

1 Espaces cycliques

1.1 Espaces cycliques

Tout étudiant ayant suivi un cours de réduction se doit constater que réduire un endomorphisme $u \in L(E)$, ce n'est rien d'autre que lui trouver des bons sous-espaces stables. Diagonaliser revient à chercher des droites stables, trigonaliser des drapeaux¹ stables, réduire des isométries des plans stables, etc. Cela suggère une étude générale des espaces stables, à commencer par leurs briques élémentaires.

Définition 1. Soit $u \in L(E)$ et $x \in E$. On note $E_{u,x}$ le plus petit sous-espace stable par u et contenant x pour l'inclusion. Un tel espace est dit *cyclique*.

Proposition 1. $E_{u,x} = \text{Vect}\{u^k(x), k \geq 0\} = K[u](x)$.

Démonstration. Par récurrence immédiate, pour tout $k \geq 0$, $u^k(x) \in E_{u,x}$ donc $\text{Vect}\{u^k(x), k \geq 0\} \subset E_{u,x}$, et est un sous-espace stable par u contenant x , d'où l'inclusion réciproque. $\square$

1.2 Polynôme minimal local

On cherche désormais à déterminer la dimension de $E_{u,x}$

Définition 2. On définit le polynôme minimal local de $u \in L(E)$ en $x \in E$ comme l'unique générateur unitaire de l'idéal $I_{u,x} = \{P \in K[X] \mid P(u)(x) = 0\}$. On le note $\mu_{u,x}$.

Proposition 2. Une base de $E_{u,x}$ est toujours donnée par $(x, u(x), \dots, u^{d-1}(x))$, où $d = \deg \mu_{u,x}$.

Démonstration. Notons $\mathcal{B} = (x, u(x), \dots, u^{d-1}(x))$. Soit $y \in E_{u,x}$. Alors $y = P(u)(x)$ pour un $P \in K[X]$. On pose la division euclidienne $P = A\mu_{u,x} + B$ avec $\deg B < d$, si bien que $y = P(u)(x) = B(u)(x) \in \text{Vect}\mathcal{B}$, donc $\mathcal{B}$ est génératrice. Soit maintenant $(\lambda_0, \dots, \lambda_{d-1}) \in K^d$ tels que $\sum_{i=0}^{d-1} \lambda_i u^i(x) = 0$. Alors en posant $P = \sum_{i=0}^{d-1} \lambda_i X^i$ on obtient $P(u)(x) = 0$ avec $\deg P < d$, ce qui impose par minimalité de $\mu_{u,x}$ que $P = 0$, et donc $\mathcal{B}$ est libre. $\square$

Corollaire 1. $\mu_{u,x}$ est le polynôme minimal de $u_{E_{u,x}}$.

1. Un drapeau est une suite de sous-espaces $0 = F_0 \subset F_1 \subset \dots \subset F_n = E$ telle que pour tout i , $\dim F_i = i$.

Démonstration. D'abord $\mu_{u,x}$ annule $u_{E_{u,x}}$ clairement, et ensuite si $P \in K[X]$ annule $u_{E_{u,x}}$ et est de degré $< d = \deg \mu_{u,x}$ alors par liberté de la famille $(u^i(x))_{i=0}^{d-1}$ on a $P = 0$. $\square$

Remarque 1. Comme $\mu_u(u)(x) = 0$, on a toujours $\mu_{u,x} \mid \mu_u$. La propriété qui suit nous dit qu'on peut toujours espérer avoir une égalité. Traduit en termes d'espaces cycliques, cela signifie qu'on peut toujours trouver des espaces cycliques de dimension maximale (égale à $\deg \mu_u$)

Théorème 1. *Soit $u \in L(E)$. Il existe $x \in E$ tel que $\mu_{u,x} = \mu_u$.*

Démonstration. Commençons par supposer que $\mu_u = P^\alpha$ pour un polynôme $P \in K[X]$ irréductible et un entier $\alpha \geq 1$. Supposons par l'absurde que pour tout $x \in E$, $\mu_{u,x} \neq P^\alpha$. Comme on a toujours $\mu_{u,x} \mid \mu_u$, $\mu_{u,x} \mid P^{\alpha-1}$ pour tout $x \in E$, et donc $P^{\alpha-1}$ annule u , i.e. $\mu_u \mid P^{\alpha-1}$ ce qui est absurde.

Passons au cas général où $\mu_u = P_1^{\alpha_1} \times \cdots \times P_r^{\alpha_r}$ est la décomposition en facteurs irréductibles de μ_u . Le lemme des noyaux nous donne $E = \bigoplus_{i=1}^r \ker P_i^{\alpha_i}(u) =: \bigoplus_{i=1}^r F_i$. On vérifie que pour tout i , $\mu_{u_{F_i}} = P_i^{\alpha_i}$ en utilisant par exemple que $\mu_{u_{F_i}} \mid P_i^{\alpha_i}$ et que $\mu_u = \text{ppcm}(\mu_{u_{F_1}}, \dots, \mu_{u_{F_r}})$. On obtient donc par le premier cas étudié, pour tout i , un $x_i \in F_i$ tel que $\mu_{u_{F_i}} = \mu_{u_{F_i}, x_i}$. Posons alors $x = \sum_{i=1}^r x_i$ et montrons que $\mu_u = \mu_{u,x}$. On écrit pour cela $\mu_{u,x}(u)(x) = 0 = \sum_{i=1}^r \mu_{u,x}(u)(x_i)$ avec pour tout i , $\mu_{u,x}(u)(x_i) \in F_i$ car F_i est u -stable, et donc pour tout i , $\mu_{u,x}(u)(x_i) = 0 = \mu_{u,x}(u_{F_i})(x_i)$, si bien que $P_i^{\alpha_i} = \mu_{u_{F_i}, x_i} \mid \mu_{u,x}$, puis $\mu_u = \text{ppcm}_i(P_i^{\alpha_i}) \mid \mu_{u,x}$. $\square$

1.3 Endomorphismes cycliques et matrices compagnons

Intéressons nous maintenant aux endomorphismes induits sur les espaces cycliques.

Définition 3. Un endomorphisme $u \in L(E)$ est dit *cyclique* s'il existe $x \in E$ tel que $E = E_{u,x}$.

Définition 4. Si $P \in K[X]$ s'écrit $P = X^n + \sum_{i=0}^{n-1} a_i X^i$, on appelle *matrice*

compagnon de P la matrice

$$C_P := \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

Proposition 3. *On a toujours $\chi_{C_P} = P$.*

Démonstration. Laissée en exercice. $\square$

Proposition 4. *$u \in L(E)$ est cyclique si et seulement s'il existe une base de E dans laquelle la matrice de u dans cette base soit une matrice compagnon.*

Démonstration. Si u est cyclique alors sa matrice dans la base $(u^i(x))_{i=0}^{d-1}$ où $d = \deg \mu_u = \mu_{u,x}$ est clairement la matrice compagnon de μ_u . Réciproquement, si $\text{Mat}_{\mathcal{B}}(u) = C_P$ pour une base $\mathcal{B} = (e_i)_{i=0}^{n-1}$ de E et $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in K[X]$, alors on a clairement $u(e_0) = e_1$, $u(e_1) = e_2$, etc, jusqu'à $u(e_{n-2}) = e_{n-1}$ puis $u(e_{n-1}) = -\sum_{i=0}^{n-1} a_i e_i$. On a donc pour tout $0 \leq i \leq n-1$, $e_i = u^i(e_0)$, puis $u^n(e_0) = u(e_{n-1}) = -\sum_{i=0}^{n-1} a_i u^i(e_0)$, i.e. $P(u)(e_0) = 0$. En particulier $\mathcal{B} = (e_0, u(e_0), \dots, u^{n-1}(e_0))$ est une base de E , donc $E = E_{u,e_0}$. $\square$

Théorème 2. *$u \in L(E)$ est cyclique si et seulement si $\mu_u = \chi_u$.*

Démonstration. Si u est cyclique alors comme on l'a vu dans la précédente preuve une matrice représentant u est C_{μ_u} , donc $\chi_u = \chi_{C_{\mu_u}} = \mu_u$. Réciproquement, si $\mu_u = \chi_u$ alors μ_u est de degré $n = \dim E$. Donnons nous $x \in E$ tel que $\mu_u = \mu_{u,x}$ (théorème 1). Alors $E_{u,x}$ est de dimension $\deg \mu_{u,x} = n$, d'où $E = E_{u,x}$. $\square$

Corollaire 2. *Soit $P \in K[X]$ unitaire. Alors $\mu_{C_P} = P$.*

Voici une illustration de l'efficacité de ce début de théorie, dont on remarquera que le point angulaire est le théorème 1.

Théorème 3 (Cayley-Hamilton). *Soit $u \in L(E)$. Alors $\chi_u(u) = 0$.*

Démonstration. Soit $x \in E$. Montrons que $\chi_u(u)(x) = 0$. Pour cela remarquons que $\chi_u(u)(x) \in E_{u,x}$ donc en particulier $\chi_u(u)(x) = \chi_{u_{E_{u,x}}}(u_{E_{u,x}})(x)$. Or $u_{E_{u,x}}$ est cyclique donc $\chi_{u_{E_{u,x}}} = \mu_{u_{E_{u,x}}} = \mu_{u,x}$, d'où le résultat. $\square$

On peut d'ors et déjà énoncer une partie du théorème de réduction de Frobenius, dont la preuve repose sur des arguments de dualité qu'on développera dans la prochaine section.

Théorème 4 (Réduction de Frobenius, existence). *Soit $u \in L(E)$. Il existe des vecteurs $x_1, \dots, x_r \in E$ tel que*

$$E = \bigoplus_{i=1}^r K[u](x_i) = \bigoplus_{i=1}^r E_{u, x_i}.$$

Matriciellement, il existe une base $\mathcal{B}$ de E dans laquelle

$$\text{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_r} \end{pmatrix},$$

où pour tout i , $P_i = \mu_{u, x_i} = \mu_{u_{E_{u, x_i}}}$ et vérifient $P_r \mid \dots \mid P_1$.

2 Dualité

2.1 Prélude sur les endomorphismes normaux

Toute l'idée de la preuve de la réduction de Frobenius se trouve dans celle, très simple, de la réduction des endomorphismes normaux. Ce paragraphe peut être sauté par le lecteur averti. Dans ce paragraphe et ce paragraphe seulement on suppose que $K = \mathbb{C}$. Pour les démonstrations voir [4].

Définition 5. Un endomorphisme $u \in L(E)$ est dit normal s'il commute avec son adjoint $u^* \in L(E)$.

Exemple 1. Les endomorphismes symétriques et antisymétriques (resp. les isométries) sont trivialement normaux car ils vérifient $u^* = \pm u$ (resp. $u^* = u^{-1}$). Parler d'endomorphismes normaux sert entre autres de parler de tous ces endomorphismes en même temps.

On traduit cela en termes d'espaces stables.

Proposition 5. $u \in L(E)$ est normal si et seulement si pour tout espace $F \subset E$ stable par u , $F^\perp$ est stable par u .

Démonstration. □

On en déduit immédiatement un théorème de réduction.

Lemme 1. *Si u est normal et F stable par u , alors l'induit u_F est normal.*

Théorème 5. *Un endomorphisme $u \in L(E)$ est normal si et seulement s'il est diagonalisable en base orthonormée.*

Remarque 2. Plus que le résultat, ce qui nous intéresse ici est l'idée de la preuve. On connaît un premier espace stable agréable - ici, une droite - puis on lui cherche un bon supplémentaire stable - ici, le supplémentaire orthogonal - sur lequel on peut appliquer le même raisonnement que pour E tout entier et donc faire marcher une récurrence sur la dimension.

2.2 Orthogonalité au sens de la dualité

On va essayer d'appliquer cette démarche pour le théorème de réduction de Frobenius. On connaît un premier espace stable agréable : $E_{u,x}$ où $x \in E$ est tel que $\mu_{u,x} = \mu_u$, donné par le théorème 1. Toute la difficulté est de lui trouver un supplémentaire stable. Ici aucun raisonnement d'orthogonalité n'est valable car on se place sur un corps quelconque K , sur lequel il n'est donc pas possible de définir un produit scalaire, la définie positivité n'ayant aucun sens. C'est là tout l'intérêt de la dualité, on remplace le produit scalaire de $\mathbb{R}^n$ ou $\mathbb{C}^n$ par le *crochet de dualité* valable sur tout corps. On ne redémontre pas les propositions, elle sont dans [5] si besoin.

Définition 6. Le *crochet de dualité* sur E est l'application bilinéaire définie sur $E \times E^*$ par

$$\forall (x, \varphi) \in E \times E^*, \langle x, \varphi \rangle := \varphi(x).$$

On peut définir une notion d'orthogonalité adaptée à $\langle \cdot, \cdot \rangle$ exactement de la même manière qu'avec les produits scalaires.

Définition 7. Soit $A \subset E$. On pose $A^\perp := \{\varphi \in E^* \mid \forall x \in A, \langle x, \varphi \rangle = 0\}$. Soit $B \subset E^*$. On pose $B^\perp := \{x \in E \mid \forall \varphi \in B, \langle x, \varphi \rangle = 0\}$.

Proposition 6. *Soit $F \subset E$ un sous-espace. Alors $\dim F^\perp = \dim E - \dim F$, et l'assertion est identique avec $F \subset E^*$.*

Remarque 3. Cette proposition nous indique, quand on cherche un supplémentaire à un sous-espace $F \subset E$, que c'est une bonne idée de le rechercher comme un $G^\perp$ où $G \subset E^*$ est de même dimension que F .

2.3 Endomorphisme transposé

Toujours dans l'esprit de généraliser les outils liés aux endomorphismes normaux, on peut se demander quel sens donner à l'adjoint dans le cadre du crochet de dualité. Pour $u \in L(E)$ on cherche $v \in L(E^*)$ tel que pour tout $(x, \varphi) \in E \times E^*$, $\langle u(x), \varphi \rangle = \langle x, v(\varphi) \rangle$. En écrivant ce que cela signifie on tombe sur $v : \varphi \mapsto u \circ \varphi$.

Définition 8. Soit $u \in L(E)$. On appelle *endomorphisme transposé* de u et on note ${}^t u$ l'endomorphisme de E^* défini par $\forall \varphi \in E^*$, ${}^t u(\varphi) = u \circ \varphi$.

Proposition 7. Soit $u \in L(E)$. Alors $\chi_{{}^t u} = \chi_u$ et $\mu_{{}^t u} = \mu_u$.

Proposition 8. Soit $u \in L(E)$.

Tout sous-espace $F \subset E$ stable par u vérifie $F^\perp \subset E^*$ stable par ${}^t u$, et réciproquement si $G \subset E^*$ est stable par ${}^t u$ alors $G^\perp \subset E$ est stable par u .

Remarque 4. Cette proposition nous permet rajouter le mot "stable" dans la remarque 3, i.e. quand on dispose d'un sous-espace **stable** $F \subset E$ dont on recherche un supplémentaire **stable**, une bonne idée est de regarder les G^T pour $G \subset E^*$ de même dimension que F et **stable** par ${}^t u$. Tout cela reflète une idée plus générale qui est qu'un bon supplémentaire de $F \subset E$ est un G^T pour $G \subset E^*$ qui se comporte avec ${}^t u$ comme F avec u .

Exemple 2. Un autre exemple de ce principe de dualité, qu'on ne met pas dans une proposition parce qu'il nous est inutile ici, est le suivant. Un endomorphisme $u \in L(E)$ injectif si et seulement si ${}^t u$ est surjectif, et on peut interchanger les mots injectif et surjectif. C'est intéressant (en dimension infinie) car c'est généralement plus simple de montrer qu'un morphisme est injectif. En effet, montrer la surjectivité revient presque à construire la réciproque, alors que l'injectivité ne demande a priori aucune construction.

3 Preuve du théorème de réduction de Frobenius

3.1 Existence [2]

Commençons par la partie existence, énoncée au théorème 4, dont tous les ingrédients ont été étudiés dans les sections précédentes.

Preuve du théorème 4. On commence par se donner un $x \in E$ tel que $\mu_{u,x} = \mu_u$ grâce au théorème 1, de telle sorte que $E_{u,x}$ soit de dimension $d = \deg \mu_u$ et donc $P_1 := \mu_u$. On cherche à faire marcher une récurrence sur la dimension de E , on cherche donc un supplémentaire de $E_{u,x}$ stable par u . Le paragraphe précédent nous suggère de le rechercher comme un $E^{*}_{t_{u,\varphi}}$ pour un $\varphi \in E^*$ tel que $\dim E^{*}_{t_{u,\varphi}} = \dim E_{u,x} = d$. Or en appliquant le théorème 1 à ${}^t u \in L(E^*)$ on obtient une forme linéaire $\varphi \in E^*$ telle que $\mu^{t_{u,\varphi}} = \mu^{t_u}$, avec $\mu^{t_u} = \mu_u$ d'après la proposition 7. On a donc que $F_\varphi = E^{*}_{t_{u,\varphi}}$ est un sous-espace de E stable par u est de dimension $\dim E - d$. On semble être tout proche de conclure mais il faut encore vérifier que $E_{u,x} \cap F_\varphi = \{0\}$. Écrivons un peu mieux cette intersection :

$$\begin{aligned} E_{u,x} \cap F_\varphi &= \{P(u)(x) \mid P \in K[X] \text{ et } \forall k \geq 0, \varphi \circ u^k \circ P(u)(x) = 0\} \\ &= \left\{ \sum_{i=0}^{d-1} a_i u^i(x) \mid \sum_{i=0}^{d-1} a_i \varphi \circ u^{k+i}(x) = 0 \right\}. \end{aligned}$$

On ne peut pas en dire grand chose, même pas qu'elle est engendrée par des $u^i(x)$ ce qui simplifierait éventuellement les calculs. En bref, ce raisonnement ne marche pas en toute généralité, il faut trouver un φ explicite qui rende ce calcul d'intersection facile. On laisse au lecteur le soin de vérifier qu'on peut définir $\varphi \in E^*$ tel que pour tout $0 \leq i < d-1$, $\varphi(u^i(x)) = 0$ et $\varphi(u^{d-1}(x)) = 1$ à partir d'une base duale par exemple, puis de montrer qu'avec un tel φ on a bien $E_{u,x} \cap F_\varphi = \{0\}$. Certes, le calcul d'intersection est rendu facile par le choix de φ , mais on a perdu le fait que $E^{*}_{t_{u,\varphi}}$ était de dimension d . Encore une fois, on laisse au lecteur le soin de le vérifier à la main, ce qui est sans difficulté. Cela étant dit, on a réuni tous les ingrédients pour avoir $E = E_{u,x} \oplus F_\varphi$ avec F_φ stable par u , donc on peut appliquer l'hypothèse de récurrence sur F_φ pour obtenir

$$E = E_{u,x} \oplus \bigoplus_{i=2}^r E_{u_{F_\varphi}, x_i}$$

où les $x_i \in F_\varphi$ et à l'évidence pour tout i , $E_{u_{F_\varphi}, x_i} = K[u_{F_\varphi}](x_i) = K[u](x_i) = E_{u, x_i}$, ce qui donne en notant $x_1 = x$,

$$E = \bigoplus_{i=1}^r K[u](x_i) = \bigoplus_{i=1}^r E_{u, x_i}.$$

De plus, par construction les polynômes $P_i = \mu_{u, x_i}$ vérifient $P_r \mid \cdots \mid P_2$, et on a naturellement $P_2 = \mu_{u, x_2} \mid \mu_u = \mu_{u, x_1} = P_1$ donc finalement $P_r \mid \cdots \mid P_2 \mid P_1$. $\square$

3.2 Unicité [3]

On s'attaque désormais à la clause d'unicité du théorème de Frobenius, qui est loin d'être anecdotique comme on le verra dans les applications.

Théorème 6. *Soit $u \in L(E)$. On suppose qu'on dispose de deux décompositions de Frobenius de u :*

$$E = \bigoplus_{i=1}^r K[u]x_i = \bigoplus_{j=1}^s K[u]y_j \quad (1)$$

pour des $x_i, y_j \in E$. Alors les suites de polynômes $(P_i)_{i=1}^r$ et $(Q_j)_{j=1}^s$ associés à ces décompositions sont les mêmes, i.e. $r = s$ et pour tout $1 \leq i \leq r$, $P_i = Q_i$. On dit que $(P_i)_i$ est la suite des invariants de similitude de l'endomorphisme u .

Avant de s'attaquer à la preuve, il est bon de comprendre la portée de ce résultat.

Corollaire 3. *Soit $u, v \in L(E)$. Il existe $\phi \in \text{GL}(E)$ tel que $v = \phi \circ u \circ \phi^{-1}$ si et seulement si u et v ont la même suite d'invariants de similitude.*

Autrement dit, on dispose d'un invariant total pour l'action de $\text{GL}_n(K)$ sur $\mathcal{M}_n(K)$ par conjugaison, et ce quelque soit le corps K , ce qui clôt en quelque sorte le problème de la réduction des endomorphismes.

Preuve du théorème 6. Tout d'abord $P_1 = Q_1 = \mu_u$ nécessairement car d'abord $P_1 = \mu_{u, x_1} \mid \mu_u$ et pour l'autre divisibilité on peut écrire pour tout i , $P_1 = P_i R_i$ pour un $R_i \in K[X]$ et donc pour tout $x \in E$, $x = \sum_{i=1}^r A_i(u)(x_i)$, d'où

$$P_1(u)(x) = \sum_{i=1}^r (P_1 A_i)(u)(x_i) = \sum_{i=1}^r (A_i R_i)(u) \circ P_i(u)(x_i) = 0.$$

Supposons maintenant que $(P_i)_i \neq (Q_j)_j$ et notons k le premier rang tel que $P_k \neq Q_k$. On vient donc de montrer que $k \geq 2$. Appliquons $P_k(u)$ aux

sommes directes de (1) :

$$P_k(u)(E) = \bigoplus_{i=1}^r P_k(u)(E_{u,x_i}) = \bigoplus_{j=1}^s P_k(u)(E_{u,y_j}). \quad (2)$$

Or $P_k(u)(E_{u,x_i}) = 0$ dès que $P_i \mid P_k$, i.e. dès que $i \geq k$ donc la première somme directe est $P_k(u)(E) = \bigoplus_{i=1}^{k-1} P_k(u)(E_{u,x_i})$. Remarquons maintenant que pour $i < k$, $P_k(u)(E_{u,x_i})$ et $P_k(u)(E_{u,y_i})$ ont même dimension. En effet, on commence par écrire $\dim P_k(u)(E_{u,x_i}) = \text{rg}(P_k(u_{E_{u,x_i}}))$ où $v_i := P_k(u_{E_{u,x_i}}) \in K[u_{E_{u,x_i}}] \cong K[X]/(P_i)$ car pour rappel $P_i = \mu_{u_{E_{u,x_i}}} = \mu_{u,x_i}$. L'endomorphisme v_i correspond dans $K[X]/(P_i)$ à la classe de P_k modulo P_i , or $i < k$ donc $P_i = Q_i$ avec de manière symétrique $K[X]/(Q_i) \cong K[u_{E_{u,y_i}}]$, si bien que l'on dispose d'un isomorphisme d'espaces vectoriels $K[u_{E_{u,x_i}}] \xrightarrow{\phi} K[u_{E_{u,y_i}}]$ envoyant $v_i = P_k(u_{E_{u,x_i}})$ sur $w_i = P_k(u_{E_{u,y_i}})$, puis

$$\text{rg}(w_i) = \text{rg}(\phi(v_i)) = \dim E - \dim \ker(\phi(v_i)) = \dim E - \dim \ker v_i = \text{rg}(v_i).$$

Au final, les deux espaces $\bigoplus_{i=1}^{k-1} P_k(u)(E_{u,x_i})$ et $\bigoplus_{i=1}^{k-1} P_k(u)(E_{u,y_i})$ ont même dimension puis (2) nous donne que $\bigoplus_{j=k}^s P_k(u)(E_{u,y_j}) = \{0\}$, i.e. pour tout $j \geq k$, $P_k(u)(E_{u,y_j}) = \{0\}$, i.e. $Q_j \mid P_k$ encore car $Q_j = \mu_{u_{E_{u,y_j}}}$. En particulier $Q_k \mid P_k$, et en appliquant le même argument mais avec $Q_k(u)$ à la place de $P_k(u)$ on aboutit à $P_k \mid Q_k$, et donc $P_k = Q_k$ car les deux polynômes sont unitaires. $\square$

4 Lien avec les extensions de corps

La réduction de Frobenius étant valable sur tout corps, elle ouvre la voie à faire interagir extensions de corps et algèbre linéaire. On se fixe dans toute ce paragraphe une extension de corps $K \subset L$.

4.1 Trucs invariants par extension de corps [2]

L'objectif de ce paragraphe est de montrer que la relation de similitude ne dépend pas du corps en un sens qui va être précisé.

Lemme 2. *Soit $A \in \mathcal{M}_n(K)$. Alors en particulier $A = \tilde{A} \in \mathcal{M}_n(L)$ et $\text{rg}(A) = \text{rg}(\tilde{A})$. Autrement dit, le rang est invariant par extension de corps.*

Démonstration. Le calcul du rang de A se fait par exemple en échellonnant A en colonne, par une méthode du type pivot de Gauss. Les opérations qu'on fait sur les lignes où les colonnes ne dépendent que des coefficients de A . En particulier, si on note k le sous corps de K engendré par les coefficients de A alors $\text{rg}_k(A) = \text{rg}_K(A) = \text{rg}_L(A)$. $\square$

Lemme 3. *Avec les mêmes notations, on a $\mu_A = \mu_{\tilde{A}}$. Autrement dit, le polynôme minimal est invariant par extension de corps.*

Démonstration. Étant donné que $\mu_A \in K[X] \subset L[X]$ et annule $\tilde{A} = A$, on a $\mu_{\tilde{A}} \mid \mu_A$. Il suffit donc de montrer que $\deg \mu_A = \deg \mu_{\tilde{A}}$, or $\deg \mu_A = \text{rg}_K(I_n, A, \dots, A^n)$ puis on conclut par le lemme précédent. $\square$

Théorème 7. *Soit $A, B \in \mathcal{M}_n(K)$. Alors A et B sont semblables sur K si et seulement si elles sont semblables sur L .*

Démonstration. Supposons que $B = PAP^{-1}$ pour une matrice de passage $P \in \text{GL}_n(L)$. Il s'agit de montrer que l'on peut trouver $Q \in \text{GL}_n(K)$ tel que $B = QAQ^{-1}$. D'après le théorème de réduction de Frobenius, A et B ont mêmes invariants de similitude sur L , disons $P_r \mid \dots \mid P_1 \in L[X]$. Montrons qu'en fait les $P_i \in K[X]$, ce qui suffit à conclure par unicité des invariants de similitude. On fait correspondre les P_i à des décompositions de $E := L^n$ en somme d'espaces cycliques :

$$E = \bigoplus_{i=1}^r L[A]x_i = \bigoplus_{i=1}^r L[B]y_i,$$

où les $x_i, y_i \in E$ sont tels que pour tout i , $P_i = \mu_{A_{E_{A,x_i}}} = \mu_{B_{E_{B,y_i}}}$, si on se permet de faire l'amalgame entre matrices et applications linéaires. On remarque enfin que pour tout i , quitte à fixer une base, les applications induites $A_{E_{A,x_i}}$ et $B_{E_{B,y_i}}$ sont à coefficients dans K , puis on conclut en utilisant l'invariance du polynôme minimal par extension de corps. $\square$

Corollaire 4. *Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice normale, i.e. ${}^tAA = A^tA$. Alors*

A est semblable sur $\mathbb{R}$ à une matrice de la forme

$$\Delta = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_r & & & \\ & & & \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} & & \\ & & & & \ddots & \\ & & & & & \begin{pmatrix} a_s & b_s \\ -b_s & a_s \end{pmatrix} \end{pmatrix} \in \mathcal{M}_n(\mathbb{R}).$$

Démonstration. D'après le théorème 5 A est semblable sur $\mathbb{C}$ à une matrice diagonalisable D , et par le théorème précédent il suffit de montrer que D est semblable sur $\mathbb{C}$ à une matrice de la forme de Δ . On écrit pour cela $D = \text{diag}(\lambda_1, \dots, \lambda_r, \alpha_1, \overline{\alpha_1}, \dots, \alpha_s, \overline{\alpha_s})$ où les $\lambda_i \in \mathbb{R}$ et les $\alpha_j \in \mathbb{C} \setminus \mathbb{R}$. On peut toujours ce ramener à ce cas quitte à changer l'ordre des vecteurs dans la base d'arrivée. On conclut à l'aide du petit lemme qui suit :

Lemme 4. Soit $\alpha = a + ib$ pour $a, b \in \mathbb{R}$ tel que $b \neq 0$. Alors il existe $P \in \text{GL}_2(\mathbb{C})$ tel que

$$\begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix} = P \begin{pmatrix} a & -b \\ b & a \end{pmatrix} P^{-1}.$$

Preuve du lemme. Les valeurs propres de la matrice de droite sont les racines de $X^2 - 2aX + a^2 + b^2 = X^2 - 2\text{Re}(\alpha)X + |\alpha|^2$, i.e. α et $\overline{\alpha}$. Comme elles sont distinctes alors la matrice est diagonalisable semblable à $\text{diag}(\alpha, \overline{\alpha})$. $\square$

$\square$

4.2 Endomorphismes semi-simples [1]

On poursuit notre étude des liens entre réduction des endomorphismes et extensions de corps en s'intéressant plus particulièrement aux liens entre diagonalisabilité et extensions de corps. Il est clair qu'une matrice $A \in \mathcal{M}_n(K)$ diagonalisable sur L n'a aucune raison d'être diagonalisable sur K , car par exemple elle peut avoir des valeurs propres dans $L \setminus K$. En revanche on peut s'intéresser aux matrices de $\mathcal{M}_n(K)$ qui sont diagonalisables dans la clôture algébrique de K qu'on notera $\overline{K}$. Cette notion est naturellement invariante par extension de corps, et on va chercher à la caractériser.

Définition 9. On dit qu'une matrice $A \in \mathcal{M}_n(K)$ est dite *semi-simple* si elle est diagonalisable dans $\overline{K}$. De la même manière un endomorphisme $u \in L(E)$ est dit semi-simple si ses matrices dans une base de E est semi-simple.

Proposition 9. *On suppose que K est un corps parfait². Une matrice $A \in \mathcal{M}_n(K)$ est semi-simple si et seulement si μ_A est sans facteur irréductible carré dans $K[X]$.*

Démonstration. A est semi-simple si et seulement si $A = \tilde{A} \in \mathcal{M}_n(\overline{K})$ est diagonalisable, i.e. si et seulement si $\mu_{\tilde{A}}$ est scindé à racines simples sur $\tilde{K}$, i.e. si et seulement si μ_A est scindé à racines simples sur $\tilde{K}$ d'après le théorème 7, et on sait que ceci est équivalent au fait que μ_A et μ'_A soient premiers entre eux dans $K[X]$. En écrivant $\mu_A = P_1^{\alpha_1} \times \cdots \times P_r^{\alpha_r}$ la décomposition de μ_A en facteurs irréductibles dans $K[X]$, on remarque que $P_1^{\alpha_1-1} \times \cdots \times P_r^{\alpha_r-1}$ divise toujours le pgcd de μ_A et μ'_A . On en tire que si un des $\alpha_i > 1$, alors μ_A et μ'_A ne sont pas premiers entre eux et donc A n'est pas semi-simple. Réciproquement, si $\mu_A = P_1 \times \cdots \times P_r$ alors, K étant parfait, les P_i sont à racines simples dans $\overline{K}$, puis μ_A également. $\square$

Le théorème de réduction de Frobenius nous aide à comprendre au moins une petite classe d'endomorphismes semi-simples.

Proposition 10. *Soit $A \in \mathcal{M}_n(K)$ où K est parfait et μ_A est irréductible sur K . Alors A est semi-simple et vérifie la propriété suivante :*
 (P_A) : "Pour tout sous espace $F \subset K^n$ stable par A , il existe un supplémentaire de F dans K^n stable par A ".

Démonstration. La première assertion découle directement de la proposition précédente. Donnons nous une décomposition de $E := K^n$ en sous-espaces cycliques : $E = \bigoplus_{i=1}^r K[A]x_i$ pour des $x_i \in E$. Comme $K[A]$ est isomorphe en tant qu'algèbre à $K[X]/(\mu_A)$ qui est un corps puisque μ_A est supposé irréductible, $K[A]$ est en fait une extension de K de degré $d = \deg \mu_A$. Les K -sous espaces $K[A]x_i$ sont en fait des $K[A]$ -droites, i.e. $K[A]x_i = \text{Vect}_{K[A]}(x_i)$. Cette discussion nous conduit à poser une structure de $K[A]$ -espace vectoriel sur E en posant tout naturellement pour tout $B = P(A) \in K[A]$ et tout $x \in E$, $B \cdot Bx = P(A)(x)$. On laisse au lecteur le soin de vérifier que c'est bien une loi de composition externe faisant de E un $K[A]$ -espace vectoriel.

². On peut simplement supposer que K est de caractéristique zéro ou bien un corps fini si on ne veut pas s'embêter avec des subtilités de théorie des corps.

Cette structure a le bon goût de vérifier que les $K[A]$ -sous espaces de E sont exactement les K -sous espaces de E stables par A (laissé en exercice). Cela étant dit, si $F \subset E$ est un K -sous-espace stable par A , alors c'est un $K[A]$ -sous-espace. On peut alors prendre G un $K[A]$ -supplémentaire de F dans E , puis G est un K -sous-espace stable par A . $\square$

Le théorème qui suit nous dit que la propriété (P_A) de la proposition précédente est en fait caractéristique des endomorphismes semi-simples.

Théorème 8. *Soit $u \in L(E)$, $E \cong K^n$, K étant un corps parfait³. Alors u est semi-simple si et seulement si la propriété (P_u) est vraie.*

Démonstration. Commençons par le sens facile. On suppose (P_u) vraie et que l'on peut écrire $\mu_u = P^2Q$ pour des polynômes $P, Q \in K[X]$ non nuls. Notons $F = \ker P(u)$ et donnons nous $G \subset E$ un supplémentaire de F stable par u . Montrons que PQ annule u . Si $x \in F$, on écrit $(PQ)(u)(x) = Q(u)(P(u)(x)) = 0$. Si $x \in G$, on écrit $(PQ)(u)(x) \in G$ car G est stable par u et $(PQ)(u)(x) \in F$ car P^2Q annule u , si bien que $(PQ)(u)(x) \in F \cap G = \{0\}$. En conclusion PQ annule u sur F et G donc sur E tout entier, puis $\mu_u = P^2Q \mid PQ$ nous donne la contradiction souhaitée.

Pour l'autre sens, on note $\mu_u = P_1 \times \cdots \times P_r$ pour des polynômes P_i unitaires irréductibles sur K et deux à deux premiers entre eux et on se donne $F \subset E$ un sous-espace stable par u . Le lemme des noyaux nous donne $E = \bigoplus_{i=1}^r \ker P_i(u) =: \bigoplus_{i=1}^r F_i$. Montrons que $F = \bigoplus_{i=1}^r F \cap F_i$. Il est clair que la somme $(F \cap F_1) + \cdots + (F \cap F_r)$ est directe et qu'elle est incluse dans F , il faut donc montrer que $F \subset \bigoplus_{i=1}^r F \cap F_i$. Le lemme des noyaux nous dit également que pour tout i , les projecteurs $p_j : E \rightarrow F_j$ associés à la somme directe $E = \bigoplus_{j=1}^r F_j$ sont des éléments de $K[u]$. On en déduit que pour tout $x \in F$, $p_j(x) \in F$ car F est stable par u . Ainsi, pour tout $x \in F$ on a $x = \sum_{j=1}^r p_j(x) \in \bigoplus_{i=1}^r F \cap F_j$.

Cela étant dit, on utilise que pour tout i , le polynôme minimal de u_{F_i} est P_i (car il divise P_i et que P_i est irréductible) et donc que l'on peut appliquer la proposition précédente à u_{F_i} pour l'espace stable $F \cap F_i$. On obtient alors pour tout i , un sous-espace G_i stable par u_{F_i} et tel que $F_i = (F \cap F_i) \oplus G_i$. Il reste à poser $G = \bigoplus_{i=1}^r G_i$ et vérifier que $E = F \oplus G$ avec G u -stable, ce qui est sans difficulté. $\square$

3. Là encore on peut simplement supposer $K \subset \mathbb{C}$ ou K corps fini.

Remarque 5. On peut comparer le théorème précédent avec ce qu'on sait sur les endomorphismes normaux (encore eux!). En effet, les endomorphismes normaux réels sont toujours diagonalisables sur $\mathbb{C} = \overline{\mathbb{R}}$, et sont caractérisés par le fait que quelque soit le sous-espace stable, l'orthogonal est stable. On peut alors espérer avoir un résultat similaire au corollaire 4 pour un endomorphisme semi-simple arbitraire.

Proposition 11. *Soit $u \in L(E)$ un endomorphisme semi-simple sur un corps K parfait. Notons $\lambda_1, \dots, \lambda_r$ les valeurs propres de u qui appartiennent à K comptées avec leur multiplicité. Alors il existe une base de E dans laquelle la matrice de u est*

$$\Delta = \begin{pmatrix} \lambda_1 & & & & \\ & \ddots & & & \\ & & \lambda_r & & \\ & & & C_{\mu_{\alpha_1, K}} & \\ & & & & \ddots \\ & & & & & C_{\mu_{\alpha_s, K}} \end{pmatrix},$$

où pour tout i , $\mu_{\alpha_i, K}$ est le polynôme minimal d'un l'élément $\alpha_i \in \overline{K}$ algébrique sur K .

Démonstration. u est semi-simple donc μ_u est sans facteur carré dans $K[X]$: $\mu_u = \prod_{i \in I} (X - \lambda_i) \times \prod_{j=1}^s P_j$ pour des $P_j \in K[X]$ deux à deux distincts et irréductibles de degré ≥ 2 , et $I \subset [1, r]$ ne contenant qu'un exemplaire de chaque λ_i . On écrit ensuite pour tout j , $P_j = \mu_{\alpha_j, K}$ après avoir choisi n'importe que $\alpha_j \in \overline{K}$ tel que $P_j(\alpha_j) = 0$. Le corps K étant parfait, les P_j sont à racines simples dans $\overline{K}$, et donc toute matrice $A \in \mathcal{M}_n(K)$ représentant u est semblable dans $\mathcal{M}_n(\overline{K})$ à la matrice $D = \text{diag}(\lambda_1, \dots, \lambda_r, \Delta_1, \dots, \Delta_s)$, où pour tout j , Δ_j est la matrice diagonale dont les valeurs diagonales sont les racines de $P_j = \mu_{\alpha_j, K}$. On écrit maintenant que pour tout j , Δ_j est semblable sur $\overline{K}$ à la matrice compagnon C_{P_j} car elle sont toutes diagonalisables de même polynôme caractéristique P_j . En recollant les morceaux et en utilisant le théorème 7 on a montré le résultat. $\square$

Références

- [1] Grégory BERTHUY. *Algèbre: le grand combat*. Calvage & Mounet, 2018.
- [2] Philippe CALDERO et Jérôme GERMONI. *Nouvelles histoires hédonistes de groupes et de géométries*. Calvage et Mounet, 2018.
- [3] Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. Editions Ellipses, 2021.
- [4] Roger MANSUY et Rached MNEIMNÉ. *Algèbre linéaire. Réduction des endomorphismes: Cours et exercices corrigés-Licence• Prépas• Capes• Agrégation*. De Boeck Supérieur, 2022.
- [5] Patrice TAUVEL. *Algèbre linéaire*. Calvage et Mounet.