Endomorphismes d'un K-espace vectoriel

Dans ce texte, K désigne un corps commutatif, d'élément unité $1 \neq 0$. Lorsque ce n'est pas précisé, E désigne un K-espace vectoriel de dimension finie n.

1. Rappels sur le déterminant

Le déterminant d'une matrice $n \times n$ à coefficients complexes (ou réels) est bien connu :

$$\det(a_{ij})_{1 \leq i,j \leq n} = \sum_{s \in S_n} \varepsilon(s) a_{s(1)1} \dots a_{s(n)n}$$

où $\varepsilon(s)$ désigne la *signature* de la permutation s.

La même formule s'applique pour les matrices dont les coefficients a_{ij} sont à valeurs dans un corps (et même un anneau !). Tous les procédés de calcul dans $\mathrm{Mat}(n, \mathbb{C})$ reposent sur une étude combinatoire et reste vrai pour l'ensemble $\mathrm{Mat}(n, A)$ des matrices à coefficients dans un anneau A (déterminant de matrices triangulaires supérieures ou inférieures ; de matrices triangulaires par blocs ; développement selon une rangée, une colonne ; identité $M\tilde{M} = \tilde{M}M = (\det M)I_n$ si $\tilde{M}$ est la transposée de la matrice des cofacteurs, égalité avec le déterminant de la matrice transposée). Pour tous ces aspects «calculatoire», nous renvoyons aux cours de L1 et L2.

Nous allons ici plutôt nous appliquer à revoir, dans le contexte d'un corps K général, le lien entre endomorphismes et matrices (dans une base donnée), ainsi que le moyen de définir le déterminant d'un endomorphisme sans faire appel à une base de l'ev, ceci *via* la notion de formes n-linéaires alternées sur E.

1.1. Lien entre endomorphismes et matrices (revue rapide) Rappelons le Théorème 1.3 du Ch.7 , réécrit ici dans le cas particulier d'un K-ev de dimension finie :

Théorème 1.1. *Soit $\bar{e} = (e_i)_{1 \leq i \leq n}$ une base de E, et $\bar{f} = (f_i)_{1 \leq i \leq n}$ une famille (quelconque) de n éléments d'un K-ev F. Alors il existe une et une seule application K-linéaire $u : E \to F$ telle que :*

$$u(\bar{e}) = \bar{f}$$

Cette application est surjective (resp. injective) si et seulement si $\bar{f}$ est génératrice (resp. libre). En particulier, c'est un isomorphisme si et seulement si $\bar{f}$ est une base de F. □

Ainsi, une fois choisie une base $\bar{e} = (e_j)_{1 \leq j \leq n}$ de E et une base $\bar{e}' = (e'_i)_{1 \leq i \leq m}$ de F, se donner une application K-linéaire $u : E \to F$ équivaut à prescrire l'image de $\bar{e}$ par u, ie. les n vecteurs $u(e_j)$, qu'on peut exprimer dans la base $\bar{e}'$:

$$u(e_j) = \sum_{i=1}^{m} a_{ij} e'_i$$

On appelle **matrice de u dans les bases $\bar{e}$, $\bar{e}'$** la matrice $m \times n$ à coefficient dans K des (a_{ij}). On la note $\mathrm{Mat}_{\bar{e},\bar{e}'}(u)$.

On retrouve ainsi la notion de multiplication de matrices, correspondant à la composition des applications linéaires :

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

La somme de matrices, correspondant à la somme d'applications K-linéaires.

Changer de base dans E (resp. dans F) revient à multiplier à droite (resp. à gauche) la matrice par celle qui exprime l'unique endomorphisme envoyant la nouvelle base sur l'ancienne (respectivement l'ancienne sur la nouvelle).

Le cas particulier qui nous intéresse ici au premier chef est celui des endomorphismes, ie. le cas $F = E$; le plus pertinent est alors de choisir comme base $\bar{e}'$ dans le E «d'arrivée» la même base $\bar{e}$ du E de départ ! On note alors simplement : $\mathrm{Mat}_{\bar{e}}(u)$.

Changer de bases équivaut alors à remplacer la matrice M associée à l'endomorphisme u dans l'ancienne base par la matrice $P^{-1}MP$ où la matrice $P = \mathrm{Mat}_{\bar{e}',\bar{e}}(Id_E)$ est la matrice de passage de l'ancienne base à la nouvelle base.

1.2. Sous-espaces u-invariants

Définition 1.2. *Un sous-espace $F \subset E$ est u-invariant si $u(F) \subset F$.*

Si F est un sev u-invariant, alors pour tout x dans E on a $u(x+F) \subset u(x)+F$. Ceci signifie qu'il existe une unique application $\bar{u} : E/F \to E/F$ telle que, si $p_F : E \to E/F$ désigne la surjection canonique : $p_F \circ u = \bar{u} \circ p_F$.

Une base $(e_1, ..., e_n)$ une base de E est dite **adaptée à** F si les k-premiers vecteurs $(e_1, ..., e_k)$ forment une base de F. Dans ce cas, la projection $(\bar{e}_{k+1}, ..., \bar{e}_n)$ des $n-k$ derniers éléments de la base par p_F forment une base de E/F.

Inversement, étant donné une base $(e_1, ..., e_k)$ une base de F et une base $(\bar{e}_{k+1}, ..., \bar{e}_n)$ de E/F, la complétion de $(e_1, ..., e_k)$ par toute famille $(e_{k+1}, ..., e_n)$ vérifiant $p_F(e_i) = \bar{e}_i$ est toujours une base de E.

Remarquons :

Proposition 1.3. *Soit $(e_1, ..., e_n)$ une base de E adaptée à F (sev $u-$invariant). Alors, la matrice de u dans cette base est une matrice par blocs de la forme :*

$$\begin{pmatrix} M & B \\ 0 & \bar{M} \end{pmatrix}$$

En outre, M est la matrice de $u_{|F}$ dans la base $(e_1, ..., e_k)$, et $\bar{M}$ est la matrice de $\bar{u}$ dans la base $(\bar{e}_{k+1}, ..., \bar{e}_n)$ □

1.3. Déterminant d'un endomorphisme de E

Définition 1.4. *Le déterminant d'un endomorphisme u de E est le déterminant de toute matrice exprimant u dans une base de E. On le note* $\det u$.

Le déterminant de u est bien défini, car le déterminant des matrices est invariant par conjugaison :

$$\det(P^{-1}MP) = (\det P^{-1})(\det M)(\det P) = (\det P^{-1})(\det P)(\det M) = \det M$$

De même, on a bien sûr pour tout u, v dans $\mathcal{L}(E)$: $\det(u \circ v) = (\det u)(\det v)$.

Proposition 1.5. *Un endomorphisme u de E est un isomorphisme si et seulement si son déterminant est non-nul.*

Démonstration. Ceci découle de l'égalité $M\widetilde{M} = \widetilde{M}M = (\det M)I_n$ déjà rappelée auparavant. □

2. Réduction d'endomorphismes

Dans toute cette section, u désigne un endomorphisme du K-espace vectoriel E de dimension finie.

Pour résoudre certaines questions qu'on peut se poser à propos de $u \in \mathcal{L}_K(E)$ (calcul d'un endomorphisme inverse, recherche d'éléments du noyau, ...), on est souvent amené à chercher une base particulière où sa matrice a une forme particulièrement simple ; par exemple :

Définition 2.1. *Un endomorphisme u est **diagonalisable** s'il existe une base de E pour laquelle la matrice associée à u est diagonale.*

Mais ce n'est pas toujours possible : tout endomorphisme n'est pas diagonalisable !

Une idée cruciale dans ce genre de question est au moins d'essayer de simplifier le problème en cherchant un sous-espace $F \subset E$ invariant par u, ie. tel que $u(F) \subset F$, permettant de se ramener à la restriction de u à F : ceci permet déjà de diminuer la dimension ! Pour décomposer l'étude de u en parties plus simples, l'idéal est de trouver une décomposition de E en somme directe de sous-espaces vectoriels u-invariants.

2.1. Sous-espaces propres

Définition 2.2. *Une **valeur propre** de u est un scalaire $\lambda \in K$ pour lequel il existe un vecteur $x \in E$ **non-nul** tel que $u(x) = \lambda.x$. Un tel vecteur x est alors appelé **vecteur propre de** u **associé à la valeur propre** λ.*

Définition 2.3. *L'ensemble des valeurs propres de u est appelé **spectre** de u, noté $Sp\ u$.*

Théorème - Définition 2.4. *Pour tout $\lambda \in K$, le noyau de $u-\lambda.\mathrm{Id}_E$ est noté $E(\lambda)$. Le scalaire λ est une valeur propre de u si et seulement si $E(\lambda)$ n'est pas réduit à $\{0\}$; $E(\lambda)$ est alors appelé **sous-espace propre associé à** λ. Les vecteurs propres de u associés à λ sont les éléments non-nuls du sous-espace vectoriel $E(\lambda)$.* □

Théorème 2.5. *Soit $(\lambda_1, ..., \lambda_k)$ une famille finie de valeurs propres de u, deux-à-deux distinctes. Alors la somme des sous-espaces propres associés $E(\lambda_i)$ est directe.* □

Corollaire 2.6. *u admet au plus n valeurs propres, et s'il en admet n, alors :*

$$E = E(\lambda_1) \oplus ... \oplus E(\lambda_n)$$

□

2.2. Diagonalisation, trigonalisation

2.2.1. Polynôme caractéristique (sur $K[X]$) d'une matrice Rappelons que K s'identifie naturellement comme un sous-anneau de l'anneau des polynômes $K[X]$. Ceci induit donc une inclusion naturelle $\mathrm{Mat}(n, K) \subset \mathrm{Mat}(n, K[X])$.

Définition 2.7. *Soit M une matrice de* $\mathrm{Mat}(n, K)$. *On appelle* ***polynôme caractéristique de*** *M le déterminant de la $K[X]$-matrice $XI_n - M$. On le note P_M, ou $P_M(X)$.*

Ainsi, ce déterminant est *a priori* un élément de l'anneau $K[X]$.

Remarque : Certains auteurs définissent le polynôme caractéristique de M par le déterminant de la $K[X]$-matrice $M - XI_n$, cela revient au même à un coefficent multplicateur $(-1)^n$ près, ainsi les racines sont identiques.

2.2.2. Polynôme caractéritique d'un endomorphisme

Théorème - Définition 2.8. *Le polynôme caractéristique de la matrice associée à u dans une base ne dépend pas du choix de la base. On l'appelle* ***polynôme caractéristique de*** *u et le note P_u, ou $P_u(X)$.*

Démonstration. Soient M, M' les matrices associées à u dans deux bases différentes. Il existe alors une matrice inversible P telle $M' = P^{-1}MP$. On a donc, dans $\mathrm{Mat}(n, K[X])$:

$$XI_n - M' = XP^{-1}I_nP - P^{-1}MP = P^{-1}(XI_n - M)P$$

L'affirmation s'en déduit par invariance du déterminant par conjugaison. □

Théorème 2.9. *Les valeurs propres de u sont exactement les racines de son polynôme caractéristique.*

Démonstration. En effet, le noyau de l'endomorphisme $\lambda.\mathrm{Id}_E - u$ contient un élément non-nul si et seulement si son déterminant est nul. □

Corollaire 2.10. *Si K est algébriquement clos, tout endomorphisme admet au moins une valeur propre.* □

Proposition 2.11. *Soit $F \subset E$ un sev u-invariant : $u(F) \subset F$. Soit $\bar{u} : E/F \to E/F$ l'endomorphisme induit. Alors, P_u est le produit du polynôme caractéristique de la restriction de u à F et du polynôme caractéristique de $\bar{u} \in \mathcal{L}_K(E/F)$.*

Démonstration. Choisir une base de E dont les premiers éléments forment une base de F. La matrice associée M ainsi que $XI_n - M$ est sous une forme en bloc, le déterminant du premier bloc étant le polynôme caractéristique de la restriction de u à F, et celui du second bloc étant le polynôme caractéristique de $\bar{u}$. □

Corollaire 2.12. *Le polynôme caractéristique de la restriction de u à un sev u-invariant F divise le polynôme caractéristique de u.* □

Corollaire 2.13. *Soit λ une valeur prore de u, soit $q(\lambda)$ la dimension de $E(\lambda)$, et soit $m(\lambda)$ la multiplicité de λ en tant que racine de P_u. Alors :*

$$1 \leq q(\lambda) \leq m(\lambda)$$

Démonstration. La restriction de u à $E(\Lambda)$ est l'homothétie de rapport λ, donc son polynôme caractéristique est $(X - \lambda)^{q(\lambda)}$. Or, d'après le corollaire précédent, ce polynôme doit diviser P_u. □

2.2.3. Endomorphismes diagonalisables

Théorème 2.14. *Les deux assertions suivantes sont équivalentes :*

(1) u est diagonalisable,

(2) le polynôme caractéristique de u est scindé, et pour toute valeur propre λ de u, la dimension de $E(\lambda)$ est égale à la multiplicité de la racine λ de P_u.

Démonstration. Une des implications est évidente. Montrons l'autre : supposons que pour toute valeur propre λ de u, la dimension $q(\lambda)$ de $E(\lambda)$ est égale à la multiplicité $m(\lambda)$ de la racine λ de P_u. Alors, comme la somme de tous les $m(\lambda)$ est le degré n de P_u, il en est de même pour la somme de tous les $q(\lambda)$. Ceci implique que la somme directe de tous les espaces propres $E(\lambda)$ est de dimension n, ie. E tout entier. Toute base de E obtenue en prenant l'union de bases de chaque espace propre est alors une base de diagonalisation. □

Comme corollaire, on obtient :

Théorème 2.15. *Si P_u admet n racines distinctes, alors u est diagonalisable.* □

2.2.4. Endomorphismes trigonalisables

Définition 2.16. *L'endomorphisme u est **trigonalisable** s'il existe une base pour laquelle la matrice associée à u est triangulaire supérieure.*

Nota Bene : Qu'une base $(e_1, ..., e_n)$ soit une base de «trigonalisation» équivaut à ce que pour tout k, le sous-espace vectoriel F_k engendré par les k-premiers éléments de la base soit u-invariant : $u(F_k) \subset F_k$.

Théorème 2.17. *Un endomorphisme u est trigonalisable si et seulement si son polynôme caractéristique est scindé sur K.*

Corollaire 2.18. *Si K est algébriquement clos, tout endomorphisme d'un K-espace vectoriel de dimension finie est trigonalisable.* □

Preuve du Théorème 2.17 : La condition est manifestement nécessaire.

Le point «difficile» est de montrer que si P_u est scindé, alors u est trigonalisable. On le fait par récurrence sur la dimension n de E : c'est évident si $n = 1$; supposons le vrai pour tout espace vectoriel de dimension $\leq n$ et considérons un K-ev E de dimension $n+1$ avec $n \geq 1$. Comme P_u est de degré ≥ 2 et scindé, il admet une racine : u admet une valeur propre λ ; il existe donc un sous-espace u-invariant non-réduit à $\{0\}$: le sous espace propre $E(\lambda)$. Si $E(\lambda)$ est E tout entier, u est l'homothétie $\lambda.\mathrm{Id}_E$ et nous avons fini. Sinon, $E(\lambda)$ est un sous-espace propre u-invariant, que nous allons noter par commodité F, qui est de dimension $k \geq 1$ et dans toute base $(e_1, ..., e_k)$ de F, la matrice de $u_{|F}{}^{|F} = \lambda Id_F$, est λI_k donc triangulaire.

D'autre part E/F est un K-ev de dimension $n+1-k \leq n$ auquel on peut appliquer l'hypothèse de récurrence : il existe une base $(\bar{e}_{k+1}, ..., \bar{e}_{n+1})$ dans laquelle $\bar{u}$ se trigonalise.

On choisit maintenant pour chaque i un vecteur e_i dans E qui se projette par la projection canonique sur $\bar{e}_i$: la famille $(e_1, ..., e_{n+1})$ est alors une base de E dans laquelle u se trigonalise. □

2.3. Polynômes d'endomorphismes

2.3.1. Puissances d'un endomorphisme

Définition 2.19. *Soit u un endomorphisme de E. On définit par récurrence sur k la puissance k-ième de u pour tout $k \in \mathbb{N}$:*

$$\begin{cases} u^0 = \mathrm{Id}_E; \\ u^{k+1} = u \circ u^k. \end{cases}$$

2.3.2. Sous-algèbre engendrée par un endomorphisme

Définition 2.20. *Soit $P = \sum_{i \geq 0} a_i X^i$ un polynôme de $K[X]$. On note $P(u)$ l'endomorphisme $\sum_{i \geq 0} a_i u^i$ de E.*

Théorème - Définition 2.21. *L'application de $K[X]$ vers $\mathcal{L}(E)$ qui envoie P sur $P(u)$ est un morphisme de K-algèbres. Son noyau est appelé **idéal annulateur de** u. Son image est notée $K(u)$.* □

Théorème - Définition 2.22. *Il existe un unique polynôme unitaire qui engendre l'idéal annulateur de u. On l'appelle **polynôme minimal de** u, et on le note μ_u.*

Démonstration. Comme $K[X]$ est principal, il s'agit de montrer que l'idéal annulateur n'est pas réduit à $\{0\}$. Or, si c'était le cas, l'application $P \to P(u)$ serait injective. C'est impossible car le K-ev $K[X]$ est de dimension infinie, et pas $\mathcal{L}(E)$. □

Proposition 2.23.

— *Un polynôme P est un multiple de μ_u si et seulement si $P(u) = 0$.*

— *En particulier, si v est la restriction de u à un sev u-invariant, alors μ_v divise μ_u.* □

2.3.3. Théorème de Cayley-Hamilton

Théorème 2.24 (admis)**.** *Soit P_u le polynôme caractéristique d'un endomorphisme u de E. Alors, $P_u(u) = 0$.*

En particulier :

Corollaire 2.25. *Le polynôme minimal μ_u divise le polynôme caractéristique P_u.* □

On en déduit un critère utile pour caractériser le polynôme minimal :

Proposition 2.26. *Les racines du polynôme minimal sont exactement celles du polynôme caractéristique.*

Démonstration. Comme μ_u divise P_u, il est clair que les racines de μ_u sont toutes des racines de P_u.

Inversement, soit λ une racine de P_u, i.e. une valeur propre de u. Soit x un vecteur propre (donc non-nul) de u pour la valeur propre λ. Alors, pour tout entier k, on a $u^k(x) = \lambda^k x$. Notons $\mu_u = \sum a_i X^i$:

$$\begin{aligned} \mu_u(u)(x) &= \sum a_i u^i(x) \\ &= \sum a_i \lambda^i x \\ &= \mu_u(\lambda)x \end{aligned}$$

Comme μ_u annule u, et comme x est non-nul, on en déduit comme voulu $\mu_u(\lambda) = 0$. □

2.4. Réduction de Jordan

2.4.1. Décomposition des noyaux

Théorème 2.27. *Soit u un endomorphisme de $\mathcal{L}(E)$ et $P_1, \ldots, P_k$ des polynômes de $K[X]$ premiers entre eux deux-à-deux, et P le produit de ces polynômes. Soit N le noyau de $P(u)$ et N_i le noyau de $P_i(u)$. Alors, N est la somme directe des N_i :*

$$N = N_1 \oplus \ldots \oplus N_k$$

Démonstration. L'inclusion $N_i \subset N$ est évidente, car $P(u) = (\ldots) \circ P_i(u)$, donc la somme $N_1 + \ldots + N_k$ (qu'on ne sait pas encore être directe) est contenue dans N.

Récurrence sur k.

- **Si $k = 1$:** Évident.
- **Si $k = 2$:** Alors $P = P_1P_2$, et d'après Bezout, il existe deux polynômes Q_1, Q_2 de $K[X]$ tels que $1 = Q_1P_1 + Q_2P_2$. En évaluant sur u : $\mathrm{Id}_E = q_1 \circ p_1 + q_2 \circ p_2$ où $p_i = P_i(u)$, $q_i = Q_i(u)$.

  On sait $N_1 + N_2 \subset N$. Soit x dans N : alors $x = x_1 + x_2$ avec $x_1 = q_2(p_2(x))$ et $x_2 = q_1(p_1(x))$. Or $p_1(x_1) = (p_1q_2p_2)(x) = (Q_2P)(u)(x) = 0$ car $x \in N$. De même, $x_2 \in N_2$, d'où $x \in N_1 + N_2$: nous avons montré $N = N_1 + N_2$.

  Soit $x \in N_1 \cap N_2$: $x = \mathrm{Id}_E(x) = q_1(p_1(x)) + q_2(p_2(x)) = 0 + 0 = 0$. D'où $N = N_1 \oplus N_2$.
- **Si $k \geq 3$: :** $P = P_1P_2'$ où $P_2' = P_2P_3 \ldots P_k$. On applique le cas $k = 2$ à ces deux polynômes :

  $$\ker P(u) = \ker P_1(u) \oplus \ker P_2'(u)$$

  Or, par hypothèse de récurrence :

  $$\ker P_2'(u) = \ker P_2(u) \oplus \ldots \oplus \ker P_k(u)$$

  Donc :

  $$N = \ker P(u) = \ker P_1(u) \oplus (\ker P_2(u) \oplus \ldots \oplus \ker P_k(u)) = N_1 \oplus \ldots \oplus N_k$$

□

□

Corollaire 2.28. *Si P est dans l'idéal annulateur de u (ie. $P(u) = 0$) alors :*

$$E = N_1 \oplus \ldots \oplus N_k$$

□

Ce corollaire s'applique au cas $P = \mu_u$, ou encore $P = P_u$ grâce au Théorème de Cayley-Hamilton.

2.4.2. Sous-espaces caractéristiques Dans toute cette section, u désigne un endomorphisme de $\mathcal{L}(E)$ dont le polynôme caractéristique est scindé (par exemple, si K est algébriquement clos). Alors :

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

où les λ_i sont les valeurs propres de u deux-à-deux distinctes.

D'après le Théorème de Cayley-Hamilton, on a :

$$\mu_u = \prod_{i=1}^{p}(X - \lambda_i)^{r_i}$$

avec $1 \leq r_i \leq m_i$.

Définition 2.29. *Le sous-espace caractéristique associé à λ_i est le noyau de $(\lambda_i \mathrm{Id}_E - u)^{r_i}$. On le note $N_i(u)$.*

D'après le Corollaire 2.28 :

Théorème 2.30. *E est la somme directe des sous-espaces caractéristiques $N_i(u)$:*

$$E = N_1(u) \oplus ... \oplus N_p(u)$$

□

Proposition 2.31. *Chaque $N_i(u)$ est u-invariant, et la seule valeur propre de la restriction de u à $N_i(u)$ est λ_i. Le polynôme minimal de $u_{|N_i(u)}$ est $(X - \lambda_i)^{r_i}$.*

Démonstration. En effet, si $(\lambda_i \mathrm{Id}_E - u)^{r_i}(x) = 0$, alors :

$$(\lambda_i \mathrm{Id}_E - u)^{r_i}(u(x)) = ((\lambda_i \mathrm{Id}_E - u)^{r_i} u)(x) = u((\lambda_i \mathrm{Id}_E - u)^{r_i}(x)) = u(0) = 0$$

ce qui montre que $N_i(u)$ est u-invariant.

Le sous-espace propre de u associé à λ_i est évidemment contenu dans $N_i(u)$, donc λ_i est valeur propre de $u_{|N_i(u)}$.

Si x est un vecteur propre de $u_{|N_i(u)}$ associé à une valeur propre λ, alors λ est aussi valeur propre de u, donc un des λ_j. Or, $N_i(u) \cap N_j(u) = \{0\}$ sauf si $i = j$: donc la seule valeur propre de $u_{|N_i(u)}$ est $\lambda = \lambda_i$.

Enfin, $(u - \lambda_i \mathrm{Id})^{r_i}$ s'annule évidemment sur $N_i(u)$, donc le polynôme minimal μ_i de $u_{|N_i(u)}$ divise $(X - \lambda_i)^{r_i}$. De plus, le produit de μ_i avec tous les $(X - \lambda_j)^{r_j}$ est un polynôme annulateur de u : il est donc divisé par μ_u. On en déduit que $(X - \lambda_i)^{r_i}$ est exactement le polynôme minimal de $u_{|N_i(u)}$. □

Proposition 2.32. *Soit m_i la multiplicité de la racine λ_i de P_u. Alors :*

$$\dim N_i(u) = m_i$$

Le polynôme caractéristique de $u_{|N_i(u)}$ est $(X - \lambda_i)^{m_i}$.

Démonstration. Soit n_i la dimension de $N_i(u)$. Le polynôme caractéristique de $u_{|N_i(u)}$ est $(X - \lambda_i)^{n_i}$ puisque λ_i est la seule valeur propre de $u_{|N_i(u)}$. Or, la décomposition en facteurs directs $E = N_1(u) \oplus ... \oplus N_p(u)$ montre (calcul d'un déterminant par blocs) que le déterminant de $X\mathrm{Id}_E - u$ est le produit des déterminants des restrictions aux $N_i(u)$. Donc P_u est le produit de tous les $(X - \lambda_i)^{n_i}$. □

Proposition 2.33. *Un endomorphisme u de E est diagonalisable si et seulement si son polynôme minimal est scindé sur K et n'a que des racines simples (de multiplicité un).*

Démonstration. Supposons u diagonalisable. Il est clair que $(X - \lambda_1)...(X - \lambda_p)$ est un polynôme annulateur de u, et doit donc être divisible par $\mu_u = \prod_{i=1}^{p}(X - \lambda_i)^{r_i}$. Comme μ_u est minimal, on doit avoir $r_i = 1$ pour tout i.

Inversement, si μ_u est scindé et $r_i = 1$ pour tout i, alors $X - \lambda_i$ annule $u_{|N_i(u)}$. Ceci signifie que $u_{|N_i(u)}$ est une homothétie, et donc, que u est diagonalisable. □

2.4.3. Endomorphismes nilpotents Pour achever la description de u, il suffit de comprendre sa restriction à chaque sous-espace caractéristique $N_i(u)$. Or, cette restriction est de la forme $u_{|N_i(u)} = \lambda_i \mathrm{Id}_{N_i(u)} + n_i$, où $n_i = u_{|N_i(u)} - \lambda_i \mathrm{Id}_{N_i(u)}$. Et ce n_i est nilpotent au sens suivant :

Définition 2.34. *Un endomorphisme u de $\mathcal{L}(E)$ est **nilpotent** s'il existe un entier k tel que $u^k = 0$. Le plus petit entier tel que $u^k = 0$ est appelé **indice de u**.*

Proposition 2.35. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent d'indice r. Alors le polynôme minimal de u est X^r.* □

Nous allons montrer que pour tout endomorphisme nilpotent, il existe une base dans laquelle l'endomorphisme s'exprime par une matrice à la forme particulièrement simple.

Étudions d'abord les matrices candidates à ce rôle :

Définition 2.36. *Une **matrice nilpotente de Jordan élémentaire** est une matrice carrée $(a_{ij})_{1\leq i,j\leq n}$ dont les coefficients sont nuls, sauf ceux «juste au-dessus de la diagonale», ie. les a_{ij} avec $j = i+1$, pour lesquels on a $a_{i,i+1} = 1$.*

Pour tout n, il existe donc une unique matrice nilpotente de Jordan dans $\mathrm{Mat}(n, K)$. Pour $n = 3$, il s'agit de :

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Proposition 2.37. *Tout endomorphisme u d'un K-espace vectoriel E de dimension n est nilpotent d'indice n si et seulement si il existe une base de E dans laquelle u s'exprime sous la forme de la matrice nilpotente de Jordan élémentaire de* $\mathrm{Mat}(n, K)$.

Démonstration.

- **La condition est suffisante :** Soit $(e_1, ..., e_n)$ une base pour laquelle la matrice associée à u soit nilpotente de Jordan. Alors si $i \neq 0$, $u(e_{i+1}) = e_i$, et $u(e_1) = 0$, donc $u^n(e_i) = 0$ pour tout i. Tous les éléments de la base sont dans $\ker u^n$, donc u^n est nul. L'indice est exactement n puisque $u^{n-1}(e_n) = e_1 \neq 0$.
- **La condition est nécessaire :** On montre l'assertion par récurrence sur n. Supposons u nilpotent d'indice n. Alors, $u^n = 0$ mais $u^{n-1} \neq 0$. Soit e_n un élément de E tel que $u^{n-1}(e_n) \neq 0$. On choisit alors $e_i := u^{n-i}(e_n)$. Remarquons que pour tout i, on a $u^i(e_i) = u^{i+n-i}(e_n) = u^n(e_n) = 0$, mais $u^{i-1}(e_i) = u^{i-1+n-i}(e_n) \neq 0$.

  Il s'agit de montrer que les e_i forment une base de E. Pour ce faire, il suffit de montrer que c'est une famille libre : supposons par l'absurde qu'il existe des scalaires α_1, ... , α_n non tous nuls et tels que $0 = \sum_{i=1}^{n} \alpha_i e_i$. Soit k le plus grand indice i tel que $\alpha_i \neq 0$: alors $e_k = \sum_{i=1}^{k-1} \alpha_k^{-1} \alpha_i e_i$. Comme tous les $u^{k-1}(e_i)$ pour $i < k$ sont nuls, on en déduit $u^{k-1}(e_k) = 0$. Contradiction.

□

Nous sommes maintenant près à traiter le cas général :

Définition 2.38. *Une **matrice nilpotente de Jordan** est une matrice carrée $(a_{ij})_{1\leq i,j\leq n}$ dont les coefficients sont nuls, sauf ceux «juste au-dessus de la diagonale», ie. les a_{ij} avec $j = i+1$ pour lesquels on a soit $a_{i,i+1} = 1$, soit $a_{i,i+1} = 0$.*

Théorème 2.39. *Tout endomorphisme u d'un K-espace vectoriel E est nilpotent si et seulement si il existe une base de E dans laquelle u s'exprime sous la forme d'une matrice nilpotente de Jordan.*

Démonstration. On montre comme précédemment que la condition est suffisante : ce qui change c'est que $u(e_{i+1})$ n'est pas forcément e_i ; mais c'est alors 0. Ainsi, çà ne fait qu'accélérer l'annulation des e_i sous l'itération par u.

Supposons maintenant que u soit nilpotent d'indice r. Pour tout entier i soit F_i le noyau de u^i. On a $F_i = E$ si $i \geq r$, et $F_0 = \{0\}$ (car $u^0 = \mathrm{Id}_E$). On a aussi les inclusions :

$$\{0\} = F_0 \subset F_1 \subset ... \subset F_{r-1} \subset F_r = E$$

Chacune de ces inclusions est stricte : en effet, s'il existe i entre 0 et $r-1$ tel que $F_{i+1} = F_i$, alors pour tout x dans E on a $u^{i+1}(u^{r-i-1}(x)) = u^r(x) = 0$, donc $u^{r-i-1}(x)$ appartient à F_{i+1} ; comme ce dernier est supposé égal à F_i, on obtient $0 = u^i(u^{r-i-1}(x)) = u^{r-1}(x)$ or par définition, r est le plus petit entier i tel que $u^i = 0$.

On choisit un supplémentaire G_0 de F_{r-1} dans $E = F_r$:

$$E = F_r = G_0 \oplus F_{r-1}$$

Nous allons montrer ensuite, par récurrence sur i, qu'on peut continuer en choisissant pour tout i $(0 \leq i \leq r-1)$ un supplémentaire G_i de F_{r-i-1} dans F_{r-i} de sorte que $u(G_{i-1}) \subset G_i$.

Supposons qu'on ait déjà construit G_0, ... , G_{i-1} :

$$F_{r-i+1} = G_{i-1} \oplus F_{r-i}$$

Comme $u(F_{r-i+1}) \subset F_{r-i}$ on a $u(G_{i-1}) \subset F_{r-i}$. En outre, comme G_{i-1} est contenu dans $\{0\} \cup F_{r-i+1} \backslash F_{r-i}$, son image par u ne rencontre F_{r-i-1} qu'en 0. Il existe donc dans F_{r-i} un supplémentaire G_i de F_{r-i-1} contenant $u(G_{i-1})$. cqfd.

Remarquons que comme $\ker u = F_0 \subset F_{r-i}$, on a $G_{i-1} \cap \ker u = \{0\}$: la restriction de u à G_i est injective. Remarquons aussi que G_{r-1} est dans $F_1 = \ker u$ un supplémentaire de $F_0 = \{0\}$ ie. F_1 tout entier. On en déduit que :

$$E = G_0 \oplus G_1 \oplus ... \oplus G_{r-1}$$

On choisit dans G_0 une base $(x_1, ..., x_k)$. Comme la restriction de u à G_0 est injective, la famille $(u(x_1), ..., u(x_k))$ est libre ; on peut la compléter en une base de G_1. On peut itérer le procédé, construisant dans chaque G_i une base $\bar{b}_i$ de sorte que, pour tout i, la base $\bar{b}_i$ contiennent les images par u de la base $\bar{b}_{i-1}$ de G_{i-1}. Comme E est la somme directe de tous les G_i, l'ensemble de ces bases définit une base B de E.

On remarque alors que, quitte à permuter les éléments de B, l'expression de u dans cette base est une matrice nilpotente de Jordan. □

2.4.4. Décomposition de Jordan On déduit du théorème précédent :

Théorème - Définition 2.40. *Soit u un endomorphisme de E dont le polynôme caractéristique est scindé sur K (c'est automatique si K est algébriquement clos). Alors il existe un unique couple n, d d'éléments de $\mathcal{L}_K(E)$ tels que :*
— $u = n + d$,
— *n est nilpotent,*
— *d est diagonalisable sur K,*
— $nd = dn$. □

Il existe alors une base de E dans lequel la matrice associée à u est de la forme «par blocs» suivante :

$$\begin{pmatrix} A_1 & 0 & ... & ... & 0 \\ 0 & A_2 & ... & ... & ... \\ ... & ... & ... & ... & ... \\ ... & ... & ... & A_{k-1} & 0 \\ 0 & 0 & ... & 0 & A_k \end{pmatrix}$$

où chaque A_i est une matrice carrée de la forme :

$$A_i = \begin{pmatrix} \lambda_i & 1 \text{ ou } 0 & 0 & ... & 0 \\ 0 & \lambda_i & 1 \text{ ou } 0 & ... & ... \\ ... & ... & ... & ... & ... \\ ... & ... & ... & \lambda_i & 1 \text{ ou } 0 \\ 0 & 0 & ... & 0 & \lambda_i \end{pmatrix}$$

ie. de la forme $\lambda_i I_p + J_p$ où λ_i est une valeur propre de u et J_p est une matrice nilpotente de Jordan.