CH09 : Réduction des endomorphismes - Aspects algébriques

Table des matières

I Polynômes d'endomorphismes / de matrices 4
1) Polynômes d'endomorphismes 4
2) Polynômes de matrices 5
II Polynômes annulateurs, polynôme minimal 8
1) Définitions et premières propriétés 8
2) Résultats en dimension finie 9
3) Puissances d'un endomorphisme 12
III Réduction et polynômes annulateurs 14
1) Lemme des noyaux 14
2) Diagonalisabilité et polynômes annulateurs 16
3) Trigonalisabilité et polynômes annulateurs 18

Dans tout le chapitre, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$, E un $\mathbb{K}$-espace vectoriel non nul et n un entier naturel non nul.

I Polynômes d'endomorphismes / de matrices

1) Polynômes d'endomorphismes

Notation
Classiquement, on notera la composition des endomorphismes de la façon suivante :

$$\forall u \in \mathcal{L}(E),\ \forall k \in \mathbb{N}, \qquad u^k = \underbrace{u \circ u \circ \cdots \circ u}_{k \text{ fois}},$$

avec la convention $u^0 = Id_E$.

Définition 1 (Valeur d'un polynôme en un endomorphisme)
Soit $P = \sum_{k=0}^{N} a_k X^k \in \mathbb{K}[X]$ et soit $u \in \mathcal{L}(E)$. On appelle **valeur de P en u** *l'endomorphisme :*

$$P(u) = \sum_{k=0}^{N} a_k u^k \in \mathcal{L}(E).$$

ATTENTION !
$P(u)$ étant un endomorphisme $E \to E$, on peut considérer l'image d'un vecteur $x \in E$ par $P(u)$, notée $[P(u)](x)$, ou plus simplement $P(u)(x)$. Ne pas confondre $P(u) \in \mathcal{L}(E)$ et $P(u)(x) \in E$.
Ne jamais écrire $P(u(x))$, cela n'aurait aucun sens !

Propriété 2 (Morphisme d'algèbres d'évaluation)
Pour tout $u \in \mathcal{L}(E)$, l'application $\varphi_u : \mathbb{K}[X] \to \mathcal{L}(E)$ définie par $\varphi_u(P) = P(u)$ est un morphisme de $\mathbb{K}$-algèbres.

Preuve
On sait que $(\mathbb{K}[X], +, \times, .)$ et $(\mathcal{L}(E), +, \circ, .)$ sont deux $\mathbb{K}$-algèbres. De plus, pour $u \in \mathcal{L}(E)$ fixé et $P = \sum_{k=0}^{N} a_k X^k$, $Q = \sum_{k=0}^{M} b_k X^k$ dans $\mathbb{K}[X]$:

- On a $\varphi_u(1) = X^0(u) = u^0 = Id_E$.
- Quitte à ajouter des coefficients nuls, on peut supposer $M = N$, donc pour tout $\lambda \in \mathbb{K}$:

$$\varphi_u(\lambda P + Q) = (\lambda P + Q)(u) = \sum_{k=0}^{N} (\lambda a_k + b_k) u^k = \lambda \sum_{k=0}^{N} a_k u^k + \sum_{k=0}^{N} b_k u^k = \lambda \varphi_u(P) + \varphi_u(Q).$$

- Enfin :

$$\varphi_u(PQ) = (PQ)(u) = \left(\sum_{k=0}^{N} a_k X^k Q \right)(u) = \sum_{k=0}^{N} a_k (X^k Q)(u)$$

(par linéarité de φ_u, que l'on a établi au point précédent). Or, pour tout $k \in \{0, \cdots, N\}$:

$$(X^k Q)(u) = \left(\sum_{l=0}^{N} b_l X^{k+l} \right)(u) = \sum_{l=0}^{N} b_l u^{k+l} = u^k \circ \left(\sum_{l=0}^{N} b_l u^l \right) = u^k \circ Q(u).$$

Donc :

$$(PQ)(u) = \sum_{k=0}^{N} a_k \left(u^k \circ Q(u) \right) = \left(\sum_{k=0}^{N} a_k u^k \right) \circ Q(u) = P(u) \circ Q(u),$$

c'est-à-dire

$$\varphi_u(PQ) = \varphi_u(P) \circ \varphi_u(Q).$$

Remarque (IMPORTANT)
Par ce morphisme d'algèbres, **toute identité polynomiale se transpose aux endomorphismes**.

Exemple
On a $X^3 - 2X + 1 = (X-1)(X^2 + X - 1)$ dans $\mathbb{K}[X]$, donc pour tout $u \in \mathcal{L}(E)$:

$$u^3 - 2u + Id_E = (u - Id_E) \circ (u^2 + u - Id_E) \text{ dans } \mathcal{L}(E).$$

Exemple
Si $P = \prod_{k=1}^{n} (X - \lambda_k) \in \mathbb{K}[X]$, alors pour tout $u \in \mathcal{L}(E)$:

$$P(u) = \prod_{k=1}^{n} (u - \lambda_k Id_E) = (u - \lambda_1 Id_E) \circ \cdots \circ (u - \lambda_n Id_E).$$

Définition 3 (Polynôme en un endomorphisme)
Soit $(u, v) \in \mathcal{L}(E)^2$. On dit que v est un polynôme en u s'il existe $P \in \mathbb{K}[X]$ tel que $v = P(u)$.

Notation
Pour $u \in \mathcal{L}(E)$, on note $\mathbb{K}[u]$ l'ensemble des polynômes en u :

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

Propriété 4 (Structure algébrique des polynômes en u)
Pour $u \in \mathcal{L}(E)$, $\mathbb{K}[u]$ est une sous-algèbre **commutative** *de $\mathcal{L}(E)$.*
De plus, $\mathbb{K}[u]$ est la plus petite sous-algèbre de $\mathcal{L}(E)$ contenant u (au sens de l'inclusion).
On dit que $\mathbb{K}[u]$ est **l'algèbre engendrée par u**.

Preuve
$\mathbb{K}[u]$ est l'image du morphisme d'algèbres $\varphi_u : \mathbb{K}[X] \to \mathcal{L}(E)$ défini par $\varphi_u(P) = P(u)$, donc $\mathbb{K}[u]$ est à la fois un sous-anneau et un sous-espace vectoriel de $\mathcal{L}(E)$, donc une sous-algèbre de $\mathcal{L}(E)$.
$\mathbb{K}[u]$ est commutative car pour tous $P, Q \in \mathbb{K}[X]$:

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

Enfin, si A est une sous-algèbre de $\mathcal{L}(E)$ contenant u, alors par stabilité par $\circ$, A contient u^k pour tout $k \in \mathbb{N}^*$, ainsi que $u^0 = Id_E$ et donc par stabilité par combinaison linéaire, A contient $P(u)$ pour tout $P \in \mathbb{K}[X]$. Donc $\mathbb{K}[u] \subset A$.

Propriété 5 (Sous-espaces stables)
Si $P \in \mathbb{K}[X]$ et $u \in \mathcal{L}(E)$, alors $Ker(P(u))$ et $Im(P(u))$ sont stables par u.
On retrouve en particulier que les sous-espaces propres de u (définis par $E_\lambda(u) = Ker(u - \lambda Id_E)$, où $\lambda \in Sp(u)$) sont stables par u.

Preuve
Cela vient du fait que $P(u)$ commute avec u :

- Si $x \in Ker(P(u))$, alors $P(u)(u(x)) = u(P(u)(x)) = u(0_E) = 0_E$, donc $u(x) \in Ker(P(u))$.
- Si $y \in Im(P(u))$, alors il existe $x \in E$ tel que $y = P(u)(x)$, donc $u(y) = u(P(u)(x)) = P(u)(u(x)) \in Im(P(u))$.

2) Polynômes de matrices

Toutes les notions précédentes se transposent comme d'habitude aux matrices carrées.

Définition 6 (Valeur d'un polynôme en une matrice carrée)
Soit $P = \sum_{k=0}^{N} a_k X^k \in \mathbb{K}[X]$ *et soit* $M \in \mathcal{M}_n(\mathbb{K})$*. On appelle* **valeur de P en M** *la matrice carrée :*

$$P(M) = \sum_{k=0}^{N} a_k M^k \in \mathcal{M}_n(\mathbb{K}).$$

Exemple
La valeur de $P = X^3 - 3X + 1$ en $M \in \mathcal{M}_n(\mathbb{K})$ est $P(M) = M^3 - 3M + I_n$.

Exemple
Calcul de $P(M)$ pour une matrice M diagonale, ou triangulaire supérieure.

Exemple
Calcul de $P(M)$ pour une matrice en blocs $M = \begin{pmatrix} A & * \\ 0 & B \end{pmatrix}$, où A et B sont carrées.

Remarque
Si $u \in \mathcal{L}(E)$ *avec* E *de dimension* $n \in \mathbb{N}^*$ *et si* $\mathcal{B}$ *est une base de* E*, alors en notant* $M = Mat_{\mathcal{B}}(u)$*, on a* $P(M) = Mat_{\mathcal{B}}(P(u))$*.*

Propriété 7 (Morphisme d'algèbres d'évaluation matricielle)
Pour tout $M \in \mathcal{M}_n(\mathbb{K})$*, l'application* $\varphi_M : \mathbb{K}[X] \to \mathcal{M}_n(\mathbb{K})$ *définie par* $\varphi_M(P) = P(M)$ *est un morphisme de* $\mathbb{K}$*-algèbres.*

Preuve
Soit $M \in \mathcal{M}_n(\mathbb{K})$, soit E un $\mathbb{K}$-espace vectoriel de dimension n et $\mathcal{B}$ une quelconque base de E.
On a un isomorphisme de $\mathbb{K}$-algèbres :

$$\psi_{\mathcal{B}} : \left\{ \begin{array}{ccc} \mathcal{L}(E) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ v & \longmapsto & Mat_{\mathcal{B}}(v) \end{array} \right. .$$

Notons $u = \psi_{\mathcal{B}}^{-1}(M)$ l'endomorphisme qui correspond à M.
On a alors $\varphi_M = \psi_{\mathcal{B}} \circ \varphi_u$ (où $\varphi_u : P \mapsto P(u)$ est le morphisme étudié auparavant), puisque pour tout $P \in \mathbb{K}[X]$:

$$(\psi_{\mathcal{B}} \circ \varphi_u)(P) = \psi_{\mathcal{B}}(P(u)) = Mat_{\mathcal{B}}(P(u)) = P(M) = \varphi_M(P).$$

On en déduit le résultat par composition de morphismes d'algèbres.

Définition 8 (Polynôme en une matrice)
Soit $(A, M) \in \mathcal{M}_n(\mathbb{K})^2$*. On dit que* A *est un polynôme en* M *s'il existe* $P \in \mathbb{K}[X]$ *tel que* $A = P(M)$*.*

Notation
Pour $M \in \mathcal{M}_n(\mathbb{K})$, on note $\mathbb{K}[M]$ l'ensemble des polynômes en M :

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

Propriété 9 (Structure algébrique des polynômes en M)
Pour $M \in \mathcal{M}_n(\mathbb{K})$*,* $\mathbb{K}[M]$ *est une sous-algèbre* **commutative** *de* $\mathcal{M}_n(\mathbb{K})$*.*
De plus, $\mathbb{K}[M]$ *est la plus petite sous-algèbre de* $\mathcal{M}_n(\mathbb{K})$ *contenant* M *(au sens de l'inclusion).*
On dit que $\mathbb{K}[M]$ *est* **l'algèbre engendrée par M**.

Preuve
Avec les notations de la preuve précédente :

$$\mathbb{K}[M] = \varphi_M(\mathbb{K}[X]) = \psi_{\mathcal{B}}(\varphi_u(\mathbb{K}[X])) = \psi_{\mathcal{B}}(\mathbb{K}[u]).$$

Ainsi, $\mathbb{K}[M]$ apparaît comme une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$, isomorphe à $\mathbb{K}[u]$. Elle possède donc les mêmes propriétés.

II Polynômes annulateurs, polynôme minimal

1) Définitions et premières propriétés

Définition 10 (Polynôme annulateur d'un endomorphisme, d'une matrice)
On appelle **polynôme annulateur** *de $u \in \mathcal{L}(E)$ (resp. de $M \in \mathcal{M}_n(\mathbb{K})$) tout polynôme $P \in \mathbb{K}[X]$ tel que $P(u) = 0_{\mathcal{L}(E)}$ (resp. $P(M) = 0_{\mathcal{M}_n(\mathbb{K})}$).*

Exemple

- Le polynôme nul annule tout endomorphisme (et toute matrice carrée).
- Pour tout $\lambda \in \mathbb{K}$, le polynôme $X - \lambda$ annule l'endomorphisme λId_E.
- Le polynôme $\prod_{k=1}^{n} (X - \lambda_k)$ est annulateur de la matrice diagonale de $\mathcal{M}_n(\mathbb{K})$ de coefficients diagonaux $(\lambda_1, \cdots, \lambda_n)$, notée $Diag(\lambda_1, \cdots, \lambda_n)$.

Remarque
Si $M = Mat_{\mathcal{B}}(u)$, alors les polynômes annulateurs de u et de M se correspondent :

$$P(u) = 0_{\mathcal{L}(E)} \iff P(M) = 0_{\mathcal{M}_n(\mathbb{K})}.$$

Propriété 11 (Polynômes annulateurs de deux matrices semblables)
Deux matrices semblables de $\mathcal{M}_n(\mathbb{K})$ possèdent les mêmes polynômes annulateurs.

Preuve
Si $B = Q^{-1}AQ$, avec $Q \in GL_n(\mathbb{K})$, alors pour tout entier $k \in \mathbb{N}$, on a $B^k = Q^{-1}A^kQ$, donc par combinaison linéaire, on obtient que

$$\forall P \in \mathbb{K}[X], \qquad P(B) = Q^{-1}P(A)Q,$$

et donc

$$\forall P \in \mathbb{K}[X], \qquad P(A) = 0_{\mathcal{M}_n(\mathbb{K})} \iff P(B) = 0_{\mathcal{M}_n(\mathbb{K})}.$$

Propriété 12 (Structure algébrique des polynômes annulateurs)
Soit $u \in \mathcal{L}(E)$. Alors, l'ensemble des polynômes annulateurs de u est un sous-espace vectoriel et un idéal de $\mathbb{K}[X]$.

Preuve
Notons $I = \{P \in \mathbb{K}[X],\ P(u) = 0_{\mathcal{L}(E)}\}$. Cet ensemble apparaît comme le noyau du morphisme de $\mathbb{K}$-algèbres

$$\varphi_u : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathcal{L}(E) \\ P & \longmapsto & P(u) \end{array} \right. ,$$

donc I est à la fois un sous-espace vectoriel de l'espace vectoriel $\mathbb{K}[X]$ (en tant que noyau d'une application linéaire) et un idéal de l'anneau commutatif $\mathbb{K}[X]$ (en tant que noyau d'un morphisme d'anneaux).

Propriété 13 (Polynôme annulateur et valeur propre)
Soit $u \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$.
Pour tout $x \in E$ et $\lambda \in \mathbb{K}$, $(u(x) = \lambda x \implies P(u)(x) = P(\lambda)x)$.
En particulier, si λ est valeur propre de u, alors $P(\lambda)$ est valeur propre de $P(u)$.

Preuve
Notons $P = \sum_{k=0}^{d} a_k X^k$. Si $u(x) = \lambda x$, alors

$$P(u)(x) = \left(\sum_{k=0}^{d} a_k u^k \right)(x) = \sum_{k=0}^{d} a_k u^k(x).$$

Une récurrence simple montre que pour tout $k \in \mathbb{N}$, $u^k(x) = \lambda^k x$. On en déduit

$$P(u)(x) = \sum_{k=0}^{d} a_k \lambda^k x = \left(\sum_{k=0}^{d} a_k \lambda^k \right) x = P(\lambda)x.$$

En particulier, si x est un vecteur propre de u associé à la valeur propre λ, alors x est un vecteur propre de $P(u)$ associé à la valeur propre $P(\lambda)$.

Théorème 14 (Valeurs propres et racines des polynômes annulateurs)
Soit $u \in \mathcal{L}(E)$. Alors, les valeurs propres de u figurent parmi les racines de tout polynôme annulateur de u, i.e. $(P(u) = 0_{\mathcal{L}(E)} \implies \forall \lambda \in Sp(u),\ P(\lambda) = 0_{\mathbb{K}})$.

Preuve
Si $P(u) = 0_{\mathcal{L}(E)}$ et si $\lambda \in Sp(u)$, alors il existe $x \neq 0_E$ tel que $u(x) = \lambda x$, donc par la proposition précédente $P(\lambda)x = P(u)(x) = 0_{\mathcal{L}(E)}(x) = 0_E$, donc $P(\lambda) = 0$.

<u>ATTENTION !</u>
Il y a seulement une inclusion : des racines d'un polynôme annulateur peuvent ne pas être valeurs propres de u.

Exemple
Un projecteur $p \in \mathcal{L}(E)$ vérifie $p \circ p = p$, donc $Q(X) = X^2 - X$ est annulateur de p, et donc $Sp(p) \subset \{0, 1\}$ mais l'inclusion peut être stricte (par exemple $p = Id_E$ est un projecteur mais son spectre est $\{1\}$, de même pour $p = 0_{\mathcal{L}(E)}$).

Exemple
Si u est nilpotent, alors il existe $p \in \mathbb{N}^*$ tel que X^p est annulateur de u, donc on retrouve ainsi que $Sp(u) \subset \{0\}$. De plus u non injectif (sinon u^p le serait par composition) donc 0 est valeur propre de u, et finalement $Sp(u) = \{0\}$.

Remarque
Tous ces résultats ont évidemment une traduction matricielle.

2) Résultats en dimension finie

Dans cette section, on va examiner ce qui se passe lorsque E est de dimension finie.

Théorème 15 (Théorème de Cayley-Hamilton)
Soit $u \in \mathcal{L}(E)$, avec E de dimension finie $n \in \mathbb{N}^*$. Alors, $\chi_u(u) = 0_{\mathcal{L}(E)}$.

Preuve
On donne deux démonstrations :

- **Version par trigonalisation**
  Fixons une base $\mathcal{B}$ de E et notons $A = Mat_{\mathcal{B}}(u) \in \mathcal{M}_n(\mathbb{K})$. Toute matrice est trigonalisable dans $\mathcal{M}_n(\mathbb{C})$, donc A est semblable dans $\mathcal{M}_n(\mathbb{C})$ à une matrice triangulaire supérieure T, de coefficients diagonaux $(\lambda_1, \cdots, \lambda_n) \in \mathbb{C}^n$, et

  $$\chi_u = \chi_A = \chi_T = \prod_{k=1}^{n} (X - \lambda_k).$$

  Montrons alors que $\chi_u(T) = 0$, cela impliquera $\chi_u(A) = 0$ (puisque deux matrices semblables ont les mêmes polynômes annulateurs), et donc $\chi_u(u) = 0$. On a :

  $$\chi_u(T) = \prod_{k=1}^{n} (T - \lambda_k I_n)$$

(produit commutatif). Calculons le produit de cette matrice avec un vecteur colonne de la base canonique, noté $E_j = (0, \cdots, 0, 1, 0, \cdots, 0)^\top$. Puisque T est triangulaire supérieure, on a

$$(T - \lambda_j I_n)E_j = \sum_{i=1}^{j} t_{i,j} E_i - \lambda_j E_j \in Vect(E_1, \cdots, E_{j-1}),$$

donc par récurrence simple sur j, on obtient

$$\forall k \in [\![1, j]\!], \qquad (T - \lambda_1 I_n) \cdots (T - \lambda_j I_n)E_k = 0_{\mathbb{C}^n}.$$

En effet :

- C'est vrai pour $j = 1$, car $(T - \lambda_1 I_n)E_1 = \lambda_1 E_1 - \lambda_1 E_1 = 0$.
- Soit $j \in [\![1, n-1]\!]$. Si

  $$\forall k \in [\![1, j]\!], \qquad (T - \lambda_1 I_n) \cdots (T - \lambda_j I_n)E_k = 0_{\mathbb{C}^n},$$

  alors par commutativité des polynômes en la matrice T, on a

  $$\forall k \in [\![1, j]\!], \qquad (T - \lambda_1 I_n) \cdots (T - \lambda_j I_n)(T - \lambda_{j+1} I_n)E_k = 0_{\mathbb{C}^n},$$

  mais également

  $$(T - \lambda_1 I_n) \cdots (T - \lambda_j I_n)(T - \lambda_{j+1} I_n)E_{j+1} = 0_{\mathbb{C}^n},$$

  puisque $(T - \lambda_{j+1} I_n)E_{j+1} \in Vect(E_1, \cdots, E_j)$.

Donc finalement avec $j = n$:

$$\forall k \in [\![1, n]\!], \qquad \chi_u(T)E_k = (T - \lambda_1 I_n) \cdots (T - \lambda_n I_n)E_k = 0_{\mathbb{C}^n},$$

c'est-à-dire $\chi_u(T) = 0_{\mathcal{M}_n(\mathbb{K})}$.

- **Version avec les matrices compagnons**
  Soit $x \in E \setminus \{0_E\}$. On va montrer que $\chi_u(u)(x) = 0_E$.
  La famille (x) est libre et E est de dimension finie, donc on peut considérer :

  $$d = \max\{k \in [\![0, n-1]\!],\ (x, u(x), \cdots, u^k(x)) \text{ est libre}\}.$$

  La famille $\mathcal{B}_x = (x, u(x), \cdots, u^d(x))$ est une base du sous-espace vectoriel $F_x = Vect(x, u(x), \cdots, u^d(x))$, et ce sev est stable par u puisque

  $$u(u^d(x)) = u^{d+1}(x) \in Vect(x, u(x), \cdots, u^d(x)),$$

  par maximalité de l'indice d. En notant

  $$u^{d+1}(x) = \sum_{k=0}^{d} a_k u^k(x)$$

  la décomposition de $u^{d+1}(x)$ dans la base $\mathcal{B}_x$, on peut représenter l'endormorphisme induit u_{F_x} par une matrice compagnon :

  $$Mat_{\mathcal{B}_x}(u_{F_x}) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & a_0 \\ 1 & \ddots & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 0 & \vdots \\ 0 & \cdots & \cdots & 1 & a_d \end{pmatrix} \in \mathcal{M}_{d+1}(\mathbb{K}).$$

  On sait calculer le polynôme caractéristique d'une telle matrice, donc

  $$\chi_{u_{F_x}}(X) = X^{d+1} - \sum_{k=0}^{d} a_k X^k.$$

On remarque que $(\chi_{u_{F_x}}(u))(x) = 0_E$. Mais $\chi_{u_{F_x}}$ divise χ_u dans $\mathbb{K}[X]$ (c'est une propriété des endomorphismes induits, déjà vue dans le chapitre 8), donc il existe $Q \in \mathbb{K}[X]$ tel que

$$\chi_u(X) = Q(X)\chi_{u_{F_x}}(X).$$

Finalement :

$$\chi_u(u) = Q(u) \circ \chi_{u_{F_x}}(u),$$

et donc

$$\chi_u(u)(x) = Q(u)\left(\chi_{u_{F_x}}(u)(x)\right) = Q(u)(0_E) = 0_E,$$

par linéarité de $Q(u)$. Ainsi, $\chi_u(u)$ est l'endomorphisme nul.

Remarque

- *Ainsi, le polynôme caractéristique de u est toujours annulateur de u.*
- *Version matricielle : pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$, $\chi_A(A) = 0_{\mathcal{M}_n(\mathbb{K})}$.*

Théorème 16 (Existence et unicité du polynôme minimal)
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.
Pour tout $u \in \mathcal{L}(E)$, il existe un unique polynôme $\pi_u \in \mathbb{K}[X]$ vérifiant :

(i) π_u est annulateur de u ;

(ii) π_u est unitaire ;

(iii) $\forall P \in \mathbb{K}[X]$, $(P(u) = 0_{\mathcal{L}(E)} \implies \pi_u$ divise $P)$.

Ce polynôme π_u est appelé **polynôme minimal** *de l'endomorphime u.*

Preuve
Fixons $u \in \mathcal{L}(E)$ et posons $I = \{P \in \mathbb{K}[X],\ P(u) = 0_{\mathcal{L}(E)}\}$. On a déjà montré que I est un idéal de $\mathbb{K}[X]$, et il est non nul, puisque $\chi_u \in I$ (par le théorème de Cayley-Hamilton) et $\deg(\chi_u) = n \geq 1$. Or, on sait que tout idéal non nul de $\mathbb{K}[X]$ possède un unique générateur unitaire (voir le chapitre 1 sur les structures algébriques). Il existe donc un unique $\pi_u \in \mathbb{K}[X]$ tel que π_u unitaire et $I = \pi_u\mathbb{K}[X]$, ce qui signifie que les éléments de I sont les polynômes P multiples de π_u dans $\mathbb{K}[X]$.

Remarque

- *Cet énoncé se transpose aux matrices $A \in \mathcal{M}_n(\mathbb{K})$, et on peut définir le polynôme minimal π_A.*
- *Le polynôme minimal de u (resp. A) est donc le polynôme non nul unitaire de plus petit degré qui annule u (resp. A).*
- *π_u (resp. π_A) est non constant.*
- *π_u divise χ_u puisque χ_u annule u (cf. théorème de Cayley-Hamilton).*

Exemple
Le polynôme minimal de λId_E est $X - \lambda$, pour tout $\lambda \in \mathbb{K}$.

Exemple
Si p est un projecteur différent de $0_{\mathcal{L}(E)}$ et de Id_E, alors $\pi_p = X(X-1)$.

Exemple
Le polynôme minimal de $A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix}$ est $\pi_A = (X-2)(X-3)$.
On peut donc avoir $\pi_A = \chi_A$.

Exemple
Le polynôme minimal de $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ est $\pi_A = (X-1)(X-2)$.
On peut donc avoir $\pi_A \neq \chi_A$.

Propriété 17 (Valeurs propres et polynôme minimal)
Soit $u \in \mathcal{L}(E)$, avec E de dimension finie $n \in \mathbb{N}^*$. Les valeurs propres de u sont exactement les racines dans $\mathbb{K}$ de son polynome minimal π_u.

Preuve
Puisque $\pi_u(u) = 0_{\mathcal{L}(E)}$, on a déjà $Sp(u)$ inclus dans les racines de π_u (par le th. 14). Réciproquement si $\lambda \in \mathbb{K}$ est racine de π_u, alors λ est racine de χ_u (qui est multiple de π_u), donc λ est valeur propre de u.

Remarque

- *Ainsi, le polynôme minimal n'a pas de racines "de trop", seulement les valeurs propres de u.*
- *Cet énoncé a bien entendu une version matricielle.*

<u>ATTENTION !</u>
Ainsi, on a $\prod_{\lambda \in Sp(u)} (X - \lambda)$ divise π_u, mais il n'y a pas toujours égalité !
(π_u n'est pas toujours scindé à racines simples).

3) Puissances d'un endomorphisme

E désigne toujours un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.

Méthode
On peut calculer les puissances d'un endomorphisme $u \in \mathcal{L}(E)$ (ou d'une matrice carrée A) directement à partir de son polynôme minimal, par division euclidienne.

Exemple
Calcul de A^n avec $A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix}$.
Le polynôme minimal de A est $\pi_A = (X-2)(X-3)$.
On a par division euclidienne :

$$\forall n \in \mathbb{N}, \qquad X^n = \pi_A(X)Q_n(X) + a_n X + b_n,$$

avec $Q_n \in \mathbb{R}[X]$, $(a_n, b_n) \in \mathbb{R}^2$ uniques.
En évaluant en $X = 2$ et $X = 3$ (les racines de π_A), on obtient les coefficients :

$$a_n = 3^n - 2^n, \qquad b_n = 3 \times 2^n - 2 \times 3^n.$$

En prenant la valeur en la matrice A, on obtient :

$$\forall n \in \mathbb{N}, \qquad A^n = \pi_A(A)Q_n(A) + a_n A + b_n I_2 = a_n A + b_n I_2.$$

Donc finalement

$$\forall n \in \mathbb{N}, \qquad A^n = (3^n - 2^n)A + (3 \times 2^n - 2 \times 3^n)I_2.$$

Remarque
Cela fonctionne avec n'importe quel polynôme annulateur de u (par exemple χ_u) mais il est plus efficace de travailler avec π_u, qui est de degré minimal.

Plus généralement, on dispose du résultat suivant :

Propriété 18 (Base des polynômes en u)
Soit $u \in \mathcal{L}(E)$, avec E de dimension finie $n \in \mathbb{N}^*$. Si $d = \deg(\pi_u)$, alors la famille $(u^k)_{0 \leq k \leq d-1}$ est une base de $\mathbb{K}[u]$. En particulier $\dim(\mathbb{K}[u]) = d \leq n = \dim(E)$.

Preuve
Notons $\pi_u = \sum_{k=0}^{d} a_k X^k$, avec $d \in \mathbb{N}^*$, les $a_i \in \mathbb{K}$ et $a_d \neq 0$.
La famille $(Id, u, \cdots, u^{d-1})$ est libre dans le sev $\mathbb{K}[u]$ car

$$\sum_{k=0}^{d-1} \lambda_k u^k = 0 \implies \sum_{k=0}^{d-1} \lambda_k X^k \text{ annule } u \implies \pi_u \text{ divise } \sum_{k=0}^{d-1} \lambda_k X^k.$$

Mais $\deg(\pi_u) = d$, donc

$$\sum_{k=0}^{d-1} \lambda_k u^k = 0 \implies \sum_{k=0}^{d-1} \lambda_k X^k = 0 \implies \lambda_0 = \cdots = \lambda_{d-1} = 0.$$

Enfin, la famille $(Id, u, \cdots, u^{d-1})$ est génératrice de $\mathbb{K}[u]$ pour tout $P \in \mathbb{K}[X]$, il existe $(Q, R) \in \mathbb{K}[X]^2$ tel que $P = \pi_u Q + R$ avec $\deg(R) < \deg(\pi_u) = d$, donc en évaluant en u :

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

Remarque
Même chose pour $\mathbb{K}[A]$, où A est une matrice carrée.

III Réduction et polynômes annulateurs

1) Lemme des noyaux

Théorème 19 (Lemme de décomposition des noyaux)
Si $P_1, \cdots, P_m \in \mathbb{K}[X]$ sont premiers entre eux deux à deux, alors pour tout $u \in \mathcal{L}(E)$:

$$Ker\left(\left(\prod_{k=1}^{m} P_k\right)(u)\right) = \bigoplus_{k=1}^{m} Ker(P_k(u)).$$

Preuve
Par récurrence sur le nombre de polynômes $m \geq 2$:

- $\boxed{\text{Initialisation : cas } m = 2}$
  Supposons $pgcd(P_1, P_2) = 1$. Alors par le théorème de Bézout, il existe $V_1, V_2 \in \mathbb{K}[X]$ tels que

  $$P_1V_1 + P_2V_2 = 1.$$

  En évaluant cette identité polynomiale en l'endomorphisme u on obtient :

  $$P_1(u) \circ V_1(u) + P_2(u) \circ V_2(u) = Id_E.$$

  * <u>Montrons que $Ker(P_1(u)) \cap Ker(P_2(u)) = \{0_E\}$</u> : si $x \in Ker(P_1(u)) \cap Ker(P_2(u))$, alors

    $$x = Id_E(x) = (P_1(u) \circ V_1(u) + P_2(u) \circ V_2(u))(x) = V_1(u)(\underbrace{P_1(u)(x)}_{=0_E}) + V_2(u)(\underbrace{P_2(u)(x)}_{=0_E}) = 0_E.$$

    (puisque $K[u]$ est commutative). La somme $Ker(P_1(u)) + Ker(P_2(u))$ est donc directe.
  * <u>Montrons que $Ker(P_1(u)) \oplus Ker(P_2(u)) \subset Ker((P_1P_2)(u))$</u> : si $x \in Ker(P_1(u))$, alors

    $$((P_1P_2)(u))(x) = ((P_2P_1)(u))(x) = P_2(u)(\underbrace{P_1(u)(x)}_{=0_E}) = 0_E,$$

    donc $Ker(P_1(u)) \subset Ker((P_1P_2)(u))$. De même, on a $Ker(P_2(u)) \subset Ker((P_1P_2)(u))$ donc $Ker(P_1(u)) \oplus Ker(P_2(u)) \subset Ker((P_1P_2)(u))$.
  * <u>Montrons que $Ker((P_1P_2)(u)) \subset Ker(P_1(u)) \oplus Ker(P_2(u))$</u> : si $x \in Ker((P_1P_2)(u))$, alors

    $$x = Id_E(x) = (P_1(u) \circ V_1(u))(x) + (P_2(u) \circ V_2(u))(x).$$

    En notant $a = (P_2(u) \circ V_2(u))(x)$ et $b = (P_1(u) \circ V_1(u))(x)$, on a donc $x = a + b$, avec $a \in Ker(P_1(u))$ et $b \in Ker(P_2(u))$ puisque

    $$P_1(u)(a) = (P_1(u) \circ P_2(u) \circ V_2(u))(x) = V_2(u)\left(\underbrace{(P_1P_2)(u)(x)}_{=0_E}\right) = 0_E,$$

    $$P_2(u)(b) = (P_2(u) \circ P_1(u) \circ V_1(u))(x) = V_1(u)\left(\underbrace{(P_1P_2)(u)(x)}_{=0_E}\right) = 0_E.$$

- $\boxed{\text{Hérédité}}$
  Supposons le résultat vrai pour $m \geq 2$ polynômes $P_1, \cdots, P_m$ et montrons-le au rang suivant : si $P_1, \cdots, P_{m+1}$ sont premiers entre eux deux à deux dans $\mathbb{K}[X]$, alors on a $pgcd((P_1 \cdots P_m), P_{m+1}) = 1$, donc par le cas $m = 2$:

  $$Ker((P_1 \cdots P_{m+1})(u)) = Ker((P_1 \cdots P_m)(u)) \oplus Ker(P_{m+1}(u)).$$

  Or par hypothèse de récurrence :

  $$Ker((P_1 \cdots P_m)(u)) = \bigoplus_{k=1}^{m} Ker(P_k(u))$$

donc

$$Ker((P_1 \cdots P_{m+1})(u)) = \left(\bigoplus_{k=1}^{m} Ker(P_k(u))\right) \oplus Ker(P_{m+1}(u)) = \bigoplus_{k=1}^{m+1} Ker(P_k(u)).$$

Exemple (Cas important)
Si $\lambda_1, \cdots, \lambda_m$ sont des scalaires de $\mathbb{K}$ deux à deux distincts, alors pour tous entiers non nuls $(\alpha_k)_{1\leq k\leq m}$, les polynômes $((X-\lambda_k)^{\alpha_k})_{1\leq k\leq m}$ sont premiers entre eux deux à deux dans $\mathbb{K}[X]$ (car ils n'ont pas de racines complexes en commun). Donc pour tout $u \in \mathcal{L}(E)$:

$$Ker\left((u-\lambda_1 Id_E)^{\alpha_1} \circ \cdots \circ (u-\lambda_m Id_E)^{\alpha_m}\right) = Ker((u-\lambda_1 Id_E)^{\alpha_1}) \oplus \cdots \oplus Ker((u-\lambda_m Id_E)^{\alpha_m}).$$

Remarque (Cas d'un polynôme annulateur)
Si $P = P_1 \cdots P_m \in \mathbb{K}[X]$ vérifie $P(u) = 0_{\mathcal{L}(E)}$ et les P_k premiers entre eux deux à deux, alors en appliquant le lemme des noyaux, on obtient une décomposition de l'espace en **somme directe de sous-espaces stables par u** *:*

$$E = \bigoplus_{k=1}^{m} Ker(P_k(u)),$$

puisque $Ker((P_1 \cdots P_m)(u)) = Ker(P(u)) = Ker(0_{\mathcal{L}(E)}) = E$.
Si de plus E est de dimension finie, alors dans toute base adaptée à une telle décomposition, la matrice de u est donc **diagonale par blocs** *:*

$$Mat_{\mathcal{B}}(u) = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_m \end{pmatrix},$$

où chaque bloc A_k (de taille $\dim(Ker(P_k(u)))$) est la matrice de l'endomorphisme induit $u_{Ker(P_k(u))}$ dans la base de $Ker(P_k(u))$ choisie.

Exemple (Projecteurs et symétries)
Si $p \in \mathcal{L}(E)$ vérifie $p \circ p = p$, alors le polynôme $Q = X^2 - X$ est annulateur de p, donc $Ker(Q(p)) = Ker(0_{\mathcal{L}(E)}) = E$. En outre, $Q = X(X-1)$ avec X et $X-1$ premiers entre eux, donc par le lemme des noyaux, on retrouve la décomposition bien connue :

$$E = Ker(p) \oplus Ker(p - Id_E).$$

De même si $s \circ s = Id_E$, on a $X^2 - 1 = (X-1)(X+1)$ qui est annulateur de s avec $X-1$ et $X+1$ premiers entre eux, donc

$$E = Ker(s - Id_E) \oplus Ker(s + Id_E).$$

Corollaire 20 (Version matricielle du lemme des noyaux)
Si $P_1, \cdots, P_m \in \mathbb{K}[X]$ sont premiers entre eux deux à deux, alors pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$:

$$Ker\left(\left(\prod_{k=1}^{m} P_k\right)(A)\right) = \bigoplus_{k=1}^{m} Ker(P_k(A)).$$

Preuve
Evident vu que pour tout $Q \in \mathbb{K}[X]$ et pour toute base $\mathcal{B}$ de E, on a

$$Mat_{\mathcal{B}}(Q(u)) = Q\left(Mat_{\mathcal{B}}(u)\right).$$

2) Diagonalisabilité et polynômes annulateurs

Théorème 21 (CNS de diagonalisabilité)
Soit $u \in \mathcal{L}(E)$ avec E de dimension finie.
Alors, il y a équivalence entre :

(i) *u est diagonalisable ;*

(ii) *Il existe un polynôme $P \in \mathbb{K}[X]$ scindé à racines simples sur $\mathbb{K}$ qui est annulateur de u ;*

(iii) *Le polynôme minimal π_u est scindé à racines simples sur $\mathbb{K}$*

Dans ce cas, le polynôme minimal de u est

$$\pi_u = \prod_{\lambda \in Sp(u)} (X - \lambda).$$

Remarque
Ce résultat se transpose aux matrices carrées.

Preuve
Notons $\lambda_1, \cdots, \lambda_m$ les valeurs propres distinctes de l'endomorphisme u.

$\boxed{(i) \implies (ii)}$ Si u est diagonalisable, alors $E = \oplus_{k=1}^m E_{\lambda_k}(u)$ (les sous-espaces propres sont supplémentaires dans E). Montrons alors que le polynôme $P = \prod_{k=1}^m (X - \lambda_k)$ est annulateur de u : si $x \in E_{\lambda_k}(u)$, alors $(u - \lambda_k Id_E)(x) = 0_E$, donc par commutativité de $\mathbb{K}[u]$:

$$P(u)(x) = (u - \lambda_1 Id_E) \circ \cdots \circ (u - \lambda_m Id_E)(x) = \left(\prod_{j \neq k} (u - \lambda_j Id_E) \right) \circ (u - \lambda_k Id_E)(x) = 0_E.$$

Donc $P(u)$ s'annule sur $E_{\lambda_k}(u)$ pour tout $k \in [\![1, m]\!]$. On en déduit par linéarité que $P(u)$ s'annule sur $\oplus_{k=1}^m E_{\lambda_k}(u) = E$, c'est-à-dire $P(u) = 0_{\mathcal{L}(E)}$.

$\boxed{(ii) \implies (iii)}$ S'il existe P scindé à racines simples annulateur de u, alors le polynôme minimal π_u divise P dans $\mathbb{K}[X]$, donc π_u est lui-même scindé à racines simples.

$\boxed{(iii) \implies (i)}$ Si π_u est scindé à racines simples, alors puisque les racines de π_u sont exactement les valeurs propres de u, on a $\pi_u = \prod_{k=1}^m (X - \lambda_k)$, ce qui entraîne par le lemme de décomposition des noyaux que

$$E = Ker(\underbrace{\pi_u(u)}_{0_{\mathcal{L}(E)}}) = \bigoplus_{k=1}^m Ker(u - \lambda_k Id_E) = \bigoplus_{k=1}^m E_{\lambda_k}(u).$$

Ainsi, les sous-espaces propres de u sont supplémentaires dans E, donc u est diagonalisable.

Remarque
On retrouve ainsi que tout projecteur de E est diagonalisable (puisqu'il est annulé par le polynôme $X^2 - X = X(X-1)$), ainsi que toute symétrie (qui est annulée par $X^2 - 1 = (X-1)(X+1)$).

Lemme 22 (Endomorphisme induit par $P(u)$)
Si F est un sous-espace vectoriel de E stable par $u \in \mathcal{L}(E)$, alors pour tout $P \in \mathbb{K}[X]$, F est stable par $P(u)$ et $P(u)_F = P(u_F)$.

Preuve
Puisque F est stable par u, alors F est stable par u^k pour tout $k \in \mathbb{N}$ (par récurrence triviale) et pour tout $x \in F$:

$$(u^k)_F(x) = u^k(x) = u_F^k(x).$$

Par combinaison linéaire, on en déduit le résultat.

Propriété 23 (Polynôme minimal d'un endomorphisme induit)
Soit $u \in \mathcal{L}(E)$, avec E de dimension finie.
Si F est un sev non nul de E stable par u, alors le polynôme minimal de u_F (l'endomorphisme induit) divise le polynôme minimal de u.

Preuve
D'après le lemme précédent, $\pi_u(u_F) = (\pi_u(u))_F = 0_{\mathcal{L}(F)}$, donc π_u est annulateur de u_F, ce qui entraîne que π_u est multiple de π_{u_F} dans $\mathbb{K}[X]$.

Théorème 24 (Diagonalisabilité d'un endomorphisme induit)
Soit $u \in \mathcal{L}(E)$, avec E de dimension finie. Si u est diagonalisable et si F est un sev non nul de E stable par u, alors l'endomorphisme induit u_F est diagonalisable.

Preuve
D'après le théorème 21, π_u est scindé à racines simples, donc π_{u_F} l'est aussi (car il divise π_u d'après la prop. 23). On en conclut (toujours par le théorème 21) que u_F est diagonalisable.

<u>ATTENTION !</u>
Bien entendu, la réciproque est fausse. Un endomorphisme induit u_F peut être diagonalisable sans que u ne le soit. Par exemple, si u n'est pas diagonalisable et si $\lambda \in Sp(u)$, alors $u_{E_\lambda(u)} = \lambda Id_{E_\lambda(u)}$ est diagonalisable.

Corollaire 25 (Propriétés des sev stables par un endomorphisme diagonalisable)
Soit $u \in \mathcal{L}(E)$ diagonalisable (avec E de dimension finie), et soit F un sev de E non nul. Alors F est stable par u si et seulement si F possède une base formée de vecteurs propres de u.

Preuve

$\boxed{\Longrightarrow}$ Si F est stable par u, alors u_F est diagonalisable (puisque u l'est) donc F possède une base formée de vecteurs propres pour u_F, qui sont également des vecteurs propres pour u.

$\boxed{\Longleftarrow}$ Si $(e_1, \cdots, e_d)$ est une base de F formée de vecteurs propres pour u, alors chaque droite $Vect(e_i)$ est stable par u, donc $F = Vect(e_1, \cdots, e_d)$ est stable par u.

Exemple
Déterminer les sous-espaces vectoriels de $\mathbb{R}^3$ stables par la matrice $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$
(c'est-à-dire stables par l'endomorphisme canoniquement associé à A).

Tout d'abord, A est diagonalisable, avec $Sp(A) = \{0, 3\}$ et

$$E_0(A) = Vect((1, -1, 0), (1, 0, -1)), \qquad E_3(A) = Vect(1, 1, 1).$$

Donc d'après le corollaire précédent, les sous-espaces stables par A sont ceux possédant une base de vecteurs propres de A.
Recherchons les sous-espaces stables par A par dimension.

- Le seul sous-espace stable de dimension 0 est $\{0\}$.
- Les droites stables par A sont les droites engendrées par des vecteurs propres (d'après un résultat du chapitre 8). Il s'agit donc de

$$\mathcal{D} = E_3(A) = Vect(1, 1, 1),$$

ainsi que la famille des droites incluses dans $E_0(A)$:

$$\mathcal{D}_{a,b} = Vect(a, b, -a - b), \qquad (a, b) \in \mathbb{R}^2 \setminus \{(0, 0)\}$$

- Les plans stables par A sont les plans $\mathcal{P} = Vect(u, v)$, où (u, v) est une famille libre de vecteurs propres de A. Selon que u, v soient dans $E_0(A)$ ou dans $E_3(A)$, on obtient les plans

$$\mathcal{P} = E_0(A) = Vect((1, -1, 0), (1, 0, -1)),$$

$$\mathcal{P}_{a,b} = Vect((1, 1, 1), (a, b, -a - b)), \qquad (a, b) \in \mathbb{R}^2 \setminus \{(0, 0)\}.$$

- Le seul sous-espace stable de dimension 3 est $\mathbb{R}^3$.

3) Trigonalisabilité et polynômes annulateurs

Dans la suite, on fixe E un $\mathbb{K}$-espace vectoriel de dimension finie, et $u \in \mathcal{L}(E)$.

Théorème 26 (CNS de trigonalisabilité)
Il y a équivalence entre :

(i) *u est trigonalisable ;*

(ii) *Il existe un polynôme $P \in \mathbb{K}[X]$ scindé sur $\mathbb{K}$ qui est annulateur de u ;*

(iii) *Le polynôme minimal π_u est scindé sur $\mathbb{K}$.*

(iv) *Le polynôme caractéristique χ_u est scindé sur $\mathbb{K}$.*

Remarque
Ce résultat se transpose aux matrices carrées.

Preuve

$\boxed{(i) \implies (ii)}$ Si u est trigonalisable, alors le polynôme caractéristique χ_u est scindé sur $\mathbb{K}$ (d'après le chapitre 8), et annulateur de u (théorème de Cayley-Hamilton).

$\boxed{(ii) \implies (iii)}$ S'il existe P scindé annulateur de u, alors le polynôme minimal π_u divise P dans $\mathbb{K}[X]$, donc π_u est lui-même scindé sur $\mathbb{K}$.

$\boxed{(iii) \implies (iv)}$ Si π_u est scindé sur $\mathbb{K}$, alors on a

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

avec $\lambda_1, \cdots, \lambda_m \in \mathbb{K}$ les valeurs propres distinctes de u, et les $\beta_k \in \mathbb{N}^*$.
Montrons alors que χ_u est également scindé sur $\mathbb{K}$. Pour cela, on représente u par une matrice $A \in \mathcal{M}_n(\mathbb{K})$, qu'on plonge dans $\mathcal{M}_n(\mathbb{C})$. Puisque π_u est annulateur de u, il est annulateur de A (en tant qu'élément de $\mathbb{C}[X]$), donc toutes les valeurs propres **complexes** de A sont racines de π_u, ce qui montre que $Sp_{\mathbb{C}}(A) \subset \{\lambda_1, \cdots, \lambda_m\} \subset \mathbb{K}$, et donc $\chi_u = \chi_A$ est scindé sur $\mathbb{K}$, et il est multiple de π_u dans $\mathbb{K}[X]$, donc $Sp_{\mathbb{C}}(A) = Sp_{\mathbb{K}}(A) = \{\lambda_1, \cdots, \lambda_m\}$ et

$$\chi_u = \prod_{k=1}^{m} (X - \lambda_k)^{\alpha_k}, \qquad 1 \leq \beta_k \leq \alpha_k.$$

$\boxed{(iv) \implies (i)}$ C'est le théorème de trigonalisation vu dans le CH.8.

Corollaire 27 (Trigonalisabilité d'un endomorphisme induit)
Si u est trigonalisable et si F est un sev non nul de E stable par u, alors l'endomorphisme induit u_F est trigonalisable.

Preuve
D'après le théorème 26, π_u est scindé, donc π_{u_F} l'est aussi (car il divise π_u d'après la prop. 23). On en conclut (toujours par le théorème 26) que u_F est trigonalisable.

Le théorème précédent ne dit pas **comment** trigonaliser explicitement. On dispose d'outils plus précis.

Définition 28 (Sous-espaces caractéristiques)
On suppose χ_u scindé sur $\mathbb{K}$.
Si $\lambda \in \mathbb{K}$ est une valeur propre de u, de multiplicité $\alpha_\lambda \in \mathbb{N}^*$, alors on appelle **sous-espace caractéristique de u associé à λ** *le sous-espace vectoriel*

$$N_\lambda(u) = Ker((u - \lambda Id_E)^{\alpha_\lambda}).$$

Ce sev est stable par u (car de la forme $Ker(P(u))$ avec $P \in \mathbb{K}[X]$).

Théorème 29 (Propriétés des sous-espaces caractéristiques)
Avec les notations précédentes, on a

(i) *Les sous-espaces caractéristiques sont supplémentaires dans E :*

$$E = \bigoplus_{\lambda \in Sp(u)} N_\lambda(u).$$

(ii) *Leur dimension est la multiplicité de la valeur propre correspondante :*

$$\forall \lambda \in Sp(u), \qquad \dim(N_\lambda(u)) = \alpha_\lambda.$$

(iii) *On peut les voir de deux manières :*

$$\forall \lambda \in Sp(u), \qquad N_\lambda(u) = Ker((u - \lambda Id_E)^{\alpha_\lambda}) = Ker((u - \lambda Id_E)^{\beta_\lambda}),$$

où β_λ est la multiplicité de la racine λ dans le polynôme minimal π_u (alors que α_λ est celle dans le polynôme caractéristique χ_u).

Preuve

(i) Puisque χ_u est scindé sur $\mathbb{K}$, on a

$$\chi_u(X) = \prod_{\lambda \in Sp(u)} (X - \lambda)^{\alpha_\lambda},$$

donc par le lemme des noyaux et le théorème de Cayley-Hamilton :

$$E = Ker(\chi_u(u)) = \bigoplus_{\lambda \in Sp(u)} Ker((u - \lambda Id_E)^{\alpha_\lambda}) = \bigoplus_{\lambda \in Sp(u)} N_\lambda(u).$$

(ii) Soit $\lambda \in Sp(u)$. Notons u_λ l'endomorphisme induit $u_{N_\lambda(u)}$ (qui est bien défini car $N_\lambda(u)$ est stable par u). On a, pour tout $x \in N_\lambda(u)$:

$$(u - \lambda Id_E)^{\alpha_\lambda}(x) = 0_E,$$

c'est-à-dire (d'après le lemme 22)

$$(u_\lambda - \lambda Id_{N_\lambda(u)})^{\alpha_\lambda}(x) = 0_E.$$

Ainsi, l'endomorphisme induit $u_\lambda - \lambda Id_{N_\lambda(u)} = n_\lambda$ est nilpotent. Il existe donc une base $\mathcal{B}_\lambda$ de $N_\lambda(u)$ telle que $Mat_{\mathcal{B}_\lambda}(n_\lambda)$ est triangulaire supérieure avec des 0 sur la diagonale, et donc $Mat_{\mathcal{B}_\lambda}(u_\lambda)$ est triangulaire supérieure avec λ sur toute la diagonale. On en déduit que

$$\chi_{u_\lambda}(X) = (X - \lambda)^{\dim(N_\lambda(u))}.$$

Mais χ_{u_λ} divise χ_u, donc $\dim(N_\lambda(u)) \leq \alpha_\lambda$.
Enfin, par supplémentarité des $N_\lambda(u)$ dans E, on a

$$\sum_{\lambda \in Sp(u)} \underbrace{(\alpha_\lambda - \dim(N_\lambda(u)))}_{\geq 0} = \sum_{\lambda \in Sp(u)} \alpha_\lambda - \sum_{\lambda \in Sp(u)} \dim(N_\lambda(u))) = \deg(\chi_u) - \dim(E) = 0,$$

donc $\alpha_\lambda - \dim(N_\lambda(u)) = 0$ pour tout $\lambda \in Sp(u)$ (somme nulle de termes positifs).

(iii) Puisque χ_u est scindé sur $\mathbb{K}$, π_u aussi. On le note :

$$\pi_u(X) = \prod_{\lambda \in Sp(u)} (X-\lambda)^{\beta_\lambda},$$

avec les $\beta_\lambda \in \mathbb{N}^*$. En appliquant encore le lemme des noyaux, cette fois avec π_u, on obtient :

$$E = Ker(\pi_u(u)) = \bigoplus_{\lambda \in Sp(u)} Ker((u-\lambda Id_E)^{\beta_\lambda}).$$

On a donc

$$\bigoplus_{\lambda \in Sp(u)} Ker((u-\lambda Id_E)^{\beta_\lambda}) = \bigoplus_{\lambda \in Sp(u)} Ker((u-\lambda Id_E)^{\alpha_\lambda}) = E.$$

Mais pour tout $\lambda \in Sp(u)$, on a $1 \leq \beta_\lambda \leq \alpha_\lambda$, donc $Ker((u-\lambda Id_E)^{\beta_\lambda}) \subset Ker((u-\lambda Id_E)^{\alpha_\lambda})$. En sommant les dimensions, on obtient

$$\sum_{\lambda \in Sp(u)} \underbrace{\left(\dim Ker((u-\lambda Id_E)^{\alpha_\lambda}) - \dim Ker((u-\lambda Id_E)^{\beta_\lambda})\right)}_{\geq 0} = \dim(E) - \dim(E) = 0,$$

donc (somme nulle de nombres positifs) :

$$\forall \lambda \in Sp(u), \qquad \dim Ker((u-\lambda Id_E)^{\alpha_\lambda}) - \dim Ker((u-\lambda Id_E)^{\beta_\lambda}) = 0.$$

On en déduit les égalités voulues.

Remarque

- *Pour chaque valeur propre λ, l'entier β_λ est l'indice de nilpotence de l'induit*

$$n_\lambda = u_{N_\lambda(u)} - \lambda Id_{N_\lambda(u)}.$$

En effet, puisque $N_\lambda(u) = Ker((u-\lambda Id_E)^{\beta_\lambda})$, on a $n_\lambda^{\beta_\lambda} = 0_{\mathcal{L}(N_{\lambda(u)})}$ d'une part, et d'autre part, $n_\lambda^{\beta_\lambda - 1} \neq 0_{\mathcal{L}(N_{\lambda(u)})}$, sinon on aurait $Ker(n_\lambda^{\beta_\lambda-1}) = N_\lambda(u)$, et par le lemme des noyaux, le polynôme non nul $Q(X) = \frac{\pi_u(X)}{X-\lambda}$ annulerait u (étant donné que $Ker(Q(u)) = \bigoplus_{\lambda \in Sp(u)} N_\lambda(u) = E$) , ce qui est impossible (car $\deg(Q) < \deg(\pi_u)$).

- *u est diagonalisable* $\iff \forall \lambda \in Sp(u),\ \beta_\lambda = 1 \iff \forall \lambda \in Sp(u),\ N_\lambda(u) = E_\lambda(u)$.

Théorème 30 (Réduction diagonale par blocs)
Si χ_u est scindé sur $\mathbb{K}$, de valeurs propres distinctes $\lambda_1, \cdots, \lambda_m$, alors il existe une base de E dans laquelle $Mat_{\mathcal{B}}(u)$ est diagonale par blocs :

$$Mat_{\mathcal{B}}(u) = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_m \end{pmatrix},$$

chaque bloc diagonal étant de la forme

$$A_i = \begin{pmatrix} \lambda_i & * & \cdots & * & * \\ 0 & \lambda_i & * & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \lambda_i & * \\ 0 & 0 & \cdots & 0 & \lambda_i \end{pmatrix} \in \mathcal{M}_{\alpha_i}(\mathbb{K}),$$

où α_i est la multiplicité de la valeur propre λ_i.

Remarque
Cette réduction est une trigonalisation améliorée (puisque chaque bloc diagonal A_i est triangulaire supérieur, la matrice $Mat_{\mathcal{B}}(u)$ est triangulaire supérieure).

Preuve
En reprenant les notations de la preuve précédente, on a la décomposition en sous-espaces stables :

$$E = \bigoplus_{\lambda \in Sp(u)} N_\lambda(u),$$

et chaque endomorphisme induit $u_\lambda = u_{N_\lambda(u)}$ est la somme d'une homothétie et d'un endomorphisme nilpotent :

$$u_\lambda = \lambda Id_{N_\lambda(u)} + n_\lambda,$$

où n_λ est d'indice de nilpotence β_λ (la multiplicité de la racine λ dans le polynôme minimal π_u). Puisque tout endomorphisme nilpotent est trigonalisable avec seule valeur propre 0 (cf. CH.8), on en déduit que pour tout $\lambda \in Sp(u)$, il existe une base $\mathcal{B}_\lambda$ de $N_\lambda(u)$ dans laquelle la matrice de n_λ est triangulaire supérieure avec des 0 sur la diagonale. Donc $Mat_{\mathcal{B}_\lambda}(u_\lambda)$ est triangulaire supérieure avec éléments diagonaux égaux à λ. En concaténant de telles bases des sous-espaces caractéristiques, on obtient une base $\mathcal{B}$ de E dans laquelle la matrice de u a la forme voulue.

Corollaire 31 (Réduction matricielle diagonale par blocs)
Soit $A \in \mathcal{M}_n(\mathbb{K})$ avec $n \in \mathbb{N}^*$. Si χ_A est scindé sur $\mathbb{K}$ alors A est semblable à une matrice diagonale par blocs, où chaque bloc diagonal est de la forme $\lambda I + N$ avec $\lambda \in Sp(A)$ et N triangulaire supérieure avec des zéros sur la diagonale (donc nilpotente).

Preuve
C'est directement la traduction matricielle du théorème précédent.

<u>ATTENTION !</u>
Toute matrice trigonalisable est donc semblable à une matrice **diagonale par blocs**, pas "diagonale tout court !".