Chapitre 9

Réduction de matrices et d'endomorphismes 2

Sommaire

Dans ce chapitre, la lettre $\mathbb{K}$ désignera un sous-corps de $\mathbb{C}$. La lettre E désigne un espace vectoriel sur $\mathbb{K}$.

9.1 Structure d'algèbre

Définition 1

Soit $\mathcal{A}$ un ensemble non vide muni de deux lois de composition interne notées $+$ et $\times$ et d'une loi de composition externe noté $\cdot$

On dit que $(\mathcal{A}, +, \cdot, \times)$ est une algèbre sur $\mathbb{K}$ si, et seulement si,

- $(\mathcal{A}, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel
- $(\mathcal{A}, +, \times)$ est un anneau
- $\forall x, y \in \mathcal{A}, \quad \forall \lambda \in \mathbb{K}, \quad \lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y)$.

Définition 2

Soit $(\mathcal{A},+,\cdot,\times)$ une algèbre sur $\mathbb{K}$.

1. La dimension de l'algèbre $(\mathcal{A},+,\cdot,\times)$ est la dimension de l'espace vectoriel $(\mathcal{A},+,\cdot)$.
2. On dit que l'algèbre $(\mathcal{A},+,\cdot,\times)$ est commutative si, et seulement si, l'anneau $(\mathcal{A},+,\times)$ est commutative.
3. On dit que l'algèbre $(\mathcal{A},+,\cdot,\times)$ est intègre si, et seulement si, l'anneau $(\mathcal{A},+,\times)$ est intègre.

Exemples : Soit E un espace vectoriel sur $\mathbb{K}$. Soit $n \in \mathbb{N}^*$. Soit X un ensemble contenant au moins deux éléments :

1. $(\mathbb{C},+,\times,\times)$ est une algèbre sur $\mathbb{R}$.
2. $(\mathbb{R},+,\times,\times)$ est une algèbre sur $\mathbb{Q}$.
3. $(\mathbb{K}[X],+,\cdot,\times)$ est une algèbre sur $\mathbb{K}$.
4. $(M_n(\mathbb{K}),+,\cdot,\times)$ est une algèbre sur $\mathbb{K}$ non commutative si $n \in [\![2,+\infty[\![$.
5. $(L(E),+,\cdot,\circ)$ est une algèbre sur $\mathbb{K}$ non commutative si $\dim(E) \geqslant 2$.
6. L'ensemble des suites à valeurs dans $\mathbb{K}$: $(\mathbb{K}^{\mathbb{N}},+,\cdot,\times)$ est une algèbre sur $\mathbb{K}$ non intègre.
7. $(\mathbb{K}^X,+,\cdot,\times)$ est une algèbre sur $\mathbb{K}$ non intègre.

Définition 3

Soit $(\mathcal{A},+,\cdot,\times)$ une algèbre sur $\mathbb{K}$ d'élément neutre pour la multiplication $1_{\mathcal{A}}$. Soit $\mathcal{B}$ un sous-ensemble de $\mathcal{A}$. On dit que $(\mathcal{B},+,\cdot,\times)$ est une sous-algèbre de $(\mathcal{A},+,\cdot,\times)$ si, et seulement si,

1. $1_A \in \mathcal{B}$.
2. $\forall x,y \in \mathcal{B}, \quad \forall \lambda,\mu \in \mathbb{K}, \quad \lambda x + \mu y \in \mathcal{B}$.
3. $\forall x,y \in \mathcal{B}, \quad x \times y \in \mathcal{B}$.

L'ensemble $(\mathcal{B},+,\cdot,\times)$ est elle-même une algèbre sur $\mathbb{K}$.

Exercice A1 : Montrer que l'ensemble des matrices triangulaires supérieures $TS_n(\mathbb{K})$ est une sous-algèbre de $(M_n(\mathbb{K}),+,\cdot,\times)$.

Exemples : On montre de même que l'ensemble des matrices triangulaires inférieures $TI_n(\mathbb{K})$ et l'ensemble des matrices diagonales $D_n(\mathbb{K})$ sont des sous-algèbres de $(M_n(\mathbb{K}),+,\cdot,\times)$.

Définition 4 (Morphisme d'algèbres)

Soit $(\mathcal{A},+,\cdot,\times)$, $(\mathcal{A}',\oplus,\cdot,\otimes)$. On dit qu'une application $f : \mathcal{A} \to \mathcal{A}'$ est un morphisme d'algèbres si, et seulement si,

1. $f(1_{\mathcal{A}}) = 1_{\mathcal{A}'}$
2. $\forall x,y \in \mathcal{A}, \quad \forall \lambda,\mu \in \mathbb{K}, \quad f(\lambda \cdot x + \mu \cdot y) = \lambda \cdot f(x) \oplus \mu \cdot f(y)$.
3. $\forall x,y \in \mathcal{A}, \quad f(x \times y) = f(x) \otimes f(y)$

Exemple : L'application de conjugaison est

$$f : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \overline{z} \end{array} \right.$$

morphisme d'algèbres de $(\mathbb{C},+,\times,\times)$ dans lui-même.

Exercice A2 : Soit $(\mathcal{A},+,\cdot,\times)$, $(\mathcal{A}',\oplus,\cdot,\otimes)$. soit $f : \mathcal{A} \to \mathcal{A}'$ un morphisme d'algèbres.

1. Montrer que l'image directe par f de toute sous-algèbre de $(\mathcal{A},+,\cdot,\times)$ est une sous-algèbre de $(\mathcal{A}',\oplus,\cdot,\otimes)$.
2. Montrer que l'image réciproque par f de toute sous-algèbre de $(\mathcal{A}',\oplus,\cdot,\otimes)$ est une sous-algèbre de $(\mathcal{A},+,\cdot,\times)$.
3. Montrer que $\mathsf{Im}(f)$ est une sous-algèbre de $(\mathcal{A}',\oplus,\cdot,\otimes)$.
4. Justifier que $\mathsf{Ker}(f)$ est un sous-espace vectoriel de $(\mathcal{A},+,\cdot)$ et un idéal de l'anneau $(\mathcal{A},+,\times)$. L'ensemble $\mathsf{Ker}(f)$ est-il une sous-algèbre de $(\mathcal{A},+,\cdot,\times)$?

9.2 Compléments sur les anneaux

9.2.1 Idéaux d'un anneau commutatif

Définition 5

Soit $(A,+,\times)$ un anneau commutatif. Soit I un sous-ensemble de A. On dit que I est un idéal de A si, et seulement si,

1. $0_A \in I$.
2. $\forall x,y \in I, \quad x+y \in I$.
3. $\forall a \in A, \quad \forall x \in I, \quad ax \in I$.

Remarque : Un idéal est en particulier un sous-groupe de $(A,+)$. En effet utilisant la propriété 3) à $a=-1$, on obtient que pour tout $x \in I$, $-x \in I$.

Exemples :

1. Soit $(A,+,\times)$ un anneau commutatif. Les ensembles $\{0_A\}$ et A sont des idéaux de A.
2. Soit $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z}$ est un idéal de $(\mathbb{Z},+,\times)$. Nous verrons un peu plus loin que tout idéal de $(\mathbb{Z},+,\times)$ est nécessairement de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.
3. Soit $P \in \mathbb{K}[X]$, l'ensemble $P\mathbb{K}[X] = \{PQ \mid Q \in \mathbb{K}[X]\}$ sont des idéaux de $(\mathbb{K}[X],+,\times)$.

Exercice A3 : Soit $A = \mathcal{F}(X,\mathbf{R})$. Soit $x \in X$. On pose $I_x = \{f \in A, f(x) = 0\}$. Montrer que I_x est un idéal.

Exercice E4 : Soit A un anneau commutatif et I un idéal de A. On appelle radical de I et on note $\sqrt{I}$ l'ensemble

$$\sqrt{I} = \{x \in A, \exists n \in \mathbf{N}, x^n \in I\}$$

Montrer que $\sqrt{I}$ est un idéal

Exercice A5 : Soit $(A,+,\times)$ un anneau commutatif. Soit I un idéal de A.

1. Montrer que si $1_A \in I$ alors $I = A$.
2. Montrer que si $\mathcal{U} \cap I \neq \varnothing$ alors $I = A$.

Exercice E6 : Quels sont les idéaux d'un corps $\mathbb{K}$?

Proposition 6

Soit A un anneau commutatif et $a \in A$. On note aA défini par

$$aA = \{ab \mid b \in A\}$$

1. L'ensemble aA est un idéal de A
2. L'ensemble aA estle plus petit idéal contenant a.

L'idéal aA s'appelle, idéal engendré par a et se note aA ou (a).

Preuve :

1. Remarquons que $aA \neq \emptyset$ car $0 \in A$.
Soit $(x, x') \in (aA)^2$, il existe $(b, b') \in A^2$ tels que
$$x = ab \text{ et } x' = ab'$$
Ainsi
$$x - x' = ab - ab' = a\left(b - b'\right) \in aA$$
On en déduit que aA est bien un sous-groupe de $(A, +)$.

Soit $x \in aA$ et $y \in A$. Il existe $b \in A$ tel que $x = ab$. Ainsi, $xy = (ab)y = a(by) \in aA$.
Par conséquent, aA est un idéal de A.
2. Soit I un idéal de A contenant a. Par définition d'un idéal, pour tout $b \in A, ab \in I$.
Cela montre que $aA \subset I$.
Ceci montre que aA est bien le plus petit idéal de A contenant a.

□

Définition 7

Soit A un anneau commutatif. Soit I un idéal de A. Il est dit principal si, et seulement si,il existe $x \in$ A tel que $I = (x)$.

Théorème 8

Les idéaux de $(\mathbb{Z}, +, \times)$ sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Preuve : Tout idéal I de $(\mathbb{Z}, +, \times)$ est un sous-groupe de $(\mathbb{Z}, +)$. Il existe $n \in \mathbb{N}$ tel que : $I = n\mathbb{Z}$.
Réciproquement, les ensembles de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$ sont bien des idéaux de $(\mathbb{Z}, +, \times)$. □

Exercice E7 : On note
$$\mathbb{D} = \left\{\frac{p}{10^n} \mid p \in \mathbb{Z}, n \in \mathbb{N}\right\}$$
l'ensemble des nombres décimaux.

1. Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.
2. Montrer que les idéaux de $\mathbb{D}$ sont principaux (c'est-à-dire de la forme $a\mathbb{D}$ avec $a \in \mathbb{D}$).

9.2.2 Arithmétique dans un anneau commutatif intègre

On peut définir la notion de divisibilité dans un anneau commutatif intègre comme nous l'avons déjà fait dans $(\mathbb{Z}, +, \times)$ et $(\mathbb{K}[X], +, \times)$.

Définition 9

Soit $(A, +, \times)$ un anneau commutatif intègre. Soit $a, b \in A$.
On dit que b divise a si, et seulement si, il existe $c \in A$ tel que $a = bc$.
Terminologie : b **divise** a
b est un **diviseur** de a
a est **divisible** par b
a est un **multiple** de b.

Exemples : Soit $(A, +, \times)$ un anneau commutatif intègre.

1. L'élément neutre 1_A pour la multiplication divise tout élément de A.
2. Tout élément a de A divise l'élément nul 0_A.

3. On a l'implication :
$$\forall a \in A, \quad (0_A | a \implies a = 0_A).$$

Définition 10

Soit $(A, +, \times)$ un anneau commutatif intègre. Soit $a \in A$. L'ensemble des multiples de a noté aA
$$aA = \{a\alpha \mid \alpha \in A\}$$
c'est un idéal de $(A, +, \times)$. L'ensemble aA est l'idéal engendré par a.

Proposition 11

Soit $(A, +, \times)$ un anneau commutatif intègre. Soit $a, b \in A$. Les assertions suivantes sont équivalentes :

1. $b \mid a$.
2. $a \in bA$.
3. $aA \subset bA$.

Preuve : L'équivalence 1) $\iff$ 2) est vraie par définition.
Supposons que 2) est vraie. Soit $a \in bA$.
Ainsi pour tout $\alpha \in A$, $a\alpha \in bA$ car bA est un idéal de A.
On en déduit que $aA \subset bA$. Donc 3) est vraie.
Réciproquement, supposons que 3) est vraie : $aA \subset bA$.
Comme $a \in aA$, on en déduit que $a \in bA$. Donc 2) est vraie.

$\square$

Définition 12

Soit $(A, +, \times)$ un anneau commutatif intègre. On dit que $(A, +, , \times)$ est principal si, et seulement si, tout idéal de A est engendré par un élément de A.

Exemple : L'anneau $(\mathbb{Z}, +, \times)$ est principal.

Proposition 13

Soit A un anneau intègre et I, J deux idéaux. La somme $I + J = \{i + j, i \in I, j \in J\}$ est un idéal de A.

Preuve : On sait que $0 \in I$ et $0 \in J$, donc $0 = 0 + 0 \in I + J$. Donc, $I + J \neq \emptyset$.
Soit $(x, y) \in (I + J)^2$. Il existe $(x_1, y_1) \in I^2$ et $(x_2, y_2) \in J^2$ tels que
$$x = x_1 + x_2 \text{ et } y = y_1 + y_2$$
Ainsi,
$$x - y = \underbrace{x_1 - y_1}_{\in I} + \underbrace{x_2 - y_2}_{\in J}$$
On a donc $x - y \in I + J$. On en déduit que $I + J$ est un sous-groupe de $(A, +)$.

Soit $x \in I + J$ et $a \in A$. Il existe donc $(x_1, x_2) \in I \times J$ tels que $x = x_1 + x_2$. On a alors
$$ax = ax_1 + ax_2 \in I + J$$
On a bien montré que $I + J$ est un idéal. $\square$

Exercice E8 : Soit A un anneau commutatif et e un élément idempotent de A (i.e. $e^2 = e$).

1. Montrer que $J = \{x \in A \mid xe = 0\}$ est un idéal de A.
2. On note $I = Ae$ l'idéal principal engendré par e. Déterminer $I + J$ et $I \cap J$.
3. Établir que pour tout idéal K de A :

$$(K \cap I) + (K \cap J) = K$$

9.2.3 Morphismes d'anneaux

Définition 14

Soit $(A, +, \times)$, $(B, \oplus, \otimes)$ des anneaux. On dit qu'une application $\varphi : A \to B$ est un morphisme d'anneaux si, et seulement si :

1. $\varphi(1_A) = 1_B$
2. $\forall x, x' \in A, \quad \varphi(x + x') = \varphi(x) \oplus \varphi(a')$
3. $\forall x, x' \in A, \quad \varphi(x \times x') = \varphi(x) \otimes \varphi(a')$

Remarques :

1. La condition 2) assure que $\varphi(0_A) = 0_B$. En effet, comme :

$$\varphi(0_A) = \varphi(0_A + 0_A) = \varphi(0_A) \oplus \varphi(0_A).$$

   Comme l'élément $f(0_A)$ admet un opposé dans le groupe $(B, \oplus)$, on peut simplifier à droite par $f(0_A)$. On en déduit que : $0_B = f(0_A)$.
2. La condition 3) ne permet pas d'obtenir $\varphi(1_A) = 1_B$. Si on essaie de faire le même raisonnement que celui qui précède,

$$\varphi(1_A) = \varphi(1_A \times 1_A) = \varphi(1_A) \otimes \varphi(1_A).$$

   Rien ne nous assure que $\varphi(1_A)$ est inversible pour la multiplication dans l'anneau $(B, \oplus, \otimes)$.

Exemples :

1. Soit $(A, +, \times)$ un anneau. L'application $\mathsf{Id}_A : A \to A$ est un morphisme d'anneaux.
2. Soit $x_0 \in \mathbb{K}$, l'application :

$$\delta_{x_0} : \left\{ \begin{array}{rcl} (\mathbb{K}[X], +, \oplus) & \to & (\mathbb{K}, +, \times) \\ P & \mapsto & P(x_0) \end{array} \right.$$

   est un morphisme d'anneaux.

Définition 15

Soit $(A, +, \times)$, $(B, \oplus, \otimes)$ des anneaux. Soit $\varphi : A \to B$ un morphisme d'anneaux.

1. L'image de φ que l'on note $\mathsf{Im}(\varphi)$ est un sous-anneau de $(B, \oplus, \otimes)$.
2. Le noyau de φ noté $\mathsf{Ker}(\varphi)$ et défini par :

$$\mathsf{Ker}(\varphi) = \{x \in A \mid \varphi(x) = 0_B\}$$

   est un idéal de $(A, +, \times)$.

Preuve :
Remarquons que $\varphi(0_A) = 0_B$ donc $0_A \in \operatorname{Ker} \varphi$ qui n'est pas vide. Soit $x, y \in \operatorname{Ker} \varphi$,

$$\varphi(x - y) = \varphi(x) - \varphi(y) = 0_B.$$

Donc $x - y \in \operatorname{Ker} \varphi$. Par conséquent, $\operatorname{Ker} \varphi$ est un sous-groupe de $(A, +)$.

Soit $x \in \operatorname{Ker} \varphi$ et $a \in A$,

$$\varphi(ax) = \varphi(a)\varphi(x) = 0_B$$

Donc $ax \in \operatorname{Ker} \varphi$.

Par conséquent, $\operatorname{Ker} \varphi$ est un idéal de A. □

Remarque : Le noyau d'un morphisme d'anneau φ n'est pas en général un sous-anneau de $(A, +, \times)$.
En effet, $\varphi(1_A) = 1_B$ n'est pas égal à 0_B sauf dans le cas d'un anneau trivial comportant un seul élément.

Exemple : Soit $x_0 \in \mathbb{K}$, reprenons le morphisme d'anneaux :

$$\delta_{x_0} : \left\{ \begin{array}{rcl} (\mathbb{K}[X], +, \times) & \to & (\mathbb{K}, +, \times) \\ P & \mapsto & P(x_0) \end{array} \right.$$

On remarque que $\mathsf{Ker}(\delta_{x_0}) = \{P \in \mathbb{K}[X] \mid P(x_0) = 0\} = \{(X - x_0)Q \mid Q \in \mathbb{K}[X]\}$ est un idéal de $(\mathbb{K}[X], +, \times)$.
D'autre part, $\mathsf{Im}(\delta_{x_0}) = \mathbb{R}$ est bien un sous-anneau de $(\mathbb{R}, +, \times)$.

Définition 16

Soit $(A, +, \times)$, $(B, \oplus, \otimes)$ des anneaux. Soit $\varphi : A \to B$ un morphisme d'anneaux.

1. Le morphisme φ est injectif si, et seulement si, $\mathsf{Ker}(\varphi) = \{0_A\}$.
2. Le morphisme φ est surjectif si, et seulement si, $\mathsf{Im}(\varphi) = B$.

Preuve : Le morphisme d'anneaux $\varphi : A \to B$ est aussi un morphisme de groupes. Il suffit d'utiliser la propriété sur les morphismes de groupes.
□

Définition 17

Soit $(A, +, \times)$, $(B, \oplus, \otimes)$ des anneaux. Soit $\varphi : A \to B$ un morphisme d'anneaux. On dit que φ est un isomorphisme d'anneaux si, et seulement si, l'application φ est bijective.

Proposition 18

1. La composée de deux isomorphismes d'anneaux est encore un isomorphisme d'anneaux.
2. L'application réciproque d'un isomorphisme d'anneaux est encore un isomorphisme d'anneaux.

Définition 19

Soit $(A, +, \times)$, $(B, \oplus, \otimes)$ des anneaux. On dit que les anneaux A et B sont isomorphes si, et seulement si, il existe un isomorphisme d'anneaux de A vers B.

9.3 Idéaux de $\mathbb{Z}$

Rappelons que :

Théorème 20

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, où $n \in \mathbb{N}$.

Remarques :

1. On a l'équivalence suivante : $n\mathbb{Z} = m\mathbb{Z}$ si et seulement si $n = \pm m$.
2. Pour $a, b \in \mathbb{Z}$, $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$ donc il existe un unique $c \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$.
3. De même, $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$ donc il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Définition 21

Soit $a, b \in \mathbb{Z}$.

1. On appelle plus grand diviseur commun de a et b l'unique entier naturel d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
   On le note $\mathrm{pgcd}(a, b)$ ou $a \wedge b$.
2. On appelle plus petit commun multiple de a et b l'unique entier naturel c tel que $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$.
   On le note $\mathrm{ppcm}(a, b)$ ou $a \vee b$.

Proposition 22 (Relation de Bachet-Bézout)

Soit $a, b \in \mathbb{Z}$.
Il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$.
Une telle relation est appelée relation de Bachet-Bézout de a et b.

Théorème 23 (Théorème de Bézout)

Soit $a, b \in \mathbb{Z}$.
Les entiers a et b sont premiers entre eux si, et seulement si, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Preuve : Supposons que $a \wedge b = 1$. Alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. Or $1 \in \mathbb{Z}$, ainsi $1 \in a\mathbb{Z} + b\mathbb{Z}$. Par conséquent, 1 s'écrit sous la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

Supposons qu'il existe $u, v \in \mathbb{Z}$ tels que $1 = au + bv$.
En multipliant par $n \in \mathbb{Z}$, on obtient

$$n = a(nu) + b(nv)$$

donc $\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$.

Comme l'inclusion réciproque est toujours vraie, on a $1.\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ et donc $a \wedge b = 1$. □

9.4 Compléments et rappels sur $\mathbb{K}[X]$

Dans ce paragraphe, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

9.4.1 Idéaux de $\mathbb{K}[X]$

Théorème 24

Les idéaux de $\mathbb{K}[X]$ sont les ensembles $(P) = P \cdot \mathbb{K}[X] = \{P \cdot Q \mid Q \in \mathbb{K}[X]\}$ pour $P \in \mathbb{K}[X]$.
Les idéaux de $\mathbb{K}[X]$ sont donc tous principaux.

Preuve :
On vérifie que $(0_{\mathbb{K}[X]})$ est un idéal de $\mathbb{K}[X]$.
Soit I un idéal de $\mathbb{K}[X]$ différent de l'idéal nul.
Soit P un polynôme non nul de I de degré minimal. Remarquons que $(P) \subset I$.
Soit $A \in I$. Effectuons la division euclidienne de A par P. On trouve :

$$A = BP + R \quad \text{avec} \quad \deg(R) < \deg(P)$$

Comme I est un idéal, $BP \in I$. D'autre part, $(I, +)$ étant un groupe, $R = A - BP \in I$.
Par minimalité du degré de P, il vient $R = 0_{\mathbb{K}[X]}$, et donc $A = BP$.
On a prouvé que $I \subset (P)$.

Par double inclusion, $(P) = I$. □

Définition 25 (PGCD de deux polynômes)

Soit $(P, Q) \in \mathbb{K}[X]^2$. On appelle PGCD de P et Q tout polynôme $D \in \mathbb{K}[X]$ tel que

$$P\mathbb{K}[X] + Q\mathbb{K}[X] = D\mathbb{K}[X]$$

Il existe un unique PGCD unitaire ou nul de P et Q noté $\mathrm{P} \wedge \mathrm{Q}$.

Remarque : Cette définition du PGCD est équivalente à la définition du PGCD vue en première année. Le théorème de Bézout découle alors directement de cette nouvelle définition.

Définition 26 (PPCM de deux polynômes)

Soit $(P, Q) \in \mathbb{K}[X]^2$. On appelle PPCM de P et Q tout polynôme $M \in \mathbb{Z}$ tel que

$$P\mathbb{K}[X] \cap Q\mathbb{K}[X] = M\mathbb{K}[X]$$

Il existe un unique PPCM unitaire ou nul de P et Q noté $\mathrm{P} \vee \mathrm{Q}$.

Remarque : Cette définition du PPCM est équivalente à la définition du PGCD vue en première année.

Théorème 27 (Relation de Bachet-Bézout)

Soit A et B deux polynômes de $\mathbb{K}[X]$ non nuls, et $D = A \wedge B$. Il existe ALORS deux polynômes U et V tels que :

$$AU + BV = D \quad \text{(relation de Bézout).}$$

Théorème 28 (de Bézout)

Soit A et B deux polynômes de $\mathbb{K}[X]$ non nuls.
Les polynômes A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $AU + BV = 1$.

Théorème 29 (Lemme de Gauss)

Soit A, B, C trois polynômes. Si $A|BC$ et si $A \wedge B = 1$ alors $A|C$.

Définition 30 (PGCD d'une famille de polynômes)

Soit $(\mathrm{P}_1, \ldots, \mathrm{P}_n) \in \mathbb{K}[X]^n$. On appelle PGCD de $\mathrm{P}_1, \ldots, \mathrm{P}_n$ tout polynôme $\mathrm{D} \in \mathbb{K}[\mathrm{X}]$ tel que

$$\sum_{i=1}^{n} \mathrm{P}_i\mathbb{K}[\mathrm{X}] = \mathrm{D}\mathbb{K}[\mathrm{X}]$$

Il existe un unique PGCD unitaire ou nul de $\mathrm{P}_1, \ldots, \mathrm{P}_n$ noté $\mathrm{P}_1 \wedge \ldots \wedge \mathrm{P}_n$.

Proposition 31 (Relation de Bachet-Bézout pour une famille de polynômes)

Soit $(\mathrm{P}_1, \ldots, \mathrm{P}_r) \in \mathbb{K}[\mathrm{X}]^r$. Il existe $(\mathrm{U}_1, \ldots, \mathrm{U}_r) \in \mathbb{K}[\mathrm{X}]^r$ tel que

$$\sum_{i=1}^{r} \mathrm{U}_i \mathrm{P}_i = \mathrm{P}_1 \wedge \ldots \wedge \mathrm{P}_r$$

9.4.2 Factorisation en produit d'éléments irréductibles

Définition 32

Soit $P \in \mathbb{K}[X]$. On dit que le polynôme P est irréductible dans $\mathbb{K}$ si, et seulement si,

1. P n'est pas un polynôme constant.
2. Les seuls diviseurs de P sont les polynômes associés à 1 et à P.

En d'autres termes :

$$\mathcal{D}(P) = \{\lambda, \mu P \mid (\lambda, \mu) \in (\mathbb{K}^*)^2\}.$$

Remarque : La précision "irréductible dans $\mathbb{K}$" peut s'avérer importante. Nous verrons que $X^2 + 1$ est irréductible dans $\mathbb{R}$, mais qu'il ne l'est pas dans $\mathbb{C}$ puisque $X^2 + 1 = (X - i)(X + i)$.

Théorème 33 (Factorisation en éléments irréductibles)

Soit $P \in \mathbb{K}[X]$ non constant. Le polynôme P s'écrit alors comme un produit de polynômes irréductibles sur $\mathbb{K}$.

Théorème 34 (de d'Alembert-Gauss)

Un polynôme complexe non constant admet au moins une racine dans $\mathbb{C}$.

Remarques :

1. Tout polynôme $P \in \mathbb{C}[X]$ de degré $n \geqslant 1$ admet donc exactement n racines dans $\mathbb{C}$ (comptées avec leur ordre de multiplicité) et peut s'écrire sous la forme :

$$P = \lambda \prod_{i=1}^{n} (X - \alpha_i) \quad (\alpha_i \in \mathbb{C})$$

2. Soient $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}$. Si α est racine de P, il en va de même pour $\bar{\alpha}$. On peut dès lors factoriser P par :

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - 2\,\mathrm{Re}(\alpha)X + |\alpha|^2 \in \mathbb{R}[X]$$

Théorème 35 (Polynômes irréductibles)

1. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
2. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et de degré 2 à discriminant négatif.

9.5 Polynômes de matrices et d'endomorphismes

Définition 36

Soit $(\mathcal{A}, +, \cdot, \times)$ une algèbre sur $\mathbb{K}$. Soit $a \in \mathcal{A}$ et $P \in \mathbb{K}[X]$ de la forme :

$$P = \sum_{k=0}^{d} \alpha_k X^k$$

avec $m \in \mathbb{N}$ et $\alpha_0, \dots, \alpha_m \in \mathbb{K}$. On note $P(a)$ l'élément de $\mathcal{A}$ défini par :

$$P(a) = \sum_{k=0}^{m} \alpha_k a^k = \alpha_0 1_A + \alpha_1 a + \cdots + \alpha_d a^d.$$

Exemple : Dans le cas où $\mathcal{A} = \mathbb{K}$ et $a \in \mathbb{K}$, l'élément $P(a)$ est tout simplement l'évaluation du polynôme P en a :

$$P(a) = \alpha_0 + \alpha_1 a + \cdots + \alpha_m a^m \in \mathbb{K}$$

Définition 37

Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$ où $d \in \mathbb{N}$.

1. Soit E un espace vectoriel sur $\mathbb{K}$ et $u \in L(E)$, on pose $P(u)$ l'endomorphisme :

$$P(u) = \sum_{k=0}^{d} a_k u^k = a_d u^d + \cdots + a_1 u + a_0 \mathsf{Id}_E.$$

2. Soit $M \in M_n(\mathbb{K})$. On pose $P(M)$ la matrice :

$$P(M) = \sum_{k=0}^{d} a_k M^k = a_d M^d + \cdots + a_1 M + a_0 I_n.$$

Remarques : Avec les notations précédentes :

1. Pour tout $n \in \mathbb{N}$, $u^n = \underbrace{u \circ \cdots \circ u}_{n \text{ fois}}$ et $u^0 = \mathsf{Id}_E$.
2. $M^0 = I_n$.

Attention ! Il y a deux erreurs à éviter absolument.

1. Oublier Id_E (respectivement I_n) dans l'écriture de $P(u)$ (respectivementde $P(M)$) en écrivant par exemple u^2+u+1 (respectivement M^2+M+1) au lieu de $u^2+u+\mathsf{Id}_E$ (respectivement M^2+M+I_n).
2. Mal placer les parenthèses. Soit $x \in E$, $P(u)(x)$ a un sens alors que $P(u(x))$ n'a en général pas de sens, on n'élève pas un vecteur à la puissance.

Proposition 38

Soit E un espace vectoriel sur $\mathbb{K}$ et $u \in L(E)$. L'application :

$$\Psi_u : \begin{cases} \mathbb{K}[X] \to L(E) \\ P \mapsto P(u) \end{cases}$$

est un morphisme d'algèbres. En d'autres termes :

1. $\Psi_u(1) = I_n$
2. $\forall (P,Q) \in \mathbb{K}[X]^2, \quad \Psi_u(P+Q) = \Psi_u(P) + \Psi_u(Q)$ ce qui revient à $(P+Q)(u) = P(u) + Q(u)$
3. $\forall (P,Q) \in \mathbb{K}[X]^2, \quad \Psi_u(P \times Q) = \Psi_u(P) \circ \Psi_u(Q)$ ce qui revient à $(P \times Q)(u) = P(u) \circ Q(u)$
4. $\forall P \in \mathbb{K}[X], \quad \forall \lambda \in \mathbb{K}, \quad \Psi_u(\lambda \cdot P) = \lambda \Psi_u(P)$ ce qui revient à $(\lambda \cdot P)(u) = \lambda \cdot P(u)$.

Preuve : $P \mapsto P(u)$ est une application linéaire et un morphisme d'anneaux : pour tous $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$,

1. $1(u) = \mathsf{Id}_E$
2. $(\lambda P + \mu Q)(u) = \lambda P(u) + \mu Q(u)$
3. $(P \times Q)(u) = P(u) \circ Q(u) = Q(u) \circ P(u)$

Justifions la dernière propriété.

Soit deux polynômes $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$. Alors,

$$PQ = \sum_{i,j \in \mathbb{N}} a_i b_j X^{i+j}$$

Or pour tous $i, j \in \mathbb{N}, u^i \circ u^j = u^{i+j} = u^j \circ u^i$. Par bilinéarité de la composition,

$$(P \times Q)(u) = \sum_{i,j \in \mathbb{N}} a_i b_j u^{i+j} = \left(\sum_{i \in \mathbb{N}} a_i u^i\right) \circ \left(\sum_{j \in \mathbb{N}} b_j u^j\right) = P(u) \circ Q(u)$$

$\square$

Définition 39

Soit E un espace vectoriel sur $\mathbb{K}$ et $u \in L(E)$. On considère l'ensemble $\mathbb{K}[u]$ défini par :

$$\mathbb{K}[u] = \{P(u) \mid P \in \mathbb{K}[X]\} = \mathsf{Vect}(u^k \mid n \in \mathbb{N}).$$

$\mathbb{K}[u]$ est l'ensemble des polynômes en u.

Remarque : Avec les notations précédentes, $\mathbb{K}[u] = \mathsf{Im}(\Psi_u)$.

Proposition 40

Soit E un espace vectoriel sur $\mathbb{K}$ et $u \in L(E)$.
$(\mathbb{K}[u], +, \circ, \cdot)$ possède une structure de d'algèbre commutative sur $\mathbb{K}$. En d'autres termes :

- $(\mathbb{K}[u], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
- $(\mathbb{K}[u], +, \circ)$ est un anneau commutatif.
- $\forall \lambda \in \mathbb{K}, \quad \forall f, g \in \mathbb{K}[u], \quad (\lambda \cdot f) \circ g = f \circ (\lambda \cdot g) = \lambda \cdot (f \circ g)$

Preuve : En tant qu'image de $\mathbb{K}[X]$ par le morphisme d'algèbres $P \mapsto P(u)$.
$(\mathbb{K}[u], +, \circ, \cdot)$ possède aussi une structure de d'algèbre.
La commutativité de $\mathbb{K}[X]$ se transmet à la sous-algèbre $\mathbb{K}[u]$ de $\mathcal{L}(E)$. $\square$

Remarque : On notera $\mathbb{K}_n[u] = \{P(u) \mid P \in \mathbb{K}_n[X]\} = \mathsf{Vect}\left\{u^k \mid k \in [\![0, n]\!]\right\}$.

Proposition 41

Soit E un espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.
$\mathbb{K}[u]$ est un sous-espace vectoriel de $\mathcal{L}(E)$ (de dimension finie).

Théorème 42

Soit $u \in \mathcal{L}(E)$. Pour tout $P \in \mathbb{K}[X]$, $\mathrm{Im}(P(u))$ et $\mathrm{Ker}(P(u))$ sont stables par u.

Définition 43

Soit $A \in \mathcal{M}_n(\mathbf{K})$, l'application

$$\begin{aligned} \Psi_A : \mathbf{K}[X] &\to \mathcal{M}_n(\mathbf{K}) \\ P &\mapsto P(A) \end{aligned}$$

est un morphisme d'algèbres ce qui signifie que :

1. $\Psi_A(1) = I_n$
2. $\forall (P, Q) \in \mathbf{K}[X]^2, \Psi_A(P + Q) = \Psi_A(P) + \Psi_A(Q)$ c'est-à-dire $(P + Q)(A) = P(A) + Q(A)$
3. $\forall (P, Q) \in \mathbf{K}[X]^2, \Psi_A(P \times Q) = \Psi_A(P) \times \Psi_A(Q)$ c'est-à-dire $(P \times Q)(A) = P(A) \times Q(A)$
4. $\forall P \in \mathbf{K}[X], \forall \lambda \in \mathbf{K}, \Psi_A(\lambda.P) = \lambda.\Psi_A(P)$ c'est-à-dire $(\lambda.P)(A) = \lambda \cdot P(A)$.

Définition 44

Soit $A \in \mathcal{M}_n(\mathbf{K})$. On note $\mathbf{K}[A] = \{P(A) \mid P \in \mathbf{K}[X]\}$. C'est l'ensemble des polynômes en A.

Proposition 45

1. $\mathbf{K}[A]$ est une sous-algèbre de $\mathcal{M}_n(\mathbf{K})$, c'est-à-dire un sous-espace vectoriel, stable par produit contenant I_n.
2. La sous-algèbre $\mathbf{K}[A]$ est commutative.
3. La famille $\left(I_n, A, A^2, \ldots\right)$ engendre $\mathbf{K}[A]$ en tant qu'espace vectoriel.

Proposition 46

Soit $A, B \in \mathcal{M}_n(\mathbb{K})$.
Si A et B sont semblables, alors, pour tout $P \in \mathbb{K}[X], P(A)$ et $P(B)$ sont aussi semblables.

Preuve : Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X], M \in \mathcal{M}_n(\mathbb{K})$ et $Q \in \mathrm{GL}_n(\mathbb{K})$.
Alors, pour tout $k \in \mathbb{N}$, $\left(Q^{-1}MQ\right)^k = Q^{-1}M^kQ$. Par combinaison linéaire, $P\left(Q^{-1}MQ\right) = Q^{-1}P(M)Q$. □

Proposition 47

Soit $u \in \mathcal{L}(E)$ et $\mathcal{B}$ une base de E. On note $A = \underset{\mathcal{B}}{\mathsf{Mat}}(u)$. Pour tout polynôme P de $\mathbf{K}[X]$,

$$\underset{\mathcal{B}}{\mathsf{Mat}}(P(u)) = P(A).$$

Preuve : Cela découle du fait que :

$$\underset{\mathcal{B}}{\mathsf{Mat}} : \begin{cases} L(E) \to M_n(\mathbb{K}) \\ u \mapsto \underset{\mathcal{B}}{\mathsf{Mat}}(u) \end{cases}$$

est un morphisme d'algèbres. □

9.6 Polynômes annulateurs

Définition 48 (Polynômes annulateurs)

1. Soit $u \in \mathcal{L}(E)$. Un polynôme P de K$[X]$ est dit annulateur de u si, et seulement si, $P(u) = 0_{\mathcal{L}(E)}$.
2. Soit $A \in \mathcal{M}_n(\mathbf{K})$. Un polynôme P de $\mathbf{K}[X]$ est dit annulateur de A si, et seulement si, $P(A) = 0_{M_n(\mathbb{K})}$.

Exemples :

1.
2.

Proposition 49

Soit E un espace vectoriel de dimension finie n.

1. Soit $u \in \mathcal{L}(E)$. L'ensemble des polynômes annulateurs de u est un idéal de $\mathbf{K}[X]$ non réduit à $\{0\}$.
2. Soit $A \in \mathcal{M}_n(\mathbf{K})$. L'ensemble des polynômes annulateurs de A est un idéal de $\mathbf{K}[X]$ non réduit à $\{0\}$.

Preuve : On remarque que pour $P \in \mathbf{K}[X]$,

$$P(u) = 0 \iff \Psi_u(P) = 0$$

où

$$\Psi_u : \mathbf{K}[X] \to \mathcal{L}(E)$$
$$P \mapsto P(u)$$

On voit donc que l'ensemble des polynômes annulateurs est le noyau d'un morphisme d'anneaux. C'est donc un idéal de $\mathbf{K}[X]$.
Montrons que $\mathsf{Ker}(\Psi_u)$ n'est pas réduit à $\{0\}$.
Comme $\mathcal{L}(E)$ est de dimension n^2, la famille $(u^0, u^1, u^2, \ldots, u^{n^2})$ est liée car elle est de cardinal $n^2 + 1 > n^2$.
On en déduit qu'il existe un combinaison linéaire non triviale

$$\sum_{i=0}^{n^2} \lambda_i u^i = 0\mathcal{L}(E)$$

Le polynôme non nul $P = \sum_{i=0}^{n^2} \lambda_i X^i$ est un polynôme annulateur de u. □

Remarque : Un endomorphisme en dimension infinie n'admet pas toujours de polynôme minimal.

Définition 50 (Polynôme minimal)

Soit E un espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$ non nul.
Il existe alors un unique polynôme unitaire qui divise tous les polynômes annulateurs de u.
Ce polynôme est appelé polynôme minimal de u et est généralement noté π_u ou μ_u.

Preuve :
Comme E est de dimension finie, l'ensemble $\{\deg(P) \mid P(u) = 0_{\mathcal{L}(E)} \text{ et } P \in \mathbb{K}[X] \text{ non nul } \}$ est une partie non vide de $\mathbb{N}$. Elle admet donc un plus petit élément que l'on notera d.
Soit μ_u un polynôme annulateur de u de degré d que l'on va supposer de plus unitaire afin de garantir l'unicité.

Soit P un polynôme annulateur quelconque de u. Par division euclidienne,

$$\exists (Q,R) \in \mathbb{K}[X], \quad P = Q \times \pi_u + R \quad \text{avec} \deg(R) < d$$

De plus $R(u) = P(u) - Q(u) \circ \pi_u(u) = 0_{\mathcal{L}(E)}$.
Comme R annule u et est de degré strictement inférieur au degré minimal d, $R = \tilde{0}$.

Ce qui prouve bien que $P = Q \times \pi_u$. □

Théorème 51

Soit E un espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$ non nul.
Soit $P \in \mathbb{K}[X]$, on a les équivalences suivantes :

$$P(u) = 0_{L(E)} \iff \pi_u \mid P$$

Proposition 52

Soit $u \in \mathcal{L}(E)$ et $\mathcal{B}$ une base de E. On pose $A = \text{Mat}_{\mathcal{B}}(u)$. Les polynômes minimaux coincident :

$$\mu_A = \mu_u.$$

Preuve : Ce sont les mêmes idéaux annulateurs car pour $P \in \mathbf{K}[X], \Phi_u(P) = 0_{\mathcal{L}(E)} \iff \Phi_A(P) = 0_{\mathcal{M}_n(\mathrm{K})}$ □

Exemples :

1.
2.

Proposition 53

Soit A et B deux matrices semblables, alors $\mu_A = \mu_B$.

Preuve : On vérifie que pour $P \in \mathbf{K}[X], P(A) = 0$ si et seulement si $P(B) = 0$. □

Théorème 54

Soit $u \in \mathcal{L}(E)$. On suppose que son polynôme minimal μ_u est de degré d alors la famille $\left(u^k\right)_{0 \leqslant k \leqslant d-1}$ est une base de $\mathbf{K}[u]$ et

$$\dim(\mathbb{K}[u]) = \mathsf{deg}(\mu_u)$$

Preuve : Par définition la famille $\left(u^k\right)_{k \in \mathbf{N}}$ est génératrice de $\mathbf{K}[u]$ mais elle n'est pas libre.

En considérant le polynôme minimal $\mu_u = \sum_{k=0}^{d} a_k X^k$ alors on a une combinaison linéaire non triviale

$$\sum_{k=0}^{d} a_k u^k = 0.$$

ce qui prouve que $(u^0, \ldots, u^d)$ est liée.
Posons $F = \text{Vect}\left(\text{Id}_E, u, \ldots, u^{d-1}\right) \subset \mathrm{K}[u]$ et montrons que $F = \mathrm{K}[u]$.
Soit $k \in \mathrm{N}$, on fait la divison euclidienne de X^k par μ_u :

$$X^k = Q \times \mu_u + S \text{ où } \deg(S) < d$$

Ainsi :

$$u^k = Q(u) \circ \mu_u(u) + S(u) = S(u) \in F$$

On a bien $F = \mathbf{K}[u]$. La famille $\left(u^k\right)_{0 \leqslant k \leqslant d-1}$ est génératrice de $\mathbf{K}[u]$.
Montrons que la famille $\left(u^k\right)_{0 \leqslant k \leqslant d-1}$ est libre.
Raisonnons par l'absurde en supposant qu'elle est liée. Il existe alors une relation de dépendance linéaire non triviale

$$\sum_{k=0}^{d-1} b_k u^k = 0$$

Si on pose $Q = \sum_{k=0}^{d-1} b_k X^k$, on a donc $Q(u) = 0$.
Le polynôme non nul Q est annulateur de u et $\mathbf{deg}(Q) < d$. Ceci contredit le caractère minimal de μ_u.
En conclusion, la famille $\left(u^k\right)_{0 \leqslant k \leqslant d-1}$ est bien une base de $\mathbf{K}[u]$. □

Proposition 55

Soit $u \in \mathcal{L}(E)$ et F un sous-espace stable par u non réduit à $\{0_E\}$.
Alors, le polynôme minimal de l'endomorphisme induit $u_{|F}$ divise celui de u.

Preuve : Remarquons que les polynômes annulateurs de u annulent $u_{|F}$. En effet, si P annule u,

$$\forall x \in F, \quad P\left(u_{|F}\right)(x) = P(u)(x) = 0_E$$

$\mu_{u_{|F}}$ divisent tous les polynômes annulateurs de $u_{|F}$, il divise tous ceux de u et en particulier μ_u. □

Exercice C9 : [Mines-Télécom] Déterminer le polynôme minimal de la matrice $A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$.

Exercice C10 : [Mines-Télécom]
Soient $n \geqslant 2$ et A la matrice carrée réelle d'ordre n dont tous les coefficients sont égaux à 1 . Donner le polynôme minimal de A.

Exercice C11 : [CCINP]
Soient n un entier $\geqslant 2$ et $f : \mathcal{M}_n(\mathbb{R}) \to \mathcal{M}_n(\mathbb{R})$ définie par $f(M) = {}^tM$. Déterminer le polynôme minimal de f.

Exercice C12 : [CCINP]
Soit A la matrice carrée d'ordre 3 suivante :

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

1. Montrer que A n'a pas de polynôme annulateur (non nul) de degré inférieur ou égal à 2 .
2. Trouver le polynôme minimal de A.
3. Montrer que A est inversible et préciser A^{-1}.

Exercice E13 :
Soit E un $\mathbb{K}$-espace vectoriel de dimension $n, u \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$. On note π_u le polynôme minimal de u. Montrer que $P(u) \in \mathrm{GL}(E)$ si, et seulement si, P et π_u sont premiers entre eux.

Exercice C14 : [Mines-Ponts]
Soit A $\in \mathcal{M}_n(\mathbb{R})$. Montrer que A admet le même polynôme minimal considérée comme une matrice de $\mathcal{M}_n(\mathbb{R})$ et comme une matrice de $\mathcal{M}_n(\mathbb{C})$.

Exercice E15 : Soit E un $\mathbb{K}$-espace vectoriel. Soit $f \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$. Montrer les implications suivantes :

1. $$(P(0) = 0) \implies \begin{cases} \mathsf{Ker}(f) \subset \mathsf{Ker}(P(f)), \\ \mathsf{Im}(P(f)) \subset \mathsf{Im}(f) \end{cases}$$

2. $$(P(0) \neq 0) \implies (\mathsf{Ker}(P(f)) \subset \mathsf{Im}(f))$$

3. $$\begin{cases} \mathsf{Ker}(f) \subset \mathsf{Ker}(P(f)) \\ \mathsf{Ker}(f) \neq \{0_E\} \end{cases} \implies (P(0) = 0)$$

9.7 Polynômes annulateurs et valeurs propres

Proposition 56

Soit E un $\mathbb{K}$-espace vectoriel. Soit $u \in \mathcal{L}(E)$.
Soit $\lambda \in \mathrm{K}$ une valeur propre de u et $x \in E_\lambda(u)$ un vecteur propre associé à λ.
Soit $P \in \mathbf{K}[X]$ alors
$$P(u)(x) = P(\lambda).x$$

Remarque : Faire attention à la position des parenthèses pour écrire une relation qui a bien un sens.

Preuve : Remarquons que pour tout $k \in \mathbb{N}$, $u^k(x) = \lambda^k x$.
Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$, par définition $P(u) = \sum_{k=0}^{d} a_k u^k \in L(E)$.
$$P(u)(x) = \left(\sum_{k=0}^{d} a_k u^k\right)(x) = \sum_{k=0}^{d} a_k u^k(x) = \sum_{k=0}^{d} a_k \lambda^k.x = \left(\sum_{k=0}^{d} a_k \lambda^k\right).x = P(\lambda)\cdot x$$

□

Corollaire 57

Soit E un $\mathbb{K}$-espace vectoriel. Soit $u \in \mathcal{L}(E)$.
Soit $\lambda \in \mathrm{K}$ une valeur propre de u.
Si P est un polynôme annulateur de u alors
$$P(\lambda) = 0.$$

Les valeurs propres de u sont PARMI les racines de tout polynôme annulateur de u.

Preuve : D'après la pa proposition précédente :
$$P(u)(x) = P(\lambda)\cdot x$$
Or P est annulateur de u.
$$P(\lambda)\cdot x = 0_{L(E)}(x) = 0_E.$$
Or $x \neq 0_E$. On en déduit que $P(\lambda) = 0$. □

Remarque : En particulier, le polynôme minimal μ_u s'annule en toutes les valeurs propres de u.
Si on note $Z(P)$ les racines d'un polynôme P annulateur de u, on a l'inclusion :
$$\mathsf{Sp}(u) \subset Z(P)$$

Proposition 58

Soit $A \in M_n(\mathbb{K})$.
Soit $\lambda \in \mathrm{K}$ une valeur propre de A et $X \in E_\lambda(A)$ un vecteur propre associé à λ.
Soit $P \in \mathbf{K}[X]$ alors

$$P(A)X = P(\lambda)X$$

Corollaire 59

Soit $A \in M_n(\mathbb{K})$.
Soit $\lambda \in \mathrm{K}$ une valeur propre de A et $X \in E_\lambda(A)$ un vecteur propre associé à λ.
Si P est un polynôme annulateur de A alors

$$P(\lambda) = 0.$$

Les valeurs propres de A sont PARMI les racines de tout polynôme annulateur de A.

9.8 Théorème de Cayley-Hamilton

Théorème 60 (de Cayley-Hamilton)

Le polynôme caractéristique d'un endomorphisme en dimension finie (ou d'une matrice) est un polynôme annulateur. Autrement dit, si E est de dimension finie,

$$\forall u \in \mathcal{L}(E), \quad \chi_u(u) = 0_{\mathcal{L}(E)}$$

ce qui revient à $\pi_u \mid \chi_u$.

$$\forall A \in M_n(\mathbb{K}), \quad \chi_A(A) = 0_{M_n(\mathbb{K})}$$

ce qui revient à $\pi_A \mid \chi_A$.

Corollaire 61

1. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.
   Le degré du polynôme minimal est inférieur ou égal à $\dim(E)$.
2. Soit $A \in M_n(\mathbb{K})$, $\mathsf{deg}(\pi_A) \leqslant n$.

Preuve : Comme $\pi_u \mid \chi_u$ et $\chi_u \neq 0_{\mathbb{K}[X]}$, alors $\mathsf{deg}(\pi_u) \leqslant \mathsf{deg}(\chi_u) = \dim(E)$. □

Théorème 62

Les racines du polynôme minimal d'un endomorphisme (respectivement d'une matrice) sont, comme pour le polynôme caractéristique, exactement ses valeurs propres.

Preuve : Notons $\lambda_1, \dots, \lambda_r$ les r valeurs propres distinctes de $u \in \mathcal{L}(E)$.
Elles sont racines de π_u en tant que polynôme annulateur :

$$(X - \lambda_1) \times \cdots \times (X - \lambda_r) \mid \pi_u$$

D'après le théorème de Cayley-Hamilton,le polynôme minimal divise le polynôme caractéristique.
Notons m_i la multiplicité de la valeur propre λ_i dans χ_u de telle sorte que

$$\chi_u = (X-\lambda_1)^{m_1} \times \cdots \times (X-\lambda_r)^{m_r}$$

Ainsi :

$$\pi_u \mid (X-\lambda_1)^{m_1} \times \cdots \times (X-\lambda_r)^{m_r}$$

π_u est donc de la forme $(X-\lambda_1)^{d_1} \times \cdots \times (X-\lambda_r)^{d_r}$ avec, pour tout $i \in [\![1, r]\!], 1 \leqslant d_i \leqslant m_i$. □

Remarque : Ce théorème facilite la recherche d'un polynôme minimal.
En effet, si $\chi_M = (X-1)^2(X-3)$, il n'y a que deux expressions possibles pour π_M : $\pi_M = (X-1)(X-3)$ ou $\pi_M = (X-1)^2(X-3)$
Il suffit alors de calculer $(M-I_n)\,(M-3I_n)$ pour pouvoir conclure.

Proposition 63

1. Une matrice de $\mathcal{M}_n(\mathbb{C})$ est nilpotente si, et seulement si, son polynôme caractéristique est X^n.
2. Soit E un $\mathbb{C}$-espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$.
   L'endomorphisme u est nilpotent si, et seulement si, son polynôme caractéristique est X^n.

Preuve : Supposons que M est nilpotente, il existe $p \in \mathbb{N}^*$ tel que $M^p = 0_{\mathcal{M}_n(\mathbb{C})}$. Le polynôme X^p annule M
0 est donc la seule valeur propre possible de M.
Or M admet au moins un valeur propre (complexe), $\mathrm{Sp}(M) = \{0\}$ puis $\chi_M = X^n$.

Réciproquement, supposons que $\chi_M = X^n$.
D'après le théorème de Cayley-Hamilton, $M^n = 0_{\mathcal{M}_n(\mathbb{C})}$ donc M est nilpotente.
On retrouve le fait que l'indice de nilpotence est inférieure ou égale à n. □

Exercice C16 : [CCINP]
On considère un entier $n \geqslant 2$. Soit $\mathrm{A} \in \mathcal{M}_n(\mathbb{C})$ telle que $\mathrm{A}^n = \mathrm{I}_n$ et telle que la famille $\left(\mathrm{I}_n,\ \mathrm{A},\ \mathrm{A}^2, \ldots, \mathrm{A}^{n-1}\right)$ soit libre. Montrer que $\mathrm{tr}(\mathrm{A}) = 0$.

Exercice C17 : [Mines-Télécom]
Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice inversible.

1. Déterminer un polynôme P tel que $\deg(P) = n-1$ et $P(A) = A^{-1}$.
2. Décrire l'ensemble des $P \in \mathbb{R}[X]$ tels que $P(A) = A^{-1}$.

Exercice E18 :
Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $u \in \mathcal{L}(E)$. On suppose que F et G sont des supplémentaires de E stables par u. On note $v = u|_F$ l'endomorphisme induit par u sur F et $w = u|_G$ celui induit sur G. Pour un endomorphisme f, on note π_f son polynôme minimal et χ_f son polynôme caractéristique.

1. Justifier que χ_v et χ_w divisent χ_u et que π_v et π_w divisent π_u.
2. Montrer que π_u est le plus petit commun multiple de π_v et π_w.

9.9 Polynômes annulateurs et réduction

9.9.1 Lemme des noyaux

Théorème 64 (Lemme de décomposition des noyaux)

Soit E un $\mathbb{K}$-espace vectoriel. Soit $u \in \mathcal{L}(E)$.
Si P_1 et P_2 sont deux polynômes premiers entre eux alors :

$$\text{Ker}\,(P_1P_2(u)) = \text{Ker}\,(P_1(u)) \oplus \text{Ker}\,(P_2(u))$$

Théorème 65 (Lemme de décomposition des noyaux)

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

Si $P_1, \dots, P_r$ sont des polynômes deux à deux premiers entre eux de produit égal à $P = \prod_{k=1}^{r} P_k$, alors :

$$\text{Ker}(P(u)) = \bigoplus_{k=1}^{r} \text{Ker}\,(P_k(u))$$

Corollaire 66

Soit E un $\mathbb{K}$-espace vectoriel. Soit $u \in \mathcal{L}(E)$.
Si $P_1, \dots, P_r$ sont des polynômes deux à deux premiers entre eux de produit P et si P annule $u \in \mathcal{L}(E)$,

$$E = \bigoplus_{i=1}^{r} \text{Ker}\,(P_i(u))$$

On peut de cette façon décomposer E en somme de sous-espaces stables par u.

9.9.2 Polynômes annulateurs et diagonalisation

Théorème 67

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.
Soit $u \in \mathcal{L}(E)$ de polynôme minimale π_u.
Les assertions suivantes sont équivalentes :

1. L'endomorphisme u est diagonalisable.
2. Il existe un polynôme scindé à racines simples qui annule u.
3. Le polynôme minimal de π_u est scindé à racines simples.

Remarque : Il se peut que le polynôme caractéristique ne soit pas à racines simples. Par exemple pour l'identité. On a $\pi_{\mathsf{Id}_E} = X - 1$ et $\chi_{\mathsf{Id}_E} = (X-1)^n$.

Preuve :
Montrons que 1) $\implies$ 2). On suppose que u est diagonalisable. Soit $\lambda_1, \dots, \lambda_r$ les valeurs propres deux à deux distinctes de u. On sait que :

$$E = \bigoplus_{k=1}^{r} \mathsf{Ker}(u - \lambda_k \mathsf{Id}_E)$$

Comme les polynômes $(X-\lambda_1),\dots,(X-\lambda_r)$ sont premiers entre eux deux à deux. Le lemme des noyaux donne :

$$E = \mathsf{Ker}\left((u-\lambda_1\mathsf{Id}_E)\circ\dots(u-\lambda_r\mathsf{Id}_E)\right)$$

Posons $P=\prod_{k=1}^{r}(X-\lambda_k)$ qui est scindé à racines simples. Alors $P(u)=0_{L(E)}$.

2) $\Rightarrow$ 3) On suppose qu'il existe un polynôme scindé à racines simples P qui annule u.
Par définition du polynôme minimal, $\pi_u \mid P$.
Donc π_u est scindé à racines simples.

3) $\Rightarrow$ 1) On suppose que π_u est scindé à racines simples. On pose :

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

On sait que $\lambda_1,\dots,\lambda_p$ sont les valeurs propres de u.
Le lemme de décomposition des noyaux donne :

$$E=\mathrm{Ker}\left(\pi_u(u)\right)=\bigoplus_{i=1}^{p}\mathrm{Ker}\left(u-\lambda_i\mathrm{id}_E\right)$$

Comme E est somme directe des sous-espaces propres de u, l'endomorphisme u est diagonalisable. □

Théorème 68

Soit $A\in M_n(\mathbb{K})$ de polynôme minimal π_A. Les assertions suivantes sont équivalentes :

1. La matrice A est diagonalisable.
2. Il existe un polynôme scindé à racines simples qui annule A.
3. Le polynôme minimal de A, π_A est scindé à racines simples.

Corollaire 69

Si u est diagonalisable, alors pour tout sous-espace vectoriel F non réduit à $\{0_E\}$ et stable par u, l'endomorphisme induit par u sur F est diagonalisable.

Preuve : On a vu que $\pi_{u_{|F}}$ divise π_u.
Comme u est diagonalisable, on sait que π_u est scindé à racines simples.
Donc $\pi_{u_{|F}}$ est aussi scindé à racines simples.
Finalement, $u_{|F}$ est diagonalisable. □

Exercice C19 : [CCINP]
Soient x un nombre réel et E_x l'ensemble des matrices $\mathrm{M}\in\mathcal{M}_n(\mathbb{R})$ vérifiant $\mathrm{M}^2+\mathrm{M}+x\mathrm{I}_n=0$.

1. Si $x\neq 0$, montrer qu'une matrice $M\in\mathrm{E}_x$ est inversible et exprimer son inverse. Quelles sont les matrices inversibles appartenant à E_0 ?
2. Pour $n=2$. Pour quelles valeurs de x tous les éléments de E_x sont ils diagonalisables dans $\mathcal{M}_n(\mathbb{R})$?
3. Toujours pour $n=2$. Déterminer l'ensemble T des traces des éléments de E_{-2}. Quel est son cardinal ?

Exercice C20 : [CCINP]
Soit $n\geqslant 2$ entier. On considère $\mathcal{M}_n(\mathbb{R})$ telle que $\mathrm{A}^2=\mathrm{I}_n$ et $\mathrm{A}\neq\pm\mathrm{I}_n$.

1. Montrer que $\mathrm{tr}(\mathrm{A})\equiv n[2]$.
2. Montrer que $|\,\mathrm{tr}(\mathrm{A})|\leqslant n-2$.

Exercice C21 : [Mines-Ponts]
Soit $A \in \mathcal{M}_n(\mathbb{R})$ telle que $A^3 + A^2 + A = 0$. Montrer que le rang de A est pair.

Exercice C22 : [Mines-Ponts]
Soit $A \in \mathrm{GL}_6(\mathbb{R})$ vérifiant $A^3 - 3A^2 + 2A = 0$ et $\mathrm{tr}(A) = 8$. Déterminer le polynôme caractéristique de A.

Exercice A23 : Donner le polynôme minimal des matrices suivantes et préciser si elles sont, ou non, diagonalisables dans $\mathcal{M}_3(\mathbb{R})$:

$$M = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 2 & 0 \\ 2 & 0 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Exercice C24 : [CCINP]
Soit $E = \mathcal{M}_2(\mathbb{R})$ et l'application φ définie sur E par

$$\varphi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

1. Montrer que φ est un endomorphisme de E.
2. Montrer que les valeurs propres sont de carré égal à 1.
3. L'endomorphisme φ est-il diagonalisable ? Quels sont les sous-espaces propres ?

Exercice C25 : [CCINP] Soit A, B et C trois matrices carrées d'ordre n à coefficients complexes. On suppose que :

$$A = B + C, \quad A^2 = B + 2C \quad \text{et } A^3 = B + 4C.$$

1. Trouver un polynôme annulateur de A et en déduire que A est diagonalisable.
2. Montrer que B et C sont diagonalisables.

Exercice E26 : On considère un entier $n \geqslant 2$. Soit l'endomorphisme

$$u : \begin{cases} \mathcal{M}_n(\mathbb{R}) \longrightarrow \mathcal{M}_n(\mathbb{R}) \\ \mathrm{M} \longmapsto \mathrm{M} + \mathrm{tr}(\mathrm{M})\mathrm{I}_n \end{cases}$$

1. Déterminer un polynôme annulateur de u de degré 2 .
2. u est-il diagonalisable ?
3. Déterminer le polynôme minimal et le polynôme caractéristique de u.

9.9.3 Réduction des endomorphismes annulés par un polynôme scindé

Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie n. Soit $u \in L(E)$. Rappelons tout d'abord que : u est trigonalisable si, et seulement si χ_u est scindé sur $\mathbb{K}$.
Supposons pour cela χ_u scindé sous la forme :

$$\chi_u = (X - \lambda_1)^{m_1} \times \cdots \times (X - \lambda_r)^{m_r}$$

où $\lambda_1, \ldots, \lambda_r$ sont les r valeurs propres deux à deux distinctes de u.
Les facteurs $(X - \lambda_i)^{m_i}$ étant deux à deux premiers entre eux.
Le lemme des noyaux et le théorème de Cayley-Hamilton assurent que :

$$E = \operatorname{Ker}\left((u - \lambda_1 \mathrm{id}_E)^{m_1}\right) \oplus \cdots \oplus \operatorname{Ker}\left((u - \lambda_r \mathrm{id}_E)^{m_r}\right)$$

Nous venons ici de construire une décomposition de E en somme directe de sous-espaces stables par u. Cette décomposition permet de trigonaliser u de manière plus précise.

Définition 70 (Sous-espace caractéristique)

Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie n.
Soit $u \in \mathcal{L}(E)$ et $\lambda \in \mathrm{Sp}(u)$.
On appelle sous-espace caractéristique de u associé à la valeur propre λ le sous-espace $\operatorname{Ker}\left((u - \lambda \mathrm{id}_E)^m\right)$ où m représente l'ordre de multiplicité de la valeur propre λ dans χ_u.
On notera par la suite F_λ ce sous-espace caractéristique.

Proposition 71 (Dimension du sous-espace caractéristique)

Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie n.
Soient $u \in \mathcal{L}(E)$ et $\lambda \in \mathrm{Sp}(u)$. Notons m l'ordre de multiplicité de λ dans χ_u. Alors

$$\dim \operatorname{Ker}\left((u - \lambda \mathsf{Id}_E)^m\right) = m.$$

Preuve : Écrivons le polynôme caractéristique χ_u sous la forme :

$$\chi_u = (X - \lambda)^m Q$$

où $(X - \lambda)^m \wedge Q = 1$.
Le lemme des noyaux assure que :

$$\mathsf{Ker}(\chi_u(u)) = \mathsf{Ker}((u - \lambda \mathsf{Id}_E)) \oplus \mathsf{Ker}\, Q(u).$$

Le théorème de Cayley-Hamilton permet d'obtenir $\mathsf{Ker}(\chi_u(u)) = \mathsf{Ker}(0_{L(E)}) = E$. Ainsi :

$$E = F_\lambda \oplus \operatorname{Ker}(Q(u))$$

Notons respectivement v et w les endomorphismes induits par u sur les sous-espaces stables F_λ et $\operatorname{Ker}(Q(u))$.
Notons $p = \dim \operatorname{Ker}\left((u - \lambda\, \mathrm{id}_E)^m\right)$.

1. Remarquons que pour tout $x \in F_\lambda$,

   $$(v - \lambda \mathsf{Id}_{F_\lambda})^m(x) = (u - \lambda \mathsf{Id}_{E_\lambda})^m(x) = 0_E$$

   On en déduit que le polynôme $(X - \lambda)^m$ annule v.
   Le scalaire λ est la seule valeur propre de v. Ainsi, $\chi_v = (X - \lambda)^p$.
2. Le scalaire λ n'est pas racine de Q. Or Q annule w, λ n'est pas donc pas racine de χ_w.

$$\chi_u = (X - \lambda)^m Q = \chi_v \cdot \chi_w = (X - \lambda)^p \cdot \chi_w$$

avec $\chi_w(\lambda) \neq 0$. Par définition de la multiplicité de la racine λ dans le polynôme χ_u,

$$m = p.$$

□

Proposition 72

Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie n.
Soit $u \in \mathcal{L}(E)$. On suppose que χ_u est scindé. Alors, en notant $\lambda_1, \ldots, \lambda_r$ les r valeurs propres deux à deux distinctes de u, en écrivant :

$$\chi_u = \prod_{i=1}^{r} (X - \lambda_i)^{m_i} \quad \text{et} \quad \pi_u = \prod_{i=1}^{r} (X - \lambda_i)^{d_i}$$

On a alors l'égalité :

$$\forall i \in [\![1, r]\!], \quad F_{\lambda_i} = \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{m_i}\right) = \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{d_i}\right)$$

Preuve : Appliquons le lemme des noyaux aux polynômes annulateurs χ_u et π_u de l'endomorphisme u :

$$E = \bigoplus_{i=1}^{r} \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{m_i}\right) = \bigoplus_{i=1}^{r} \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{d_i}\right)$$

Or pour tout $i \in [\![1, r]\!]$,

$$\operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{d_i}\right) \subset \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{m_i}\right).$$

Ainsi pour tout $i \in [\![1, r]\!]$,

$$\dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{d_i}\right) \leqslant \dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{m_i}\right)$$

D'autre part, en prenant les dimensions des sommes directes :

$$\sum_{i=1}^{r} \dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{m_i}\right) = \sum_{i=1}^{r} \dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{d_i}\right).$$

$$\sum_{i=1}^{r} \underbrace{\left(\dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{m_i}\right) - \dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{d_i}\right)\right)}_{\geqslant 0} = 0$$

On en déduit que pour tout $i \in [\![1, r]\!]$,

$$\dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{d_i}\right) - \dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{m_i}\right) = 0$$

$$\dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{d_i}\right) = \dim \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{m_i}\right)$$

En conclusion pour tout $i \in [\![1, r]\!]$,

$$\operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{d_i}\right) = \operatorname{Ker}\left((u - \lambda_i \operatorname{id}_E)^{m_i}\right).$$

□

Théorème 73

Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie n.
Soit $u \in \mathcal{L}(E)$.
On suppose qu'il existe un polynôme scindé annulant u, alors l'espace vectoriel E est la somme directe de sous-espaces stables par u sur chacun desquels u induit la somme d'une homothétie et d'un endomorphisme nilpotent.

Théorème 74

Soit $M \in \mathcal{M}_n(\mathbb{K})$.
On suppose qu'il existe un polynôme scindé annulant M, alors M est semblable à une matrice de la forme :

$$\left(\begin{array}{c|c|c}
\begin{matrix} \lambda_1 & * & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & \lambda_1 \end{matrix} & & \\
\hline
 & \ddots & \\
\hline
 & & \begin{matrix} \lambda_r & * & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & \lambda_r \end{matrix}
\end{array}\right).$$

Preuve : En reprenant les notations et résultats précédents, on sait que :

$$E = \bigoplus_{i=1}^{r} \operatorname{Ker}\left((u - \lambda_i \mathrm{id}_E)^{m_i}\right) = \bigoplus_{i=1}^{r} F_i$$

Chaque sous-espace F_i est de dimension $m_i \in \mathbb{N}^*$.
Notons u_i l'endomorphisme induit par u sur F_i.
Rappelons que $P_i = (X - \lambda_i)^{m_i}$ annule u_i.
Comme λ_i est la seule racine de P_i, c'est l'unique valeur propre de u_i.
Posons

$$n_i = u_i - \lambda_i \mathrm{id}_{F_i}$$

On remarque que n_i est nilpotent. En effet, pour tout $x \in F_i$,

$$n_i^{m_i}(x) = (u - \lambda_i \mathrm{id}_E)^{m_i}(x) = 0_E$$

Ainsi, $n_i^{m_i} = 0_{\mathcal{L}(F_i)}$.

□

Exercice E27 :
Soient u et v deux endomorphismes diagonalisables d'un $\mathbb{K}$-espace vectoriel de dimension finie E tels que $u \circ v = v \circ u$. Montrer que u et v diagonalisent dans une base commune.

Exercice E28 :
Soient u et v deux endomorphismes trigonalisables d'un $\mathbb{K}$-espace vectoriel E de dimension finie tels que $u \circ v = v \circ u$. Montrer que u et v trigonalisent dans une base commune.

Exercice C29 : [Mines-Télécom]
Soit $A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$.

1. A est-elle diagonalisable ? Donner ses valeurs propres complexes et déterminer une matrice D diagonable semblable à A.
2. Soit $\mathrm{M} \in \mathcal{M}_3(\mathbb{R})$ non nulle telle que $\mathrm{M}^3 + \mathrm{M} = 0$. Montrer que M est semblable à D.
3. A et M sont-elles semblables dans $\mathcal{M}_3(\mathbb{C})$? $\mathcal{M}_3(\mathbb{R})$?

Exercice C30 : [CCINP]
Soit E un espace vectoriel de dimension finie et p un projecteur de E. Pour tout $u \in \mathcal{L}(E)$, on pose :

$$\Phi(u) = \frac{1}{2}(p \circ u + u \circ p).$$

1. Montrer que Φ est un endomorphisme de l'espace $\mathcal{L}(E)$.
2. Φ est-il diagonalisable ?
3. Préciser les valeurs propres de Φ (on distinguera les cas particuliers $p = \mathrm{Id}_E, p = 0$).

Exercice C31 : [CCINP]

Soient $\mathrm{A} \in \mathcal{M}_n(\mathbb{R})$ et $\mathrm{B} = \begin{pmatrix} \mathrm{A} & \mathrm{A} \\ 0 & 0 \end{pmatrix} \in \mathcal{M}_{2n}(\mathbb{R})$.

1. Donner le rang de B en fonction du rang de A.
2. Montrer que, pour tout $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$,

$$\mathrm{P}(\mathrm{B}) = \begin{pmatrix} \mathrm{P}(\mathrm{A}) & \mathrm{P}(\mathrm{A}) \\ 0 & 0 \end{pmatrix} + \mathrm{P}(0) \begin{pmatrix} 0 & -\mathrm{I}_n \\ 0 & \mathrm{I}_n \end{pmatrix}$$

3. On suppose que A est diagonalisable. Montrer que B l'est aussi, et donner ses valeurs propres.