible et diagonalisable sur \mathbb{C} . Démontrer que la matrice A est diagonalisable sur \mathbb{C} .

5.2. Polynôme minimal et diagonalisabilité d'un endomorphisme induit

Corollaire 48. — Supposons que E est de dimension finie. Soient $u \in \mathcal{L}(E)$ et F un sous-espace vectoriel de E stable par u . On note u_F l'endomorphisme de F l'induit par u .

- (a) Le polynôme π_{u_F} divise le polynôme π_u dans $\mathbb{K}[X]$.
- (b) Si u est diagonalisable alors u_F l'est également.

5.3. Codiagonalisation (HP)

Exercice 49. — Supposons que E est de dimension finie $n \geq 1$.

1. Soient u et v deux endomorphismes de E , diagonalisables et tels que $u \circ v = v \circ u$. Démontrer qu'il existe une base \mathcal{B} de E telle que les matrices $\text{Mat}_{\mathcal{B}}(u)$ et $\text{Mat}_{\mathcal{B}}(v)$ soient diagonales.
2. Soient A et B deux matrices de $\mathcal{M}_n(\mathbb{K})$, diagonalisables sur \mathbb{K} et telles que $AB = BA$. Démontrer qu'il existe une matrice $P \in \text{GL}_n(\mathbb{K})$ telle que les matrices $P^{-1}AP$ et $P^{-1}BP$ soient diagonales.

5.4. Caractérisations algébriques de la trigonalisabilité

Théorème 50. — Soient u un endomorphisme d'un \mathbb{K} -espace vectoriel E de dimension finie et $M \in \mathcal{M}_n(\mathbb{K})$.

Les trois assertions suivantes sont équivalentes.

- (a) L'endomorphisme u est trigonalisable.
- (b) Il existe un polynôme $P \in \mathbb{K}[X]$ scindé sur \mathbb{K} tel que $P(u) = 0_{\mathcal{L}(E)}$.
- (c) Le polynôme minimal π_u de u est scindé sur \mathbb{K} .

Les trois assertions suivantes sont équivalentes.

- (a) La matrice M est trigonalisable sur \mathbb{K} .
- (b) Il existe un polynôme $P \in \mathbb{K}[X]$ scindé sur \mathbb{K} tel que $P(M) = 0_{\mathcal{M}_n(\mathbb{K})}$.
- (c) Le polynôme minimal π_M de M est scindé sur \mathbb{K} .

Démonstration. Nous ne considérons que le cas des endomorphismes.

- (a) \implies (b) — Supposons l'endomorphisme u trigonalisable. Son polynôme caractéristique χ_u est scindé sur \mathbb{K} et il annule u d'après le théorème de Cayley-Hamilton.

- (b) \implies (c) — Supposons qu'il existe $\alpha_1, \dots, \alpha_r$ des éléments de \mathbf{K} deux à deux distincts et $m_1, \dots, m_r \in \mathbf{N}^*$ tel que le polynôme :

$$P = \prod_{i=1}^r (X - \alpha_i)^{m_i}$$

annule u . Ainsi :

$$P \in \text{Ann}(u) = \pi_u \mathbf{K}[X]$$

et π_u divise P dans $\mathbf{K}[X]$. D'après le théorème fondamental de l'arithmétique dans $\mathbf{K}[X]$:

$$\exists (m'_1, \dots, m'_r) \in \prod_{i=1}^r \llbracket 0, m_i \rrbracket \quad \pi_u = \prod_{i=1}^r (X - \alpha_i)^{m'_i}$$

et π_u est scindé sur \mathbf{K} .

- (c) \implies (a) — Supposons qu'il existe $\alpha_1, \dots, \alpha_r$ des éléments de \mathbf{K} deux à deux distincts et $m_1, \dots, m_r \in \mathbf{N}^*$ tel que :

$$\pi_u = \prod_{i=1}^r (X - \alpha_i)^{m_i} .$$

Comme les polynômes $X - \alpha_1, \dots, X - \alpha_r$ sont irréductibles, unitaires et deux à deux distincts, les polynômes $(X - \alpha_1)^{m_1}, \dots, (X - \alpha_r)^{m_r}$ sont deux à deux premiers entre eux. D'après le lemme des noyaux :

$$(*) \quad \text{Ker}(\pi_u(u)) = \bigoplus_{i=1}^r \text{Ker}((u - \alpha_i \text{id}_E)^{m_i}) .$$

Comme $\pi_u(u) = 0_{\mathcal{L}(E)}$, l'identité (*) s'écrit encore :

$$(**) \quad E = \bigoplus_{i=1}^r \underbrace{\text{Ker}((u - \alpha_i \text{id}_E)^{m_i})}_{=: F_i} .$$

Fixons $i \in \llbracket 1, r \rrbracket$. Le sous-espace F_i est stable par u . Nous pouvons donc considérer l'endomorphisme u_{F_i} de F_i induit par u , i.e. :

$$u_{F_i} \left| \begin{array}{ccc} \text{Ker}((u - \alpha_i \text{id}_E)^{m_i}) & \longrightarrow & \text{Ker}((u - \alpha_i \text{id}_E)^{m_i}) \\ x & \longmapsto & u(x) . \end{array} \right.$$

Comme, pour tout $x \in \text{Ker}((u - \alpha_i \text{id}_E)^{m_i})$:

$$(u_{F_i} - \alpha_i \text{id}_{F_i})^{m_i}(x) = (u - \alpha_i \text{id}_E)^{m_i}(x) = 0_E .$$

L'endomorphisme $u_{F_i} - \alpha_i \text{id}_{F_i}$ de F_i est nilpotent. Il existe donc une base \mathcal{B}_i de F_i telle que la matrice $\text{Mat}_{\mathcal{B}_i}(u_{F_i} - \alpha_i \text{id}_{F_i})$ soit triangulaire supérieure stricte. Nous en déduisons que la matrice :

$$\text{Mat}_{\mathcal{B}_i}(u_{F_i}) = \text{Mat}_{\mathcal{B}_i}(u_{F_i} - \alpha_i \text{id}_{F_i}) + \alpha_i \text{Mat}_{\mathcal{B}_i}(\text{id}_{F_i}) = \text{Mat}_{\mathcal{B}_i}(u_{F_i} - \alpha_i \text{id}_{F_i}) + \alpha_i I_{\dim(F_i)}$$

est triangulaire supérieure, avec des coefficients diagonaux tous égaux à α_i .

D'après (**) la famille :

$$\mathcal{B} := \mathcal{B}_1 \# \dots \# \mathcal{B}_r$$

est une base de E . Comme les sous-espaces F_1, \dots, F_r sont stables par u :

$$\text{Mat}_{\mathcal{B}}(u) = \text{diag}(\text{Mat}_{\mathcal{B}_1}(u_{F_1}), \dots, \text{Mat}_{\mathcal{B}_r}(u_{F_r})) .$$

Comme chacune des matrices : $\text{Mat}_{\mathcal{B}_1}(u_{F_1}), \dots, \text{Mat}_{\mathcal{B}_r}(u_{F_r})$ est triangulaire supérieure, la matrice $\text{Mat}_{\mathcal{B}}(u)$ est, elle aussi, triangulaire supérieure. □

5.5. Cotrigonalisation (HP)

Exercice 51. — Supposons que E est de dimension finie $n \geq 1$.

1. Soient u et v deux endomorphismes de E , trigonalisables et tels que $u \circ v = v \circ u$. Démontrer qu'il existe une base \mathcal{B} de E telle que les matrices $\text{Mat}_{\mathcal{B}}(u)$ et $\text{Mat}_{\mathcal{B}}(v)$ soient triangulaires supérieures.
2. Soient A et B deux matrices de $\mathcal{M}_n(\mathbf{K})$, trigonalisables sur \mathbf{K} et telles que $AB = BA$. Démontrer qu'il existe une matrice $P \in \text{GL}_n(\mathbf{K})$ telle que les matrices $P^{-1}AP$ et $P^{-1}BP$ soient triangulaires supérieures

6. Sous-espaces caractéristiques d'un endomorphisme à polynôme caractéristique scindé

6.1. Décomposition de l'espace en somme directe de sous-espaces caractéristiques, si χ_u est scindé sur \mathbf{K}

Théorème 52. — Supposons E de dimension finie $n \geq 1$ et considérons un endomorphisme u de E tel que χ_u est scindé sur \mathbf{K} . Notons $\lambda_1, \dots, \lambda_r$ ses valeurs propres deux à deux distinctes et m_1, \dots, m_r leurs multiplicités respectives, de sorte que

$$\chi_u = \prod_{i=1}^r (X - \lambda_i)^{m_i}$$

(a) Pour tout $i \in \llbracket 1, r \rrbracket$, le sous-espace :

$$N_i := \text{Ker}((u - \lambda_i \text{id}_E)^{m_i})$$

est appelé sous-espace caractéristique associé à la valeur propre λ_i .

(b) L'endomorphisme u décompose l'espace E en :

$$E = \bigoplus_{i=1}^r N_i \quad [\text{décomposition en somme directe de sous-espaces caractéristiques}] .$$

(c) Pour tout $i \in \llbracket 1, r \rrbracket$, $\dim(N_i) = m_i$.

Remarque 53. — On conserve les notations du théorème 52. Soit $i \in \llbracket 1, r \rrbracket$. On a l'inclusion :

$$E_{\lambda_i}(u) := \text{Ker}(u - \lambda_i \text{id}_E) \subset \text{Ker}((u - \lambda_i \text{id}_E)^{m_i}) =: N_i .$$

Mais cette inclusion peut-être stricte. Par exemple si u est l'endomorphisme de \mathbf{K}^2 défini par :

$$u \begin{cases} \mathbf{K}^2 & \longrightarrow \mathbf{K}^2 \\ (x, y) & \longmapsto (y, 0) \end{cases}$$

alors 0 est la seule valeur propre de u , $\chi_u = X^2$ et :

$$\text{Ker}(u - 0 \text{id}_{\mathbf{R}^2}) = \text{Ker}(u) = \text{Vect}((1, 0)) \subsetneq \text{Ker}((u - 0 \text{id}_{\mathbf{R}^2})^2) = \mathbf{R}^2 .$$

6.2. De la classe de similitude d'une matrice à polynôme caractéristique scindé sur \mathbf{K}

Corollaire 54. — Soit une matrice $M \in \mathcal{M}_n(\mathbf{K})$ tel que χ_M scindé sur \mathbf{K} . Notons $\lambda_1, \dots, \lambda_r$ ses valeurs propres deux à deux distinctes et m_1, \dots, m_r leurs multiplicités respectives, de sorte que :

$$\chi_M = \prod_{i=1}^r (X - \lambda_i)^{m_i} .$$

Alors il existe des matrices :

$$T_1 \in \mathcal{T}_{m_1}^{++}(\mathbf{K}), \dots, T_r \in \mathcal{T}_{m_r}^{++}(\mathbf{K}) \quad [\text{matrices triangulaires supérieures strictes}]$$

telles que M est semblable à la matrice diagonale par blocs :

$$\begin{pmatrix} \lambda_1 I_{m_1} + T_1 & & & \\ & \lambda_2 I_{m_2} + T_2 & & \\ & & \ddots & \\ & & & \lambda_r I_{m_r} + T_r \end{pmatrix} .$$

Exercice 55. — Soient un entier $n \geq 2$ et $M \in \mathcal{M}_n(\mathbf{K})$ telle que χ_M est scindé sur \mathbf{K} . Démontrer que les deux assertions suivantes sont équivalentes.

- (a) la matrice M est diagonalisable sur \mathbf{K} ;
- (b) la matrice $\exp(M)$ est diagonalisable sur \mathbf{K} .

On pourra introduire deux matrices D et N telles que :

$$M = D + N \quad , \quad DN = ND \quad , \quad D \text{ est diagonalisable sur } \mathbf{K} \quad , \quad N \text{ est nilpotente}$$

en justifiant que de telles existent.

Comme χ_M est scindé sur \mathbf{K} , il existe un entier $r \geq 2$, des scalaires $\lambda_1, \dots, \lambda_r$ et des nombres entiers naturels non nuls m_1, \dots, m_r tels que :

$$\chi_M = \prod_{i=1}^r (X - \lambda_i)^{m_i} .$$

- *Implication (a) \implies (b).* — Supposons la matrice M diagonalisable sur \mathbf{K} . Alors, il existe $P \in \mathbf{GL}_n(\mathbf{K})$ telle que :

$$M = P \operatorname{diag}(\lambda_1 I_{m_1}, \dots, \lambda_r I_{m_r}) P^{-1} .$$

Ainsi :

$$\forall K \in \mathbf{N} \quad \sum_{k=0}^K \frac{M^k}{k!} = P \operatorname{diag} \left(\left(\sum_{k=0}^K \frac{\lambda_1^k}{k!} \right) I_{m_1}, \dots, \left(\sum_{k=0}^K \frac{\lambda_r^k}{k!} \right) I_{m_r} \right) P^{-1} .$$

Grâce à la continuité du produit matriciel, en faisant tendre K vers $+\infty$, il vient :

$$\exp(M) = P \operatorname{diag}(e^{\lambda_1} I_{m_1}, \dots, e^{\lambda_r} I_{m_r}) P^{-1} .$$

La matrice $\exp(M)$ est donc diagonalisable.

- *Implication (b) \implies (a).* — Supposons la matrice $\exp(M)$ diagonalisable. D'après le théorème 54, il existe des matrices $T_1 \in \mathcal{F}_{m_1}^{++}(\mathbf{K}), \dots, T_r \in \mathcal{F}_{m_r}^{++}(\mathbf{K})$ et une matrice $P \in \mathbf{GL}_n(\mathbf{K})$ telles que :

$$\begin{aligned} M &= P \operatorname{diag}(\lambda_1 I_{m_1} + T_1, \dots, \lambda_r I_{m_r} + T_r) P^{-1} \\ &= \underbrace{P \operatorname{diag}(\lambda_1 I_{m_1}, \dots, \lambda_r I_{m_r}) P^{-1}}_D + \underbrace{P \operatorname{diag}(T_1, \dots, T_r) P^{-1}}_N . \end{aligned}$$

La matrice D est diagonalisable sur \mathbf{K} , la matrice N est nilpotente $\chi_N = X^n$, les matrices D et N commutent (un calcul de produit par blocs permet de le vérifier aisément) et, par construction, $M = D + N$. Comme les matrices D et N commutent :

$$\exp(M) = \exp(D) \exp(N) = \exp(D) + \exp(D)(\exp(N) - I_n) .$$

- *La matrice $\exp(D)(\exp(N) - I_n)$ est diagonalisable.* — Les arguments exposés dans la première implication livrent :

$$\exp(D) = P \operatorname{diag}(e^{\lambda_1} I_{m_1}, \dots, e^{\lambda_r} I_{m_r}) P^{-1} .$$

La matrice $\exp(D)$ est donc diagonalisable.

Comme les matrices D et N commutent, les matrices $M = D + N = N + D$ et D commutent, d'où :

$$\exp(M) \exp(D) = \exp(M + D) = \exp(D + M) = \exp(D) \exp(M) .$$

Puisque les matrices $\exp(M)$ et $\exp(D)$ sont diagonalisables et commutent, elles sont codiagonalisables (cf. exercice 54), i.e. il existe une matrice $Q \in \mathbf{GL}_n(\mathbf{K})$ telle que les matrices :

$$Q^{-1} \exp(M) Q \quad \text{et} \quad Q^{-1} \exp(D) Q$$

soient diagonales. Nous en déduisons :

$$\exp(D)(\exp(N) - I_n) = \exp(M) - \exp(D) = Q \underbrace{(Q^{-1} \exp(M) Q - Q^{-1} \exp(D) Q)}_{\text{matrice diagonale}} Q^{-1}.$$

La matrice $\exp(D)(\exp(N) - I_n)$ est donc diagonalisable.

— La matrice $\exp(D)(\exp(N) - I_n)$ est nilpotente. — En adaptant les arguments exposés dans la première implication, il vient :

$$\exp(N) = P \operatorname{diag}(\exp(T_1), \dots, \exp(T_r)) P^{-1}$$

puis :

$$\exp(N) - I_n = P \operatorname{diag}(\exp(T_1) - I_{m_1}, \dots, \exp(T_r) - I_{m_r}) P^{-1}.$$

Comme les matrices T_1, \dots, T_r sont triangulaires supérieures strictes, les matrices $\exp(T_1) - I_{m_1}, \dots, \exp(T_r) - I_{m_r}$ sont également triangulaires supérieures strictes.

Nous en déduisons que la matrice $\exp(N) - I_n$ est nilpotente (son polynôme caractéristique est X^n).

Comme les matrices D et N commutent :

$$\exp(D)(\exp(N) - I_n) = \exp(D + N) - \exp(D) = \exp(N + D) - \exp(D) = (\exp(N) - I_n) \exp(D).$$

Nous avons établi que la matrice $\exp(N) - I_n$ est nilpotente et que les matrices $\exp(N) - I_n$ et $\exp(D)$ commutent. Nous en déduisons que la matrice $\exp(D)(\exp(N) - I_n)$ est également nilpotente.

La matrice $\exp(D)(\exp(N) - I_n)$ est diagonalisable et nilpotente. Elle est donc nulle (son polynôme caractéristique est X^n donc son polynôme minimal, qui divise X^n et est scindé à racines simples sur \mathbf{K} , est X).

La matrice $\exp(D)$ étant inversible (d'inverse $\exp(-D)$), nous en déduisons que :

$$\exp(N) = I_n.$$

La matrice nilpotente N est annulée par X^n . Ainsi :

$$\exp(N) = I_n + \sum_{k=1}^{n-1} \frac{N^k}{k!}.$$

puis :

$$O_{\mathcal{M}_n(\mathbf{K})} = \exp(N) - I_n = \sum_{k=1}^{n-1} \frac{N^k}{k!} = N \left(\sum_{k=1}^{n-1} \frac{N^{k-1}}{k!} \right) = N \left(I_n + \sum_{k=2}^{n-1} \frac{N^{k-1}}{k!} \right)$$

En trigonalisant la matrice nilpotente N (semblable à une matrice triangulaire supérieure stricte), on démontre que la matrice :

$$I_n + \sum_{k=2}^{n-1} \frac{N^{k-1}}{k!}$$

est semblable à une matrice triangulaire supérieure, avec uniquement des 1 sur la diagonale. Elle est donc inversible.

Par suite, la matrice N est nulle et $M = D$ est diagonalisable.