Réduction des endomorphismes

Position du problème. Outils.

1. INTRODUCTION

Dans toute la suite, k désigne un **corps**. Ce sera, le plus souvent, celui des réels $\mathbf{R}$ ou des complexes $\mathbf{C}$ mais on ne s'interdit pas le corps des rationnels $\mathbf{Q}$ ou les corps finis, par exemple celui des entiers modulo p lorsque p est premier ; on le note $\mathbf{Z}/p\mathbf{Z}$ ou $\mathbf{F}_p$.
Sauf mention du contraire, on ne considérera, dans cette partie, que des espaces vectoriels de **dimension finie** sur k, c'est-à-dire engendrés par une partie finie. Si E est un tel espace vectoriel, il a au moins une **base** $\mathcal{B}$. Toutes les bases de E ont le même nombre d'éléments. Le nombre d'éléments n de $\mathcal{B}$ est la **dimension** de E.
Le résultat suivant est important. Il permet de **classer** les **sous-espaces vectoriels** d'un espace vectoriel E.

Théorème 1.1. *Soient E un k-espace vectoriel de dimension finie et F un sous-espace. Alors F est de dimension finie sur k, $\dim F \leq \dim E$ et l'on a égalité si et seulement si $F = E$.*

Un **endomorphisme** u de E est une application k-linéaire

$$\begin{array}{rcl} u : E & \longrightarrow & E \\ v & \longmapsto & u(v) \end{array}$$

L'ensemble des endomorphismes de E est un k-espace vectoriel et même une k-algèbre (le vérifier : le produit est induit par la composition des endomorphismes). On le note $\mathrm{End}(E)$ ou parfois $\mathcal{L}(E)$.

Théorème 1.2 (du rang). *Soient E un k-espace vectoriel de dimension finie et u un endomorphisme de E. On a*

$$\dim \ker u + \mathrm{rg}(u) = \dim E$$

où l'on appelle rang de u (que l'on note $\mathrm{rg}(u)$) la dimension de l'image $u(E)$, notée aussi $\mathrm{Im} u$.

1.3. **Le problème de la réduction des endomorphismes.** peut être formulé ainsi, de façon encore imprécise : ramener l'étude d'un endomorphisme $u \in \mathrm{End}(E)$ à celle d'endomorphismes "plus simples", c'est-à-dire des endomorphismes d'un espace vectoriel de dimension plus petite ou d'un type fixé. Par exemple, pour λ dans k, on considère qu'une **homothétie de rapport** λ :

$$\begin{array}{rcl} h_\lambda : E & \longrightarrow & E \\ v & \longmapsto & \lambda v \end{array}$$

est un objet simple.

La première chose à remarquer est qu'en général, la restriction d'un endomorphisme à un sous-espace vectoriel $F \subset E$ n'est pas un endomorphisme. Ce n'est le cas que si $u(F)$ est contenu dans F. On dit alors que F est **stable** par u. On voit donc que la recherche de sous-espaces stables est importante.

Exemple 1.3.1. Dans un espace vectoriel E de dimension 2 sur k, muni d'une base (e_1, e_2), on définit l'endomorphisme u par :

$$\begin{array}{rcl} u : \quad E & \longrightarrow & E \\ a_1e_1 + a_2e_2 & \longmapsto & a_2e_1 \end{array}$$

Le théorème 1.1 permet de classer les sous-espaces vectoriels de E. En dimension 2, il n'y a que E. En dimension 0, il n'y a que $\{0\}$. Restent les sous-espaces vectoriels de dimension 1 de E, engendrés par un vecteur non nul , qu'on appellera droites vectorielles de E.
Le vecteur e_1 a pour image 0. La droite vectorielle F qu'il engendre est donc stable par u.
Une droite F' différente de F est engendrée par un vecteur $e_2 + \lambda e_1$ avec λ dans k et $e_2 = (0, 1)$. On a $u(e_2 + \lambda e_1) = e_1$ qui n'est pas dans F'. Le sous-espace F est donc le seul sous-espace non trivial, c'est-à-dire différent de E et de $\{0\}$, qui est stable par u. En particulier, il ne peut pas exister de **supplémentaire** de F stable par u.

1.4. **Décomposition en somme directe.** Soient E un espace vectoriel de dimension finie sur k et E_i, $1 \leq i \leq r$ une famille finie de sous-espaces vectoriels de E. Les propriétés suivantes sont équivalentes :

(1) Tout vecteur x de E se décompose de manière unique en une somme de vecteurs $\sum_{i=1}^r x_i$, avec $x_i \in E_i$.
(2) $\sum_{i=1}^r \dim E_i = \dim E$ et tout vecteur x de E se décompose en une somme de vecteurs $\sum_{i=1}^r x_i$, avec $x_i \in E_i$.
(3) $\sum_{i=1}^r \dim E_i = \dim E$ et il n'existe pas de décomposition non triviale du vecteur nul sur les E_i, $1 \leq i \leq r$.
(4) On obtient une base de E en réunissant des bases des E_i, $1 \leq i \leq r$.

Lorsque l'une de ses assertions est vraie, on dit que E est la somme directe des E_i, $1 \leq i \leq r$ et on écrit

$$E = \bigoplus_{i=1}^r E_i.$$

Voici une première formulation du problème de la réduction des endomorphismes :

1.5. **Diagonalisation :** *Diagonaliser un endomorphisme u de E c'est trouver une décomposition de E en* somme directe

$$E = \bigoplus_{i=1}^{r} E_i \tag{1.5.1}$$

de sous-espaces E_i stables par u, tels que, pour $1 \leq i \leq r$, la restriction $u_i = u_{|E_i}$ de u à E_i soit une homothétie.

Remarquer que l'endomorphisme de l'exemple 1.3.1 ne se laisse pas "réduire" ainsi. On verra dans la suite des formulations moins exigeantes du problème de réduction des endomorphismes qui, de ce fait, aura plus souvent une solution.

1.6. **Bases, matrices.** Une base $\mathcal{B} = \{e_1, \ldots, e_n\}$ étant fixée, pour se donner un endomorphisme $u \in \mathrm{End}(E)$, il suffit de se donner les images $u(e_1), \ldots, u(e_n)$ des vecteurs de la base $\mathcal{B}$. Réciproquement, à toute donnée de n vecteurs $f_1, \ldots, f_n$ de E, il correspond un unique élément u dans $\mathrm{End}(E)$ tel que $u(e_i) = f_i$ pour $1 \leq i \leq n$.
Un vecteur x de E se décompose de manière unique sur la base $\mathcal{B}$ en

$$x = \sum_{i=1}^{n} x_i e_i.$$

La matrice de x dans la base $\mathcal{B}$ est la matrice a n lignes et une colonne avec x_i à la ligne numéro i.
Pour j de 1 à n, on écrit les coordonnées dans la base $\mathcal{B}$ du vecteur $u(e_j)$ dans la j-ème colonne d'un tableau carré : on obtient ainsi la **matrice** de u dans la base $\mathcal{B}$ que l'on notera $\mathrm{Mat}_{\mathcal{B}}(u)$. L'ensemble de ces matrices sera noté $\mathcal{M}_n(k)$. C'est un espace vectoriel de dimension n^2 sur k. Le vérifier en en donnant une base.
Appelons y l'image de x par u et notons X (resp. Y) la matrice du vecteur x (resp. y) dans la base $\mathcal{B}$. Notons A la matrice de u dans la base $\mathcal{B}$. L'égalité $y = u(x)$ se traduit, dans la base $\mathcal{B}$, par l'égalité matricielle

$$Y = AX \tag{1.6.1}$$

Exemple 1.6.1. Soit λ un élément de k. Dans une base quelconque de E, la matrice de l'homothétie de rapport λ est $\lambda \mathrm{I}_n$, matrice dont tous les coefficients diagonaux sont égaux à λ et tous les autres nuls. Pour $\lambda = 1$ on a la matrice I_n de l'identité Id_E de E, notée Id quand il n'y a pas d'ambiguïté.

1.7. **Changements de base.** Si $\mathcal{B}' = (e'_1, \ldots, e'_n)$ est une autre base de E, nous notons X' (resp. Y', A') la matrice de x (resp. y, u) dans la base $\mathcal{B}'$. Définissons la **matrice de passage** P de la base $\mathcal{B}$ à la base $\mathcal{B}'$ comme *la matrice de $\mathcal{M}_n(k)$ dont la colonne de numéro j est formée des coordonnées dans la base $\mathcal{B}$, du vecteur de numéro j de la base $\mathcal{B}'$.*

On a donc successivement, en notant $P_{i,j}$ les coefficients de la matrice P,

$$e'_j = \sum_{i=1}^{n} P_{i,j} e_i$$

pour $1 \leq j \leq n$, puis

$$x = \sum_{j=1}^{n} x'_j e'_j = \sum_{j=1}^{n} x'_j \sum_{i=1}^{n} P_{i,j} e_i.$$

En utilisant l'unicité de la décomposition de x dans la base $\mathcal{B}$ on traduit ce qui précède en

$$x_i = \sum_{j=1}^{n} P_{i,j} x'_j$$

pour $1 \leq i \leq n$. Enfin, on rassemble ces n égalités en une égalité matricielle :

$$X = PX'$$

ce qui s'exprime par le slogan suivant : "la matrice de passage est la matrice qui donne les anciennes coordonnées d'un vecteur au moyen des nouvelles".
On remarque que le passage de $\mathcal{B}'$ à $\mathcal{B}$ est l'opération inverse du passage de $\mathcal{B}$ à $\mathcal{B}'$: la matrice de passage P est donc inversible et son inverse P^{-1} est la matrice de passage de $\mathcal{B}'$ à $\mathcal{B}$.
Pour les matrices du vecteur $y = u(x)$ dans les bases $\mathcal{B}$ et $\mathcal{B}'$ on a aussi $Y = PY'$. On en déduit, au vu de 1.6.1, que, pour tout vecteur x de E, $PY' = APX'$ soit encore $Y' = P^{-1}APX'$, ce qui signifie que la matrice A' de u dans la base $\mathcal{B}'$ n'est autre que $P^{-1}AP$.

1.8. **Déterminant.** On calcule le déterminant d'une matrice A de $\mathcal{M}_n(k)$ en le **développant** relativement à une des lignes (resp. une des colonnes) de A.
Précisément, voici comment développer $\det(A)$ par rapport à la colonne de numéro j : si on note $a_{i,j}$ les coefficients de A, on obtient une relation de récurrence

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j}\, \Delta_{i,j}$$

où $\Delta_{i,j}$ est le déterminant de la matrice de $\mathcal{M}_{n-1}(k)$ obtenue en supprimant la j-ème colonne et la i-ème ligne de A. Le déterminant d'une matrice de $\mathcal{M}_1(k)$ est égal à son unique coefficient.
Les **propriétés fondamentales du déterminant** sont les suivantes : pour tout A, B dans $\mathcal{M}_n(k)$,

$$\det(A) \text{ inversible } \iff rg(A) = n \iff A \text{ inversible.}$$

et

$$\det(AB) = \det(A)\det(B).$$

De cette dernière relation on déduit d'abord que, si P est inversible, alors $\det(P^{-1}) = (\det P)^{-1}$ puis que

$$\det P^{-1}AP = \det A.$$

On peut donc parler du **déterminant d'un endomorphisme** u de $\mathrm{End}(E)$: c'est le déterminant de la matrice de u dans une base $\mathcal{B}$ de E.

1.9. **Diagonalisation des matrices.** On vient d'étudier la correspondance entre l'algèbre $\mathrm{End}(E)$ et l'algèbre de matrices $\mathcal{M}_n(k)$. Une base étant choisie on associe à un endomorphisme u sa matrice $\mathrm{Mat}_{\mathcal{B}}(u)$ dans cette base. Cette application

$$\begin{array}{rcl} \mathrm{End}(E) & \longrightarrow & \mathcal{M}_n(k) \\ u & \longmapsto & \mathrm{Mat}_{\mathcal{B}}(u) \end{array} \tag{1.9.1}$$

est un isomorphisme de k-algèbres (le vérifier) qui *dépend de la base choisie*.
On peut donc donner un équivalent de la diagonalisation des endomorphismes : étant donnée une matrice A, trouver une matrice inversible P telle que la matrice $P^{-1}AP$ soit diagonale.
L'ensemble des matrices inversibles de $\mathcal{M}_n(k)$ est un groupe pour la multiplication des matrices que l'on note $\mathrm{GL}_n(k)$ (groupe linéaire). C'est pour cela que l'on dit de manière précise et non ambigüe :

Diagonaliser une matrice A de $\mathcal{M}_n(k)$ sous le groupe linéaire $\mathrm{GL}_n(k)$, c'est trouver une matrice $P \in \mathrm{GL}_n(k)$ telle que la matrice $P^{-1}AP$ soit diagonale.

Vérifier que les deux formulations 1.5 et 1.9 sont bien équivalentes : pour cela, considérer la matrice de l'endomorphisme u dans une base adaptée à la décomposition 1.5.1, c'est-à-dire une base de E obtenue en réunissant des bases de chacun des E_i, $1 \leq i \leq m$.
Puisqu'il y a équivalence, la matrice de l'endomorphisme u de l'exemple 1.3.1 n'est pas diagonalisable sous le groupe $\mathrm{GL}_2(k)$. Écrire cette matrice et trouver d'autres exemples analogues.

2. Endomorphismes diagonalisables.

2.1. **Polynôme caractéristique.** Si u est dans $\mathrm{End}(E)$ et λ dans k, alors $u - \lambda\mathrm{Id}$ est encore un endomorphisme de E.
Le théorème du rang et les propriétés du déterminant montrent que les conditions suivantes sont équivalentes :

(1) $(u - \lambda\mathrm{Id})$ non inversible
(2) $\det(u - \lambda\mathrm{Id}) = 0$
(3) $\ker(u - \lambda\mathrm{Id}) \neq \{0\}$
(4) $\exists x \in E$, $x \neq 0$ et $u(x) = \lambda x$

On dit alors que λ est une **valeur propre** de u et que le sous-espace vectoriel $E_\lambda = \ker(u - \lambda\mathrm{Id})$ est le **sous-espace propre** associé. Tout vecteur non nul de E_λ est appelé **vecteur propre** de valeur propre λ.

En calculant le déterminant de $(u - \lambda\mathrm{Id})$, on s'aperçoit que c'est une fonction polynomiale de λ de degré exactement $n = \dim E$. Un endomorphisme d'un espace vectoriel de dimension finie a donc seulement un nombre fini de valeurs propres, au plus n précisément.
Toujours en calculant le déterminant de la matrice de $u - \lambda\mathrm{Id}$ dans une base $\mathcal{B}$, on trouve :

$$\det(u - \lambda\mathrm{Id}) = (-1)^n\lambda^n + (-1)^{n-1}\mathrm{tr}(u)\lambda^{n-1} + \ldots + \det u \tag{2.1.1}$$

où $\mathrm{tr}(u)$ est la somme des coefficients diagonaux de la matrice $\mathrm{Mat}_{\mathcal{B}}(u)$. Comme le déterminant de l'endomorphisme $u - \lambda\mathrm{Id}$ ne dépend pas de la base choisie, c'est que $\mathrm{tr}(u)$ ne dépend pas non plus de la base choisie.

Remarque : Trouver la faille dans les 4 lignes qui précédent et la réparer. Indication : k a-t-il suffisamment d'éléments ?

On vient de voir que $\lambda \longmapsto \det(u - \lambda\mathrm{Id})$ est une fonction polynôme sur k. Si le corps k est infini, cette fonction provient d'un unique polynôme de $k[X]$ que l'on appelle **polynôme caractéristique** de u et que l'on note χ_u.
Si k est fini, on sait qu'il existe des polynômes non nuls de $k[X]$ qui s'annulent sur tout k, donc induisent une fonction polynôme nulle sur k (par exemple, si p est premier, considérer le polynôme $X^p - X$ de $\mathbf{F}_p[X]$). Une fonction polynôme peut alors provenir de plusieurs polynômes.
Pour définir dans ce cas aussi le polynôme caractéristique, il faut être plus prudent et faire un détour : on remarque et on vérifie que

(1) si A est une matrice à coefficients dans k, la matrice $A - XI_n$ est une matrice à coefficients dans $k[X]$;
(2) les règles de calcul du déterminant n'utilisent que les opérations $+$ et $\times$, donc sont valables pour les matrices à coefficients dans n'importe quel anneau commutatif, en particulier dans l'anneau des polynômes $k[X]$;
(3) le déterminant d'une matrice à coefficients dans $k[X]$ ainsi défini (c'est un élément de $k[X]$), il continue de vérifier les propriétés fondamentales de 1.8. Attention toutefois ! dans un corps, tout élément non nul est inversible ; en revanche, les seuls éléments inversibles de $k[X]$ sont les polynômes de degré 0, c'est-à-dire les constantes non nulles.

Exemple 2.1.1. Considérer la matrice de $\mathcal{M}_n(\mathbf{Q}[X])$

$$M := \begin{pmatrix} 1 - X & 1 \\ 0 & -X \end{pmatrix}$$

Calculer son déterminant. Est-il inversible dans $\mathbf{Q}[X]$? dans le corps des fractions rationnelles $\mathbf{Q}(X)$?

La matrice M est-elle inversible dans $\mathcal{M}_n(\mathbf{Q}[X])$? dans $\mathcal{M}_n(\mathbf{Q}(X))$?

Définition 2.2. *Soit E un espace vectoriel de dimension finie n sur k et u un endomorphisme de E. Soit $\mathcal{B}$ une base de E et A la matrice de u dans la base $\mathcal{B}$. La matrice $A - X\mathrm{I}_n$ est une matrice à coefficients dans $k[X]$. Son déterminant est un polynôme de $k[X]$. Il ne dépend que de u et pas du choix de la base $\mathcal{B}$. On l'appelle* polynôme caractéristique *de u et on le note χ_u.*

On a alors (comparer avec 2.1.1)

$$\chi_u(X) = (-1)^n X^n + (-1)^{n-1}\mathrm{tr}(u)X^{n-1} + \ldots + \det u$$

En particulier, si $n = 2$,

$$\chi_u(X) = X^2 - \mathrm{tr}(u)X + \det u$$

2.3. **Sous-espaces stables.** Soit u un endomorphisme d'un espace vectoriel E de dimension finie n et $F \subset E$ un sous-espace stable par u de dimension $m \leq n$. On a vu que la restriction $u_{|F}$ est alors un endomorphisme de F.
Choisissons, pour nos calculs de déterminants, une base $\mathcal{B}$ de E obtenue en complétant une base de F. La matrice de u dans la base $\mathcal{B}$ s'écrit alors

$$A = \begin{pmatrix} B & D \\ 0 & C \end{pmatrix}$$

où $B \in \mathcal{M}_m(k)$ est la matrice de la restriction $u_{|F}$, C (resp. D) étant une matrice de $\mathcal{M}_{n-m}(k)$ (resp. une matrice de $\mathcal{M}_{m,n-m}(k)$. En développant le déterminant de $A - X\mathrm{I}_n$ par rapport aux premières colonnes, on s'aperçoit que

$$\det(A - X\mathrm{I}_n) = \det(B - X\mathrm{I}_m)\det(C - X\mathrm{I}_{n-m})$$

autrement dit :

Proposition 2.4. *Soit u un endomorphisme d'un espace vectoriel E de dimension finie n sur k. Le polynôme caractéristique de la restriction de u à un sous-espace stable par u* divise *le polynôme caractéristique de u.*
En particulier, si λ, élément de k, est une racine de χ_u de multiplicité $m_\lambda > 0$, λ est valeur propre de u et

$$1 \leq \dim E_\lambda \leq m_\lambda.$$

On dit qu'un polynôme de degré d de $k[X]$ est **scindé** sur k s'il se factorise en un produit de d polynômes de $k[X]$ du premier degré, donc, en regroupant les facteurs, en un produit

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

où les λ_i, $1 \leq i \leq r$ sont tous distincts et la somme $\sum_i m_i$ est égale à d. Remarquer que les $(X - \lambda_i)^{m_i}$, $1 \leq i \leq r$ sont alors **premiers entre eux** deux à deux.
Si k est algébriquement clos (par exemple $k = \mathbf{C}$), tout polynôme de $k[X]$ est scindé sur k. En revanche, le polynôme $X^2 - 2$ n'est pas scindé sur $\mathbf{Q}$.

Le corollaire suivant est une reformulation de 1.5.

Corollaire 2.5. *Un endomorphisme u d'un espace vectoriel de dimension finie sur k est diagonalisable si et seulement si son polynôme caractéristique χ_u est scindé sur k et si pour toute racine λ de χ_u on a $\dim E_\lambda = m_\lambda$.*

Démonstration. Si on sait que u est diagonalisable, on travaille dans une base adaptée à la décomposition 1.5.1 et on vérifie les assertions concernant χ_u et la dimension des espaces propres.
Pour la réciproque, notons que la somme des dimensions des E_λ est égale à la somme des multiplicités c'est-à-dire au degré $\deg(\chi_u)$, encore égal à $\dim E$. Il reste donc à démontrer (voir 1.4 (3)) qu'il n'existe pas de décomposition non triviale du vecteur nul sur les E_λ. Supposons qu'il en existe au moins une et prenons celle qui contient le plus petit nombre de composantes non nulles, nombre que nous appelons s.
On a donc, quitte à indexer les valeurs propres :

$$\sum_{i=1}^{s} x_i = 0 = u(0) = u(\sum_{i=1}^{s} x_i) = \sum_{i=1}^{s} \lambda_i x_i$$

ce qui montre que $\sum_{i=2}^{s}(\lambda_1 - \lambda_i)x_i = 0$, ce qui constitue une décomposition du vecteur nul avec $s-1$ composantes non nulles. $\square$

Nouvelle formulation : *Diagonaliser un endomorphisme u d'un espace vectoriel E de dimension finie sur k, c'est trouver une base de E formée de vecteurs propres de u.*

Corollaire 2.6. *Un endomorphisme d'un espace vectoriel de dimension finie n sur k dont le polynôme caractéristique χ_u a n racines simples est diagonalisable.*

Démonstration. Soient $\lambda_1, \ldots, \lambda_n$ les valeurs propres, distinctes deux à deux. Pour tout i, $1 \leq i \leq n$, on a, d'après la proposition 2.4, $1 \leq \dim E_{\lambda_i} \leq m(\lambda_i) = 1$ d'où $\dim E_{\lambda_i} = 1$.
D'après 1.4 on en déduit que $E = \bigoplus_{i=1}^{n} E_{\lambda_i}$. $\square$

Exemple 2.6.1. Calculer le polynôme caractéristique et les sous-espaces propres de l'endomorphisme décrit à l'exemple 1.3.1. Conclure.
On considère maintenant un k-espace vectoriel E de dimension finie n, muni d'une base $(e_1, \ldots, e_n)$ et un endomorphisme décrit par :

$$u(e_1) = 0,\ u(e_2) = e_1, \ldots, u(e_n) = e_{n-1}$$

ou si l'on préfère par

$$e_n \longmapsto e_{n-1} \longmapsto \cdots \longmapsto e_1 \longmapsto 0$$

Calculer le polynôme caractéristique χ_u et les sous-espaces propres de l'endomorphisme u. Conclure. Déterminer tous les sous-espaces de E stables par u.