Algèbres de dimension finie

Antoine MOUZARD

Résumé

Ce cours a pour but de présenter la notion d'algèbre de dimension finie à travers les différents exemples du programme de l'agrégation externe. Il illustre ainsi le lien entre différentes leçons d'algèbres et peut permettre d'enrichir les exemples et applications.

Table des matières

1 Algèbres sur un anneau commutatif unitaire

Définition. *Une algèbre sur un anneau commutatif unitaire A est la donnée de $(E, A, +, \cdot, \times)$ où $(E, +)$ est un groupe commutatif, pour tout $a, b \in A$ et $x, y \in E$ on a*

$$\begin{aligned}(a+b)\cdot x &= a\cdot x + b\cdot x,\\ a\cdot(x+y) &= a\cdot x + a\cdot y,\\ a\cdot(b\cdot x) &= (ab)\cdot x,\\ 1\cdot x &= x,\end{aligned}$$

et $\times : E \times E \longrightarrow E$ est bilinéaire. L'algèbre est dite associative ou commutative si l'opération $\times$ est associative ou commutative. Elle est dite unitaire si elle possède un élément neutre pour la loi $\times$.

Dans toute la suite, les algèbres seront implicitement supposées associatives et unitaires. Dans le cas où l'anneau est un corps $\mathbb{K}$, E est un $\mathbb{K}$-espace vectoriel muni d'une loi interne bilinéaire $\times$; ce sera le cas dans la plupart de nos exemples. Dans ce cas, on peut parler de la dimension d'une $\mathbb{K}$-algèbre comme étant sa dimension en tant que $\mathbb{K}$-espace vectoriel. Les trois exemples principaux que nous allons étudier ici sont l'algèbre $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ en une indeterminée, toute extension $\mathbb{L}$ d'un corps $\mathbb{K}$ et l'algèbre $\mathscr{L}(E)$ des endomorphismes d'un $\mathbb{K}$-espace vectoriel E de dimension finie.

Définition. *Un morphisme de A-algèbre de E vers F est une application $f : E \to F$ telle que f est un morphisme de groupe de $(E, +)$ dans $(F, +)$ et pour tout $a \in A$ et $x, y \in E$*

$$\begin{aligned}f(x+y) &= f(x) + f(y)\\ f(a\cdot x) &= a\cdot f(x)\\ f(x\times y) &= f(x)\times f(y)\\ f(1_E) &= 1_F.\end{aligned}$$

S'il est bijectif, on parle d'isomorphisme de A-algèbre.

Étant donné un élément x dans une A-algèbre E, on dispose alors du morphisme d'évaluation défini par

$$ev_x : \begin{array}{ccc} A[X] & \to & E \\ P & \mapsto & P(a) \end{array}.$$

Son noyau est un idéal de $A[X]$, c'est l'ensemble des polynômes annulateurs de x. Dans le cas où A est un corps, $A[X]$ est principal est son noyau est $A[X]$ tout entier ou engendrée par un unique élément unitaire, on parle alors d'éléments transcendants ou algèbriques.

Définition. *Soient $\mathbb{K}$ un corps et E une $\mathbb{K}$-algèbre. Soit $x \in E$. Si ev_x est injectif, alors x est dit transcendant. Sinon x est dit algèbrique et le noyau de ev_x est un idéal de $\mathbb{K}[X]$ engendré par un unique polynôme unitaire appelé polynôme minimal de x et noté Π_x.*

L'image de ev_x est une sous-algèbre de A qu'on appelle l'algèbre engendrée par x, c'est la plus petite sous-algèbre de A contenant x au sens de l'inclusion. On la note parfois $\langle x \rangle$. Comme une intersection d'algèbre est une algèbre, l'algèbre engendrée par x est aussi l'intersection de toutes les sous-algèbres de A contenant x,

$$\langle x \rangle = \bigcap_{x \in \bar{E} \text{ sous-algèbre de E}} \bar{E}.$$

Exemple.
- *Dans le cas des endomorphisme, on se donne un $\mathbb{K}$-espace vectoriel E et on considère l'algèbre $\mathscr{L}(E)$ munie de la composition. L'évaluation d'un polynôme $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{K}[X]$ en un endormorphisme u est un exemple, avec*

$$ev_u(P) = P(u) = a_0 \cdot Id + a_1 \cdot u + a_2 \cdot u \circ u + \ldots + a_n \cdot u \circ \ldots \circ u \in \mathscr{L}(E).$$

  Son image $\mathbb{K}[u]$ est une sous-algèbre commutative de $\mathscr{L}(E)$ et on a

$$\mathbb{K}[X]/(\Pi_u) \simeq \mathbb{K}[u].$$

  avec Π_u le polynôme minimal de u.
- *Pour un espace vectoriel E de dimension n, on peut se donner une base $\mathcal{B}$. Dans ce cas, on dispose du morphisme d'algèbre*

$$\begin{array}{ccc} \mathscr{L}(E) & \to & \mathcal{M}_n(\mathbb{K}) \\ u & \mapsto & \underset{\mathcal{B}}{\mathrm{mat}}(u) \end{array}$$

  et deux bases différentes donnent deux morphismes d'algèbre différents.

Dans le cas d'une algèbre de dimension finie sur le corps $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, on dispose aussi d'une structure d'espace vectoriel de dimension finie qu'on peut munir de différentes normes, toutes équivalentes. Une norme est dite d'algèbre si

$$\forall x, y \in E, \quad \|x \times y\| \leq \|x\| \cdot \|y\|,$$

c'est-à-dire si elle est sous-multiplicative. Par exemple, la norme $\|M\|_\infty = \sup_{i,j} |m_{ij}|$ n'est pas une norme d'algèbre sur $\mathcal{M}_n(\mathbb{R})$ alors que toute norme subordonnée est une norme d'algèbre. En particulier, à partir de n'importe quelle norme $\|\cdot\|$ sur une algèbre E, la norme

$$\|y\|_A := \sup_{\|x\|=1} \|x \times y\|$$

est une norme d'algèbre sur A. On peut alors étudier la convergence de suites et séries comme par exemple l'exponentielle. En effet, pour tout $n \in \mathbb{N}$ et $x \in E$, on a

$$\left\| \sum_{k=0}^{n} \frac{x^k}{k!} \right\| \leq \sum_{k=0}^{n} \frac{\|x\|^k}{k!}$$

donc la série est normalement convergente.

Définition. *Dans une $\mathbb{K}$-algèbre E avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, on appelle exponentielle de $x \in E$ la somme*

$$\exp(x) := \sum_{k \geq 0} \frac{x^k}{k!}.$$

L'ensemble des polynômes en un élément étant un sous-espace vectoriel de E, il est fermé donc $\exp(x)$ est un polynôme en x. L'exponentielle d'un élément dans une algèbre apparaît dans différents domaines comme par exemple les équations différentielles ou les algèbres de Lie.

Théorème. *Si $A \in \mathcal{M}_n(\mathbb{C})$, alors*

$$\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times,$$

où $\mathbb{C}[A]^\times$ désigne les éléments inversibles de l'anneau $\mathbb{C}[A]$.

Preuve : On a d'abord

$$\mathbb{C}[A]^\times = \mathbb{C}[A] \cap GL_n(\mathbb{C}).$$

La première inclusion étant immédiate, on considère $M \in \mathbb{C}[A] \cap GL_n(\mathbb{C})$. On a

$$\chi_M(0) = \det(M)$$

et le théorème de Cayley-Hamilton assure alors que $M^{-1} \in \mathbb{C}[M] \subset \mathbb{C}[A]$, ce qui permet de conclure, M étant un polynôme en A.

On montre alors que $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \det^{-1}(\mathbb{C}^*)$ est un connexe de $\mathbb{C}[A]$. Soient $M_0, M_1 \in \mathbb{C}[A]^\times$. Si on pose

$$M(t) = (1-t)M_0 + tM_1, \quad 0 \leq t \leq 1,$$

alors le chemin reste dans $\mathbb{C}[A]$ mais le déterminant de $M(t)$ peut s'annuler. Or la fonction

$$z \in \mathbb{C} \mapsto \det\big(M(z)\big)$$

est polynomiale en z donc elle s'annule en un nombre fini de points. $\mathbb{C}$ privé de ce nombre fini de points est connexe par arc donc on peut trouver un chemin γ qui relie 0 et 1 sans passer par ces points. Ainsi $M \circ \gamma$ relie M_0 à M_1, ce qui permet de conclure que $\mathbb{C}[A]^\times$ est connexe par arc donc connexe.

Comme $\exp(\mathbb{C}[A]) \subset \mathbb{C}[A]^\times$ est non vide, il suffit de montrer que $\exp(\mathbb{C}[A])$ est ouvert et fermé dans $\mathbb{C}[A]^\times$ pour conclure à l'aide d'un argument de connexité. On commence par montrer que c'est un ouvert. On a

$$d_0\exp = \mathrm{Id}$$

qui est inversible. D'après le théorème d'inversion locale appliqué dans $\mathbb{C}[A]$, l'exponentielle envoie un voisinage $\mathcal{U}$ de 0 dans $\mathbb{C}[A]$ sur un voisinage $\mathcal{V}$ de I_n dans $\mathbb{C}[A]^\times$. Pour $M \in \mathbb{C}[A]$,

$$\mathcal{V}_M := \{Ve^M \ ; \ V \in \mathcal{V}\}$$

est un voisinage de e^M dans $\exp(\mathbb{C}[A])$. En effet, pour tout $V \in \mathcal{V}$, il existe $U \in \mathcal{U}$ telle que $V = e^U$ et on a

$$Ve^M = e^U e^M = e^{U+M} \in \exp(\mathbb{C}[A])$$

car U et M commutent en tant que polynôme en A, ce qui montre que $\exp(\mathbb{C}[A])$ est un ouvert de $\mathbb{C}[A]^\times$. Pour montrer que c'est un fermé, on montre que son complémentaire $X := \mathbb{C}[A]^\times \backslash \exp(\mathbb{C}[A])$ est un ouvert. Pour cela, on montre que

$$X = \bigcup_{M \in X} M \cdot \exp(\mathbb{C}[A]).$$

La première inclusion est vraie car $I_n = e^0 \in \exp(\mathbb{C}[A])$. Réciproquement, soient $M \in X$ et $P(A) \in \mathbb{C}[A]$. On considère $N := Me^{P(A)}$. On a $M \in X$ donc

$$M = Ne^{-P(A)} \notin \exp(\mathbb{C}[A])$$

et N n'est pas dans $\exp(\mathbb{C}[A])$ ce qui démontre l'inclusion réciproque. On peut alors conclure que X est ouvert, $M \cdot \exp(\mathbb{C}[A])$ l'étant pour M inversible.

□

Corollaire. *L'application* $\exp : \mathcal{M}_n(\mathbb{C}) \to GL_n(\mathbb{C})$ *est surjective. L'image de l'application* $\exp : \mathcal{M}_n(\mathbb{R}) \to GL_n(\mathbb{R})$ *est*

$$\{A^2 \ ; A \in GL_n(\mathbb{R})\}.$$

Preuve : Pour $A \in GL_n(\mathbb{C})$, $A \in \mathbb{C}[A]^\times$ donc par le théorème précédent, il existe $P \in \mathbb{C}[X]$ tel que

$$A = e^{P(A)}$$

ce qui permet de conclure pour la surjectivité. Pour le cas réel, on considère $M \in \mathcal{M}_n(\mathbb{R})$. La première inclusion découle de l'identité

$$\left(e^{\frac{M}{2}}\right)^2 = e^M.$$

Réciproquement, il existe $P \in \mathbb{C}[X]$ tel que $M = e^{P(M)}$ grâce au théorème précédent. On a aussi $M = e^{\overline{P}(M)}$ car M est à coefficients réels. On peut alors conclure avec

$$M^2 = e^{(P+\bar{P})(M)}.$$

□

Une autre série qui peut être intéressante est la série géométrique. Pour $\|x\| < 1$, la série est absoluement convergente et vérifie

$$\sum_{n\geq 0} x^n = (1+x)^{-1}.$$

En particulier, cela implique que la boule ouverte de centre 1 et de rayon 1 est toujours incluse dans $A^\times$. Pour $y \in A^\times$, on a

$$y + x = y(1 + y^{-1}x)$$

donc la boule ouverte de centre y et de rayon $\|y\|^{-1}$ est incluse dans $A^\times$. En particulier, on a que $A^\times$ est un ouvert de A sans utiliser la théorie du déterminant avec un moyen d'obtenir des boules explicites d'élément inversibles.

2 Extension de corps

Définition. — *Un corps* $(\mathbb{K}, +, \cdot)$ *est un anneau commutatif unitaire où tous les éléments non nuls sont inversibles.*

— *Une extension d'un corps* $\mathbb{K}$ *est une* $\mathbb{K}$*-algèbre* $\mathbb{L}$ *qui est aussi un corps. On a alors une injection de* $\mathbb{K}$ *dans* $\mathbb{L}$ *et on note* $\mathbb{K} \hookrightarrow \mathbb{L}$*. On appelle degrée de l'extension la dimension de* $\mathbb{L}$ *en tant que* $\mathbb{K}$*-espace vectoriel. On le note* $[\mathbb{L} : \mathbb{K}]$ *et on dit que l'extension est de degré fini si* $[\mathbb{L} : \mathbb{K}] < \infty$*.*

Par exemple, on a $\mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ et $[\mathbb{C} : \mathbb{R}] = 2$ et $[\mathbb{R} : \mathbb{Q}] = \infty$. Le théorème suivant est très utile lorsque l'on travaille avec plusieurs extensions de corps emboîtées.

Théorème (de la base téléscopique)**.** *Soient* $\mathbb{K} \hookrightarrow \mathbb{L} \hookrightarrow \mathbb{M}$ *deux extensions de corps emboîtées. Alors*

$$\Big(\ [\mathbb{M} : \mathbb{K}] < \infty \ \Big) \quad \iff \quad \Big(\ [\mathbb{M} : \mathbb{L}] < \infty \quad et \quad [\mathbb{L} : \mathbb{K}] < \infty \ \Big).$$

Dans ce cas, on a

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}].$$

Preuve : Soient $(e_i)_{1\leq i\leq n}$ une base de $\mathbb{M}$ sur $\mathbb{L}$ et $(f_j)_{1\leq j\leq m}$ une base de $\mathbb{L}$ sur $\mathbb{K}$. On va montrer que $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$ avec $I = [\![1, n]\!]$ et $J = [\![1, m]\!]$. Montrons d'abord qu'elle est libre sur $\mathbb{K}$. Soient $(\lambda_{ij})_{(i,j)\in I\times J} \in \mathbb{K}$ tels que

$$\sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_{ij} e_i f_j = 0.$$

Alors

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} \lambda_{ij} f_j\right) e_i = 0$$

avec $\displaystyle\sum_{j=1}^{m} \lambda_{ij} f_j \in \mathbb{L}$ pour tout $i \in I$. Comme la famille $(e_1, \ldots, e_n)$ est libre sur $\mathbb{L}$, on en déduit

$$\sum_{j=1}^{m} \lambda_{ij} f_j = 0$$

pour tout $i \in I$. On conclut en utilisant la liberté de la famille $(f_1, \ldots, f_m)$ sur $\mathbb{K}$. Elle est aussi génératrice. En effet, soit $x \in \mathbb{M}$. Alors il existe $\lambda_1, \ldots, \lambda_n \in \mathbb{L}$ tels que

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

car $(e_1, \ldots, e_n)$ est une famille génératrice de $\mathbb{M}$ sur $\mathbb{L}$. De même, pour tout $i \in I$ il existe $\lambda_{i1}, \ldots, \lambda_{im} \in \mathbb{K}$ tels que

$$\lambda_i = \sum_{j=1}^{m} \lambda_{ij} f_j$$

ce qui permet de conclure.

□

Si on se donne une partie A de $\mathbb{L}$, on note $\mathbb{K}(A)$ le plus petit sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et A. Si $A = \{\alpha_1, \ldots, \alpha_n\}$, on note $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$ le corps engendré par A et $\mathbb{K}$. Cela correspond à la $\mathbb{K}$-algèbre de $\mathbb{L}$ engendrée par A. Étant donné un corps $\mathbb{K}$, on dispose de l'algèbre $\mathbb{K}[X]$ des polynômes en une indeterminée qui admet le corps $\mathbb{K}$ comme sous-algèbre. On peut l'utiliser pour construire des extensions de $\mathbb{K}$. En effet, pour tout polynôme irréductible $P \in \mathbb{K}[X]$, l'idéal engendré $(P) := P\mathbb{K}[X]$ est maximal donc ${}^{\mathbb{K}[X]}\!/_{(P)}$ est une extension de $\mathbb{K}$. Cela permet de construire des nouveaux corps à partir des corps classiques comme ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$. On a par exemple

$$\mathbb{C} \simeq {}^{\mathbb{R}[X]}\!/_{(X^2+1)}.$$

On peut ainsi contruire des corps de rupture et des corps de décomposition.

Définition. *Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme irréductible. Une extension $\mathbb{L}$ de $\mathbb{K}$ est un corps de rupture de P sur $\mathbb{K}$ si $\mathbb{L} = \mathbb{K}(\alpha)$ avec $P(\alpha) = 0$. Une extension $\mathbb{L}$ de $\mathbb{K}$ est un corps de décomposition de P sur $\mathbb{K}$ si $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ avec $P(\alpha_1) = \ldots = P(\alpha_n) = 0$ et P est un produit de facteurs de degré 1 dans $\mathbb{L}[X]$.*

Le résultat suivant garantie non seulement l'existence des corps de rupture et de décomposition, mais aussi l'unicité à isomorphisme près.

Théorème. *Pour tout corps $\mathbb{K}$ et polynôme irréductible $P \in \mathbb{K}[X]$, il existe un unique à isomorphisme près corps de rupture de P sur $\mathbb{K}$. De plus, pour tout polynôme $P \in \mathbb{K}[X]$, il existe un unique à isomorphisme près corps de décomposition de P sur $\mathbb{K}$.*

Preuve : On commence par l'existence et l'unicité des corps de rupture. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Alors $\mathbb{L} := {}^{\mathbb{K}[X]}/_{(P)}$ est un corps car P est irréductible. $\mathbb{K}$ s'injecte bien dans $\mathbb{L}$ et en notant x l'image de X dans $\mathbb{L}$, on a $\mathbb{L} = \mathbb{K}(x)$ et $P(x) = 0$ ce qui donne l'existence. Pour l'unicité, soit $\mathbb{L} = \mathbb{K}(x)$ un corps de rupture de P sur $\mathbb{K}$. On considère le morphisme de $\mathbb{K}$-algèbre

$$\varphi : \left| \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{L} \\ Q & \mapsto & Q(x) \end{array} \right. .$$

Comme P est le polynôme minimal de x sur $\mathbb{K}$, on a $\mathrm{Ker}(\varphi) = (P)$ ce qui donne

$${}^{\mathbb{K}[X]}/_{(P)} \simeq \mathbb{L}.$$

Pour l'existence d'un corps de décomposition, on raisonne par récurrence sur le degré du polynôme. Si P est de degré 1, alors $\mathbb{K}$ est un corps de décomposition de P sur $\mathbb{K}$. Supposons que P est de degré $n \geq 2$. Si P est un facteur de polynôme de degré 1, alors $\mathbb{K}$ est un corps de décomposition de 0. Sinon, il existe un facteur irreductible P' de P de degré plus grand que 2. Soit $\mathbb{L} = \mathbb{K}(x_1)$ un corps de rupture de P' sur K. Alors il existe $Q \in \mathbb{L}[X]$ tel que

$$P' = (X - x_1)Q$$

avec $\deg(Q) < \deg(P') \leq \deg(P)$ ainsi, par hypothèse de récurrence, il existe un corps $\mathbb{M} = \mathbb{L}(x_2, \ldots, x_n)$ de décomposition de Q sur $\mathbb{L}$. Ainsi, P est scindé sur $\mathbb{M} = \mathbb{K}(x_1, x_2, \ldots, x_n)$ donc $\mathbb{M}$ est un corps de décomposition de P sur $\mathbb{K}$.

□

Exemple. *Le polynôme $P = X^2 - 1$ n'a pas de racine dans $\mathbb{R}$. Le corps $\mathbb{C} = \mathbb{R}(i)$ est un corps de rupture de P mais aussi un corps de rupture puisqu'il s'écrit alors*

$$X^2 - 1 = (X - i)(X + i).$$

Cependant, un corps de rupture n'est pas nécessairement de décomposition. Par exemple, $\mathbb{K} = \mathbb{Q}$ and $Q = X^3 - 2$ admet comme corps de rupture par exemple $\mathbb{Q}(j\sqrt[3]{2})$ sur lequel il n'est pas scindé.

Les morphismes de corps sont les morphismes d'anneaux unitaires, en particulier l'unité est envoyée sur l'unité. Ils sont tous injectifs car les seuls idéaux d'un corps sont $\mathbb{K}$ et $\{0\}$.

Définition. *Soit $\mathbb{K}$ un corps. Alors*

$$\varphi_{\mathbb{K}} : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ n & \mapsto & n \cdot 1 \end{array}$$

est un morphisme d'anneaux. Son noyau est un idéal de $\mathbb{Z}$, on appelle caractéristique de $\mathbb{K}$ l'entier $p = \mathrm{car}(\mathbb{K})$ tel que $\mathrm{Ker}(\varphi_{\mathbb{K}}) = p\mathbb{Z}$. La caractéristique est un nombre premier si elle est non nulle.

Le morphisme donne aussi un sous-corps de $\mathbb{K}$. Si $\mathbb{K}$ est de caractéristique nulle, alors le morphisme est injectif et $\mathbb{K}$ contient un sous-corps isomorphe à $\mathbb{Q}$, il est en particulier infini. Si $\mathbb{K}$ est un corps fini, alors il admet un sous-corps k isomorphe à ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ avec $p = \mathrm{car}(\mathbb{K})$. $\mathbb{K}$ étant une extension fini de k, il a une structure de ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$-espace vectoriel de dimension fini donc il existe $r \in \mathbb{N}^*$ tel que le cardinal de $\mathbb{K}$ est p^r. Le théorème suivant est une réciproque.

Théorème. *Soient p un nombre premier est $r \in \mathbb{N}^*$. Alors il existe un unique à isomorphisme près corps fini de cardinal $q = p^r$. On le note souvent $\mathbb{F}_q$.*

Preuve : Soit $\mathbb{K}$ un corps de cardinal q. Pour tout $x \in \mathbb{K}^\times$, on a $x^{q-1} = 1$ donc tout élément de $\mathbb{K}$ est racine du polynôme $X^q - X$. D'après la remarque précédente, la caractéristique d'un corps de cardinal $q = p^r$ est p et il admet comme sous-corps $\mathbb{Z}/p\mathbb{Z}$. Ainsi, $\mathbb{K}$ est un corps de décomposition de $X^q - X \in \mathbb{Z}/p\mathbb{Z}[X]$ ce qui conclut l'unicité à isomorphisme près. Pour l'existence, on considère $\mathbb{K}$ le corps de décomposition de

$$P := X^q - X \in \mathbb{Z}/p\mathbb{Z}[X]$$

sur $\mathbb{Z}/p\mathbb{Z}$ et $k \subset \mathbb{K}$ l'ensemble des racines de P dans $\mathbb{K}$. Alors k est un corps car

$$\big(x^q = x \quad \text{et} \quad y^q = y\big) \quad \Longrightarrow \quad (x+y)^q = x^q + y^q = x + y.$$

De plus,

$$P' = qX^{q-1} - 1 = -1$$

car $q = p^r$ donc P est à racines simples et ainsi $|k| = q$.

□

Dans le cas où $r = 1$, on a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Dans le cas où $r > 1$, on sait que c'est une extension de corps de $\mathbb{Z}/p\mathbb{Z}$ et on a vu que l'on pouvait construire des extensions d'un corps $\mathbb{K}$ à l'aide de polynômes irréductibles sur $\mathbb{K}[X]$. $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$. En particulier, le groupe $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ étant de cardinal $q-1$, on a $x^q = x$ pour tout $x \in \mathbb{F}_q$.

Théorème. *On a*

$$|\mathcal{M}_n(\mathbb{F}_q)| = q^{n^2} \quad \textit{et} \quad |GL_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i).$$

Preuve : Le calcul pour $\mathcal{M}_n(\mathbb{F}_q)$ est immédiat. Pour $GL_n(\mathbb{F}_q)$, il suffit de compter les bases de $(\mathbb{F}_q)^n$ car une matrice est inversible si et seulement si elle envoie une base sur une base. Pour le premier vecteur, il suffit qu'il soit non nul donc il y a $q^n - 1$ choix. Ensuite, il faut retirer la droite engendrée par ce vecteur, il y a donc $q^n - q$ choix. Il faut alors retirer un plan et ainsi de suite, ce qui donne

$$|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1})$$

□

Théorème. *Soient p premier, $r \in \mathbb{N}^*$ et $\mathcal{D}_n(q)$ l'ensemble des matrices diagonalisables de $\mathcal{M}_n(q) := \mathcal{M}_n(\mathbb{F}_q)$. Alors, en notant $GL_n(q) := GL_n(\mathbb{F}_q)$ et avec la convention $|GL_0(q)| = 1$, on a*

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1,\dots,m_q \in \mathbb{N} \\ m_1+\dots+m_q = n}} \frac{|GL_n(q)|}{\prod_{i=1}^{q} |GL_{m_i}(q)|}.$$

Preuve : On va utiliser l'action par conjugaison de $GL_n(q)$ sur $\mathcal{D}_n(q)$. On commence par décrire les orbites. Soit $M \in \mathcal{D}_n(q)$. On a

$$\mathrm{Orb}(M) = \{PMP^{-1} \ ; \ P \in GL_n(q) \ \}.$$

M est diagonalisable donc il existe $m = (m_1, \dots, m_q) \in \mathbb{N}^q$ tel que $D_m \in \mathrm{Orb}(M)$ avec

$$D_m = \begin{pmatrix} \alpha_1 I_{m_1} & & 0 \\ & \ddots & \\ 0 & & \alpha_q I_{m_q} \end{pmatrix}$$

en notant $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$. De plus, si $D_{m'} \in \mathrm{Orb}(D_m)$, alors

$$\chi_{D_{m'}} = \chi_{D_m} = \prod_{i=1}^{q} (X - \alpha_i)^{m_i},$$

donc $m = m'$. On a donc montré que

$$\mathcal{D}_n(q) = \bigsqcup_{m_1+\dots+m_q=n} \mathrm{Orb}(D_m).$$

Par la relation orbite-stabilisateur, on a

$$\Big|\mathrm{Orb}(D_m)\Big| = \frac{|GL_n(q)|}{|\mathrm{Stab}(D_m)|}$$

et il suffit de trouver le cardinal des stabilisateurs. Soit $P \in \mathrm{Stab}(D_m)$, alors $PD_m = D_m P$. Pour $X \in E_\lambda(D_m)$, on a $D_m PX = PD_m X = \lambda PX$ et donc $PX \in E_\lambda(D_m)$. Or $\mathbb{K}^n = \bigoplus_\lambda E_\lambda(D_m)$ donc

$$P = \begin{pmatrix} P_1 & & 0 \\ & \ddots & \\ 0 & & P_q \end{pmatrix}$$

avec $P_i \in GL_{m_i}(q)$. Réciproquement, P de cette forme vérifie $PD_m = D_m P$ donc

$$\Big|\mathrm{Stab}(D_m)\Big| = \prod_{i=1}^{q} |GL_{m_i}(q)|$$

et on peut alors conclure

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1,\dots,m_q \in \mathbb{N} \\ m_1+\dots+m_q=n}} \frac{|GL_n(q)|}{\prod_{i=1}^{q} |GL_{m_i}(q)|}.$$

□

On introduit la fonction de Möbius μ définie par

$$\mu : \begin{array}{ccc} \mathbb{N} & \to & \{-1, 0, 1\} \\ n = p_1^{\alpha_1} \dots p_r^{\alpha_r} & \mapsto & \left| \begin{array}{cc} 1 & \text{si } r \text{ est pair et } \forall i, \alpha_i = 1 \\ -1 & \text{si } r \text{ est impair et } \forall i, \alpha_i = 1 \\ 0 & \text{sinon} \end{array} \right. \end{array}$$

où $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n.

Lemme (Formule d'inversion de Möbius)**.** *Soient $f, g : \mathbb{N}^* \to \mathbb{R}$ telles que*

$$\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d).$$

Alors

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d),$$

avec μ la fonction de Möbius.

Preuve : On note $S_n := \sum_{d|n} \mu(d)$. Pour $n = 1$, on a $S_1 = 1$ et pour $n \geq 2$, on considère P l'ensemble des diviseurs premiers de n et on a

$$S_n = \sum_{D \subset P} \mu\left(\prod_{d \in D} d\right) = \sum_{D \subset P} (-1)^{|D|} = \sum_{i=0}^{|P|} \binom{|P|}{i} (-1)^i = (1-1)^{|P|} = 0.$$

On a alors

$$\begin{aligned}\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d' | \frac{n}{d}} g(d') \\ &= \sum_{dd'|n} \mu(d) g(d') \\ &= \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(d) \\ &= \sum_{d'|n} g(d') S_{\frac{n}{d'}} = g(n).\end{aligned}$$

□

Théorème. *Le nombre de polynômes irréductible de degré n dans $\mathbb{F}_q[X]$ est*

$$\frac{q-1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Preuve : On commence par montrer que

$$P := X^{q^n} - X = \prod_{d|n} \prod_{D \in I_q^d} D,$$

où I_q^n est l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[X]$ de degré n. Soit D un diviseur irréductible unitaire de P de degré d. Soit $\alpha \in \mathbb{F}_{q^n}$ une racine de D, car D divisant P et P étant scindé sur $\mathbb{F}_{q^n}$, les racines de D sont dans $\mathbb{F}_{q^n}$. Alors D est irréductible sur $\mathbb{F}_q$ et $D(\alpha) = 0$ donc c'est le polynôme minimal de α sur $\mathbb{F}_q$. D'après le théorème de la base téléscopique, on a

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)] \cdot [\mathbb{F}_q(\alpha) : \mathbb{F}_q],$$

donc $d = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ divise $n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$. Réciproquement, soient d un diviseur de n et D un polynôme irréductible unitaire de degré d. Soit $\mathbb{F}_q(\alpha)$ le corps de rupture de D. Alors

$$\mathbb{F}_q(\alpha) \simeq \mathbb{F}_{q^d} \hookrightarrow \mathbb{F}_{q^n},$$

où l'isomorphisme découle de l'unicité des corps finis et l'inclusion de $d|n$. Ainsi, α est aussi une racine de P. Or D est irréductible sur $\mathbb{F}_q$ donc il est à racines simples dans $\mathbb{F}_{q^n}$ et donc D divise P. De plus, P est scindé à racines simples sur $\mathbb{F}_{q^n}$ car $P' = -1$ dans $\mathbb{F}_{q^n}[X]$. Donc chaque diviseur irréductible de P est de multiplicité 1 et donc

$$P = \prod_{d|n} \prod_{D \in I_q^d} D.$$

On a alors en passant au degré

$$q^n = \sum_{d|n} d|I_q^n|.$$

Grâce à la formule d'inversion de Möbius, on en déduit

$$n|I_q^n| = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d,$$

et la formule finale en multipliant par $q-1$ car on a compté seulement les polynômes irréductibles unitaires.

□

Remarque. *On utilise le fait qu'un polynôme irréductible dans $\mathbb{F}_q[X]$ est à racines simples dans un corps où il est scindé. Ici, D est scindé sur $\mathbb{F}_{q^n}$ et irréductible sur $\mathbb{F}_q$. En voici une preuve.*

Supposons par l'absurde qu'il existe $\alpha \in \mathbb{F}_{q^n}$ une racine double de D. Alors D est irréductible sur $\mathbb{F}_q$ et $D(\alpha) = 0$ donc D est le polynôme minimal de α sur $\mathbb{F}_q$. Or $D'(\alpha) = 0$ et $deg(D') < deg(D)$ donc $D' = 0$. Ainsi, on a $D = R_0(X^p)$ avec $R \in \mathbb{F}_q[X]$. Avec le morphisme de Frobenius qui est bijectif sur le corps fini $\mathbb{F}_q$, on a $D = R_1^p$ avec $R_1 \in \mathbb{F}_q[X]$ ce qui est absurde car D est irréductible dans $\mathbb{F}_q[X]$. En caractéristique nulle, on aurait pu conclure car $D' = 0$ implique que D est constant.

3 Algèbre des polynômes d'endomorphisme et réduction

Comme on l'a vu avec le morphisme d'évaluation d'un endomorphisme $u \in \mathscr{L}(E)$, la structure de l'algèbre $\mathbb{K}[u]$ est entièrement déterminée par la donnée du polynôme minimal et on a

$$\mathbb{K}[u] \sim {}^{\mathbb{K}[X]}\!/_{(\Pi_u)} \sim {}^{\mathbb{K}[X]}\!/_{(P_1^{\alpha_1})} \times \ldots \times {}^{\mathbb{K}[X]}\!/_{(P_r^{\alpha_r})}$$

où $\Pi_u = P_1^{\alpha_1} \ldots P_r^{\alpha_r}$ est la décomposition en facteurs irréductibles de Π_u.

Définition. *Soient E un espace vectoriel et $u \in \mathscr{L}(E)$. Un sous-espace vectoriel F de E est stable par u si*

$$\forall x \in F, u(x) \in F.$$

La restriction de u à F est alors une application linéaire, on l'appelle l'induite de u sur F et on la note $u|_F$.

On peut déduire des propriétés de $u|_F$ à partir de celle de u, par exemple la proposition suivante.

Proposition. *Si F est stable par u, alors $\Pi_{u_F} | \Pi_u$. Si $E = F_1 \oplus \ldots \oplus F_r$ décomposition en sous-espaces stables, alors π_u est le ppcm de $\Pi_{u_{F_1}}, \ldots, \Pi_{u_{F_r}}$.*

Par exemple de $\mathrm{Ker}(P(u))$ et $\mathrm{Im}(P(u))$ stables par u. Réduire l'endomorphisme revient à trouver des sous-espaces stables intéréssants. Une décomposition de l'espace en sous-espaces stables donnent une représentation matricielle par bloc de l'endomorphisme. Un outil pratique pour en construire est donné par le théorème suivant.

Théorème (Lemme des noyaux)**.** *Soient E un $\mathbb{K}$-espace vectoriel et $u \in \mathscr{L}(E)$. Si $P_1, \ldots, P_n \in \mathbb{K}[X]$ sont premiers entre eux deux à deux, alors*

$$\mathrm{Ker}\big((P_1 \ldots P_n)(u)\big) = \bigoplus_{i=1}^{n} \mathrm{Ker}\big(P_i(u)\big).$$

En particulier, un polynôme annulateur donne une décomposition de l'espace. Dans le cas de Π_u, la décomposition obtenue est

$$E = \oplus_{i=1}^{r} \mathrm{Ker}\Big(P_i^{\alpha_i}(u)\Big) = \oplus_{i=1}^{r} F_i$$

et dans ce cas, on a en plus $\Pi_{u_{F_i}} = P_i^{\alpha_i}$. On retrouve par exemple le résultat suivant.

Théorème. *Soient E un $\mathbb{K}$-espace vectoriel et $u \in \mathscr{L}(E)$. Si P admet un polynôme annulateur scindé à racines simples, alors u est diagonalisable. De plus, Π_u est scindé à racines simples sur $\mathbb{K}$ si et seulement si u est diagonalisable.*

Le premier critère est nécéssaire mais pas suffisant. Il est très utile en pratique comme par exemple dans la théorie des représentation pour un groupe abélien fini. En effet, si on se donne $\rho : G \to GL_n(\mathbb{C})$ une représentation d'un tel groupe, on a

$$\chi(g)^{|G|} = \chi\left(g^{|G|}\right) = \mathrm{Id}$$

donc $X^{|G|} - 1$ est un polynôme annulateur de $\chi(g)$ pour tout $g \in G$. Ce dernier étant scindé à racines simples, on en déduit que $\chi(g)$ est diagonalisable. Dans le cas particulier des corps finis, on a la proposition suivante.

Proposition. *Soit $M \in \mathcal{M}_n(\mathbb{F}_q)$. Alors M est diagonalisable si et seulement si $X^q - X$ est un polynôme annulateur de M.*

Preuve : La condition est suffisante car $X^q - X$ est scindé à racines simples sur $\mathbb{F}_q$. Si on suppose M diagonalisable, alors il existe $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q$ et $P \in GL_n(\mathbb{F}_q)$ tels que

$$M = PDP^{-1}$$

avec $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. On a donc

$$M^q = PD^qP^{-1} = PDP^{-1} = M$$

ce qui permet de conclure, où la dernière inégalité vient du morphisme de Frobenius qui est l'identité dans un corps fini.

□

La proposition suivante fait le lien entre le polynôme minimal d'un endormorphisme et l'ensemble des polynômes annulateurs d'un endormorphisme en un vecteur donné. Il est en particulier très utile pour démontrer le théorème de Frobenius sur les invariants de similitude.

Proposition. *Soit $u \in \mathscr{L}(E)$ avec E un espace vectoriel de dimension finie. On note Π_u le polynôme minimal de u et Π_u^x le polynôme unitaire qui engendre l'idéal*

$$\{P \in \mathbb{K}[X] \ ; \ P(u)(x) = 0\}.$$

Alors il existe $x \in E$ tel que $\Pi_u^x = \Pi_u$.

Preuve : On commence par traiter le cas où $\Pi_u = P^\alpha$ avec P un polynôme irréductible. On a

$$\forall x \in E, \exists n \in [\![0, \alpha]\!], \ P^n(u)(x) = 0,$$

et on cherche $x \in E$ tel que $P^n(u)(x) \neq 0$ pour $n < \alpha$. Supposons par l'absurde que pour tout $x \in E$, il existe $n < \alpha$ tel que $P^n(u)(x) = 0$. Alors $P^{\alpha-1}(u) = 0$, c'est-à-dire Π_u divise $P^{\alpha-1}$ ce qui est absurde. Dans le cas général, on considère

$$\Pi_u = \prod_{i=1}^{r} P_i^{\alpha_i}$$

la décomposition en facteurs irréductibles de Π_u dans $\mathbb{K}[X]$. D'après le lemme des noyaux, on a

$$E = \bigoplus_{i=1}^{r} \mathrm{Ker}\Big(P_i^{\alpha_i}(u)\Big).$$

On note $E_i := \mathrm{Ker}\Big(P_i^{\alpha_i}(u)\Big)$. On sait par ce qui précède que pour tout $i \in [\![1, r]\!]$, il existe $x_i \in E_i$ tel que $\Pi_{u_{E_i}}^{x_i} = \Pi_{u_{E_i}}$. On pose $x = x_1 + \ldots + x_r$ et on montre que

$$\Pi_u^x = \Pi_u.$$

Comme Π_u^x divise Π_u, il suffit de montrer que Π_u divise Π_u^x, c'est-à-dire que Π_u^x est un polynôme annulateur de u. On a

$$0 = \Pi_u^x(u)(x) = \sum_{i=1}^{r} \Pi_u^x(u)(x_i).$$

Comme les E_i sont en somme directe et stable par u, on en déduit que $\Pi_u^x(u)(x_i) = 0$ pour tout i. Donc $\Pi_{u_{E_i}}^{x_i} = \Pi_{u_{E_i}}$ divise Π_u^x et ainsi $\Pi_u^x(u)$ est nul sur chaque E_i et donc sur E, d'où le résultat.

□

4 Réduction de Jordan

Si on cherche à étudier un endomorphisme u sur un espace vetoriel E de dimension finie, il est pratique d'avoir une base de E dans lequel il est simple à utiliser et étudier, l'idéal étant d'avoir une base dans laquelle la matrice de u est diagonale. Il est alors naturel d'étudier les vecteurs et valeurs propres associés à u et d'utiliser ces outils pour réduire u, c'est-à-dire trouver une base de telle sorte que la matrice de u y soit aussi simple que possible. Ces problèmes peuvent aussi bien apparaître dans des problèmes d'analyse, de probabilités et d'algèbres que ce soit par exemple avec les équations différentielles, l'étude de vecteurs aléatoires ou la théorie des représentation. On se fixe un corps $\mathbb{K}$ et un $\mathbb{K}$-espace vectoriel E de dimension finie n.

Définition. *Soit $u \in \mathscr{L}(E)$. On appelle vecteur propre de u tout vecteur non nul $x \in E$ tel que $u(x)$ est proportionnel à x. On dit que $\lambda \in \mathbb{K}$ est une valeur propre de u s'il existe un vecteur non nul $x \in E$ tel que*

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

Dans ce cas, x est un vecteur propre de u et on dit que x est un vecteur propre associé à la valeur propre λ.

La relation d'un vecteur propre signifie que x est annulé par l'endormorphisme $u - \lambda \cdot \mathrm{Id}$ donc λ est une valeur propre de u si et seulement si

$$\mathrm{Ker}(u - \lambda \cdot \mathrm{Id}) \neq \{0\}.$$

Avec le déterminant, on a alors λ valeur propre de u si et seulement si $\det(u - \lambda \cdot \mathrm{Id}) = 0$. Pour chaque base de E qu'on se fixe, on obtient une matrice $A \in \mathcal{M}_n(\mathbb{K})$ et λ doit être solution de l'équation algébrique à coefficients dans $\mathbb{K}$

$$\det(A - \lambda \cdot I_n) = 0.$$

En particulier, cette relation ne change pas si on remplace A par PAP^{-1}. On a alors un polynôme qui donne exactement la relation algèbrique qui caractérise les valeurs propres d'un endomorphisme.

Définition. *Étant donné un endomorphisme $u \in \mathscr{L}(E)$, on appelle polynôme caractéristique de u noté χ_u le polynôme définit par*

$$\chi_u(X) := \det(u - X \cdot \mathrm{Id}) \in \mathbb{K}[X].$$

Cela permet par exemple de répondre à la question d'existence de valeurs propres comme question d'existence de solution à une équation polynomiale. On voit alors que le corps de base est particulièrement important, en particulier il existe toujours des valeurs propres lorsque le corps est algèbriquement clos. En particulier, étant donné que le degré de χ_u est la dimension de E, le nombre de valeur propre est inférieur à la dimension. On dit qu'un endomorphisme u a toutes ses valeurs propres dans $\mathbb{K}$ si toutes les racines de χ_u sont dans $\mathbb{K}$, ie χ sindé dans $\mathbb{K}[X]$. On obtient alors une condition nécéssaire et suffisante de trigonalisation ainsi qu'une condition nécéssaire de diagonalisation.

Proposition. *Un endomorphisme u est trigonalisable si et seulement si toutes ses valeurs propres sont dans $\mathbb{K}$. Si elles sont toutes distinctes, alors u est diagonalisable.*

Cela est évidemment nécéssaire, on peut montrer par récurrence que c'est suffisant. En particulier, tout endomorphisme est trigonalisable dans un corps algébriquement clos. Cependant, ce résultat peut être très utile même sur un corps quelconque comme on va le voir avec le cas des endomorphsimes nilpotents, 0 étant toujours dans le corps $\mathbb{K}$. Maintenant, peut-on trouver une condition nécéssaire et suffisante pratique pour savoir si un endomorphisme est diagonalisable ? Cela revient à étudier l'existence d'une base de E de vecteurs propres associés à u. Le critère suffisant précédent n'est évidemment pas nécéssaire en regardant par exemple l'endomorphisme identité. Pour cela, on introduit la notion de sous-espace propre associé à u ainsi que les multiplicités algébriques et géométriques de u.

Définition. *Soient $u \in \mathscr{L}(E)$ et λ une valeur propre de u. On appelle sous-espace propre de E associé à λ l'espace des vecteurs propres de u associés à λ*

$$E_u(\lambda) := \mathrm{Ker}(u - \lambda \cdot \mathrm{Id}).$$

On appelle multiplicité géométrique de λ la dimension de $E_u(\lambda)$ et multiplicité algébrique de λ la multiplicité $m_u(\lambda)$ de λ en tant que valeur propre de χ_u.

On appelle multiplicité géométrique $\dim\big(E_u(\lambda)\big)$ car c'est la dimension de l'espace vectoriel des vecteurs propres associés à λ alors que $m_u(\lambda)$ découle de la caractérisation en terme de relations algébriques des valeurs propres. On a par définition que

$$\sum_{\lambda \in \mathrm{Sp}(u)} m_\lambda(u) = n$$

alors qu'en général on a seulement

$$\sum_{\lambda \in \mathrm{Sp}(u)} \dim\big(E_u(\lambda)\big) \leq n.$$

En effet, on peut montrer que les sous-espaces propres sont en sommes directes. On se donne $x_i \in E_u(\lambda_i)$ pour $1 \leq i \leq r$ avec $\lambda_1, \ldots, \lambda_r$ les valeurs propres de u. En notant $F = \mathrm{Vect}(x_1, \ldots, x_r)$, on a F stable par u et l'endormorphisme induit $u|_F$ possède r valeurs propres distinctes. Cela implique

$$r \leq \dim(f) \leq r$$

donc la famille $(x_1, \ldots, x_r)$ est libre donc

$$\bigoplus_{\lambda \in \mathrm{Sp}(u)} E_u(\lambda) \subset E.$$

Cela permet d'énoncer un critère nécéssaire et suffisant de diagonalisabilité avec la proposition suivante.

Proposition. *Un endomorphisme u est diagonalisable si et seulement pour tout valeur propre λ, on a $\dim\big(E_u(\lambda)\big) = m_u(\lambda)$.*

Preuve : La condition est nécéssaire car les sous-espaces propres sont en somme directe. Supposons u diagonalisable et notons $\lambda_1, \ldots, \lambda_r$ ses différentes valeurs propres. Alors il existe une base de E dans laquelle la matrice de u est diagonale par bloc avec les $\lambda_i I_{m_i}$ sur sa diagonale avec $m_i = m_u(\lambda_i)$. Alors le polynôme caractéristique est

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

ce qui permet de conclure.

□

Le lemme des noyaux montre une fois de plus l'importance des polynômes annulateurs car ils donnent des décompositions de l'espace et on sait que les valeurs propres de u sont incluses dans les racines de tous polynômes annulateur. Il est donc intéréssant d'en trouver et le théorème de Cayley-Hamilton nous en donne un. Il est facile de voir qu'il est valable dans le cas où u est diagonalisable mais il reste vrai pour tout endomorphisme.

Théorème (de Cayley-Hamilton)**.** *Le polynôme caractéristique χ_u est un polynôme annulateur de u, c'est-à-dire*

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

Si le polynôme caractéristique est scindé, on peut l'écrire sous la forme

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

Dans ce cas, le lemme des noyaux donne la décomposition de E en sous-espaces stables

$$E = \bigoplus_{i=1}^{r} \operatorname{Ker}\Big((u - \lambda_i \cdot \mathrm{Id})^{m_i}\Big).$$

Sur chaque sous-espace stable, on est ramené à l'étude de l'endomorphisme nilpotent $u - \lambda_i \cdot \mathrm{Id}$. On peut montrer qu'étant donné un endormophisme nilpotent $n \in \mathscr{L}(E)$, il existe une base de E telle que la matrice de n dans cette base soit nulle avec eventuellement des 1 sur la surdiagonale. Cela donne la décomposition de Jordan énoncé dans le théorème suivant.

Théorème. *Soit $u \in \mathscr{L}(E)$. Alors toutes les valeurs propres de u sont dans $\mathbb{K}$ si et seulement s'il existe une base de E dans laquelle la matrice de u est diagonale par bloc avec sur la diagonale des blocs de Jordan*

$$J_\lambda := \begin{pmatrix} \lambda & 1 & & (0) \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & (0) & & \lambda \end{pmatrix}$$

où $\lambda \in \mathrm{Sp}(u)$.

Il existe de nombreuses décompositions pour un endomorphisme comme par exemple la décomposition de Dunford ou celle de Frobenius avec différents avantages.