# Réduction des endomorphismes

## Trigonalisation. Théorème de Cayley-Hamilton.

### 3. Trigonalisation

Il s'agit d'une version moins exigeante de la réduction des endomorphismes.

**Théorème 3.1** (trigonalisation d'un endomorphisme)**.** *Soit $E$ un espace vectoriel de dimension finie sur $k$ et $u$ un endomorphisme de $E$. Les deux propriétés suivantes sont équivalentes :*

(1) *Le polynôme caractéristique $\chi_u$ est scindé sur $k$.*

(2) *Il existe une suite croissante de $n$ sous-espaces vectoriels stables par $u$*

$$\{0\} \subsetneq F_1 \subsetneq F_2 \subsetneq \ldots \subsetneq F_n = E.$$

*De plus, si on indexe les racines $(\lambda_1, \ldots, \lambda_n)$ de $\chi_u$, on peut choisir $F_i$de telle sorte que la restriction $u_{|F_i}$ ait exactement $(\lambda_1, \ldots, \lambda_i)$ pour valeurs propres pour $1 \leq i \leq n$.*

Donnons tout de suite la version matricielle de l'assertion (2) : puisque les $F_i$ sont tous distincts, le théorème 1.1 force $\dim F_i = i$ pour $1 \leq i \leq n$. Choisissons une base $\mathcal{B} = (e_1, e_2, \ldots, e_n)$ *adaptée* à la suite croissante de sous-espaces, c'est-à-dire qui vérifie : $e_1$ est une base de $F_1$, que l'on complète par $e_2$ en une base de $F_2$, que l'on complète ... En résumé, $(e_1, e_2, \ldots, e_i)$ est une base de $F_i$ pour tout $i$ entre 1 et $n$. La matrice $T$ de $u$ dans la base $\mathcal{B}$ est *triangulaire supérieure* : si on note $a_{i,j}$ $1 \leq i, j \leq n$ ses coefficients on a :

$$a_{i,j} = 0 \text{ dès que } i > j$$

et

$$T = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ 0 & a_{2,2} & * & * \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{n,n} \end{pmatrix}.$$

Le polynôme caractéristique $\chi_u$ se calcule aisément dans cette base. Il vaut :

$$\chi_u(X) = \prod_{i=1}^{n} (a_{i,i} - X)$$

Les éléments diagonaux sont donc les valeurs propres de $u$ comptés avec leur multiplicité dans le polynôme $\chi_u$. De plus, $e_1$ est un vecteur propre associé à la valeur propre $a_{1,1}$. On a donc, grâce à la correspondance 1.9.1, un théorème équivalent au précédent :

**Théorème 3.2** (trigonalisation d'une matrice sous le groupe linéaire)**.** *Soit $A$ une matrice de $\mathcal{M}_n(k)$. Les deux propriétés suivantes sont équivalentes :*

(1) *Le polynôme $\det(A - X\mathrm{I}_n)$ est scindé sur $k$.*

(2) *Il existe une matrice inversible $P \in \mathrm{GL}_n(k)$ telle que $P^{-1}AP$ soit triangulaire supérieure.*

*De plus, si on indexe les racines $(\lambda_1, \ldots, \lambda_n)$ de $\det(A - X\mathrm{I}_n)$, on peut trouver $P \in \mathrm{GL}_n(k)$ de telle sorte que $P^{-1}AP$ soit triangulaire supérieure avec des coefficients diagonaux égaux, dans cet ordre, à $(\lambda_1, \ldots, \lambda_n)$.*

On appellera le polynôme $\det(A - X\mathrm{I}_n)$ *polynôme caractéristique* de $A$ et on le notera $\chi_A$.

*Démonstration.* Notons $A$ la matrice de $u$ dans une base donnée $\mathcal{B}_0$ de $E$. La preuve se fait par récurrence sur la dimension de $E$. Si $n = 0$ il n'y a rien à faire. Sinon, il existe au moins un vecteur propre de $u$ associé à la valeur propre $\lambda_1$ ; on le note $e_1$. Il existe donc une base $\mathcal{B}_1$ de $E$, obtenue en complétant $(e_1)$, dans laquelle la matrice $A_1$ de $u$ a pour première colonne

$$\begin{pmatrix} \lambda_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

ce qui signifie qu'il existe une matrice $P_1 \in \mathrm{GL}_n(k)$ telle que $A_1 = P_1^{-1}AP_1$ avec

$$A_1 = \begin{pmatrix} \lambda_1 & * & \cdots & * \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$$

et $B \in \mathcal{M}_{n-1}(k)$. Le développement de $\det(A_1 - X\mathrm{I}_n)$ montre que

$$\chi_u(X) = (\lambda_1 - X)\det(B - X\mathrm{I}_{n-1})$$

On en déduit que $\det(B - X\mathrm{I}_{n-1})$ est scindé sur $k$ égal à $\prod_{i=2}^{n}(\lambda_i - X)$. Par hypothèse de récurrence il existe une matrice $Q$ de $\mathrm{GL}_{n-1}(k)$ telle que $Q^{-1}BQ$ est triangulaire supérieure dans $\mathcal{M}_{n-1}(k)$, avec des coefficients diagonaux égaux à $\lambda_2, \ldots, \lambda_n$. Considérons la matrice suivante de $\mathcal{M}_n(k)$ :

$$P_2 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Q & \\ 0 & & & \end{pmatrix}$$

On vérifie que son inverse est

$$P_2^{-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Q^{-1} & \\ 0 & & & \end{pmatrix}$$

et la matrice $P_2^{-1}A_1P_2$ est de la forme requise :

$$P_2^{-1}A_1P_2 = \begin{pmatrix} \lambda_1 & * & \cdots & * \\ 0 & & & \\ \vdots & & Q^{-1}BQ & \\ 0 & & & \end{pmatrix}$$

puisque $Q^{-1}BQ$ est triangulaire supérieure, de coefficients diagonaux égaux à $\lambda_2, \ldots, \lambda_n$. La matrice de passage recherchée est donc le produit $P_1P_2$. □

### 3.3. **Application : théorème de Cayley-Hamilton.**

On vient de voir que lorsque le polynôme caractéristique de $u$ est scindé, il existe une suite de $n$ sous-espaces vectoriels stables par $u$

$$\{0\} \subsetneqq F_1 \subsetneqq F_2 \subsetneqq \ldots \subsetneqq F_n = E.$$

Pour tout $i$, $1 \leq i \leq n$ on a $u(F_i) \subset F_i$. De plus,

$$(u - \lambda_i \mathrm{Id})(F_i) \subset F_{i-1}$$

(en posant $F_0 = \{0\}$). En effet, pour tout $i$, $1 \leq i \leq n$, on a $u(e_i) = \lambda_i e_i + b_i$ avec $b_i \in F_{i-1}$. On en déduit successivement que $(u - \lambda_n \mathrm{Id})(F_n) \subset F_{n-1}$,
$(u - \lambda_{n-1}\mathrm{Id})(u - \lambda_n \mathrm{Id})(F_n) \subset F_{n-2}$, ...

$$(u - \lambda_1 \mathrm{Id})(u - \lambda_2 \mathrm{Id}) \cdots (u - \lambda_n \mathrm{Id})(E) \subset \{0\}$$

ce qui signifie que l'endomorphisme $\prod_{i=1}^n (u - \lambda_i \mathrm{Id})$ est l'endomorphisme nul dans $\mathrm{End}(E)$.
Ceci constitue l'énoncé du théorème de Cayley-Hamilton pour $u$.
Si $\chi_u$ n'est pas scindé sur $k$, il l'est sûrement sur la clôture algébrique $\bar{k}$ de $k$ (on admettra ici qu'elle existe). On procède alors comme suit. Désignons par $A$ la matrice de $u$ dans une base $\mathcal{B}$ de $E$. Elle est dans $\mathcal{M}_n(k)$. On peut la considérer comme un élément de $\mathcal{M}_n(\bar{k})$. Comme telle, c'est la matrice d'un endomorphisme de $(\bar{k})^n$ dont le polynôme caractéristique (celui de $A$ !) est scindé sur $\bar{k}$. On en déduit que $\chi_A(A) = 0$. Cet énoncé, a priori sur $\bar{k}$, est en fait un énoncé sur $k$, puisque aussi bien le polynôme caractéristique $\chi_A$ que $A$ sont à coefficients dans $k$.

**Théorème 3.4** (Cayley-Hamilton)**.** *Soit $u$ un endomorphisme d'un espace vectoriel $E$ de dimension finie sur $k$ et $\chi_u$ son polynôme caractéristique (à coefficients dans $k$). On a alors $\chi_u(u) = 0$ dans* $\mathrm{End}(E)$.

Posons $\mathcal{J}_u := \{P \in k[X] \mid P(u) = 0 \text{ dans } \mathrm{End}(E)\}$. L'ensemble $\mathcal{J}_u$ est une partie de l'anneau des polynômes qui est un groupe pour l'addition et absorbant pour la multiplication. C'est un *idéal* de $k[X]$.

**Corollaire 3.5.** *L'idéal $\mathcal{J}_u$ n'est pas réduit au polynôme nul. Il contient toujours le polynôme caractéristique $\chi_u$.*

Exercice 3.6. Rappeler pourquoi $\mathrm{End}(E)$ est une $k$-algèbre de dimension finie $n^2$.
En déduire, sans utiliser le théorème de Cayley-Hamilton, qu'il existe un polynôme non nul $P \in k[X]$, de degré inférieur à $n^2$, tel que $P(u) = 0$ .

Exercice 3.7. Montrer, à l'aide de la division euclidienne des polynômes, que tout idéal de $k[X]$ est engendré par un élément unique à multiplication par un inversible près.
Montrer que tout idéal non nul de $k[X]$ a un unique générateur unitaire.

**Définition 3.8.** *Soit $u$ un endomorphisme d'un espace vectoriel de dimension finie sur $k$.*
*On appelle* polynôme minimal *de $u$, noté $m_u$, le générateur unitaire de l'idéal $\mathcal{J}_u$.*

◇ L'ensemble des endomorphismes de $E$ est une $k$-algèbre. La multiplication est la composition des endomorphismes. Cette multiplication n'est pas commutative : en général $u \circ v$ n'est pas égal à $v \circ u$. Cependant, lorsqu'on se limite à des compositions qui ne font intervenir que $u$ et ses puissances (y compris $u^0 = \mathrm{Id}$), alors la multiplication est commutative et on retrouve les règles de calcul de l'anneau des polynômes. Ainsi, $u$ étant donné, tout polynôme $P$ de $k[X]$ permet de construire un endomorphisme $P(u)$ de $\mathrm{End}(E)$. L'ensemble de ces endomorphismes est une *sous-algèbre commutative* de $\mathrm{End}(E)$ que l'on note $k[u]$. On peut résumer ce qui précède en disant que

$$\begin{array}{rcl} \mathrm{ev}_u : k[X] & \longrightarrow & k[u] \subset \mathrm{End}(E) \\ P & \longmapsto & P(u) \end{array}$$

est un morphisme de $k$-algèbres commutatives. Attention toutefois ! Ce morphisme, surjectif par construction, n'est pas injectif en général (jamais si $E$ est de dimension finie !). Son noyau est notre idéal $\mathcal{J}_u$.
Dans les livres on appelle souvent un élément de $\mathcal{J}_u$ *polynôme annulateur* de $u$, par contagion avec le polynôme annulateur d'un module sur $k[X]$. Nous adopterons ce vocabulaire, même si le sens n'est pas évident : on ne voit pas bien, à notre stade, qui annule qui, du polynôme ou de l'endomorphisme. ◇

Comme le polynôme minimal divise tous les éléments de $\mathcal{J}_u$, il divise a fortiori $\chi_u$. Il ne lui est pas toujours égal, même à un inversible près : considérer une homothétie de rapport $\lambda \in k$. Quel est son polynôme caractéristique ?

Son polynôme minimal est $X - \lambda$. Réciproquement si le polynôme minimal d'un endomorphisme $u$ est $X - \lambda$, c'est que $u$ est l'homothétie de rapport $\lambda$.

**Lemme 3.9.** *Soit $u$ dans* $\mathrm{End}(E)$ *et $\lambda \in k$ une valeur propre de $u$. Alors $\lambda$ est une racine de $m_u$.*

*Démonstration.* Il y a au moins un vecteur propre $x$ (non nul !) associé à la valeur propre $\lambda$. On a donc $u(x) = \lambda x$ et par suite, pour tout polynôme $P$ de $k[X]$,

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

On en déduit, comme $m_u(u)$ est l'endomorphisme nul, que $m_u(u)(x) = m_u(\lambda)x = 0$, puis, comme $x$ n'est pas nul, que $m_u(\lambda) = 0$. $\square$

Nous avons donc démontré :

**Proposition 3.10.** *Soit $u$ un endomorphisme d'un espace vectoriel de dimension finie $n$ sur $k$. Supposons le polynôme caractéristique scindé sur $k$ en*

$$\chi_u(X) = (-1)^n \prod_{i=1}^{r} (X - \lambda_i)^{m_i}, \text{ avec } \sum_{i=1}^{r} m_i = n.$$

*où les $\lambda_i$, $1 \leq i \leq r$, sont deux à deux distincts. Le polynôme minimal est alors scindé sur $k$ en*

$$\mathrm{m}_u(X) = \prod_{i=1}^{r} (X - \lambda_i)^{N_i}$$

*avec $1 \leq N_i \leq m_i$ pour $1 \leq i \leq r$.*

Exercice 3.11. Reprendre l'endomorphisme décrit à l'exemple 2.6.1. Montrer que son polynôme minimal est $X^n$. Pour cela, remarquer d'abord que c'est une puissance de $X$, puis montrer que $u^{n-1}$ n'est pas nul dans $\mathrm{End}(E)$.

Exercice 3.12. On se donne un corps $k$, un polynôme unitaire $P$ de degré $n$ dans $k[X]$ et l'espace vectoriel $E = k_{n-1}[X]$ de dimension $n$ sur $k$, des polynômes de degré au plus $n - 1$.
À tout polynôme $Q$ de $k[X]$, on associe le reste de la division euclidienne de $Q$ par $P$ qui est un élément de $k_{n-1}[X]$. Montrer qu'on définit ainsi une application linéaire de $k[X]$ dans $k_{n-1}[X]$.
On considère alors l'application suivante de $E$ dans lui-même : à un polynôme $Q(X)$ de $E = k_{n-1}[X]$ on associe le reste de la division par $P(X)$ du produit $XQ(X)$. Montrer que c'est un endomorphisme $u$ de $E$ Calculer les puissances de $u$. Montrer que le polynôme minimal de $u$ est égal à $P$. Quel est le polynôme caractéristique ?
Si $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$, montrer que, dans la base des monômes de $E = k_{n-1}[X]$, la matrice de $u$ est :

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & 0 & -a_1 \\ \vdots & \ddots & \ddots & & \vdots \\ 0 & & \ddots & 0 & -a_{n-2} \\ 0 & 0 & & 1 & -a_{n-1} \end{pmatrix}$$

On l'appelle *matrice compagnon* du polynôme $P$.
Considérer le cas où $P(X) = X^n$ et comparer avec l'exercice précedent.