

MÉMOIRE DE MASTER 2

LEÇON 151

**Sous-espaces stables par un endomorphisme ou
une famille d'endomorphismes d'un espace
vectoriel de dimension finie. Applications.**

ÉTIENNE AFFALOU
École Normale Supérieure de Rennes

Encadrant : CHRISTOPHE MOURUGANE

Année scolaire 2025-2026



école
normale
supérieure



**Université
de Rennes**

Introduction

Quand on fait de la diagonalisation des endomorphismes en dimension finie, on cherche des droites stables en somme directe. Dans un cadre tout à fait général, on ne peut pas toujours trouver une décomposition de l'espace en somme directe de droites stables.

On relaxe donc l'hypothèse sur la dimension des sous-espaces stables recherchés, pour aboutir à une réduction par blocs. Pour obtenir un théorème de trigonalisation par blocs, chercher un sous-espace stable suffit, puisque prendre un supplémentaire quelconque donne une matrice triangulaire supérieure par blocs. Par contre, si on décide de faire de la diagonalisation par blocs, on recherche un sous-espace vectoriel stable qui admet un supplémentaire stable.

L'objectif de ce mémoire est entre autres de mettre en valeur trois grandes méthodes pour le recherche d'un supplémentaire stable : le lemme des noyaux qui donne directement une décomposition en somme directe de sous-espaces stables, l'orthogonalité dans le cadre euclidien pour les endomorphismes normaux, et la dualité pour trouver la réduction de Frobenius ainsi que les invariants de similitude.

Au passage, on s'intéresse à certains critères de réduction simultanée dans le cas d'une famille d'endomorphismes. On verra que la condition nécessaire et suffisante de commutativité pour la co-diagonalisation devient une condition suffisante pour la co-trigonalisation. On montrera alors le théorème de Lie-Kolchin qui permet de donner un critère algébrique et topologique sur la famille d'endomorphismes pour avoir de la co-trigonalisation.

Plan de la leçon

1	Généralités	2
1.1	Sous-espaces stables, endomorphisme induit	2
1.2	Dualité	3
1.3	Lemme des noyaux	4
2	Applications à la réduction	5
2.1	Sous-espaces propres, sous-espaces caractéristiques	5
2.2	Réduction simultanée	7
2.3	Réduction	8
3	Endomorphismes remarquables	10
3.1	Endomorphismes cycliques	10
3.2	Endomorphismes normaux	13

1 Généralités

1.1 Sous-espaces stables, endomorphisme induit

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel. Soit $u \in \mathcal{L}(E)$.
On dit qu'un sous-espace vectoriel F de E est **stable** par u lorsque $u(F) \subset F$.

RAPPEL : Soit E un espace vectoriel sur un corps $\mathbb{K}$. Soit $u \in \mathcal{L}(E)$. Par la propriété universelle de l'anneau de polynômes $\mathbb{K}[X]$, il existe un unique morphisme de $\mathbb{K}$ -algèbres de $\mathbb{K}[X]$ dans $\mathcal{L}(E)$ défini par

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

L'image de ce morphisme est l'ensemble des polynômes en u , noté $\mathbb{K}[u]$. Si $P \in \mathbb{K}[X]$, on note $P(u)$ au lieu de $\varphi_u(P)$.

EXEMPLES : Si $u \in \mathcal{L}(E)$, l'image $\text{Im}(u)$ de u et les noyaux $\ker(P(u))$ pour $P \in \mathbb{K}[X]$ sont stables par u .

MOTIVATION Soit $u \in \mathcal{L}(E)$ avec E un $\mathbb{K}$ -espace vectoriel de dimension finie. Si on arrive à décomposer E en somme directe de sous-espaces $F_1, \dots, F_p$ qui sont tous stables par u , alors dans une base adaptée à la décomposition, la matrice de u est diagonale par blocs.

REMARQUE : Si un sous-espace vectoriel F d'un espace vectoriel E est stable par deux endomorphismes u et v , alors F est stable par toute combinaison linéaire de u et v , et F est stable par $u \circ v$.

PROPOSITION 1.1.1 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel. Soient $u \in \mathcal{L}(E)$ et $v \in \text{GL}(E)$.
Si F est un sous-espace vectoriel de E stable par u , alors $v(F)$ est stable par $v \circ u \circ v^{-1}$.

PREUVE : Supposons que F est un sous-espace vectoriel de E stable par u . Soit $y \in v(F)$. Par définition, $\exists x \in F$ tel que $y = v(x)$. Ainsi,

$$(v \circ u \circ v^{-1})(y) = v(u(v^{-1}(y))) = v(u(v^{-1}(v(x)))) = v(u(x)) \in v(F)$$

car $u(x) \in F$. Ainsi, $(v \circ u \circ v^{-1})(y) \in v(F)$, et donc $v(F)$ est stable par $v \circ u \circ v^{-1}$.

La notion d'endomorphisme induit est à bien distinguer de la notion de restriction à un sous-espace vectoriel.

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel. Soit $u \in \mathcal{L}(E)$.
Si F est un sous-espace vectoriel de E stable par u , l'endomorphisme **induit** par u sur F est l'endomorphisme $u_F \in \mathcal{L}(F)$ défini par $\forall x \in F, u_F(x) = u(x)$.

RAPPEL : Soit E un espace vectoriel de dimension finie sur un corps $\mathbb{K}$. Soit $u \in \mathcal{L}(E)$. Le morphisme de $\mathbb{K}$ -algèbres $\varphi_u : \mathbb{K}[X] \rightarrow \mathcal{L}(E)$ ne peut pas être injectif. En effet, $\mathbb{K}[X]$ est de dimension infinie sur $\mathbb{K}$ alors que $\mathcal{L}(E)$ est de dimension finie égale à $\dim(E)^2$. On en déduit que l'idéal $\ker(\varphi_u)$ n'est pas trivial. Ainsi, il existe un polynôme $\mu_u \in \mathbb{K}[X]$, que l'on peut prendre unitaire pour le rendre unique, tel que $\ker(\varphi_u)$ est l'idéal engendré par μ_u . Ce polynôme μ_u est appelé **polynôme minimal** de u , et fournit un isomorphisme $\mathbb{K}[X]/(\mu_u) \simeq \mathbb{K}[u]$.

PROPOSITION 1.1.2 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel. Soit $u \in \mathcal{L}(E)$.
Si F est un sous-espace vectoriel de E stable par u , alors $\mu_{u_F} \mid \mu_u$.

PREUVE : Pour tout $x \in F$, on a $\mu_u(u_F)(x) = \mu_u(u)(x) = 0$, donc μ_u annule u_F . Ainsi, $\mu_{u_F} \mid \mu_u$.

COROLLAIRE Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel. Soit $u \in \mathcal{L}(E)$.
On suppose que $E = F \oplus G$ avec F et G stables par u . Alors $\mu_u = \mu_{u_F} \vee \mu_{u_G}$.

PREUVE : Par la proposition 1.1.2, μ_{u_F} et μ_{u_G} divisent μ_u . Donc $\mu_{u_F} \vee \mu_{u_G}$ divise μ_u .

Mais pour tout $x \in E$, $\exists(x_F, x_G) \in F \times G$ tel que $x = x_F + x_G$ d'où

$$\begin{aligned}(\mu_{u_F} \vee \mu_{u_G})(u)(x) &= (\mu_{u_F} \vee \mu_{u_G})(u)(x_F) + (\mu_{u_F} \vee \mu_{u_G})(u)(x_G) \\ &= (\mu_{u_F} \vee \mu_{u_G})(u_F)(x_F) + (\mu_{u_F} \vee \mu_{u_G})(u_G)(x_G) \\ &= 0.\end{aligned}$$

Donc $\mu_{u_F} \vee \mu_{u_G}$ annule u , et on en déduit que $\mu_{u_F} \vee \mu_{u_G} = \mu_u$.

EXEMPLES : On étudie les sous-espaces stables par des endomorphismes particuliers. Soit E un $\mathbb{K}$ -espace vectoriel.

- Toute droite vectorielle de E est stable par une homothétie u .
Inversement, si $u \in \mathcal{L}(E)$ stabilise les droites vectorielles de E , alors $\forall x \in E, \exists \lambda_x \in \mathbb{K}$ tel que $u(x) = \lambda_x x$. Soient $x, y \in E \setminus \{0\}$. Si la famille (x, y) est liée, alors $\exists \mu \in \mathbb{K}$ tel que $y = \mu x$ et $\lambda_y y = u(y) = u(\mu x) = \mu \lambda_x x = \lambda_x y$ donc comme $y \neq 0$, on a $\lambda_x = \lambda_y$. Sinon, (x, y) est libre. Dans ce cas, on a $\lambda_x x + \lambda_y y = u(x) + u(y) = u(x + y) = \lambda_{x+y}(x + y)$. Par liberté, on a $\lambda_x = \lambda_{x+y} = \lambda_y$. On en déduit que $\exists \lambda \in \mathbb{K}$ tel que $\forall x \in E \setminus \{0\}, u(x) = \lambda x$. C'est vrai aussi quand $x = 0$, donc u est une homothétie de rapport λ .
- Soit $p \in \mathcal{L}(E)$ un projecteur. On va montrer que F est stable par p si et seulement si $F = A \oplus B$ avec A un sous-espace vectoriel de $\ker(p)$ et B un sous-espace vectoriel de $\text{Im}(p)$.
Soit F un sous-espace vectoriel de E stable par p . Comme p est un projecteur, l'induit p_F est encore un projecteur, donc $F = \ker(p_F) \oplus \text{Im}(p_F)$ (en effet, si $x \in F$, alors $x = x - p_F(x) + p_F(x)$ avec $x - p_F(x) \in \ker(p_F)$ et $p_F(x) \in \text{Im}(p_F)$, et si $y \in \ker(p_F) \cap \text{Im}(p_F)$, alors $\exists x \in F$ tel que $y = p_F(x)$ et $0 = p_F(y) = p_F^2(x) = p_F(x) = y$). Ainsi, F est somme directe d'un sous-espace vectoriel de $\ker(p)$ et d'un sous-espace vectoriel de $\text{Im}(p)$.
Inversement, si $F = A \oplus B$ avec A un sous-espace de $\ker(p)$ et B un sous-espace de $\text{Im}(p)$, alors F est stable par p . En effet, si $x \in F$, alors $\exists(x_A, x_B) \in A \times B$ tel que $x = x_A + x_B$ d'où $p(x) = p(x_A) + p(x_B)$, avec $x_B = p(x')$ pour un certain $x' \in E$, de sorte que $p(x) = 0 + p(x') = x_B \in F$.
- On suppose que la caractéristique de $\mathbb{K}$ est différente de 2. Soit $s \in \mathcal{L}(E)$ une symétrie. Montrons que F est stable par s si et seulement si $F = A \oplus B$ avec A un sous-espace vectoriel de $\ker(s - \text{id}_E)$ et B un sous-espace vectoriel de $\ker(s + \text{id}_E)$.
Si F est un sous-espace vectoriel de E stable par s , comme précédemment, l'induit s_F de s sur F est encore une symétrie. On montre alors que $F = \ker(s_F - \text{id}_F) \oplus \ker(s_F + \text{id}_F)$. Si $x \in F$, on a $2x = s_F(x) + x - (s_F(x) - x)$ donc comme $2 \neq 0$, $x = ((s_F(x) + x)/2) - ((s_F(x) - x)/2)$. De plus, si $y \in \ker(s_F - \text{id}_F) \cap \ker(s_F + \text{id}_F)$, $\exists x_1, x_2 \in F$ tels que $y = s_F(x_1) - x_1 = s_F(x_2) + x_2$. Ainsi, $s_F(y) = x_1 - s_F(x_1) = x_2 + s_F(x_2)$, d'où $y = s_F(x_2) + x_2 = -(s_F(x_1) - x_1) = -y$ et $2y = 0$ et comme $2 \neq 0$, $y = 0$.
Le sens réciproque se traite comme le cas des projecteurs, toujours en utilisant le fait que $s^2 = \text{id}_E$.
Une autre méthode consiste à écrire $s = 2p - \text{id}_E$ où $p^2 = p$ pour utiliser ce qu'on vient de faire sur les projecteurs. En effet, on aura $(s + \text{id}_E)/2 = p$, donc $\ker(s + \text{id}_E)$ et $\text{Im}(s + \text{id}_E)$ sont stables par p , avec $\text{Im}(s + \text{id}_E) = \ker(s - \text{id}_E)$ (l'inclusion $\text{Im}(s + \text{id}_E) \subset \ker(s - \text{id}_E)$ se fait bien, et l'autre inclusion se fait en écrivant $x = s(x/2) + (x/2)$ pour $x \in \ker(s - \text{id}_E)$).

1.2 Dualité

Si E est un espace vectoriel de dimension finie sur un corps $\mathbb{K}$, on note E^* l'espace vectoriel sur $\mathbb{K}$ des applications linéaires de E dans $\mathbb{K}$ (l'ensemble des formes linéaires sur E).

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel. Soit $A \subset E$.

L'**orthogonal** de A est $A^\perp = \{\varphi \in E^* \mid \forall x \in A, \varphi(x) = 0\}$. C'est un sous-espace vectoriel de E^* .

DÉFINITION Soit $\mathbb{K}$ un corps. Soient E et F deux $\mathbb{K}$ -espaces vectoriels. Soit $u \in \mathcal{L}(E, F)$.

La **transposée** de u , notée u^T est l'application linéaire

$$\begin{aligned}u^T : F^* &\longrightarrow E^* \\ \varphi &\longmapsto \varphi \circ u\end{aligned}$$

PROPOSITION 1.2.1 Soient E un espace vectoriel de dimension finie et F un sous-espace vectoriel de E .

Soit $u \in \mathcal{L}(E)$. Alors, F est stable par u si et seulement si $F^\perp$ est stable par u^T .

PREUVE : Supposons que F est stable par u . Dans ce cas, $\forall \varphi \in F^\perp, \forall x \in F$, on a

$$u^T(\varphi)(x) = (\varphi \circ u)(x) = \varphi(u(x)) = 0$$

car $u(x) \in F$. Ainsi, $F^\perp$ est stable par u^T . Inversement, si $F^\perp$ est stable par u^T , on a $\forall \varphi \in F^\perp, \forall x \in F$, $0 = u^T(\varphi)(x) = \varphi(u(x))$. En spécifiant à φ nulle uniquement sur F (c'est possible en dimension finie), on en déduit que $u(x) \in F$ donc que F est stable par u .

REMARQUE : Nous ferons usage de la dualité pour donner les invariants de similitude d'un endomorphisme en dimension finie (voir la sous-partie 3.1).

1.3 Lemme des noyaux

Un outil élémentaire mais très utile pour la recherche de sous-espaces vectoriels stables est le suivant.

LEMME Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel. Soit $u \in \mathcal{L}(E)$. Soient $N \in \mathbb{N}^*$ et $P_1, \dots, P_N \in \mathbb{K}[X]$. On pose $P = P_1 \cdots P_N$ et on suppose que les P_k sont premiers entre eux deux à deux. Alors,

$$\ker(P(u)) = \bigoplus_{k=0}^N \ker(P_k(u)).$$

De plus, les projecteurs de $\ker(P(u))$ sur $\ker(P_i(u))$ sont des polynômes en u .

PREUVE : Pour tout $j \in \{1, \dots, N\}$, on pose $Q_j = \prod_{k \neq j} P_k$.

Les Q_j sont premiers entre eux dans leur ensemble, donc $\exists A_1, \dots, A_N \in \mathbb{K}[X]$ tels que $1 = A_1 Q_1 + \dots + A_N Q_N$. En effet, si le pgcd des Q_k est non constant, il a un diviseur irréductible, qui divise Q_1 donc P_j , et Q_j donc P_i pour $i \neq j$ ce qui est absurde par hypothèse sur les P_k .

Soit $x \in \ker(P(u))$. L'algèbre $\mathbb{K}[u]$ est commutative, donc si $j \in \{1, \dots, N\}$, $x_j = A_j(u)(Q_j(u))(x) \in \ker(P_j(u))$.

Comme $x = x_1 + \dots + x_N$, il suffit de montrer que la somme est directe pour conclure.

Or si $x_1 + \dots + x_N = 0$ où $\forall k \in \{1, \dots, N\}, x_k \in \ker(P_k(u))$, alors en appliquant successivement les $A_k(u) \circ Q_k(u)$, on obtient $x_k = 0$ pour $k \in \{1, \dots, N\}$ et la somme est directe.

De plus, vu le travail qui précède, le projecteur de $\ker(P(u))$ dans $\ker(P_k(u))$ est $A_k(u) \circ Q_k(u)$.

REMARQUE : En particulier, si P est annulateur de u dans l'énoncé du lemme des noyaux, alors on a une décomposition en somme directe de tout l'espace. Si on se place en dimension finie, on obtient la **décomposition de Fitting** suivante.

THÉORÈME 1.3.1 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.

Alors, il existe un unique couple (N, F) de sous-espaces vectoriels de E stables par u tels que $E = N \oplus F$, u_N est nilpotent et u_F est inversible.

De plus, il existe $d \in \mathbb{N}$ tel que pour $n \in \mathbb{N}$, $n \geq d$, on a $N = \ker(u^n)$ et $F = \text{Im}(u^n)$.

PREUVE : On écrit $\mu_u(X) = X^d Q(X)$ avec $d \in \mathbb{N}$ et $Q(0) \neq 0$, de sorte que X^d et Q soient premiers entre eux. On applique le lemme des noyaux pour obtenir $E = \ker(u^d) \oplus \ker(Q(u))$. On pose $N = \ker(u^d)$ et $F = \ker(Q(u))$. En tant que noyaux de polynômes en u , N et F sont des sous-espaces vectoriels stables par u tels que $E = N \oplus F$, et u_N est nilpotent car $u_N^d = 0$. De plus, u_F est injectif car $\ker(u_F) = \ker(u) \cap F \subset N \cap F = \{0\}$. On en déduit que u_F est inversible car E est de dimension finie.

Supposons que $E = N' \oplus F'$ où N' et F' sont deux sous-espaces vectoriels de E stables par u tels que $u_{N'}$ est nilpotent et $u_{F'}$ est inversible. Les polynômes $\mu_{u_{N'}}$ et $\mu_{u_{F'}}$ sont premiers entre eux, car $\mu_{u_{N'}}(X)$ est une puissance de X ($u_{N'}$ est nilpotent) alors que $\mu_{u_{F'}}(X)$ n'est pas multiple de X car $u_{F'}$ est injectif. Ainsi, par le corollaire de la proposition 1.1.2, on a $\mu_u = \mu_{u_{N'}} \mu_{u_{F'}}$. On en déduit que $\mu_{u_{N'}} = X^d$ et que $\mu_{u_{F'}} = Q$.

Ainsi, $N' \subset N$. Inversement, si $x \in N$, on a $x = x_{N'} + x_{F'}$ avec $x_{N'} \in N'$ et $x_{F'} \in F'$, donc en appliquant u^d , on obtient $u^d(x_{F'}) = u_{F'}^d(x_{F'}) = 0$, ce qui fournit $x_{F'} = 0$ car $u_{F'}$ est injectif, d'où $x = x_{N'} \in N'$. Ainsi, $N = N'$. Si $x \in F'$, alors $Q(u)(x) = Q(u_{F'})(x) = 0$ car $\mu_{u_{F'}} = Q$, d'où $x \in F$. Donc $F' \subset F$ et par égalité des dimensions, on a bien $F = F'$.

On a prouvé l'existence et l'unicité, il reste à montrer que $F = \text{Im}(u^d)$. Soit $x \in F$.

Comme Q et X^d sont premiers entre eux, $\exists A, B \in \mathbb{K}[X]$ tels que $1 = AQ + BX^d$ d'où $x = A(u)(Q(u)(x)) + B(u)(u^d(x)) = B(u)(u^d(x)) = u^d(B(u)(x)) \in \text{Im}(u^d)$. Ainsi, $F \subset \text{Im}(u^d)$ et par le théorème du rang, on a

$\dim(\text{Im}(u^d)) = \dim(E) - \dim(\ker(u^d)) = \dim(\ker(Q(u)))$ d'où $F = \text{Im}(u^d)$.

Enfin, on montre que $\ker(u^{d+1}) = \ker(u^d)$, on aura $\text{Im}(u^{d+1}) = \text{Im}(u^d)$ par inclusion et égalité des dimensions, puis par récurrence on aura terminé.

Tout d'abord, on a toujours $\ker(u^d) \subset \ker(u^{d+1})$. Maintenant si $x \in \ker(u^{d+1})$, on écrit $x = x_N + x_F$ avec $x_N \in N$ et $x_F \in F$. Ainsi, $0 = u^{d+1}(x) = u^{d+1}(x_N) + u^{d+1}(x_F) = u(u^d(x_N)) + u(u^d(x_F)) = u(u^d(x_F)) = u_F(u_F^d(x_F))$ car F est stable par u . Mais u_F est injective, donc $u^d(x) = u^d(x_N) + u_F^d(x_F) = u_F^d(x_F) = 0$ et $x \in \ker(u^d)$. D'où $\ker(u^d) = \ker(u^{d+1})$, puis $N = \ker(u^n)$ pour $n \in \mathbb{N}$, $n \geq d$.

Une application de la décomposition de Fitting est le calcul du nombre de matrices nilpotentes de $\mathcal{M}_n(\mathbb{F}_q)$ pour $n \geq 2$ et q une puissance d'un nombre premier (cet ensemble de matrices nilpotentes est parfois appelé **cône nilpotent**).

PROPOSITION 1.3.1 Soit $n \in \mathbb{N}$ tel que $n \geq 2$. Soit q une puissance d'un nombre premier. On note $N_n(\mathbb{F}_q)$ l'ensemble des matrices nilpotentes de $\mathcal{M}_n(\mathbb{F}_q)$. Alors, $|N_n(\mathbb{F}_q)| = q^{n(n-1)}$.

PREUVE : Notons $E = \mathbb{F}_q^n$. Par le théorème 1.3.1, le cardinal de $\mathcal{L}(E)$ est égal au cardinal de l'ensemble

$$\{(N, u_N, F, u_F) \mid E = N \oplus F, u_N \in \mathcal{L}(N) \text{ nilpotent}, u_F \in \mathcal{L}(F) \text{ inversible}\}.$$

Ainsi, si $\nu_{k,n}$ est le nombre de couples (N, F) de sous-espaces vectoriels de E tels que $E = N \oplus F$ avec $\dim(N) = k$,

$$|\mathcal{M}_n(\mathbb{F}_q)| = \sum_{k=0}^n \nu_{k,n} |N_k(\mathbb{F}_q)| |\text{GL}_{n-k}(\mathbb{F}_q)|.$$

Soit $k \in \{0, \dots, n\}$. On fait agir $\text{GL}_n(\mathbb{F}_q)$ sur l'ensemble des couples (N, F) de sous-espaces vectoriels de E tels que $E = N \oplus F$ avec $\dim(N) = k$ par $g \in \text{GL}_n(\mathbb{F}_q)$ envoie (N, F) sur $(g(N), g(F))$. Cette action est bien définie, et le stabilisateur d'un (N, F) se construit comme une matrice diagonale par bloc, avec un premier bloc rempli d'une matrice de $\text{GL}_k(\mathbb{F}_q)$, et un second avec une matrice de $\text{GL}_{n-k}(\mathbb{F}_q)$. Les couples (N, F) ont des stabilisateurs de même cardinal, donc la relation orbite-stabilisateur assure que

$$\nu_{k,n} = \frac{|\text{GL}_n(\mathbb{F}_q)|}{|\text{GL}_k(\mathbb{F}_q)| |\text{GL}_{n-k}(\mathbb{F}_q)|}.$$

Ainsi, en reportant dans notre première égalité, on obtient

$$\frac{q^{n^2}}{|\text{GL}_n(\mathbb{F}_q)|} = \frac{|\mathcal{M}_n(\mathbb{F}_q)|}{|\text{GL}_n(\mathbb{F}_q)|} = \sum_{k=0}^n \frac{|N_k(\mathbb{F}_q)|}{|\text{GL}_k(\mathbb{F}_q)|}.$$

En particulier, on a

$$\frac{|N_n(\mathbb{F}_q)|}{|\text{GL}_n(\mathbb{F}_q)|} = \frac{q^{n^2}}{|\text{GL}_n(\mathbb{F}_q)|} - \frac{q^{(n-1)^2}}{|\text{GL}_{n-1}(\mathbb{F}_q)|}.$$

Or $|\text{GL}_n(\mathbb{F}_q)| / |\text{GL}_{n-1}(\mathbb{F}_q)| = q^{1+\dots+n-1}(q^n - 1) \dots (q - 1) / [q^{1+\dots+n-2}(q^{n-1} - 1) \dots (q - 1)] = q^{n-1}(q^n - 1)$ d'où

$$|N_n(\mathbb{F}_q)| = q^{n^2} - \frac{|\text{GL}_n(\mathbb{F}_q)|}{|\text{GL}_{n-1}(\mathbb{F}_q)|} q^{(n-1)^2} = q^{n^2} - q^{n-1}(q^n - 1)q^{n^2-2n+1} = q^{n^2}(1 - q^{-2n+1+2n-1} + q^{-2n+1+n-1}).$$

Finalement, on a bien

$$|N_n(\mathbb{F}_q)| = q^{n^2}(1 - 1 + q^{-n}) = q^{n^2-n} = q^{n(n-1)}.$$

REMARQUE : On en déduit que si $n \in \mathbb{N}$ est tel que $n \geq 2$ et si q est la puissance d'un nombre premier, la proportion de matrices nilpotentes de $\mathcal{M}_n(\mathbb{F}_q)$ est $q^{n(n-1)}/q^{n^2} = q^{-n}$, si bien que la proportion de matrices nilpotentes devient faible quand n est grand, ou quand q est grand.

2 Applications à la réduction

2.1 Sous-espaces propres, sous-espaces caractéristiques

On commence par rappeler les définitions de base de la réduction.

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel. Soit $u \in \mathcal{L}(E)$.

Si $\lambda \in \mathbb{K}$ est tel qu'il existe $x \in E \setminus \{0\}$ avec $u(x) = \lambda x$, on dit que λ est une **valeur propre** de u , et que x est un **vecteur propre** associé. Le **sous-espace propre** de u associé à une valeur propre λ est $E_\lambda(u) = \ker(u - \lambda \text{id}_E)$. L'ensemble des valeurs propres de u est appelé le **spectre** de u et noté $\text{Sp}(u)$.

REMARQUE : Les sous-espaces propres d'un endomorphisme u sont stables par u (noyaux d'un polynôme en u).

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.

Le **polynôme caractéristique** de u est le polynôme $\chi_u(X) = \det(X \text{id}_E - u) \in \mathbb{K}[X]$.

On ramène alors la recherche de valeurs propres à la recherche de racines d'un polynôme.

PROPOSITION 2.1.1 Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.

Les racines du polynôme caractéristique sont les valeurs propres de u .

PREUVE : On a $\lambda \in \text{Sp}(u)$ si et seulement si $\lambda \text{id}_E - u$ n'est pas inversible.

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.

Si $\chi_u(X)$ est scindé sur $\mathbb{K}$ et si $\lambda \in \text{Sp}(u)$, le **sous-espace caractéristique** de u associé à λ est le sous-espace $\ker((u - \lambda \text{id}_E)^m)$ où m est la multiplicité du facteur $(X - \lambda)$ dans $\chi_u(X)$.

REMARQUE : Lorsqu'ils sont bien définis, les sous-espaces caractéristiques d'un endomorphisme u sont des noyaux d'un polynôme en u . Ils sont donc stables par u .

PROPOSITION 2.1.2 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.

Soit F un sous-espace vectoriel de E stable par u . Alors, $\chi_{u_F} \mid \chi_u$.

PREUVE : On complète une base de F en une base de E , et on exprime la matrice de u dans cette base. Cette matrice est triangulaire supérieure par blocs, et on en déduit que $\chi_{u_F} \mid \chi_u$ par un calcul de déterminant d'une matrice triangulaire supérieure par blocs.

On déduit de cette proposition le très important théorème de Cayley-Hamilton.

THÉORÈME 2.1.1 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie n . Soit $u \in \mathcal{L}(E)$.

Alors, $\chi_u(u) = 0$.

PREUVE : Soit $x \in E \setminus \{0\}$. Montrons que $\chi_u(u)(x) = 0$. La famille $(x, u(x), \dots, u^n(x))$ est liée.

Ainsi, on peut prendre le plus grand entier naturel d tel que $(x, u(x), \dots, u^d(x))$ soit libre. Par construction de notre entier d , $\exists (a_0, \dots, a_d) \in \mathbb{K}^{d+1}$ tel que $u^{d+1}(x) + a_d u^d(x) + \dots + a_0 x = 0$. Notons $F = \langle x, u(x), \dots, u^d(x) \rangle$. Le sous-espace vectoriel F de E est stable par u et $\mathcal{B} = (x, u(x), \dots, u^d(x))$ est une base de F . Dans la base $\mathcal{B}$, la matrice de u_F est de la forme

$$\text{mat}_{\mathcal{B}}(u_F) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d-1} \\ 0 & \cdots & 0 & 1 & -a_d \end{pmatrix} \quad \text{donc } \chi_{u_F}(X) = \begin{vmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & a_{d-1} \\ 0 & \cdots & 0 & -1 & X + a_d \end{vmatrix}.$$

En faisant les opérations $L_1 \leftarrow L_1 + X L_2 + X^2 L_3 + \dots + X^d L_{d+1}$ sur le déterminant, sa première ligne a d premières coordonnées nulles, et sa coordonnée en $d+1$ est $a_0 + a_1 X + a_2 X^2 + \dots + a_d X^d + X^{d+1}$. En développant par rapport à la première ligne, on obtient alors $\chi_{u_F}(X) = (-1)^{1+d+1} \times (a_0 + a_1 X + \dots + a_d X^d + X^{d+1}) \times (-1)^d = a_0 + a_1 X + a_2 X^2 + \dots + a_d X^d + X^{d+1}$ car il reste un déterminant triangulaire de taille d avec des -1 sur la diagonale. En particulier, $\chi_{u_F}(u)(x) = 0$. Mais par la proposition 2.1.2, $\chi_{u_F} \mid \chi_u$, donc $\exists Q \in \mathbb{K}[X]$ tel que $\chi_u = Q \times \chi_{u_F}$. Ainsi, $\chi_u(u)(x) = (Q(u) \circ \chi_{u_F})(x) = Q(u)(\chi_{u_F}(u)(x)) = Q(u)(0) = 0$.

Nous ferons usage de ce théorème et du lemme des noyaux pour trouver la décomposition de Jordan-Chevalley d'un endomorphisme u pour lequel χ_u est scindé.

2.2 Réduction simultanée

On va donner un critère qui permet de réduire simultanément une famille d'endomorphismes.

PROPOSITION 2.2.1 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel. Soient $u, v \in \mathcal{L}(E)$. Supposons que $u \circ v = v \circ u$. Alors, $\ker(u)$ et $\text{Im}(u)$ sont stables par v .

PREUVE : Soit $x \in \ker(u)$. Alors $u(v(x)) = v(u(x)) = v(0) = 0$ donc $v(x) \in \ker(u)$. Soit $y \in \text{Im}(u)$. Par définition $\exists x \in E, u(x) = y$. Ainsi, $v(y) = v(u(x)) = u(v(x)) \in \text{Im}(u)$.

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $N \in \mathbb{N}^*$. Une famille $(u_1, \dots, u_N) \in (\mathcal{L}(E))^N$ est **co-diagonalisable** (resp. **co-trigonalisable**) lorsqu'il existe une base de E dans laquelle tous les $u_i, i \in \{1, \dots, N\}$ ont une matrice diagonale (resp. triangulaire supérieure).

Pour la co-diagonalisation, on a une condition nécessaire et suffisante forte.

PROPOSITION 2.2.2 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $N \in \mathbb{N}^*$. Une famille $(u_1, \dots, u_N) \in (\mathcal{L}(E))^N$ est co-diagonalisable si et seulement si $\forall i, j \in \{1, \dots, N\}, u_i \circ u_j = u_j \circ u_i$.

PREUVE : Si la famille est co-diagonalisable, par produit matriciel de matrices diagonales, les u_i commutent deux à deux. Montrons l'autre sens par récurrence sur N . Pour $N = 1$, le résultat est évident. Soit $N \in \mathbb{N}^*$. Supposons que toute famille de N endomorphismes diagonalisables qui commutent deux à deux est co-diagonalisable. Soit $(u_1, \dots, u_{N+1})$ une famille d'endomorphismes diagonalisables qui commutent entre eux. Si tous les u_i sont des homothéties, le résultat est direct. Sinon, il existe un endomorphisme (par exemple u_{N+1}) qui admet au moins deux sous-espaces propres. On écrit alors $E = E_{N+1} \oplus F$ avec E_{N+1} un sous-espace propre de u_{N+1} et F la somme des autres sous-espaces propres de u_{N+1} (c'est possible car u_{N+1} est diagonalisable). Ces deux sous-espaces sont stables par $u_1, \dots, u_N$ (commutativité). Par hypothèse de récurrence, les $(u_1, \dots, u_N)$ sont co-diagonalisables sur E_{N+1} et sur F , d'où le résultat en concaténant une base de E_{N+1} et une base de F .

Pour la co-trigonalisation, on a un premier résultat qui donne une condition suffisante.

PROPOSITION 2.2.3 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $N \in \mathbb{N}^*$. Soit $(u_1, \dots, u_N) \in (\mathcal{L}(E))^N$ une famille d'endomorphismes trigonalisables telle que $\forall i, j \in \{1, \dots, N\}, u_i \circ u_j = u_j \circ u_i$. Alors, $(u_1, \dots, u_N)$ est co-trigonalisable.

PREUVE : Il suffit d'adapter la preuve de la proposition 2.2.2. Pour l'hérédité, il suffit de prendre un sous-espace propre de l'un des endomorphismes et de remarquer que ce sous-espace est stable par les autres endomorphismes. Dans une base adaptée, on peut donc appliquer l'hypothèse de récurrence pour conclure.

REMARQUE : La preuve n'utilise pas le fait que la famille d'endomorphismes est finie.

PROPOSITION 2.2.4 Soit $n \in \mathbb{N}^*$. Soit G un sous-groupe connexe de $\text{GL}_n(\mathbb{C})$. Alors, $D(G)$ est connexe.

PREUVE : Tout d'abord, notons que le produit matriciel (polynomial) et le passage à l'inverse (fraction rationnelle avec dénominateur jamais nul sur $\text{GL}_n(\mathbb{C})$) sont continus. Ainsi, notant S l'ensemble des commutateurs des éléments de G , S est l'image de $G \times G$ par l'application continue $(g, h) \mapsto ghg^{-1}h^{-1}$ avec $G \times G$ connexe. Ainsi, l'ensemble S est connexe, et on en déduit que $\forall m \in \mathbb{N}^*, S^m$ est connexe. Pour tout $m \in \mathbb{N}^*$, notant S_m l'image de S^m par l'application continue $(s_1, \dots, s_m) \mapsto s_1 \cdots s_m$, S_m est connexe. Enfin, on remarque que $D(G)$ est la réunion pour $n \in \mathbb{N}^*$ des S_m (l'inverse d'un commutateur est un commutateur, et l'identité est réalisée par un commutateur d'un élément avec lui-même). Comme l'identité appartient à chacun des S_m , $D(G)$ est connexe comme réunion de connexes qui ont un élément en commun.

Nous allons utiliser cette proposition pour démontrer le théorème de Lie-Kolchin suivant. Ce théorème permet de

relaxer l'hypothèse de la proposition 2.2.3, au prix d'un ajout sur la structure algébrique et topologique de la famille d'endomorphismes.

THÉORÈME 2.2.1 Soit $n \in \mathbb{N}^*$. Soit G un sous-groupe connexe résoluble de $\mathrm{GL}_n(\mathbb{C})$. Alors, il existe une base de $\mathbb{C}^n$ qui trigonalise tous les éléments de G .

PREUVE : On va montrer le résultat par récurrence forte sur n .

Dans le cas $n = 1$, le groupe G est nécessairement abélien, et la proposition 2.2.3 permet de conclure.

Soit $n \in \mathbb{N}^* \setminus \{1\}$. Supposons que $\forall k \in \{1, \dots, n-1\}$, pour tout sous-groupe connexe résoluble G de $\mathrm{GL}_k(\mathbb{C})$, il existe une base de $\mathbb{C}^k$ qui trigonalise tous les éléments de G . Soit G un sous-groupe connexe résoluble de $\mathrm{GL}_n(\mathbb{C})$. Par la proposition 2.2.3, on peut supposer G non abélien. Soit m le plus petit entier naturel non nul et différent de 1 tel que $D^m(G)$ est trivial (G est résoluble non abélien). On note $H = D^{m-1}(G)$.

Encore par la proposition 2.2.3, comme H est abélien, le premier élément d'une base commune de trigonalisation des éléments de H fournit un vecteur propre x commun aux éléments de H . Notons P l'ensemble des vecteurs propres communs aux éléments de H . Nous venons de voir que $P \neq \emptyset$.

Maintenant, H est distingué dans G (les sous-groupes dérivés sont caractéristiques) donc $\forall h \in H, \forall g \in G$,

$$h(g(x)) = g(g^{-1}hg)(x) = g(\lambda x) = \lambda g(x).$$

Ainsi, $g(x) \in P$. Pour tout $y \in P$, on note $\Lambda_y : H \rightarrow \mathbb{C}$ qui envoie $h \in H$ sur sa valeur propre en y . Pour tout $h \in H$, on définit $L_h : G \rightarrow \mathbb{C}$ qui envoie $g \in G$ sur $\Lambda_{g(x)}(h) = \Lambda_x(hg^{-1})$. Cette application est continue car composée de $g \mapsto ghg^{-1}$ (continue sur G car polynomiale en les coefficients de g) et de $z \mapsto \Lambda_x(z)$ (continue sur H car ils stabilisent tous la droite engendrée par x). L'image de G par L_h est donc un connexe de $\mathbb{C}$ qui est inclus dans le spectre de h . C'est un connexe fini de $\mathbb{C}$, donc un singleton.

Soit V le sous-espace vectoriel engendré par les éléments de la forme $g(x)$ où $g \in G$.

Comme V est engendré par des éléments qui sont stables par G , V est lui-même stable par G et V est non trivial car $x \in V$ (si $h \in H$, $h(x) = \lambda x$ donc $x = (1/\lambda)\lambda x = (1/\lambda)h(x) \in V$ car $H \subset G$).

Maintenant, $V \neq \mathbb{C}^n$. En effet, si $V = \mathbb{C}^n$, les éléments de H sont tous des homothéties. Mais ce sont aussi des commutateurs, donc leur déterminant vaut 1, et les rapports des homothéties de H sont des racines n -ièmes de l'unité. Ainsi, H est fini et connexe par la proposition 2.2.4. Donc H est un singleton, ce qui est absurde par construction de H (H ne peut pas être trivial).

Pour conclure la preuve, on choisit un supplémentaire W de V de sorte que les éléments de G aient une matrice triangulaire supérieure par blocs dans une base adaptée à la décomposition $V \oplus W$. Il ne reste plus qu'à expliquer que l'on peut appliquer l'hypothèse de récurrence. On note $\rho : G \rightarrow \mathrm{GL}(V)$ (resp. $\rho' : G \rightarrow \mathrm{GL}(W)$) l'application qui envoie g sur l'application induite par g sur V (resp. projection sur W parallèlement à V de l'application induite par g sur W). Les applications ρ et ρ' sont des morphismes continus donc $\rho(G)$ (resp. $\rho'(G)$) est un sous-groupe connexe résoluble de $\mathrm{GL}(V)$ (resp. $\mathrm{GL}(W)$). Il suffit alors d'appliquer l'hypothèse de récurrence à ces deux images pour conclure.

Ici, la difficulté réside dans la recherche d'un sous-espace stable par tous les éléments du groupe G considéré. Pour cela, on utilise l'hypothèse topologique (connexité) faite sur G ainsi que l'hypothèse algébrique (résolubilité).

2.3 Réduction

Comme annoncé plus tôt, nous allons prouver un théorème de réduction en utilisant le lemme des noyaux et le théorème de Cayley-Hamilton dans le cas où le polynôme caractéristique est scindé : la décomposition de Jordan-Chevalley.

THÉORÈME 2.3.1 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$. On suppose que χ_u est scindé sur $\mathbb{K}$. Alors, $\exists!(d, n) \in (\mathcal{L}(E))^2$ tel que d est diagonalisable, n est nilpotent, $u = d + n$ et $n \circ d = d \circ n$. De plus, d et n sont des polynômes en u .

PREUVE : On écrit $\chi_u(X) = \prod_{i=1}^p (X - \lambda_i)^{m_i}$ avec $p \in \mathbb{N}^*$, $m_i \in \mathbb{N}^*$ et les λ_i deux à deux distincts.

Pour $i \in \{1, \dots, p\}$, posons $N_i = \ker((u - \lambda_i \mathrm{id}_E)^{m_i})$. Par le théorème 2.1.1 et le lemme des noyaux, on peut écrire $E = N_1 \oplus \dots \oplus N_p$. De plus, notant p_i le projecteur sur N_i parallèlement à la somme directe des N_k pour $k \neq i$, nous avons $d = \sum_{i=1}^p \lambda_i p_i$ est diagonalisable et est un polynôme en u (les projecteurs sont des polynômes en u). On pose alors $n = u - d$, et on vérifie que n est nilpotent sur chacun des N_i donc nilpotent, et comme d et n sont des polynômes en u , $d \circ n = n \circ d$.

Montrons maintenant l'unicité. Donnons un autre couple (d', n') comme dans le théorème. On a $u = d + n$ et $u = d' + n'$ donc $d - d' = n' - n$. Comme $d' \circ n' = n' \circ d'$, n' et d' commutent avec $u = d' + n'$ donc avec les polynômes en u . En particulier, d' commute avec d et n' commute avec n . Donc par la proposition 2.2.2 $d - d'$ est encore diagonalisable, et $n' - n$ est encore nilpotent par la formule du binôme de Newton. En particulier, $d - d'$ est diagonalisable et nilpotent donc $d - d' = 0$ puis $n' - n = 0$, d'où le résultat.

EXEMPLE : Soit $M \in \mathcal{M}_2(\mathbb{C})$. On suppose que M est de trace nulle. On a donc $\chi_M(X) = X^2 + \det(M)$. Si $\det(M) \neq 0$, alors $\chi_M(X)$ est scindé à racines simples sur $\mathbb{C}$ donc M est diagonalisable. Sinon, $M^2 = 0$ et M est nilpotente. Dans tous les cas M est sa propre décomposition de Jordan-Chevalley.

MOTIVATION On peut utiliser la décomposition de Jordan-Chevalley pour calculer l'exponentielle d'une matrice. Par exemple, si $M \in \mathcal{M}_n(\mathbb{C})$ où $n \in \mathbb{N}^*$ s'écrit $M = D + N$ avec D diagonalisable, N nilpotente et $ND = DN$, on a $\exp(M) = \exp(D)\exp(N)$ avec $\exp(D)$ qui est facile à calculer une fois que D est diagonalisée, et $\exp(N)$ qui est une somme finie.

EXEMPLE : Nous allons calculer la décomposition de Jordan-Chevalley de

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Tout d'abord, $\chi_A(X) = (X - 1)^2(X - 2)$ donc on cherche $\ker((A - I_3)^2)$ et $\ker(A - 2I_3)$. Pour cela, on écrit

$$(A - I_3)^2 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

ce qui prouve que $f_1 = (1, 0, 0)$ et $f_2 = (0, 1, 0)$ forment une base de $\ker((A - I_3)^2)$. On cherche enfin un vecteur propre pour la valeur propre 2 et on trouve $f_3 = (2, 1, 1)$. Dans la base (f_1, f_2, f_3) la matrice de la partie diagonalisable de A est donc diagonale avec dans l'ordre 1, 1 puis 2 sur la diagonale. Dans la base canonique (e_1, e_2, e_3) , l'image par la partie diagonalisable de $e_3 = -2f_1 - f_2 + f_3$ est $-2f_1 - f_2 + 2f_3 = 2e_1 + e_2 + 2e_3$. Ainsi,

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

est la décomposition de Jordan-Chevalley de A . L'expression de e_3 dans la base (f_1, f_2, f_3) fournit directement

$$A = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

En faisant un calcul d'inverse, on en déduit que

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

avec les deux termes de la somme qui commutent. On peut alors calculer l'exponentielle de A en remarquant que

$$\exp \left(\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} e & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & e^2 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

par continuité de la conjugaison, et que

$$\exp \left(\begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ainsi, par commutativité, on peut écrire

$$\exp(A) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} e & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & e^2 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} e & e & 2e^2 - 3e \\ 0 & e & e^2 - e \\ 0 & 0 & e^2 \end{pmatrix}.$$

PROPOSITION 2.3.1 Soit $n \in \mathbb{N}^*$. Soit M une matrice de $\mathcal{M}_n(\mathbb{C})$.
Alors, M est diagonalisable si et seulement si $\exp(M)$ est diagonalisable.

PREUVE : Si M est diagonalisable, la continuité de la conjugaison assure que $\exp(M)$ est diagonalisable. Supposons que $\exp(M)$ est diagonalisable. On écrit la décomposition de Jordan-Chevalley $M = D + N$ avec D diagonalisable, N nilpotente et $DN = ND$. On a alors $\exp(M) = \exp(D + N) = \exp(D)\exp(N) = \exp(D) + \exp(D)(\exp(N) - I_n)$. Comme D est diagonalisable, $\exp(D)$ est diagonalisable. Ensuite, comme D et N commutent, N commute avec $\exp(D)$. Ainsi, si k est le plus petit entier naturel tel que $N^k = 0$, on a

$$e^D(e^N - I_n) = e^D \sum_{j=1}^{k-1} \frac{N^j}{j!} = e^D N \sum_{j=1}^{k-1} \frac{N^{j-1}}{j!}$$

avec N qui commute avec e^D et avec le polynôme en N . Cela prouve que $e^D(e^N - I_n)$ est nilpotente (en effet $(e^D(e^N - I_n))^k = 0$). Enfin, $\exp(D)$ commute avec N donc avec les polynômes en N , donc $\exp(D)$ commute avec $\exp(D)(\exp(N) - I_n)$. Ainsi, $\exp(M) = \exp(D) + \exp(D)(\exp(N) - I_n)$ est la décomposition de Jordan-Chevalley de $\exp(M)$. Mais $\exp(M)$ est diagonalisable donc par unicité dans la décomposition, $\exp(D)(\exp(N) - I_n) = 0$. Comme $\exp(D)$ est inversible, $\exp(N) = I_n$. Si $k \neq 1$, on a donc

$$\sum_{j=0}^{k-1} \frac{N^j}{j!} = I_n \text{ d'où } N + \sum_{j=2}^{k-1} \frac{N^j}{j!} = 0 \text{ soit } N = -\sum_{j=2}^{k-1} \frac{N^j}{j!} \text{ donc } N^{k-1} = -\sum_{j=2}^{k-1} \frac{N^{k-2+j}}{j!} = 0$$

ce qui est absurde par minimalité de k . Donc $k = 1$ et $N = 0$, d'où $M = D$ est diagonalisable.

3 Endomorphismes remarquables

3.1 Endomorphismes cycliques

Nous étudions maintenant une famille d'endomorphismes particuliers avec pour objectif principal la théorie des invariants de similitude et la décomposition de Frobenius.

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.
On dit que u est un **endomorphisme cyclique** lorsqu'il existe $x \in E$ tel que la famille $(x, u(x), \dots, u^{n-1}(x))$ est une base de E ($n \in \mathbb{N}^*$ est la dimension de E).

PROPOSITION 3.1.1 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.
On suppose que u est cyclique. Alors, le degré de μ_u est égal à $n = \dim(E)$, et donc $\mu_u = \chi_u$.

PREUVE : Tout d'abord, le degré de μ_u est plus grand que n car sinon, la famille $(x, u(x), \dots, u^{n-1}(x))$ serait liée (où x est un élément de E tel que $(x, u(x), \dots, u^{n-1}(x))$ est une base). Par définition, il existe un polynôme de degré strictement inférieur à n tel que $u^n(x) = P(u)(x)$. Montrons que $X^n - P$ annule u . Pour $j \in \{0, \dots, n-1\}$, on a

$$(u^n - P(u))(u^j(x)) = u^j((u^n - P(u))(x)) = u^j(u^n(x) - P(u)(x)) = u^j(0) = 0$$

donc $X^n - P$ annule u sur une base de E , donc $X^n - P$ annule u et est de degré n . Ainsi, le degré de μ_u est inférieur à n , et au final, le degré de μ_u est bien égal à n .

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.
Si $x \in E$, on note $\mu_{u,x}$ l'unique générateur unitaire de l'idéal $\{P \in \mathbb{K}[X] \mid P(u)(x) = 0\}$.

REMARQUE : Il y a un nombre fini de $\mu_{u,x}$ pour x parcourant E , car les $\mu_{u,x}$ sont des diviseurs unitaires de μ_u .

LEMME Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.

Soient $m \in \mathbb{N}^*$ et $E_1, \dots, E_m$ des sous-espaces vectoriels de E stables par u et en somme directe. Soit $(x_1, \dots, x_m) \in E_1 \times \dots \times E_m$. On pose $x = x_1 + \dots + x_m$. Alors, $\mu_{u,x} = \text{ppcm}(\mu_{u,x_i}, i \in \{1, \dots, m\})$.

PREUVE : Soit $P \in \mathbb{K}[X]$ tel que $\mu_{u,x} \mid P$. Montrons que $\forall i \in \{1, \dots, m\}, \mu_{u,x_i} \mid P$. On a

$$0 = P(u)(x) = \sum_{i=1}^m P(u)(x_i)$$

avec $\forall i \in \{1, \dots, m\}, P(u)(x_i) \in E_i$ par stabilité par u de E_i . Comme la somme est directe, on a bien $\forall i \in \{1, \dots, m\}, P(u)(x_i) = 0$, soit $\mu_{u,x_i} \mid P$. Inversement, si pour tout $i \in \{1, \dots, m\}, \mu_{u,x_i} \mid P$, on a bien $P(u)(x) = 0$ en décomposant $x = x_1 + \dots + x_m$, d'où $\mu_{u,x} \mid P$.

La proposition suivante est très importante en algèbre linéaire. C'est un corollaire du lemme des noyaux.

PROPOSITION 3.1.2 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.

Alors, $\exists x \in E$ tel que $\mu_{u,x} = \mu_u$.

PREUVE : On commence par le cas où μ_u est une puissance d'un polynôme irréductible unitaire $\mu_u = P^r$ où $r \in \mathbb{N}^*$. Comme $P^{r-1} \mid P^r$ avec $P^{r-1} \neq P^r$, le polynôme P^{r-1} n'annule pas u . Soit donc $x \in E$ tel que $P^{r-1}(u)(x) \neq 0$. Maintenant, $\mu_{u,x} \mid P^r = \mu_u$ avec P irréductible, donc $\exists k \in \{0, \dots, r\}$ tel que $\mu_{u,x} = P^k$. Mais $k = r$ car sinon, on aurait $\mu_{u,x} \mid P^{r-1}$ et donc $P^{r-1}(u)(x) = 0$ ce qui est absurde. Ainsi, on a bien $\mu_{u,x} = \mu_u$. On se place alors dans le cas général et on décompose μ_u en

$$\mu_u = \prod_{i=1}^m P_i^{r_i}$$

avec $P_1, \dots, P_m$ irréductibles unitaires deux à deux premiers entre eux et $\forall i \in \{1, \dots, m\}, r_i \in \mathbb{N}^*$. Ainsi, notant $E_i = \ker(P_i^{r_i})$ pour $i \in \{1, \dots, m\}$, le lemme des noyaux fournit une décomposition de E en somme directe des E_i . Soit $i \in \{1, \dots, m\}$. Montrons que $\mu_{u_{E_i}} = P_i^{r_i}$. Tout d'abord, on a bien $\mu_{u_{E_i}} \mid P_i^{r_i}$ car $P_i^{r_i}$ annule u_{E_i} . Mais si $\mu_{u_{E_i}}$ divise strictement $P_i^{r_i}$, on a $\mu_{u_{E_i}} \mid P_i^{r_i-1}$, donc $\text{ppcm}(P_1^{r_1}, \dots, P_i^{r_i-1}, \dots, P_m^{r_m})$ annule u et divise strictement μ_u qui est égal à $\text{ppcm}(P_k^{r_k}, k \in \{1, \dots, m\})$ par le corollaire de la proposition 1.1.2. C'est absurde, donc $\mu_{u_{E_i}} = P_i^{r_i}$. Le cas du début de la preuve assure qu'on peut trouver $x_i \in E_i$ tel que $\mu_{u,x_i} = P_i^{r_i}$ pour tout $i \in \{1, \dots, m\}$. En posant $x = x_1 + \dots + x_m$, le lemme précédent permet d'écrire $\mu_{u,x} = \text{ppcm}(P_i^{r_i}, i \in \{1, \dots, m\}) = \mu_u$, d'où le résultat.

PROPOSITION 3.1.3 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.

On suppose que le degré de μ_u est égal à $n = \dim(E)$. Alors, u est cyclique.

REMARQUE : Nous avons donc une condition nécessaire et suffisante pour la cyclicité d'un endomorphisme en dimension finie en combinant les propositions 3.1.1 et 3.1.3.

PREUVE : D'après la proposition 3.1.2, il existe un $x \in E$ tel que $\mu_{u,x} = \mu_u$. La famille $(x, u(x), \dots, u^{n-1}(x))$ est clairement une famille libre (sinon, on serait en contradiction avec la minimalité de μ_u), donc c'est une base vu son cardinal. Donc u est cyclique.

Le théorème suivant est le théorème de réduction de Frobenius, qui permet de définir les invariants de similitude.

THÉORÈME 3.1.1 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie n . Soit $u \in \mathcal{L}(E)$.

Il existe un $r \in \mathbb{N}^*$ et une suite $F_1, \dots, F_r$ de sous-espaces vectoriels stables par u tels que

$$E = \bigoplus_{i=1}^r F_i$$

avec $\forall i \in \{1, \dots, r\}$, l'induit u_{F_i} est cyclique, et notant P_i le polynôme minimal de u_{F_i} , si $i \neq r$, on a $P_{i+1} \mid P_i$. De plus, la suite de polynômes $P_1, \dots, P_r$ ne dépend que de u et pas du choix des F_i .

REMARQUE : Ce théorème de réduction ne requiert aucune hypothèse supplémentaire sur l'endomorphisme considéré.

PREUVE : On commence par l'existence. Notons k le degré du polynôme minimal μ_u . Par le lemme précédent, on peut se donner $x \in E$ tel que $\mu_{u,x} = \mu_u$. On note F le sous-espace vectoriel engendré par $x, u(x), \dots, u^{k-1}(x)$. Par définition, F est de dimension k , est stable par u et notant $e_i = u^{i-1}(x)$ pour $i \in \{1, \dots, k\}$, la famille $(e_1, \dots, e_k)$ est une base de F . On recherche alors un supplémentaire de F qui est stable par u .

Pour cela, on commence par compléter $(e_1, \dots, e_k)$ en une base $(e_1, \dots, e_n)$ de E . On considère ensuite la base duale $(e_1^*, \dots, e_n^*)$, et on note

$$G = \Gamma^\perp \text{ où } \Gamma = \{(u^i)^T(e_k^*) \mid i \in \mathbb{N}\}$$

où l'orthogonal de Γ est pris au sens de la dualité. Comme Γ est stable par u^T , la proposition 1.2.1 assure que G est stable par u . Nous allons maintenant montrer que $E = F \oplus G$.

Tout d'abord, si $y \in F \cap G$ et $y \neq 0$, on peut écrire $y = a_1 e_1 + \dots + a_p e_p$ où les a_i sont pris dans $\mathbb{K}$ et $a_p \neq 0$ avec $p \leq k$. On compose alors l'égalité par $(u^{k-p})^T(e_k^*)$. Comme $y \in G$, on obtient

$$0 = e_k^*(a_1 e_{k-p+1} + \dots + a_p e_{p+k-p}) = a_p \neq 0$$

ce qui est absurde. Ainsi, $F \cap G = \{0\}$.

Pour en conclure que $E = F \oplus G$, il suffit de montrer que $n = \dim(F) + \dim(G)$, donc que la dimension du sous-espace vectoriel engendré par Γ est k car on veut montrer $\dim(\Gamma^\perp) = n - k$. On regarde alors l'application linéaire $\varphi : \mathbb{K}[u] \rightarrow \text{Vect}(\Gamma)$ qui envoie $P(u)$ sur $e_k^* \circ P(u)$ pour tout $P \in \mathbb{K}[X]$. Vu la définition de Γ , notre application linéaire φ est surjective. Mais si $e_k^* \circ P(u) = 0$ avec $P(u) \in \mathbb{K}[u]$ non nul, on peut écrire $P = a_1 \text{id}_E + \dots + a_p u^{p-1}$ avec $p \leq k$ en prenant P modulo μ_u , donc en appliquant l'hypothèse en $u^{k-p}(x)$,

$$0 = (e_k^* \circ P)(u^{k-p}(x)) = e_k^*(a_1 u^{k-p}(x) + \dots + a_p u^{k-1}(x)) = e_k^*(a_1 e_{k-p+1} + \dots + a_p e_k) = a_p \neq 0$$

ce qui est absurde. Donc φ est injective, donc c'est un isomorphisme. En particulier, $\dim(\Gamma^\perp) = n - k$ comme annoncé car $\dim(\mathbb{K}[u]) = k$, d'où $E = F \oplus G$. Comme G est stable par u , le polynôme minimal de u_G divise le polynôme minimal de u_F , car $\mu_{u_F} = \mu_u$. On applique alors ce que l'on vient de faire à u_G , et on a la décomposition voulue après un nombre fini d'étapes (car le degré du polynôme minimal n'est jamais nul).

Montrons maintenant l'unicité de la suite de polynômes. Soient $r, s \in \mathbb{N}^*$. On se donne $F_1, \dots, F_r$ et $G_1, \dots, G_s$ deux suites de sous-espaces vectoriels de E stables par u qui vérifient les conditions de l'énoncé. On note $P_i = \mu_{u_{F_i}}$ et $Q_j = \mu_{u_{G_j}}$ pour $i \in \{1, \dots, r\}$ et $j \in \{1, \dots, s\}$. Par les relations de divisibilité des deux suites de polynômes, on a $P_1 = \mu_u = Q_1$. Comme $\deg(P_1) + \dots + \deg(P_r) = \deg(Q_1) + \dots + \deg(Q_s)$, il existe un premier indice j tel que $P_j \neq Q_j$. Pour $k \geq j$, $P_j(u)(F_k) = 0$ donc

$$P_j(u)(E) = P_j(u)(F_1) \oplus \dots \oplus P_j(u)(F_{j-1}) \text{ et } P_j(u)(E) = P_j(u)(G_1) \oplus \dots \oplus P_j(u)(G_{j-1}) \oplus \dots \oplus P_j(u)(G_s).$$

On remarque que pour $i \in \{1, \dots, j-1\}$, comme $P_i = Q_i$, il existe une base de F_i et une base de G_i telles que la matrice de u dans les deux bases soit la matrice compagnon associée à $P_i = Q_i$. On en déduit que $\dim(P_j(u)(F_i)) = \dim(P_j(u)(G_i))$ pour tout $i \in \{1, \dots, j-1\}$, donc que $\dim(P_j(u)(G_i)) = 0$ pour tout $i \in \{j, \dots, s\}$. Ainsi, $Q_j \mid P_j$. En inversant les rôles, on obtient aussi $P_j \mid Q_j$ donc (polynômes unitaires) $P_j = Q_j$ ce qui est absurde. D'où le résultat d'unicité souhaité.

REMARQUE : Nous venons de voir qu'un sous-espace cyclique de dimension maximale admet un supplémentaire stable.

DÉFINITION Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie n . Soit $u \in \mathcal{L}(E)$.

On appelle **invariants de similitude** de u la suite de polynômes $P_1, \dots, P_r$ du théorème précédent.

REMARQUE : En utilisant le théorème de réduction de Frobenius, on peut déduire une forme matricielle. Si u est un endomorphisme d'un espace vectoriel de dimension finie, notant $P_1, \dots, P_r$ ses invariants de similitude, dans une base bien choisie, la matrice de u est diagonale par blocs, avec des blocs égaux aux matrices compagnon des polynômes $P_1, \dots, P_r$. Cela permet de justifier l'appellation invariants de similitude.

En particulier, l'écriture matricielle assure que P_1 est le polynôme minimal de u , et que $P_1 \cdots P_r$ est le polynôme caractéristique. On en déduit que μ_u et χ_u ont les mêmes facteurs irréductibles.

PROPOSITION 3.1.4 Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie n . Soient $u, v \in \mathcal{L}(E)$. Alors, u et v sont semblables si et seulement s'ils ont les mêmes invariants de similitude.

PREUVE : La remarque précédente montre que si u et v ont les mêmes invariants de similitude, u et v sont semblables à une même matrice diagonale par blocs avec des blocs qui sont des matrices compagnons des invariants de similitude, donc u et v sont semblables.
Inversement, si u et v sont semblables, en reprenant la preuve de l'unicité dans le théorème de réduction de Frobenius, on voit que u et v ont les mêmes invariants de similitude.

REMARQUE : On en déduit que les orbites de l'action par conjugaison du groupe linéaire sur les matrices sont entièrement caractérisées par les invariants de similitude.

PROPOSITION 3.1.5 Soit $\mathbb{K}$ un corps. Soit $n \in \mathbb{N}^*$. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors, les invariants de similitude de A vue dans $\mathcal{M}_n(\mathbb{K})$ ou dans $\mathcal{M}_n(\mathbb{L})$ sont les mêmes.

PREUVE : On utilise le fait que A est semblable à une matrice diagonale par blocs où les blocs sont les matrices compagnon des invariants de similitude dans $\mathcal{M}_n(\mathbb{K})$, puis l'unicité dans le théorème de réduction de Frobenius en voyant l'égalité dans $\mathcal{M}_n(\mathbb{L})$.

REMARQUE : On en déduit que deux matrices à coefficients dans un corps $\mathbb{K}$ sont semblables sur $\mathbb{K}$ si et seulement si elles sont semblables sur une extension $\mathbb{L}$ de $\mathbb{K}$.

EXEMPLE : On retrouve un résultat bien connu en prenant $\mathbb{K} = \mathbb{R}$ et $\mathbb{L} = \mathbb{C}$.

3.2 Endomorphismes normaux

On va maintenant se placer dans le cadre des espaces euclidiens. Rappelons à ce titre que le théorème de Riesz permet de définir l'adjoint u^* d'un endomorphisme u , et de montrer que cet adjoint est encore une application linéaire. On rappelle aussi qu'en base orthonormée, la matrice de u^* est la transposée de la matrice de u .

DÉFINITION Soit $n \in \mathbb{N}^*$. Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien de dimension n . Soit $u \in \mathcal{L}(E)$. On dit que u est un **endomorphisme normal** si $u^* \circ u = u \circ u^*$.

EXEMPLES : Les endomorphismes symétriques, les endomorphismes antisymétriques et les endomorphismes orthogonaux sont des endomorphismes normaux.

PROPOSITION 3.2.1 Soit $n \in \mathbb{N}^*$. Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien de dimension n . Soit $u \in \mathcal{L}(E)$ normal. Soit F un sous-espace vectoriel de E stable par u . Alors $F^\perp$ est stable par u (orthogonal pour $\langle \cdot, \cdot \rangle$).

PREUVE : Si $F = \{0\}$ ou $F = E$, le résultat est évident. Sinon, on écrit $E = F \oplus F^\perp$ et dans une base orthonormée $\mathcal{B}$ adaptée à la décomposition, on a

$$\text{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix} \text{ et } \text{Mat}_{\mathcal{B}}(u^*) = \begin{pmatrix} A_1^T & 0 \\ A_2^T & A_3^T \end{pmatrix}$$

avec u normal, donc par produit matriciel par blocs,

$$\begin{pmatrix} A_1 A_1^T + A_2 A_2^T & * \\ * & * \end{pmatrix} = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix} \begin{pmatrix} A_1^T & 0 \\ A_2^T & A_3^T \end{pmatrix} = \begin{pmatrix} A_1^T & 0 \\ A_2^T & A_3^T \end{pmatrix} \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix} = \begin{pmatrix} A_1^T A_1 & * \\ * & * \end{pmatrix}.$$

Comme $A_1 A_1^T + A_2 A_2^T = A_1^T A_1$, en passant la trace, on obtient que la trace de $A_2 A_2^T$ est nulle. On en déduit que $A_2 = 0$, et que $F^\perp$ est stable par u vu la forme de la matrice de u dans la base $\mathcal{B}$.

REMARQUE : L'orthogonalité est un outil très utile pour trouver un supplémentaire stable pour les endomorphismes normaux. Nous allons en déduire un théorème de réduction des endomorphismes normaux dans la suite.

PROPOSITION 3.2.2 Soit $n \in \mathbb{N}^*$. Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien de dimension n . Soit $u \in \mathcal{L}(E)$. Alors, il existe une droite ou un plan stable par u .

PREUVE : Si u a une valeur propre réelle, il suffit de prendre un vecteur propre x associé, et la droite vectorielle engendrée par x convient. Sinon, le polynôme minimal μ_u n'a aucun facteur de degré 1, donc il a un facteur

irréductible de degré 2 qui s'écrit donc $X^2 + bX + c$ avec $b, c \in \mathbb{R}$ et $b^2 - 4c < 0$. L'endomorphisme $u^2 + bu + \text{id}_E$ n'est pas injectif, donc $\exists x \in \ker(u^2 + bu + \text{id}_E)$ tel que $x \neq 0$. Le sous-espace vectoriel engendré par x et $u(x)$ est donc de dimension 2 et est stable par u .

Pour démontrer par récurrence un théorème de réduction des endomorphismes normaux, il faut donc traiter le cas de la dimension 2. On utilise pour cela la proposition suivante.

PROPOSITION 3.2.3 Soit E un espace euclidien de dimension 2. Soit $u \in \mathcal{L}(E)$ normal. Alors, soit u est diagonalisable en base orthonormée, soit u s'écrit matriciellement sous la forme

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \text{ où } (a, b) \in \mathbb{R} \times \mathbb{R}^*$$

en base orthonormée.

PREUVE : Si u a une valeur propre réelle λ_1 , notant x_1 un vecteur propre associé, l'orthogonal de la droite engendré par x_1 est stable par u d'après la proposition 3.2.1, et c'est une droite vu la dimension de E . Donc u est diagonalisable en base orthonormée.

Sinon, on se fixe une base orthonormée $\mathcal{B}$ et on écrit la condition pour que u soit normal

$$\text{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \text{ où } (a, b, c, d) \in \mathbb{R}^4 \text{ et } \begin{pmatrix} a^2 + b^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{pmatrix} = \begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix}.$$

En particulier, $b = \pm c$ et $ab + cd = ac + bd$ donc $(a - d)(b - c) = 0$. Mais χ_u n'a pas de valeur propre réelle donc (discriminant négatif de $X^2 - (a + d)X + ad - bc$) $(a + d)^2 - 4(ad - bc) < 0$. Mais si $b = c$, on aurait $(a - d)^2 + 4b^2 < 0$ ce qui est absurde. Donc $b = -c$ et $a = d$, d'où le résultat.

On en déduit le théorème de réduction des endomorphismes normaux sur un espace euclidien par récurrence forte sur la dimension de l'espace euclidien.

THÉORÈME 3.2.1 Soit $n \in \mathbb{N}^*$. Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien de dimension n . Soit $u \in \mathcal{L}(E)$ normal. Alors, il existe une base orthonormée $\mathcal{B}$ dans laquelle la matrice de u est

$$\text{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} D_p & 0 & \cdots & 0 \\ 0 & R_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & R_r \end{pmatrix}$$

avec $p \in \mathbb{N}$ tel que $p \leq n$, $r \in \mathbb{N}$ tel que $2r \leq n$, D_p une matrice diagonale de taille p et $\forall i \in \{1, \dots, r\}$,

$$R_i = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$$

où $(a_i, b_i) \in \mathbb{R} \times \mathbb{R}^*$ (en particulier $p + 2r = n$ et si p ou r est nul, les blocs correspondants n'existent pas).

PREUVE : On fait une preuve par récurrence sur $n = \dim(E)$. Le cas $n = 1$ est évident, et le cas $n = 2$ a été traité dans la proposition 3.2.3. Pour l'hérédité, on utilise la proposition 3.2.2 pour trouver une droite ou un plan stable. Si c'est une droite, on ajoute un scalaire en haut à gauche de la matrice de l'hypothèse de récurrence, et la proposition 3.2.1 permet de conclure. Si c'est un plan, on ajoute un bloc comme dans la proposition 3.2.3, et on utilise encore 3.2.1 et l'hypothèse de récurrence pour conclure. Il suffit alors de réordonner les vecteurs de la base orthonormée obtenue pour avoir la forme annoncée.

Nous allons appliquer ce théorème aux endomorphismes symétriques pour obtenir le théorème spectral, puis aux endomorphismes orthogonaux pour avoir le théorème de réduction associé.

PROPOSITION 3.2.4 Soit M une matrice symétrique réelle. Alors, M est diagonalisable en base orthonormée.

PREUVE : On applique le théorème précédent, la condition $M^T = M$ interdit les blocs de la forme R_i .

Au passage, on peut aussi démontrer un théorème de réduction des matrices antisymétriques en employant la même méthode.

PROPOSITION 3.2.5 Soit M une matrice antisymétrique réelle de taille n . Alors, les valeurs propres non nulles de M sont imaginaires pures, et M est semblable à

$$\begin{pmatrix} 0_p & 0 & \cdots & 0 \\ 0 & R_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & R_r \end{pmatrix}$$

avec $p \in \mathbb{N}$ tel que $n, r \in \mathbb{N}$ tel que $2r \leq n$ et $\forall i \in \{1, \dots, r\}$,

$$R_i = \begin{pmatrix} 0 & -b_i \\ b_i & 0 \end{pmatrix}$$

où $b_i \in \mathbb{R}^*$ (en particulier $p + 2r = n$ et si p ou r est nul, les blocs correspondants n'existent pas).

PREUVE : On applique le théorème précédent et les coefficients diagonaux sont nuls car $M^T = -M$.

PROPOSITION 3.2.6 Soit $n \in \mathbb{N}^*$. Soit E un espace euclidien de dimension n . Soit $u \in O(E)$.

Toutes les valeurs propres de u sont de module 1, et il existe une base orthonormée $\mathcal{B}$ dans laquelle la matrice de u est de la forme

$$\text{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} I_p & 0 & 0 & \cdots & 0 \\ 0 & -I_q & 0 & \ddots & \vdots \\ 0 & 0 & R_1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & R_r \end{pmatrix}$$

où $p, q, r \in \mathbb{N}$ sont tels que $p + q + 2r = n$ et $\forall i \in \{1, \dots, r\}$, $\exists \theta_i \in]0, 2\pi[\setminus \{\pi\}$ tel que $R_i = \begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix}$.

PREUVE : Si λ est une valeur propre et x un vecteur propre associé, $|\lambda| \|x\|^2 = \|u(x)\|^2 = \langle u(x), u(x) \rangle = \langle x, u^*(u(x)) \rangle = \|x\|^2$ donc $|\lambda| = 1$. Les seules valeurs propres réelles potentielles sont donc 1 et -1 , d'où la présence des blocs I_p et $-I_q$. Pour $i \in \{1, \dots, r\}$, on a $R_i R_i^T = I_2$ donc $a_i^2 + b_i^2 = 1$ avec $b_i \neq 0$, d'où l'écriture sous la forme de l'énoncé.

Bibliographie

- [CL05] Antoine Chambert-Loir. *Algèbre corporelle*. Ellipses, 2005.
- [VB05] Jérôme Malick et Gabriel Peyré Vincent Beck. *Objectif agrégation*. H et K, 2005.
- [Gou21] Xavier Gourdon. *Les maths en tête. Algèbre et probabilités*. Ellipses, 2021.
- [Rom21] Jean Étienne Rombaldi. *Mathématiques pour l'agrégation - Algèbre et géométrie*. De Boeck Supérieur, 2021.
- [RM22] Roger Mansuy et Rached Mneimné. *Algèbre linéaire. Réduction des endomorphismes*. De Boeck Supérieur, 2022.