Pour ji : 25.2, 25.12, 24.14

Compléments sur les anneaux

3 Algèbre

3.1 Définition

Définition. Soit $\mathbb{K}$ un corps. On dit que $(A, +, \times, \cdot)$ est une **algèbre sur** $\mathbb{K}$, ou $\mathbb{K}$-algèbre, lorsque :

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

L'algèbre est **commutative** si $\times$ l'est, **intègre** si l'anneau $(A, +, \times)$ l'est, **de dimension finie** si l'espace vectoriel $(A, +, \cdot)$ l'est.

3.2 Exemples de référence

Exemple.

- $\mathbb{K}^n$, muni de sa structure produit, est une algèbre sur $\mathbb{K}$.
- $\mathbb{K}[X]$, muni de ses lois usuelles, est une algèbre.
- $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ est une algèbre.
- Pour E espace vectoriel sur $\mathbb{K}$, $(\mathcal{L}(E), +, \circ, \cdot)$ est une algèbre.
- Pour X ensemble quelconque, $\mathcal{F}(X, \mathbb{K}) = \mathbb{K}^X$, muni de ses opérations usuelles, est une algèbre.

$$\varphi : \mathcal{L}(E) \longrightarrow \mathcal{M}_n(\mathbb{K})$$
$$u \longmapsto \mathrm{Mat}(u, \mathcal{B})$$

3.3 Sous-algèbre

Définition. Soit $(A, +, \times, \cdot)$ une algèbre. Alors B est une **sous-algèbre** de A si et seulement si :

- B est un sous-anneau de $(A, +, \times)$
- B est un sous-espace vectoriel de $(A, +, \cdot)$

Proposition. B est une sous-algèbre de $(A, +, \times, \cdot)$ lorsque :

- $B \subset A$ ~~$1_A \in B$ donc $B \neq \emptyset$~~
- ~~B stable par $+$~~
- ~~B stable par passage à l'opposé~~
- $1_A \in B$ donc $B \neq \emptyset$
- B stable par $\times$
- B stable par combinaisons linéaires

Exemple. L'ensemble $\mathcal{D}_n(\mathbb{K})$ des matrices diagonales est une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$.

Exemple. L'ensemble $\mathcal{T}_n^s(\mathbb{K})$ des matrices triangulaires supérieures est une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$.

stable par $\times$

(voir le lien avec les espaces stables

$\mathrm{Vect}(e_1)$

$\mathrm{Vect}(e_1, e_2)$

$\mathrm{Vect}(e_1, e_2, e_3)$ ...

3.4 Morphisme d'algèbre

Définition. Soit $(A, +, \times, \cdot), (B, +, \times, \cdot)$ deux algèbres sur $\mathbb{K}$ et $f : A \to B$. On dit que f est un **morphisme d'algèbres** lorsque :

- f est un morphismes d'anneaux
- f est linéaire

Remarque. *Pour vérifier que f est un morphisme d'algèbre, on vérifie que :*

- $f(\lambda a + \mu b) = \lambda f(a) + \mu f(b)$
- $f(a \times b) = f(a) \times f(b)$
- $f(1_A) = 1_B$

Exemple. Soit $t \in \mathbb{K}$ fixé. L'application $P \mapsto P(t)$ est un morphisme d'algèbres entre $\mathbb{K}[X]$ et $\mathbb{K}$ muni de leurs lois usuelles.

Remarque. *On pourrait définir noyau et image d'un morphisme d'algèbres $A \to B$. L'image est une sous-algèbre de B, le noyau est un sous-espace vectoriel et un idéal de A, mais pas en général une sous-algèbre.*

$\underline{t=1}$

$$\varphi : \mathbb{R}[X] \longrightarrow \mathbb{R}$$
$$P \longmapsto P(1)$$

$(\mathbb{R}[X], +, \times, \cdot)$ algèbre

$(\mathbb{R}, +, \times, \times)$ algèbre

φ morphisme d'algèbre ?

$$\varphi(\lambda P + \mu Q) = (\lambda P + \mu Q)(1)$$
$$= \lambda P(1) + \mu Q(1)$$
$$= \lambda \varphi(P) + \mu \varphi(Q)$$

$$\varphi(P \times Q) = (P \times Q)(1)$$
$$= P(1)\, Q(1)$$
$$= \varphi(P) \times \varphi(Q)$$

$\varphi(1_{\mathbb{R}[X]})$

neutre de X dans $\mathbb{R}[X]$

c'est $X^0 = 1$

$$\varphi(1) = X^0(1)$$
$$= 1$$

le neutre de $\times$ dans $\mathbb{R}$

donc φ morphisme d'algèbre.

Autre exemple : $\varphi : \mathcal{L}(E) \longrightarrow \mathcal{M}_n(\mathbb{R})$

$\mathcal{B}$ fixé. $\qquad u \longmapsto \mathrm{Mat}(u, \mathcal{B})$

$$\mathrm{Mat}(\lambda u + \mu v) = \lambda \,\mathrm{Mat}(u) + \mu \,\mathrm{Mat}(v)$$
$$\mathrm{Mat}(u \circ v) = \mathrm{Mat}(u) \times \mathrm{Mat}(v)$$
$$\mathrm{Mat}(\mathrm{Id}_E) = I_n$$

Polynômes d'endomorphisme, polynômes de matrice

1 Polynôme d'un endomorphisme

1.1 Définition

Définition. Si $u \in \mathcal{L}(E)$, et $P = p_d X^d + \cdots + p_1 X + p_0 \in \mathbb{K}[X]$, on définit le **polynôme de l'endomorphisme** u :

$$P(u) = p_d u^d + \cdots + p_1 u + p_0 \mathrm{Id}_E$$

C'est un endomorphisme de E.
On note $\mathbb{K}[u]$ l'ensemble des polynômes de l'endomorphisme u.
On dit qu'un endomorphisme v est un **polynôme de l'endomorphisme** u lorsque $v \in \mathbb{K}[u]$, i.e. lorsqu'il existe $P \in \mathbb{K}[X]$ tel que $v = P(u)$.

Remarque. *u^k désigne $\underbrace{u \circ \cdots \circ u}_{k \text{ fois}}$.*

$P(u)$ n'est pas de la fonction polynomiale associée à P évaluée en u.

Exemple. Avec $P = X^3 - 2X + 1$, $P(u) = u^3 - 2u + \mathrm{Id}_E$, et donc $P(u)(x) = u^3(x) - 2u(x) + x$.

Définition. On dit que P est **annulateur de** u lorsque $P(u) = 0_{\mathcal{L}(E)}$.

Vect $(X^3, X^2, X^1, \underbrace{X^0}_{1})$

$P = X^3 - 2X + 1X^0$ $\quad P(1)$

$P(u) = u^3 - 2u + 1u^0$

$= u^3 - 2u + \mathrm{Id}_E \in \mathcal{L}(E)$

$P(u) : E \longrightarrow E$

$x \longmapsto u^3(x) - 2u(x) + x$

$u(u(u(x))) - 2u(x) + x$

$\big(P(u)\big)(x)$

$P(u)(x)$

$\cancel{P(u(x))}$

$\cancel{(u(x))^3} - - -$

pas de x dans E

1.2 Morphisme d'algèbres $P \mapsto P(u)$

Théorème.

$(\mathbb{K}[X],+,\times,\cdot)$ $(\mathcal{L}(E),+,\circ,\cdot)$

Soit $u \in \mathcal{L}(E)$. On note :

$$\phi_u : \begin{array}{rcl} \mathbb{K}[X] & \to & \mathcal{L}(E) \\ P & \mapsto & P(u) \end{array}$$

- ϕ_u est un morphisme d'algèbres
- $\operatorname{Im} \phi_u = \mathbb{K}[u]$
- $\operatorname{Ker} \phi_u$ est un idéal de $\mathbb{K}[X]$

Preuve: Mque: $\overset{1}{*}$ $\phi_u(\lambda P + \mu Q) = \lambda \phi_u(P) + \mu \phi_u(Q)$

cf $\boxed{25.3}$ $\overset{2}{*}$ $\phi_u(P \times Q) = \phi_u(P) \circ \phi_u(Q)$ ← ⚠

$\overset{3}{*}$ $\phi_u(X^0) = Id_E$

$\overset{1}{*}$ Mque $(\lambda P + \mu Q)(u) = \lambda P(u) + \mu Q(u)$

avec $P = \sum_{k=0}^{\cancel{p}\ +\infty} a_k X^k$ $Q = \sum_{k=0}^{\cancel{q}\ +\infty} b_k X^k$

$\lambda P + \mu Q = \sum_{k=0}^{n} (\lambda a_k + \mu b_k) X^k$ où $n \geqslant p, q$.

$(\lambda P + \mu Q)(u) = \sum_{k=0}^{n} (\lambda a_k + \mu b_k) u^k$

$= \lambda \sum_{k=0}^{n} a_k u^k + \mu \sum_{k=0}^{n} b_k u^k$

(calcul dans l'ev $\mathcal{L}(E)$)

$= \lambda P(u) + \mu Q(u)$

$\overset{3}{*}$ $X^0(u) = Id_E$ par déf.

$\overset{2}{*}$ Mque $(P \times Q)(u) = P(u) \circ Q(u)$

$\cancel{PQ(u) = P(u) Q(u)}$

1er cas : P et Q sont des monômes.

$$(X^i \times X^j)(u) = (X^{i+j})(u)$$
$$= u^{i+j} \quad (\text{au sens de } \circ)$$
$$= u^i \circ u^j \quad (\text{dans } \mathcal{L}(E))$$
$$= \left(X^i(u)\right) \circ \left(X^j(u)\right)$$

2e cas : $P = X^i$, $Q = \sum_{j=0}^{q} b_j X^j$

$$\left(X^i \times Q\right)(u) = \left(\sum_{j=0}^{q} b_j X^{i+j}\right)(u)$$

$$= \sum_{j=0}^{q} b_j X^{i+j}(u) \quad \text{par } \tfrac{1}{*}$$

φ_u linéaire

$$= \sum_{j=0}^{q} b_j X^i(u) \circ X^j(u)$$

par 1er cas

$$= X^i(u) \circ \left(\sum_{j=0}^{q} b_j X^j(u)\right)$$

$$= X^i(u) \circ Q(u)$$

3e cas : $P = \sum_{i=0}^{p} a_i X^i$ et Q qcq

$$(P \times Q)(u) = \left(\sum_{i=0}^{p} a_i X^i Q\right)(u)$$

$$= \sum_{i=0}^{p} a_i \left(X^i Q\right)(u) \quad \text{par } \frac{1}{*}$$

$$= \sum_{i=0}^{n} a_i \, X^i(u) \circ Q(u) \quad \text{par } 2^e \text{ cas}$$

$$= \left(\sum_{i=0}^{n} a_i \, u^i \right) \circ Q(u)$$

par calcul dans $\mathcal{L}(E)$

$$= P(u) \circ Q(u)$$

M2 avec $P = \sum_{k=0}^{+\infty} a_k X^k$ où $(a_k)_k$ à support fini

$Q = \sum_{k=0}^{+\infty} b_k X^k$ — $(b_k)_k$ ——

$$(P \times Q)(u) = \left(\sum_{n=0}^{+\infty} c_n X^n \right)(u)$$

avec $c_n = \sum_{k=0}^{n} a_k b_{n-k}$

$$= \sum_{n=0}^{+\infty} c_n u^n$$

$$P(u) \circ Q(u) = \Big(\underbrace{\sum_{i=0}^{+\infty}}_{\text{finie}} a_i u^i \Big) \circ \Big(\underbrace{\sum_{j=0}^{+\infty}}_{\text{finie}} b_j u^j \Big)$$

$$= \underbrace{\sum_{i=0}^{+\infty}}_{\text{finie}} \underbrace{\sum_{j=0}^{+\infty}}_{\text{finie}} a_i b_j \, u^{i+j}$$

paquets $i+j=n$

$$= \sum_{n=0}^{+\infty} \underbrace{\sum_{k=0}^{n} a_k b_{n-k}}_{c_n} u^n$$

$$= (P \times Q)(u)$$

Donc $\phi_u : P \longmapsto P(u)$ est un morphisme d'algèbres.

$\mathrm{Im}\, \phi_u = \mathbb{K}[u]$ ben oui ! par définition

$$\mathrm{Ker}\, \phi_u = \{ P \in \mathbb{K}[X] \text{ tq } P(u) = 0_{\mathcal{L}(E)} \}$$

$$= \{ \text{polynômes annulateurs de } u \}$$

idéal de $\mathbb{K}[X]$

car noyau d'un morphisme d'anneaux.

Exemple. Comme $P = X^3 - 2X + 1 = (X-1)(X^2+X-1)$, par le morphisme ϕ_u, on déduit $u^3 - 2u + \mathrm{Id}_E = (u - \mathrm{Id}_E) \circ (u^2 + u - \mathrm{Id}_E)$.

$$u^3 - 2u + 2\mathrm{Id}_E = P(u)$$

$$= \left((X-1) \times (X^2 + X - 1) \right)(u)$$

$$= (X-1)(u) \circ (X^2 + X - 1)(u)$$

$$= (u - \mathrm{Id}_E) \circ (u^2 + u - \mathrm{Id}_E)$$

Proposition.

$$\begin{aligned}\mathbb{K}[u] &= \{P(u),\ P \in \mathbb{K}[X]\} \\ &= \mathrm{Vect}\left((u^n)_{n\in\mathbb{N}}\right)\end{aligned}$$

$\mathbb{K}[u]$ est une sous-algèbre commutative de $\mathcal{L}(E)$.

car $\mathbb{K}[u] = \mathrm{Im}\, \phi_u$

$= \mathrm{Vect}\left(\phi_u(1), \phi(X), \dots, \phi_u(X^k), \dots\right)$

Règles de calcul. Pour P, Q polynômes, $u \in \mathcal{L}(E)$ et $\lambda, \mu \in \mathbb{K}$:

$$(\lambda P + \mu Q)(u) = \lambda P(u) + \mu Q(u)$$
$$(PQ)(u) = P(u) \circ Q(u)$$
$$P(u) \text{ et } Q(u) \text{ commutent}$$
$$1(u) = \mathrm{Id}_E$$

X^0

$$\begin{aligned} P(u) \circ Q(u) &= (P \times Q)(u) \\ &= (Q \times P)(u) \quad \text{car } \mathbb{K}[X] \text{ est commutatif.} \\ &= Q(u) \circ P(u) \end{aligned}$$

$\mathbb{K}[u]$ sous-algèbre commutative.

1.3 Polynôme minimal d'un endomorphisme d'un espace de dimension finie

Définition. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, et $u \in \mathcal{L}(E)$. Le morphisme :

$$\begin{array}{rcl} \phi_u : \mathbb{K}[X] & \to & \mathcal{L}(E) \\ P & \mapsto & P(u) \end{array}$$

n'est pas injectif. $\operatorname{Ker} \phi_u$ est un idéal non nul de $(\mathbb{K}[X], +, \times)$, appelé **idéal des polynômes annulateurs de** u. Il existe un unique polynôme unitaire, noté π_u et appelé **polynôme minimal de** u, tel que :

$$\operatorname{Ker} \phi_u = (\pi_u) = \{\pi_u Q,\ Q \in \mathbb{K}[X]\}$$

Remarque. *On peut aussi trouver la notation μ_u pour le polynôme minimal de u.*

$n = \dim E$

la famille $(1, X, X^2, \dots, X^{n^2})$ libre dans $\mathbb{K}[X]$

$(\phi_u(1), \phi_u(X), \dots, \phi_u(X^{n^2}))$ famille

de $\mathbb{K}[u]$ à n^2+1 éléments dans $\mathcal{L}(E)$

de dimension n^2

donc cette famille est liée !

$\exists\, a_0, \dots, a_{n^2}$ non tous nuls tq

$$a_0 \phi_u(1) + a_1 \phi_u(X) + \dots + a_{n^2} \phi_u(X^{n^2}) = 0$$

$$\| $$

$$a_0 \mathrm{Id}_E + a_1 u + \dots + a_n u^{n^2}$$

$$\| $$

$$P(u)$$

où $P = a_0 + a_1 X + \dots + a_{n^2} X^{n^2}$

$\in \operatorname{Ker} \phi_u$ et $P \neq 0$

Proposition. Pour $u \in \mathcal{L}(E)$ où E est de dimension finie :

$$Q(u) = 0 \iff \pi_u \mid Q$$

π_u est le polynôme unitaire de plus petit degré qui annule u.

Remarque. *Si E n'est pas de dimension finie et $u \in \mathcal{L}(E)$, alors u peut avoir un polynôme minimal, ou pas.*

on peut avoir $\operatorname{Ker} \phi_u = \{0_{\mathbb{K}[X]}\}$.

Exemple. Déterminer le polynôme minimal d'un projecteur, i.e. un endomorphisme p tel que $p \circ p = p$.

Oh! $Q = X^2 - X$ annule p

car $Q(p) = p^2 - p = 0$

$\Pi_p \mid Q$ donc $\Pi_p = X$ ou $(X-1)$ ou $X^2 - X$

- Si p projecteur non trivial, $p \neq 0_{\mathcal{L}(E)}$ et $p \neq \mathrm{Id}_E$

donc X et $(X-1)$ ne sont pas annulateurs

de p donc $\boxed{\Pi_p = X^2 - X} = X(X-1)$ racines $0, 1$

- Si $p = 0$ ou $p = \mathrm{Id}_E$, p est un projecteur (bof...)

$\Pi_0 = 1$

cf après

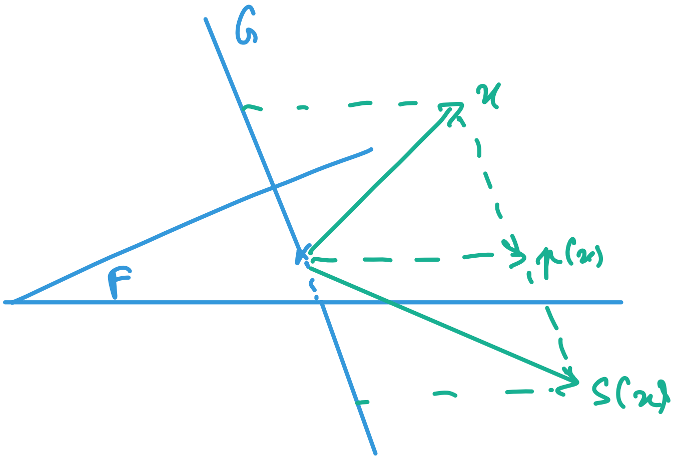
Exemple. Déterminer le polynôme minimal d'une homothétie $\lambda \mathrm{Id}_E$.

Oh! $P = X - \lambda = X - \lambda X^0$

est annulateur de $\lambda \mathrm{Id}_E$

donc $\Pi_{\lambda \mathrm{Id}_E} = X - \lambda$

Exemple. Déterminer le polynôme minimal d'une symétrie, i.e. un endomorphisme s tel que $s \circ s = \mathrm{Id}_E$.



On suppose F et G $\neq \{0_E\}$

sinon $s = \mathrm{Id}_E$

ou $s = -\mathrm{Id}_E$

$F \oplus G = E$

$s \circ s = \mathrm{Id}_E$ donc $X^2 - 1$ annule s

donc $\pi_s \mid X^2 - 1 = (X-1)(X+1)$

donc $\pi_s = X - 1$ ou $X+1$ ou $X^2 - 1$

on a exclu $s = \mathrm{Id}_E$ et $s = -\mathrm{Id}_E$

donc $\pi_s = X^2 - 1 = (X-1)(X+1)$ racines ± 1

Exemple. On considère $D : P \mapsto P'$ dans $\mathcal{L}(\mathbb{K}[X])$. Montrer que D n'admet pas de polynôme minimal.

$E = \mathbb{K}[X]$

On suppose $\exists\, Q \neq 0_{\mathbb{K}[X]}$ annulateur de D.

on note $Q = \sum_{k=0}^{q} a_k X^k$ les a_k non tous nuls

$$a_0 \mathrm{Id} + a_1 D + \dots + a_q D^q = Q(D) = 0_{\mathcal{L}(\mathbb{K}[X])}$$

ie $\forall P \in \mathbb{K}[X]$

$$a_0 P + a_1 P' + \dots + a_q P^{(q)} = 0_{\mathbb{K}[X]}$$

En particulier avec $P = X^q$

or $(P, P', \dots, P^{(q)})$ est échelonnée donc

libre, donc $a_0 = \dots = a_q = 0$

Contradiction.

1.4 Base de $\mathbb{K}[u]$

Théorème.

Soit $u \in \mathcal{L}(E)$ admettant un polynôme minimal π_u, et on note $d = \deg(\pi_u)$. Alors $(u^k)_{0 \leqslant k \leqslant d-1}$ est une base de $\mathbb{K}[u]$.

Remarque.

- *Dans le cas du théorème,* $\dim \mathbb{K}[u] = \deg \pi_u$.
- ϕ_u : $P \mapsto P(u)$ *induit dans le cas du théorème un isomorphisme entre les espaces vectoriels* $(\mathbb{K}_d[X], +, \cdot)$ *et* $(\mathbb{K}[u], +, \cdot)$.
- *Si* u *n'admet pas de polynôme minimal, c'est-à-dire lorsque* ϕ_u *est injective,* ϕ_u *est un isomorphisme d'algèbres entre* $(\mathbb{K}[X], +, \times, \cdot)$ *et* $(\mathbb{K}[u], +, \circ, \cdot)$.

en particulier si E est de dim finie.

$$\mathbb{K}[u] = \mathrm{Vect}(\mathrm{Id}_E, u, \dots, u^{d-1})$$

(On savait $\mathbb{K}[u] = \mathrm{Vect}(\mathrm{Id}_E, u, \dots, u^{d-1}, \dots, u^4, \dots)$

Exemple : p projecteur non trivial

$\pi_p = X(X-1)$ de degré 2

Tout polynôme en p est CL de Id_E et p.

$$p^4 + 3p^2 + p - \mathrm{Id}_E \in \mathrm{Vect}(\mathrm{Id}_E, p)$$

Preuve :

Soit $P \in \mathbb{K}[X]$

Mque $P \in \mathrm{Vect}(\mathrm{Id}_E, u, \dots, u^{d-1})$

On effectue la div eucl. de P par Π_u

d'où Q, R tq $\begin{cases} P = \Pi_u Q + R \\ R \in \mathrm{Vect}(1, X, \dots, X^{d-1}) \end{cases}$

$\deg(R) < \deg(\Pi_u)$

$$\begin{aligned} P(u) &= (\Pi_u Q + R)(u) \\ &= (\Pi_u Q)(u) + R(u) \\ &= \underbrace{\Pi_u(u)}_{0_{\mathcal{L}(E)}} \circ Q(u) + R(u) \\ &= R(u) \\ &\in \mathrm{Vect}(\mathrm{Id}_E, u, \dots, u^{d-1}) \end{aligned}$$

$0_{\mathcal{L}(E)}$ car Π_u annulateur de u