Réduction (2)

Polynômes d'un endomorphisme, d'une matrice carrée

1. Pour $u \in \mathscr{L}(E)$, morphisme d'algèbres $P \mapsto P(u)$ de $\mathbb{K}[X]$ dans $\mathscr{L}(E)$. Le noyau de ce morphisme est l'idéal annulateur de u. Son image est la sous-algèbre commutative $\mathbb{K}[u]$ de $\mathscr{L}(E)$.
2. Polynôme minimal d'un endomorphisme d'un espace de dimension finie, d'une matrice carrée. Il est unitaire et noté π (ou μ).
3. Si d est le degré du polynôme minimal de u, alors $(\mathrm{Id}, u, \ldots, u^{d-1})$ est une base de $\mathbb{K}[u]$.
4. Si $u(x) = \lambda x$, alors $P(u)(x) = P(\lambda)x$.
5. Si P est un polynôme annulateur de u, toute valeur propre de u est racine de P.
6. Les racines de π_u dans $\mathbb{K}$ sont les valeurs propres de u.

Lemme de décomposition des noyaux

Polynômes annulateurs et réduction

7. Un endomorphisme est diagonalisable si, et seulement si, il admet un polynôme annulateur scindé à racines simples, si, et seulement si, son polynôme minimal est scindé à racines simples. Version matricielle.
8. Un endomorphisme est trigonalisable si, et seulement si, il admet un polynôme annulateur scindé, si, et seulement si, son polynôme minimal est scindé. Version matricielle.
9. Polynôme minimal d'un endomorphisme induit. Diagonalisabilité d'un endomorphisme induit par un endomorphisme diagonalisable.

Théorème de Cayley-Hamilton et sous-espaces caractéristiques

1. Théorème de Cayley-Hamilton (démonstration non exigible).
2. Sous-espaces caractéristiques d'un endomorphisme à polynôme caractéristique scindé. Dimension d'un espace caractéristique.
3. E est somme directe des sous-espaces caractéristiques.
4. Traduction matricielle de cette décomposition : similitude à une matrice diagonale par blocs, chaque bloc diagonal étant triangulaire supérieur et à termes diagonaux égaux.

Dans tout le chapitre, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$, qui en pratique sera $\mathbb{R}$ ou $\mathbb{C}$. E est un $\mathbb{K}$-espace vectoriel.

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

1.1 définitions

Définition 1

Soit $P = a_0 + a_1 X + \cdots + a_p X^p$ un polynôme de $\mathbb{K}[X]$. Soit $u \in \mathscr{L}(E)$. Soit $A \in \mathcal{M}_n(\mathbb{K})$.

1. On note $P(u)$ l'endomorphisme $P(u) = a_0 \mathrm{Id}_{\mathbf{E}} + a_1 u + \cdots + a_p u^p \in \mathscr{L}(E)$.
2. On note $P(A)$ la matrice $P(A) = a_0 \mathbf{I_n} + a_1 A + \cdots + a_p A^p \in \mathcal{M}_n(\mathbb{K})$.

On appelle *polynôme en* u tout endomorphisme de la forme $P(u)$ avec $P \in \mathbb{K}[X]$. L'ensemble des polynômes en u est noté $\mathbb{K}[u]$.
On appelle *polynôme en* A toute matrice de la forme $P(A)$ avec $P \in \mathbb{K}[X]$. L'ensemble des polynômes en A est noté $\mathbb{K}[A]$.

Par exemple, lorsque $P(X) = 7X^2 - 2X + 3$,
$P(A)$ est la matrice :

$P(u)$ est l'endomorphisme :

et pour $x \in E$, $P(u)(x)$ est le vecteur :

Attention à la lecture et aux parenthèses ! $P(u)(x)$ désigne

Exercice 1 : Soit $M \in \mathcal{M}_n(\mathbb{K})$ de coefficients diagonaux $d_1, \ldots, d_n$ et P un polynôme de $\mathbb{K}[X]$.

1. Calculer $P(M)$ lorsque M est une matrice diagonale.
2. Lorsque M est triangulaire supérieure, que dire de $P(M)$?

Propriété 1

- Soit $x \in E$, $\lambda \in \mathbb{K}$. On suppose que $u(x) = \lambda x$. Alors $P(u)(x) = P(\lambda)x$.
- Soit $X \in \mathcal{M}_{n,1}(\mathbb{K})$. On suppose que $AX = \lambda X$. Alors $P(A)X = P(\lambda)X$.

Nous en verrons une utilité en propriété 4.

Remarque : lorsque E est de dimension finie, on passe facilement d'un polynôme d'endomorphisme à un polynôme de matrice. Si $\mathcal{B}$ est une base de E, on a

$$\mathrm{mat}_{\mathcal{B}}(P(u)) = P(\mathrm{mat}_{\mathcal{B}}\, u)$$

1.2 sous-algèbre engendrée par un endomorphisme ou une matrice carrée

Propriété 2

- Soit u un endomorphisme de E. L'application

$$\begin{pmatrix} \mathbb{K}[X] & \longrightarrow & \mathscr{L}(E) \\ P & \longmapsto & P(u) \end{pmatrix}$$

est un morphisme d'algèbres.
L'image de ce morphisme, $\mathbb{K}[u]$, est une sous-algèbre commutative de $\mathscr{L}(E)$. On a

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

- Soit $A \in \mathcal{M}_n(\mathbb{K})$. L'application

$$\begin{pmatrix} \mathbb{K}[X] & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ P & \longmapsto & P(u) \end{pmatrix}$$

est un morphisme d'algèbres. L'image de ce morphisme, $\mathbb{K}[A]$, est une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$. On a

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

> On retiendra en particulier que deux polynômes en u commutent, que deux polynômes en A commutent. Par exemple, sans calculs :
>
> $$(A^2+A^3)(I-A) = (I-A)(A^2+A^3) \qquad (f-\mathrm{Id}_E)\circ(f+2\,\mathrm{Id}_E)\circ(f-3\,\mathrm{Id}_E) = (f-3\,\mathrm{Id}_E)\circ(f-\mathrm{Id}_E)\circ(f+2\,\mathrm{Id}_E)$$

Remarque : $\mathbb{K}[u]$ est la plus petite sous-algèbre de $\mathscr{L}(E)$ contenant u, on l'appelle *algèbre engendrée par u*.

Exercice 2 : Expliciter l'algèbre engendrée par $M_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et l'algèbre engendrée par $M_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Exercice 3 : Soient $u \in \mathscr{L}(E)$ et $P \in \mathbb{K}[X]$. Montrer que $\ker P(u)$ et $\operatorname{Im} P(u)$ sont des sous-espaces vectoriels de E stables par u, et plus généralement sont stables par $Q(u)$, où $Q \in \mathbb{K}[X]$.

1.3 lemme de décomposition des noyaux

Théorème 1 – lemme de décomposition des noyaux - version 1

Si P_1 et P_2 sont deux polynômes de $\mathbb{K}[X]$ premiers entre eux, et si $u \in \mathscr{L}(E)$, on a :

$$\ker(P_1P_2(u)) = \ker(P_1(u)) \oplus \ker(P_2(u))$$

Théorème 2 – lemme de décomposition des noyaux - version 2

Si $P_1, \ldots, P_r$ sont des polynômes de $\mathbb{K}[X]$ premiers entre eux deux à deux et de produit égal à P, et si $u \in \mathscr{L}(E)$, on a :

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

On rappelle que deux polynômes sont premiers entre eux si, et seulement si, ils n'ont aucune racine complexe en commun. Ainsi $(X-a)^n$ et $(X-b)^m$ sont premiers entre eux lorsque $a \neq b$.

Exercice 4 : Nous traitons l'exemple d'un projecteur et d'une symétrie d'un espace vectoriel E.

Exercice 5 : En introduisant $u(f) = f'$, déterminer l'ensemble des solutions réelles de l'équation différentielle $y^{(3)} - y'' - y' - 2y = 0$.

2 Polynômes annulateurs et applications

2.1 généralités

Définition 2

- Soit u un endomorphisme de E. On appelle polynôme annulateur de u tout polynôme $P \in \mathbb{K}[X]$ tel que $P(u) = 0_{\mathscr{L}(E)}$.
- Soit $A \in \mathcal{M}_n(\mathbb{K})$. On appelle polynôme annulateur de A tout polynôme $P \in \mathbb{K}[X]$ tel que $P(A) = 0$.

L'ensemble des polynômes annulateurs de u est le noyau du morphisme d'algèbres

$$\begin{pmatrix} \mathbb{K}[X] & \longrightarrow & \mathscr{L}(E) \\ P & \longmapsto & P(u) \end{pmatrix}$$

C'est un idéal de $\mathbb{K}[X]$, appelé *idéal annulateur* de u.

Théorème 3

Tout endomorphisme d'un espace vectoriel de dimension finie admet au moins un polynôme annulateur non nul. Il y a même une infinité de tels polynômes.

Exercice 6 : Dans $E = \mathbb{K}[X]$, on considère $u : P \mapsto XP$. Montrer que u ne possède pas de polynôme annulateur autre que le polynôme nul.

Propriété 3

Si A et B sont deux matrices semblables alors A et B ont les mêmes polynômes annulateurs.

Méthode – détermination de u^{-1}

Si u admet un polynôme annulateur de terme constant non nul, alors on peut déterminer u^{-1} et u^{-1} est un polynôme en u. On a un résultat similaire pour les matrices.

Exercice 7 : Soit $A \in \mathcal{M}_n(\mathbb{K})$ vérifiant $A^4 - A^2 + 7I = 0$. Montrer que A est inversible et déterminer son inverse.

2.2 utilité des polynômes annulateurs pour la réduction

Propriété 4

Si P est un polynôme annulateur de u et λ une valeur propre de u, alors λ est racine de P :

$$\mathrm{Sp}(u) \subset \{ \text{ racines de } P \text{ polynôme annulateur de } u \ \}$$

Toutes les racines de P ne sont pas forcément valeurs propres de u.

Exercice 8 : Soit n un entier supérieur ou égal à 2 et f un endomorphisme de $\mathbb{K}^n$ tel que $(f - \mathrm{Id})^n = 0$. Sans calcul, déterminer $\ker f$ et $\mathrm{Im}\, f$.

Exercice 9 :
E est un espace vectoriel de dimension finie et f est un endomorphisme de E satisfaisant : $f^2 = -f$.

1. Situer les valeurs propres possibles de f.
2. Montrer que f est diagonalisable.

Exercice 10 : Soit u un endomorphisme nilpotent et non nul d'un espace vectoriel E de dimension finie. Montrer que u n'est pas diagonalisable.

Exercice 11 : Soit $n \geqslant 2$, et A une matrice non nulle de $\mathcal{M}_n(\mathbb{R})$. On considère l'endomorphisme f qui à toute matrice de $\mathcal{M}_n(\mathbb{R})$ associe :

$$f(M) = \mathrm{Tr}(A)M - \mathrm{Tr}(M)A$$

1. Montrer que f n'est pas l'endomorphisme nul.
2. (a) Déterminer un polynôme annulateur de f.
   (b) Donner les valeurs propres possibles de f.
3. Montrer que 0 est valeur propre de f.
4. Montrer que, si $\mathrm{Tr}(A) = 0$, alors f n'est pas diagonalisable.
5. On suppose dans cette question que la trace de A est non nulle. Montrer que f est diagonalisable.

Théorème 4

Soit u un endomorphisme d'un espace vectoriel de dimension finie.
u est diagonalisable si et seulement s'il possède un polynôme annulateur scindé à racines simples.

Corollaire 1

Si u est diagonalisable, alors pour tout sous-espace vectoriel F stable par u, l'endomorphisme induit par u sur F est diagonalisable.

Exercice 12 : Retrouver que les projecteurs et les symétries d'un espace vectoriel de dimension finie sont diagonalisables.

Exercice 13 : Soit M la matrice d'ordre n ne contenant que des 1. Donner un polynôme annulateur de M et montrer que M est diagonalisable.

Exercice 14 : Montrer que $A^\top$ est diagonalisable si et seulement si A est diagonalisable.

N'êtes-vous pas en train de vous demander où a disparu le polynôme caractéristique $\chi_A = \det(XI_n - A)$ sur lequel nous avions consacré tout le chapitre Réduction (1) ? Il fait ici son grand retour ! Dans un théorème admis, conformément au programme.

Théorème 5 – théorème de Cayley-Hamilton

Le polynôme caractéristique d'un endomorphisme en dimension finie (ou d'une matrice) est un polynôme annulateur. Autrement dit, si E est de dimension finie,

$$\chi_u(u) = 0_{\mathscr{L}(E)} \qquad \chi_A(A) = 0$$

Terminons par un résultat qui sera démontré plus loin (théorème 7), quand nous aurons présenté la notion de polynôme minimal. On rappelle qu'un polynôme scindé est non nul par définition.

Corollaire 2

u est trigonalisable si, et seulement s'il possède un polynôme annulateur scindé.

3 Polynôme minimal et applications

3.1 généralités

Nous avons vu que l'ensemble des polynômes annulateurs de l'endomorphisme u était un idéal de $\mathbb{K}[X]$. Et nous avons appris au chapitre Anneaux que les idéaux de $\mathbb{K}[X]$ étaient de la forme $P_0\mathbb{K}[X]$ avec $P_0 \in \mathbb{K}[X]$. Enfin, nous avons vu que $P_0\mathbb{K}[X] = P_1\mathbb{K}[X]$ si, et seulement si, P_0 et P_1 sont associés. Si P_0 et P_1 sont de plus supposés unitaires, alors $P_0 = P_1$.

Définition 3

- Soit u un endomorphisme d'un espace vectoriel de dimension finie. L'idéal annulateur de u admet un unique générateur unitaire appelé *polynôme minimal* de u, noté π_u.

$$\{P \in \mathbb{K}[X],\ P(u) = 0_{\mathscr{L}(E)}\} = \pi_u\,\mathbb{K}[X]$$

- L'idéal annulateur de la matrice A admet un unique générateur unitaire appelé *polynôme minimal* de A, noté π_A.

$$\{P \in \mathbb{K}[X],\ P(A) = 0\} = \pi_A\,\mathbb{K}[X]$$

Remarques :

— $P(u) = 0$ si, et seulement si, $\pi_u | P$, et $P(A) = 0$ si, et seulement si, $\pi_A | P$. En particulier, le polynôme minimal divise le polynôme caractéristique. On s'aperçoit aussi que le polynôme minimal est **minimal en degré** parmi les polynômes annulateurs de u.

— Si A est la matrice de u dans la base $\mathcal{B}$, alors $\pi_u = \pi_A$. Deux matrices semblables ont même polynôme minimal, égal au polynôme minimal de l'endomorphisme qu'elles représentent.

— En dimension infinie, u n'admet pas nécessairement de polynôme annulateur non nul, et donc pas forcément de polynôme minimal.

— Si F est un sous-espace vectoriel stable par u, alors le polynôme minimal de l'endomorphisme induit $u_{|F}$ divise celui de u.
En effet,

$$\forall x \in F, \quad \pi_u(u_{|F})(x) = \pi_u(u)(x) = 0$$

et $\pi_{u_{|F}}$ divise tous les polynômes annulateurs de $u_{|F}$.

Exercice 15 : Déterminer le polynôme minimal de $A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix}$.

Exercice 16 : Quel est le polynôme minimal d'un endomorphisme nilpotent ?

Exercice 17 : Déterminer le polynôme caractéristique puis le polynôme minimal de $A = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$.

Propriété 5

Si d est le degré du polynôme minimal de u, alors la famille $(\mathrm{Id}, u, u^2, \ldots, u^{d-1})$ est une base de $\mathbb{K}[u]$.
Si d est le degré du polynôme minimal de A, alors la famille $(I_n, A, A^2, \ldots, A^{d-1})$ est une base de $\mathbb{K}[A]$.
On a

$$\dim \mathbb{K}[u] = d \leqslant \dim E \qquad \text{et} \qquad \dim \mathbb{K}[A] = d \leqslant n$$

Méthode – décomposition de $P(u)$ dans la base précédente

Soit u admettant un polynôme minimal de degré d. Pour $P \in \mathbb{K}[X]$, on effectue la division euclidienne de P par π_u :

$$P = Q\pi_u + R \text{ avec } \deg(R) < d$$

On a $P(u) = R(u)$. Connaître R permet donc de décomposer $P(u)$ dans la base $(\mathrm{Id}, u, u^2, \ldots, u^{d-1})$ de $\mathbb{K}[u]$.
En prenant $P = X^k$, on peut calculer les puissances de u.

Exercice 18 : Soit $A = \begin{pmatrix} 0 & 1 & -1 \\ -3 & 4 & -3 \\ -1 & 1 & 0 \end{pmatrix}$. On admet que $A^2 - 3A + 2I_3 = 0$.

Montrer que $(X-1)(X-2)$ est le polynôme minimal de A. En déduire les puissances de A, A^n pour $n \geqslant 2$.

3.2 utilité du polynôme minimal pour la réduction

Propriété 6

Les valeurs propres de u (respectivement A) sont exactement les racines de son polynôme minimal.

Une erreur classique consiste à croire qu'il suffit d'enlever les puissances du polynôme caractéristique pour obtenir le polynôme minimal. Par exemple, si $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$, par déterminant d'une matrice triangulaire, $\chi_A = (X-1)^2(X-2)^2$. Cependant, on vérifie que $(X-1)(X-2)$ n'annule pas A. On a en fait

$$\pi_A = (X-1)(X-2)^2$$

Théorème 6

Un endomorphisme u est diagonalisable si et seulement si l'une des deux conditions suivantes est vérifiée :

- Il existe un polynôme scindé à racines simples annulant u.
- Le polynôme minimal de u est scindé à racines simples.

Sous l'une de ces conditions, $\pi_u = \prod\limits_{\lambda \in \mathrm{Sp}(u)} (X - \lambda)$.

Le théorème s'adapte pour une matrice.

> Ce théorème montre que pour que A soit diagonalisable, π_A ne doit pas contenir de facteur de la forme $(X - \lambda)^\alpha$ avec $\alpha > 1$.

Exercice 19 : Soit $A = \begin{pmatrix} 0 & -3 & -5 \\ -1 & 0 & -3 \\ 1 & 2 & 5 \end{pmatrix}$. A est-elle diagonalisable ?

Théorème 7

Un endomorphisme u est trigonalisable si et seulement si l'une des deux conditions suivantes est vérifiée :

- Il existe un polynôme scindé annulant u.
- Le polynôme minimal de u est scindé.

Le théorème s'adapte pour une matrice.

4 Sous-espaces caractéristiques

Notre but est ici d'affiner la trigonalisation de u lorsque u est trigonalisable, ce qui est le cas lorsque χ_u (ou, de manière équivalente, π_u) est scindé.
Supposons pour cela χ_u scindé et écrivons-le sous la forme

$$\chi_u = (X - \lambda_1 \operatorname{Id})^{m_1} \dots (X - \lambda_r \operatorname{Id})^{m_r} \qquad \text{où } \lambda_1, \dots, \lambda_r \text{ sont les } r \text{ valeurs propres distinctes de } u$$

Les facteurs $(X - \lambda_i)^{m_i}$ étant premiers entre eux deux à deux, on peut appliquer le lemme de décomposition des noyaux.

$$\ker \chi_u(u) = \ker(u - \lambda_1 \operatorname{Id})^{m_1} \oplus \dots \oplus \ker(u - \lambda_r \operatorname{Id})^{m_r}$$

Par le théorème de Cayley-Hamilton, $\chi_u(u) = 0$. On a donc la décomposition de E :

$$E = \ker(u - \lambda_1 \operatorname{Id})^{m_1} \oplus \dots \oplus \ker(u - \lambda_r \operatorname{Id})^{m_r}$$

C'est une décomposition de E en somme directe de sous-espaces stables par u. Cette décomposition ne requiert qu'une seule condition : le caractère scindé de χ_u. Cette condition est toujours vérifiée dans $\mathbb{C}$.

Définition 4

Soient $u \in \mathscr{L}(E)$ de polynôme caractéristique scindé et λ une valeur propre de u. On appelle *sous-espace caractéristique* de u associé à la valeur propre λ le sous-espace

$$\ker((u - \lambda \operatorname{Id}_E)^m)$$

où m est l'ordre de multiplicité de la valeur propre λ dans χ_u.

Propriété 7

Soit $A \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. A est semblable à une matrice diagonale par blocs où chaque bloc diagonal est triangulaire supérieur à coefficients diagonaux égaux.

Si $\chi_A = \prod_{i=1}^{r} (X - \lambda_i)^{m_i}$, A est semblable à une matrice diagonale par blocs de la forme suivante.

$$\begin{pmatrix} \begin{bmatrix} \lambda_1 & & (*) \\ & \ddots & \\ (0) & & \lambda_1 \end{bmatrix} & & & & & \\ & \begin{bmatrix} \lambda_2 & & (*) \\ & \ddots & \\ (0) & & \lambda_2 \end{bmatrix} & & & & \\ & & \ddots & & & \\ & & & \ddots & & \\ & & & & \ddots & \\ & & & & & \begin{bmatrix} \lambda_r & & (*) \\ & \ddots & \\ (0) & & \lambda_r \end{bmatrix} \end{pmatrix}$$

Propriété 8 – dimension d'un sous-espace caractéristique

On a $\dim \ker((u - \lambda \operatorname{Id}_E)^m) = m$ où m est l'ordre de multiplicité de la valeur propre λ dans χ_u.

5 Quelques applications pour terminer

La liste suivante des applications n'est certes pas exhaustive, mais vous permet de vous préparer à quelques situations classiques.

5.1 calculs de puissances

— Par diagonalisation et $A^n = PD^nP^{-1}$ (voir Réduction (1)).

— Disposant d'un polynôme annulateur de A, on peut calculer le reste R_n dans la division euclidienne de X^n par ce polynôme annulateur. On a $A^n = R_n(A)$ (voir exercice en page 8).

5.2 recherche d'un commutant

Voir chapitre Réduction (1).

5.3 équations différentielles

— Système différentiel et diagonalisation (voir Réduction (1) et chapitre Équations différentielles).

— Équations différentielles linéaires et lemme de décomposition des noyaux (voir exercice en page 4).

5.4 recherche de sous-espace vectoriel stables

- La droite $\mathrm{Vect}(e)$ est stable par u si et seulement si e est vecteur propre de u (vu au chapitre Réduction (1)).
- Si u est diagonalisable, F est stable par u si et seulement si F possède une base formée de vecteurs propres de u. (Ce résultat est à redémontrer si vous l'utilisez).

6 Annexe : quelques éléments de démonstrations

Propriété 1

On considère un scalaire λ et un vecteur x tels que $u(x) = \lambda x$.
On remarque que $f^2(x) = u(f(x)) = u(\lambda x) = \lambda u(x) = \lambda.\lambda x = \lambda^2 x$ et on a l'idée de généraliser.

Soit $\mathcal{P}_k$ la propriété : « $f^k(x) = \lambda^k x$ » qu'on montre par récurrence pour $k \geqslant 0$.
- On a $f^0(x) = \mathrm{Id}(x) = x = 1.x = \lambda^0 x$ donc $\mathcal{P}_0$ est vraie.
- Supposons $\mathcal{P}_k$ vraie pour un certain entier naturel k.

On a

$$\begin{aligned} u^{k+1}(x) &= u(u^k(x)) = u(\lambda^k x) \text{ (hypothèse de récurrence)} \\ &= \lambda^k u(x) = \lambda^k.\lambda x \\ &= \lambda^{k+1} x \end{aligned}$$

$\mathcal{P}_{k+1}$ est vraie, ce qui achève la récurrence.

Soit $Q(X) = a_0 + a_1 X + \cdots + a_p X^p$. On a :

$$\begin{aligned} Q(u)(x) &= (a_0 \mathrm{Id} + a_1 u + a_2 u^2 + \cdots + a_p u^p)(x) \\ &= a_0 x + a_1 u(x) + \cdots + a_p u^p(x) \\ &= a_0 x + a_1 \lambda x + a_2 \lambda^2 x + \cdots + a_p \lambda^p x \\ &= (a_0 + a_1 \lambda + a_2 \lambda^2 + \cdots + a_p \lambda^p) x \\ &= Q(\lambda) x \end{aligned}$$

Propriété 2

Notons $f : P \mapsto P(u)$.
On a $f(1) = \mathrm{Id}_E$.
Soient $P = \sum\limits_{k=0}^{p} a_k X^k$ et $Q = \sum\limits_{k=0}^{q} b_k X^k$. Quitte à adjoindre des coefficients nuls à P ou à Q, on peut supposer que $q = p$. Pour $\lambda, \mu \in \mathbb{K}$, on a :

$$\begin{aligned} f(\lambda P + \mu Q) &= f\Big(\sum_{k=0}^{p} (\lambda a_k + \mu b_k) X^k\Big) = \sum_{k=0}^{p} (\lambda a_k + \mu b_k) u^k \\ &= \lambda \sum_{k=0}^{p} a_k u^k + \mu \sum_{k=0}^{p} b_k u^k \\ &= \lambda f(P) + \mu f(Q) \\ f(PQ) &= f\Big(\sum_{0 \leqslant k, \ell \leqslant p} a_k b_\ell X^{k+\ell}\Big) = \sum_{0 \leqslant k, \ell \leqslant p} a_k b_\ell u^{k+\ell} \\ f(P) \circ f(Q) &= P(u) \circ \left(\sum_{\ell=0}^{p} b_\ell u^\ell \right) \\ &= \sum_{\ell=0}^{p} b_\ell P(u) \circ (u^\ell) \text{ par linéarité de } P(u) \\ &= \sum_{\ell=0}^{p} b_\ell \sum_{k=0}^{p} a_k u^k \circ (u^\ell) = \sum_{\ell=0}^{p} b_\ell \sum_{k=0}^{p} a_k u^{k+\ell} \\ &= f(PQ) \end{aligned}$$

Donc f est bien un morphisme d'algèbres.
Remarque importante : par ce morphisme, toute identité polynomiale se transpose aux endomorphismes. Par exemple, $X^2 - 1 = (X-1)(X+1)$ donne $u^2 - \mathrm{Id}_E = (u - \mathrm{Id}_E) \circ (u + \mathrm{Id}_E)$.

L'image d'un morphisme d'algèbre est une sous-algèbre de l'ensemble d'arrivée, donc $\mathbb{K}[u]$ est une sous-algèbre de $\mathscr{L}(E)$. La rédaction de la commutativité est faite dans l'énoncé de la propriété.

Si $\mathcal{A}$ est une sous-algèbre de $\mathscr{L}(E)$ contenant u alors par récurrence, $u^n \in \mathcal{A}$ pour tout $n \in \mathbb{N}$, puis $\mathbb{K}[u] = \mathrm{Vect}\{u^k,\, k \in \mathbb{N}\} \subset \mathcal{A}$.

Théorème 1

Tout, ou presque, va reposer sur une identité de Bézout. Il existe A et B polynômes de $\mathbb{K}[X]$ tels que

$$AP_1 + BP_2 = 1 \quad \text{puis } A(u) \circ P_1(u) + B(u) \circ P_2(u) = \mathrm{Id}$$

- $\ker(P_1(u))$ est un sous-espace vectoriel de $\ker(P_1P_2(u))$. En effet, si $P_1(u)(x) = 0$, alors

$$(P_1P_2)(u)(x) = (P_2P_1)(u)(x) = (P_2(u) \circ P_1(u))(x) = P_2(u)(0_E) = 0_E$$

De même, $\ker(P_2(u))$ est un sous-espace vectoriel de $\ker(P_1P_2(u))$. Donc $\ker(P_1(u)) + \ker(P_2(u))$ est un sous-espace vectoriel de $\ker(P_1P_2(u))$.

- Soit $x \in \ker(P_1P_2(u))$.

$$x = \mathrm{Id}(x) = \underbrace{[A(u) \circ P_1(u)](x)}_{=x_1} + \underbrace{[B(u) \circ P_2(u)](x)}_{=x_2}$$

On montre que $x_1 \in \ker P_2(u)$ et $x_2 \in \ker P_1(u)$.
À ce stade, $\ker(P_1P_2(u)) = \ker(P_1(u)) + \ker(P_2(u))$.

- Enfin, si $x \in \ker(P_1(u)) \cap \ker(P_2(u))$, alors avec l'identité de Bézout,

$$x = A(u) \circ P_1(u)(x) + B(u) \circ P_2(u)(x) = A(u)(0) + B(u)(0) = 0$$

et la somme est directe.

Ce théorème est valable sans hypothèse sur la dimension de E. On aboutit, par récurrence, à la version 2.

Propriété 3

Par le calcul à partir de la relation de similitude $B = Q^{-1}AQ$.
Les matrices A et B représentent le même endomorphisme u. Heureusement qu'elles ont les mêmes polynômes annulateurs !

Propriété 4 concernant l'utilité des polynômes annulateurs pour situer les valeurs propres

Soit P un polynôme annulateur de u.
Soit $\lambda \in \mathrm{Sp}(u)$. Il existe $x \neq 0$ tel que $u(x) = \lambda x$. Par la propriété 1, on a : $P(u)(x) = P(\lambda)x$.
Comme $P(u) = 0_{\mathscr{L}(E)}$, on obtient : $P(\lambda)x = 0$. Enfin, $x \neq 0$ donc $P(\lambda) = 0$ et λ est une racine de P.

Théorème 3

Comme E est de dimension n, $\dim \mathscr{L}(E) = \dim L(E, E) = \dim E \times \dim E = n^2$.
La famille $(\mathrm{Id}, f, f^2, \dots, f^{n^2})$ comporte plus de vecteurs que la dimension de $\mathscr{L}(E)$: c'est une famille liée. Il existe des scalaires $(a_i)_{0 \leqslant i \leqslant n^2}$ non tous nuls tels que :

$$a_0 \mathrm{Id} + a_1 f + a_2 f^2 + \cdots + a_{n^2} f^{n^2} = 0_{\mathscr{L}(E)}$$

Le polynôme $P(X) = \sum_{k=0}^{n^2} a_k X^k$ est un polynôme non nul annulateur de f.
Si P est un polynôme annulateur de f, pour tout polynôme Q, les polynômes PQ et QP sont des polynômes annulateurs de f. En effet :

$$\begin{array}{rcl}
(QP)(f) & = & (PQ)(f) \text{ (commutativité du produit dans } \mathbf{R}[x]) \\
& = & P(f) \circ Q(f) \text{ (propriété des polynômes d'endomorphisme)} \\
& = & 0_{\mathscr{L}(E)} \circ Q(f) \\
& = & 0_{\mathscr{L}(E)}
\end{array}$$

Il s'ensuit qu'il existe une infinité de polynômes annulateurs de f.

Théorème 4

- Supposons que u est diagonalisable. En notant $\lambda_1, \dots, \lambda_p$ les valeurs propres de u, on a :

$$E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_p}$$

Soit $P = (X - \lambda_1) \dots (X - \lambda_p)$. P est scindé à racines simples. On a $P(u) = (u - \lambda_1 \mathrm{Id}_E) \circ \dots (u - \lambda_p \mathrm{Id}_E)$. En tant que polynômes en u, les endomorphismes $u - \lambda_i \mathrm{Id}_E$ commutent. Dès lors, on arrive à montrer que pour $x_i \in E_{\lambda_i}$, $P(u)(x_i) = 0$. La restriction de $P(u)$ à chaque sous-espace propre est nulle. Par propriété (ou en réécrivant la décomposition de $x \in E$ dans la somme directe), $P(u) = 0$.

- Réciproquement, s'il existe un polynôme annulateur P de u scindé et à racines simples, avec le lemme de décomposition des noyaux, on arrive à montrer que $E = \ker P(u)$ est somme directe (des) d'espaces propres de u. u est donc diagonalisable.

Corollaire 1

Comme u est diagonalisable, u admet un polynôme P scindé à racines simples. On a encore $P(u_F) = 0$. Donc par le même théorème, u_F est diagonalisable.

Propriété 5

Comprenons l'idée pour commencer. On introduit le polynôme minimal π_u de u, de degré d (avec $d \leqslant \dim E$ car π_u divise χ_u). On écrit

$$\pi_u = X^d - (a_{d-1}X^{d-1} + \cdots + a_1 X + a_0)$$

et alors

$$u^d = a_0 \operatorname{Id}_E + a_1 u + \cdots + a_{d-1}u^{d-1}$$

On compose par u application linéaire :

$$u^{d+1} = a_0 u + a_1 u^2 + \cdots + a_{d-1}u^d$$

Mais u^d est combinaison linéaire de $\operatorname{Id}, u, \ldots, u^{d-1}$, donc on obtient une expression

$$u^{d+1} = b_0 \operatorname{Id}_E + b_1 u + \cdots + b_{d-1}u^{d-1}$$

On peut répéter ce processus.

Démonstration : Commençons par montrer que $\mathbb{K}[u] = \operatorname{Vect}(\operatorname{Id}, u, \ldots, u^{d-1})$. On a déjà l'inclusion $\operatorname{Vect}(\operatorname{Id}, u, \ldots, u^{d-1}) \subset \mathbb{K}[u]$. Réciproquement, soit $P \in \mathbb{K}[X]$. Par division euclidienne, on peut écrire $P = Q\pi_u + R$ avec $\deg R < d$. On a alors

$$P(u) = Q(u) \circ \pi_u(u) + R(u) = R(u) \in \operatorname{Vect}(\operatorname{Id}, u, \ldots, u^{d-1})$$

Ainsi $\mathbb{K}[u] \subset \operatorname{Vect}(\operatorname{Id}, u, \ldots, u^{d-1})$ puis l'égalité.

Montrons maintenant que la famille $(\operatorname{Id}, u, \ldots, u^{d-1})$ est libre. Supposons que $a_0 \operatorname{Id}_E + a_1 u + \cdots + a_{d-1}u^{d-1} = 0$.
Pour $P = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1}$, on a $P(u) = 0$. Comme $\deg P < \deg \pi_u$, on a $P = 0$ puis $a_0 = a_1 = a_{d-1} = 0$.
Ainsi, la famille $(\operatorname{Id}, u, \ldots, u^{d-1})$ est libre et c'est donc une base de $\mathbb{K}[u]$.

Propriété 6

Comme π_u est un polynôme annulateur de u, $\operatorname{Sp}(u) \subset \{\text{racines de } \pi_u\}$.
Soit λ une racine de π_u. Comme π_u divise χ_u, λ est aussi une valeur propre de χ_u. Nous avons appris au chapitre Réduction (1) que $\operatorname{Sp}(u) = \{\text{racines de } \chi_u\}$. Donc λ est valeur propre de u.
Remarque : il s'ensuit que le polynôme $\prod\limits_{\lambda \in \operatorname{Sp}(u)} (X - \lambda)$ divise π_u.

Théorème 6

Notons :

1. u est diagonalisable
2. il existe P scindé à racines simples tel que $P(u) = 0$
3. π_u est scindé à racines simples.

(1) $\Leftrightarrow$ (2) a été vu dans le théorème 4.
(2) $\Rightarrow$ (3) facile : $\pi_u | P$.
(3) $\Rightarrow$ (2) facile car $\pi_u(u) = 0$.

Théorème 7 comprenant le corollaire 2

Démonstration admise en classe. $\mathbb{K}$ est un sous-corps de $\mathbb{C}$. Notons :

1. A est trigonalisable
2. χ_A est scindé
3. il existe P scindé dans $\mathbb{K}$ tel que $P(A) = 0$
4. π_A est scindé dans $\mathbb{K}$.

(1) $\Leftrightarrow$ (2). On a montré cette équivalence au chapitre Réduction (1).
(2) $\Rightarrow$ (3). Par hypothèse, le polynôme caractéristique χ_A est scindé, et il est annulateur par le théorème de Cayley-Hamilton.
(3) $\Rightarrow$ (4). $\pi_A | P$

Dernier point. Approche algébrique sur les polynômes – pour moi – à ne pas faire avec les étudiants
(4) $\Rightarrow$ (2). On sait que

$$\operatorname{Sp}_{\mathbb{K}}(A) = \{\text{racines dans } \mathbb{K} \text{ de } \pi_A\} = \{\text{racines dans } \mathbb{K} \text{ de } \chi_A\}$$

On fait attention, parce que $\pi_A | \chi_A$ pourrait théoriquement donner par exemple
$\pi_A = (X+1)(X-2)$ et $\chi_A = (X+1)(X-2)(X^2+1)$, mais on va montrer qu'en réalité, ce genre de situation est exclu.

Regardons A comme matrice complexe. Notons π'_A son nouveau polynôme minimal, dans $\mathbb{C}$. Le polynôme caractéristique,

lui, ne change pas (égal dans $\mathbb{K}$ comme dans $\mathbb{C}$).
Dans $\mathbb{K}$ comme dans $\mathbb{C}$, $\pi_A(A)=0$, donc $\pi'_A|\pi_A$. Donc

$$\{\text{racines dans } \mathbb{C} \text{ de } \pi'_A\} \subset \{\text{racines dans } \mathbb{C} \text{ de } \pi_A\} \tag{1}$$

Par ailleurs,

$$\mathrm{Sp}_{\mathbb{C}}(A) = \{\text{racines dans } \mathbb{C} \text{ de } \pi'_A\} = \{\text{racines dans } \mathbb{C} \text{ de } \chi_A\} \tag{2}$$

Par (1) et (2),

$$\{\text{racines dans } \mathbb{C} \text{ de } \chi_A\} \quad \subset \quad \{\text{racines dans } \mathbb{C} \text{ de } \pi_A\}$$

Or

$$\begin{aligned}
\{\text{racines dans } \mathbb{C} \text{ de } \pi_A\} &= \{\text{racines dans } \mathbb{K} \text{ de } \pi_A\} \quad (\pi_A \text{ est scindé dans } \mathbb{K}) \\
&= \{\text{racines dans } \mathbb{K} \text{ de } \chi_A\} \quad (\text{propriété du spectre}) \\
&\subset \{\text{racines dans } \mathbb{C} \text{ de } \chi_A\} \quad (\mathbb{K} \subset \mathbb{C})
\end{aligned}$$

Il y a donc partout égalité. π_A et χ_A ont donc les mêmes racines, et ce dans $\mathbb{K}$ comme dans $\mathbb{C}$. On rappelle que $\pi_A|\chi_A$ et que π_A est scindé dans $\mathbb{K}$. Donc χ_A est scindé. Ouf !

- **Dernier point. Approche par les sous-espaces caractéristiques – je choisis cette approche**

Soit u l'endomorphisme de $\mathbb{K}^n$ canoniquement associé à A. Supposons le polynôme minimal π_u de u scindé dans $\mathbb{K}[X]$. On peut écrire

$$\pi_u = \prod_{k=1}^{m} (X-\lambda_k)^{\alpha_k}$$

avec $\lambda_1, \ldots, \lambda_m$ les valeurs propres distinctes de u. Par le lemme de décomposition des noyaux

$$E = \bigoplus_{k=1}^{m} \ker(u-\lambda_k \,\mathrm{Id}_E)^{\alpha_k}$$

Soit $F = \ker(u-\lambda_k \,\mathrm{Id}_E)^{\alpha_k}$. L'espace F est stable par u car u et $(u-\lambda_k \,\mathrm{Id}_E)^{\alpha_k}$ commutent.
On peut introduire $n_k = u_F - \lambda_k \,\mathrm{Id}_F \in \mathscr{L}(F)$ et on a $n^{\alpha_k} = 0$. Ainsi $u_F = \lambda_k \,\mathrm{Id}_F + n_k$ avec n_k nilpotent.
Comme n_k est nilpotent, n_k est trigonalisable et sa seule valeur propre est 0 (vu au chapitre Réduction (1)).
Il existe une base $\mathcal{B}_k$ dans laquelle la matrice de n_k est triangulaire supérieure. En concaténant ces bases $\mathcal{B}_1, \ldots, \mathcal{B}_m$, on obtient une base de E dans laquelle la matrice de u est triangulaire supérieure. u est donc trigonalisable. Et A aussi.

Propriété 7

Très semblable à la démonstration du théorème 7. Démonstration faite en classe.

Propriété 8

Résulte de la démonstration de la propriété précédente.

Exercice classique sur la recherche de sous-espace vectoriel stables en page 11

($\Leftarrow$) $F = \mathrm{Vect}(v_1, \ldots, v_r)$, $u(F) = \mathrm{Vect}(u(v_1), \ldots, u(v_r)) = \mathrm{Vect}(\lambda_1 v_1, \ldots, \lambda_r v_r) \subset F$.
($\Rightarrow$) Par le cours, u_F est diagonalisable. Il existe une base de F constituée de vecteurs propres de $u_F : w_1, \ldots, w_r$. Les w_i sont dans E et ce sont des vecteurs propres de u.