EMINES — CPI2A (CLASS2030)

01
Algèbre engendrée

AUTEUR

Samy Youssoufine

DERNIÈRE MISE À JOUR

21 septembre 2026

DÉPÔT PRINCIPAL

maths2.txt.ma

LIEN MIROIR (SECOURS)

samy-y.github.io/maths-cpi2a

Table des matières

1 Notions de base 2

2 Morphismes d'algèbres et algèbres engendrées 5

3 Dimension de l'algèbre engendrée par un élément 8

4 Éléments inversibles de $\mathbb{K}[a]$ 13

1 Notions de base

Définition 1 **(Algèbre)**

$(E, +, \cdot, \times)$ est dite une $\mathbb{K}$-algèbre si :

1. $(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
2. $(E, +, \times)$ est un anneau.
3. L'application "produit" $f : E \times E \to E$ définie par $(x, y) \mapsto xy$ est bilinéaire. Après calculs, on obtient que pour tout $x, y \in E$ et $\lambda \in \mathbb{K}$:
   (a) $(\lambda x)y = \lambda(xy)$
   (b) $x(\lambda y) = \lambda(xy)$

Si l'anneau $(E, +, \times)$ est commutatif (resp. intègre), alors l'algèbre $(E, +, \cdot, \times)$ est dite commutative (resp. intègre).

Rappel 1

On dit que $(A, +, \times)$ est un anneau si :

1. $(A, +)$ est un groupe abélien/commutatif.
2. $\times$ est associative dans A et admet un élément neutre 1_A.
3. $\times$ est distributive (à gauche et à droite) par rapport à $+$, i.e. :

$$\begin{cases} \forall x, y, z \in A, & x(y + z) = xy + xz \\ \forall x, y, z \in A, & (x + y)z = xz + yz \end{cases}$$

Si la loi $\times$ est commutative, l'anneau est dit **commutatif**.

Attention !

Un anneau est par définition unitaire.

Méthode **(Justification de la simplification)**

Par définition, le produit est bilinéaire si et seulement si pour tous $x, y \in E$, les applications partielles $L_x : z \mapsto xz$ et $R_y : z \mapsto zy$ sont linéaires.

Or, l'additivité de ces applications partielles est déjà garantie par la structure d'anneau de $(E, +, \times)$ via la distributivité :

$$(x_1 + x_2)y = x_1y + x_2y \quad \text{et} \quad x(y_1 + y_2) = xy_1 + xy_2$$

Une application additive ($\forall x, y \in E, \varphi(x + y) = \varphi(x) + \varphi(y)$) entre espaces vectoriels étant linéaire si et seulement si elle est homogène ($\forall \lambda \in \mathbb{K}, \varphi(\lambda z) = \lambda\varphi(z)$), la bilinéarité se ramène strictement aux deux conditions d'homogénéité :

$$\forall (x, y) \in E^2, \quad \forall \lambda \in \mathbb{K}, \quad (\lambda x)y = \lambda(xy) = x(\lambda y)$$

Exemple 1

1. **Algèbre des matrices** : $(\mathcal{M}_n(\mathbb{K}), +, \cdot, \times)$ est une $\mathbb{K}$-algèbre non commutative et non intègre si $n \geq 2$. En effet, $E_{1,1} \times E_{1,2} = E_{1,2}$ mais $E_{1,2} \times E_{1,1} = 0$.
2. **Algèbre des endomorphismes** : $(\mathcal{L}(E), +, \cdot, \circ)$ est une $\mathbb{K}$-algèbre non commutative et non intègre si $\dim E \geq 2$. En effet, $\mathcal{L}(E)$ est isomorphe à $\mathcal{M}_n(\mathbb{K})$ avec $n = \dim E$. Son élément unité est l'application identité id_E.
3. **Algèbre des polynômes** : $(\mathbb{K}[X], +, \cdot, \times)$ est une $\mathbb{K}$-algèbre commutative et intègre. Son élément unité est le polynôme constant $1 \in \mathbb{K}[X]$. Utiliser la loi rond $\circ$ au lieu de $\times$ n'est pas possible parce que la distributivité n'est pas conservée ; les polynômes ne sont pas des applications linéaires, ce qui fait que $(\mathbb{K}[X], +, \circ)$ n'est pas un anneau, et donc $(\mathbb{K}[X], +, \cdot, \circ)$ n'est pas une algèbre.
4. **Algèbre des applications de I vers $\mathbb{R}$** : $(\mathbb{R}^I, +, \cdot, \times)$ est une $\mathbb{K}$-algèbre avec $x + y : t \mapsto x(t) + y(t)$ et $xy : t \mapsto x(t)y(t)$. Son élément unité est l'application $1_{\mathbb{R}^I} : t \mapsto 1$ de $I \to \mathbb{R}$. Il s'agit d'une algèbre commutative mais non intègre (même en se restreignant à des applications continues !). En effet, en posant $x(t) = t + |t|$ et $y(t) = t - |t|$ (non nulles), on trouve que $xy = t^2 - |t|^2 = 0$.

Définition 2 **(Sous-algèbre)**

Soit E une $\mathbb{K}$-algèbre.

S est dite **sous-algèbre** de E si S est un sous-espace vectoriel de E et un sous-anneau de E.

Rappel 2

Un sous-anneau S d'un anneau $(A, +, \times)$ est un sous-ensemble $S \subset A$ tel que :

1. S est non vide (il doit contenir au moins l'élément 1_A).
2. S est stable par addition et multiplication, c'est-à-dire :

$$\forall x, y \in S, \quad x + y \in S \text{ et } x \times y \in S$$

Propriété 1

S est une sous-algèbre de E si et seulement si :

1. $1_E \in S$
2. $\forall x, y \in S, \forall \lambda \in \mathbb{K}, \begin{cases} \lambda x + y \in S \\ xy \in S \end{cases}$

Démonstration. Le sens direct découle immédiatement de la définition d'une sous-algèbre unitaire. Réciproquement, supposons ces conditions vérifiées :

— Comme $1_E \in S$, la partie S est non vide. La stabilité par combinaisons linéaires ($\lambda x + y \in S$) en fait donc un sous-espace vectoriel de $(E, +, \cdot)$.

— Cette structure vectorielle garantit déjà la stabilité par soustraction (pour $\lambda = -1$), ce qui assure que $(S, +)$ est un sous-groupe additif. En y ajoutant la stabilité par produit ($xy \in S$) et la présence de l'unité ($1_E \in S$), S est également un sous-anneau de $(E, +, \times)$.

S hérite de la structure d'algèbre unitaire. □

Exemple 2

$T_n^s(\mathbb{K})$ (l'ensemble des matrices triangulaires supérieures) est une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$. En effet : $x \in T_n^s(\mathbb{K}) \iff \forall i > j, x_{i,j} = 0$. On peut alors retrouver les conditions de caractérisation d'une sous-algèbre :

1. I_n est diagonale donc triangulaire supérieure.
2. — Si $i > j$, on a $(xy)_{ij} = \sum_{k=1}^{n} x_{ik}y_{kj}$. Dans le cas où $i \leq k$ et $k \leq j$, on aura $i \leq j$ ce qui est absurde. Donc $\forall k \in [\![1, n]\!]$, on a $i > k$ ou $k > j$, c'est-à-dire $x_{ik} = 0$ ou $y_{kj} = 0$. Par suite, $x_{ik}y_{kj} = 0$ pour tout $k \in [\![1, n]\!]$ et donc $(xy)_{ij} = 0$ pour tout $i > j$.
   — Clairement, $\forall \lambda \in \mathbb{K}, \forall i > j, (\lambda x + y)_{ij} = \lambda x_{ij} + y_{ij} = 0$.
   — La stabilité est vérifiée et donc $xy \in T_n^s(\mathbb{K})$.

2 Morphismes d'algèbres et algèbres engendrées

Définition 3 **(Morphisme d'algèbres)**

Soient E et F deux $\mathbb{K}$-algèbres. Une application $f : E \to F$ est dite un morphisme d'algèbres si :

1. $\forall (x, y) \in E^2, \forall \lambda \in \mathbb{K}, f(\lambda x + y) = \lambda f(x) + f(y)$ et $f(x \times y) = f(x) \times f(y)$
2. $f(1_E) = 1_F$

Remarque

Si S est une sous-algèbre de E, alors $u(S)$ est une sous-algèbre de F, en particulier pour $S = E$. Alors $\mathrm{Im}(u) = u(E)$ est une sous-algèbre de F. En revanche, ce n'est pas vrai pour le noyau $\mathrm{Ker}(u)$, qui est un sous-espace vectoriel de E mais jamais un sous-anneau parce qu'il ne contient pas l'élément unité 1_E (car $f(1_E) = 1_F \neq 0$). Néanmoins, le noyau a une structure d'idéal de E ; il est absorbant car $\forall x \in E, \forall y \in \mathrm{Ker}(u), xy \in \mathrm{Ker}(u)$.

En résumé :

1. $\mathrm{Im}(u)$ est une sous-algèbre de F.
2. $\mathrm{Ker}(u)$ est un idéal de E. Il est bien bilatère, c'est-à-dire que $E\ \ker(u) \subset \ker(u), \ker(u)\ E \subset \ker(u)$ et $(\ker(u), +)$ est un sous-groupe de $(E, +)$.

Rappel 3

Un idéal I d'un anneau $(A, +, \times)$ est un sous-ensemble $I \subset A$ tel que :

1. I est un sous-groupe de $(A, +)$.
2. I est absorbant par rapport à la multiplication, c'est-à-dire :

$$\forall x \in A, \forall y \in I, \quad xy \in I \text{ et } yx \in I$$

Qu'on peut aussi écrire $AI \subset I$ et $IA \subset I$.

Exemple 3

Soit E une $\mathbb{K}$-algèbre, $a \in E$, et $f : \mathbb{K}[X] \to E$ l'application définie par $f(P) = P(a)$ avec $P(a) = \sum_{k=1}^{n} \lambda_k a^k + \lambda_0 \cdot 1_E$. Alors f est un morphisme d'algèbres. En effet, pour tout $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, on a :

1. $f(\lambda P + Q) = (\lambda P + Q)(a) = \lambda P(a) + Q(a) = \lambda f(P) + f(Q)$
2. $f(PQ) = (PQ)(a) = P(a)Q(a) = f(P)f(Q)$
3. $f(1_{\mathbb{K}[X]}) = 1_{\mathbb{K}[X]}(a) = 1_E$

En conséquence, $\mathrm{Im}(f) = \{P(a) \mid P \in \mathbb{K}[X]\}$ est une sous-algèbre de E engendrée par l'élément a. On la note $\mathbb{K}[a]$. Il s'agit aussi de la plus petite sous-algèbre de E contenant a.

Propriété 2

$\mathbb{K}[a] = \{P(a) \mid P \in \mathbb{K}[X]\}$ est la plus petite sous-algèbre de E contenant a.

Démonstration. L'ensemble $\mathbb{K}[a]$ est une sous-algèbre de E (image de $\mathbb{K}[X]$ par le morphisme d'éva-

luation) et contient $a = X(a)$.

Soit S une sous-algèbre de E contenant a. Comme S est un sous-anneau unitaire, $a^0 = 1_E \in S$, puis par stabilité sous le produit, $a^k \in S$ pour tout $k \in \mathbb{N}$. S étant également un sous-espace vectoriel, il est stable par combinaisons linéaires : pour tout $P = \sum_{k=0}^{n} \lambda_k X^k \in \mathbb{K}[X]$, on a $P(a) = \sum_{k=0}^{n} \lambda_k a^k \in S$.

On en déduit l'inclusion $\mathbb{K}[a] \subset S$, ce qui établit que $\mathbb{K}[a]$ est la plus petite sous-algèbre de E contenant a. □

Exemple 4

Soient $E = \mathcal{M}_2(\mathbb{R})$ et $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. On pose :

$$S = \left\{ \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \;\middle|\; (\alpha, \beta) \in \mathbb{R}^2 \right\} = \mathrm{Vect}\left(I_2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right)$$

Montrons que $\mathbb{R}[A] = S$.

1. Inclusion $\mathbb{R}[A] \subset S$: Le polynôme caractéristique de A donne la relation annulatrice :

$$A^2 - \mathrm{tr}(A)A + \det(A)I_2 = A^2 - 2A - 3I_2 = 0$$

Pour tout $n \in \mathbb{N}$, la division euclidienne de X^n par $P(X) = X^2 - 2X - 3 = (X+1)(X-3)$ s'écrit :

$$X^n = Q(X)P(X) + a_n X + b_n$$

En évaluant en $X = -1$ et $X = 3$, on obtient :

$$\begin{cases} (-1)^n = -a_n + b_n \\ 3^n = 3a_n + b_n \end{cases} \iff \begin{cases} a_n = \frac{1}{4}\left(3^n - (-1)^n\right) \\ b_n = \frac{1}{4}\left(3^n + 3(-1)^n\right) \end{cases}$$

Comme $P(A) = 0$, il vient :

$$A^n = a_n A + b_n I_2 = \begin{pmatrix} a_n + b_n & 2a_n \\ 2a_n & a_n + b_n \end{pmatrix} \in S$$

S étant un sous-espace vectoriel stable par combinaison linéaire, pour tout $Q \in \mathbb{R}[X]$, $Q(A) = \sum \lambda_k A^k \in S$. Donc $\mathbb{R}[A] \subset S$.

2. Inclusion $S \subset \mathbb{R}[A]$: Soit $M = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \in S$. On cherche $(x, y) \in \mathbb{R}^2$ tel que $M = xI_2 + yA$:

$$\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} x+y & 2y \\ 2y & x+y \end{pmatrix} \iff \begin{cases} y = \frac{\beta}{2} \\ x = \alpha - \frac{\beta}{2} \end{cases}$$

Le système admet toujours une solution, d'où $M \in \mathrm{Vect}(I_2, A) \subset \mathbb{R}[A]$, ce qui donne $S \subset \mathbb{R}[A]$.

On conclut que $\mathbb{R}[A] = S$.

Remarque **(Méthode alternative pour A^n via le binôme de Newton)**

En posant $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, on remarque que $B^2 = I_2$ et $A = I_2 + 2B$. Comme I_2 et B commutent,

la formule du binôme assure l'existence de scalaires (α_n, β_n) tels que :

$$A^n = (I_2 + 2B)^n = \alpha_n I_2 + \beta_n B = \begin{pmatrix} \alpha_n & \beta_n \\ \beta_n & \alpha_n \end{pmatrix} \in S$$

Dans l'exemple précédent, on peut simplifier les expressions de α_n et β_n trouvées. En effet, nous avons seulement utilisé le fait que la matrice $B^2 = I_2$. On peut aussi prendre $B = I_2$ pour que les calculs précédents donnent $A = I_2 + 2I_2 = 3I_2$ et au final obtenir $3^n I_2 = \alpha_n I_2 + \beta_n I_2 = (\alpha_n + \beta_n) I_2$. Par conséquent, on obtient $\alpha_n + \beta_n = 3^n$.

On pourrait aussi prendre la matrice $B = -I_2$ pour retrouver $B^2 = I_2$ et obtenir $(-1)^n I_2 = \alpha_n I_2 - \beta_n I_2 = (\alpha_n - \beta_n) I_2$. Par conséquent, on obtient $\alpha_n - \beta_n = (-1)^n$. En résolvant le système d'équations obtenu :

$$\begin{cases} \alpha_n + \beta_n = 3^n \\ \alpha_n - \beta_n = (-1)^n \end{cases}$$

On trouve $\alpha_n = \frac{3^n + (-1)^n}{2}$ et $\beta_n = \frac{3^n - (-1)^n}{2}$. Ces expressions peuvent être différentes selon la base (A, B) choisie, mais on retrouve la même expression pour A^n.

Rappel 4

Un idéal I de $\mathbb{K}[X]$ est soit nul soit engendré par un polynôme unitaire P de $\mathbb{K}[X]$. En effet, si $I \neq \{0\}$, on peut choisir un polynôme $P \in I$ de degré minimal (via double-inclusion dont un sens est démontré par division euclidienne) pour montrer que $I = P_0 \mathbb{K}[X]$.

3 Dimension de l'algèbre engendrée par un élément

Propriété 3 **(Étude de dimension)**

Soit $a \in E$. L'ensemble $I_a = \{P \in \mathbb{K}[X] \mid P(a) = 0\}$ est un idéal de $\mathbb{K}[X]$, appelé l'idéal annulateur de a. Deux cas disjoints se présentent :

1. Si $I_a = \{0\}$, le morphisme d'évaluation induit un isomorphisme $\mathbb{K}[X] \simeq \mathbb{K}[a]$. La famille $(a^k)_{k\in\mathbb{N}}$ est une base de $\mathbb{K}[a]$ et $\dim(\mathbb{K}[a]) = \infty$.
2. Si $I_a \neq \{0\}$, il existe un unique polynôme unitaire $\pi_a \in \mathbb{K}[X]$, appelé polynôme minimal de a, tel que :
$$I_a = \pi_a\mathbb{K}[X], \quad \text{c'est-à-dire} \quad P(a) = 0 \iff \pi_a \mid P$$
En posant $d = \deg(\pi_a)$, la famille $(1_E, a, a^2, \dots, a^{d-1})$ est une base de $\mathbb{K}[a]$, et $\dim(\mathbb{K}[a]) = d$.

Démonstration. Considérons le morphisme d'algèbres $f : \mathbb{K}[X] \to \mathbb{K}[a]$ défini par $P \mapsto P(a)$, surjectif par définition, de noyau $\ker(f) = I_a$.

1. Cas $I_a = \{0\}$: L'application f est injective, donc est un isomorphisme d'espaces vectoriels. L'image de la base canonique $(X^k)_{k\in\mathbb{N}}$ de $\mathbb{K}[X]$ par cet isomorphisme est $(f(X^k))_{k\in\mathbb{N}} = (a^k)_{k\in\mathbb{N}}$, qui constitue ainsi une base de $\mathbb{K}[a]$. En particulier, $\dim(\mathbb{K}[a]) = \infty$.

2. Cas $I_a \neq \{0\}$: L'anneau $\mathbb{K}[X]$ étant principal, l'idéal non nul I_a admet un unique générateur unitaire noté π_a, de degré minimal $d = \deg(\pi_a) \geq 1$. Montrons que $\mathcal{B} = (1_E, a, \dots, a^{d-1})$ est une base de $\mathbb{K}[a]$:

- **Liberté :** Soit $(\lambda_0, \dots, \lambda_{d-1}) \in \mathbb{K}^d$ tel que $\sum_{k=0}^{d-1} \lambda_k a^k = 0$. Le polynôme $Q = \sum_{k=0}^{d-1} \lambda_k X^k$ vérifie $Q(a) = 0$, donc $Q \in I_a$, d'où $\pi_a \mid Q$. Or, $\deg(Q) \leq d - 1 < \deg(\pi_a)$, ce qui impose $Q = 0$, et par identification $\lambda_0 = \cdots = \lambda_{d-1} = 0$. La famille est libre.
- **Génération :** Pour tout $x \in \mathbb{K}[a]$, il existe $P \in \mathbb{K}[X]$ tel que $x = P(a)$. La division euclidienne de P par π_a donne $P = Q\pi_a + R$ avec $\deg(R) < d$. Comme $\pi_a(a) = 0$, on en déduit :
$$x = P(a) = Q(a)\pi_a(a) + R(a) = R(a) \in \mathrm{Vect}(1_E, a, \dots, a^{d-1})$$

La famille $(1_E, a, \dots, a^{d-1})$ est libre et génératrice, c'est donc une base de $\mathbb{K}[a]$, d'où $\dim(\mathbb{K}[a]) = d$. □

Exemple 5

Soit $A = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})$ avec $n \geq 2$.

Un calcul direct donne $A^2 = nA$, c'est-à-dire $A^2 - nA = 0$. Le polynôme $P(X) = X(X - n)$ est donc annulateur de A, d'où :

$$\pi_A \mid X(X-n) \implies \pi_A \in \{1,\ X,\ X-n,\ X(X-n)\}$$

On élimine les diviseurs stricts :

- $\pi_A \neq 1$ car $1(A) = I_n \neq 0$.
- $\pi_A \neq X$ car $A \neq 0$.

— $\pi_A \neq X - n$ car $A \neq nI_n$ (pour $n \geq 2$).

On en déduit que $\pi_A = X^2 - nX$. Par conséquent, $\deg(\pi_A) = 2$, la famille (I_n, A) forme une base de $\mathbb{R}[A]$ et $\dim(\mathbb{R}[A]) = 2$.

Exercice 1

Soit $u \in \mathcal{L}(E)$ avec $2 \leq \dim(E) < \infty$ tel que $\mathrm{rg}(u) = 1$. Montrer que $\Pi_u = X^2 - \mathrm{Tr}(u)X$.

Correction **(Exercice 1)**

Comme $\mathrm{rg}(u) = 1$, $\dim(\ker(u)) = \dim(E) - 1$ par théorème du rang. Pour simplifier, on notera $\dim(E) = n$. On a donc $\dim(\ker(u)) = n - 1$. On construit alors la base de $\ker(u)$ suivante : $\mathcal{B}_{\ker(u)} = (e_1, \ldots, e_{n-1})$. On complète cette base en une base de E en ajoutant un vecteur $e_n \notin \ker(u)$, ce qui donne $\mathcal{B}_E = (e_1, \ldots, e_{n-1}, e_n)$ (par théorème de la base incomplète). On a alors $u(e_n) \neq 0$ et $u(e_i) = 0$ pour tout $i \in [\![1, n-1]\!]$. On peut donc écrire la matrice $[u]_{\mathcal{B}_E}$ de u dans la base $\mathcal{B}_E$:

$$[u]_{\mathcal{B}_E} = \begin{pmatrix} 0 & 0 & \ldots & 0 & \alpha_1 \\ 0 & 0 & \ldots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & \alpha_{n-1} \\ 0 & 0 & \ldots & 0 & \alpha_n \end{pmatrix}$$

avec $\alpha_n \neq 0$ car $u(e_n) \neq 0$. On calcule alors la trace de u :

$$\mathrm{Tr}(u) = \sum_{i=1}^{n} [u]_{\mathcal{B}_E}(i,i) = 0 + 0 + \cdots + 0 + \alpha_n = \alpha_n$$

On calcule ensuite u^2 :

$$[u^2]_{\mathcal{B}_E} = [u]_{\mathcal{B}_E}^2 = \begin{pmatrix} 0 & 0 & \ldots & 0 & \alpha_1 \\ 0 & 0 & \ldots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & \alpha_{n-1} \\ 0 & 0 & \ldots & 0 & \alpha_n \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & \ldots & 0 & \alpha_1\alpha_n \\ 0 & 0 & \ldots & 0 & \alpha_2\alpha_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & \alpha_{n-1}\alpha_n \\ 0 & 0 & \ldots & 0 & \alpha_n^2 \end{pmatrix}$$

On remarque que $[u^2]_{\mathcal{B}_E} = \alpha_n [u]_{\mathcal{B}_E}$, ce qui implique que $u^2 = \alpha_n u$. Comme $\alpha_n = \mathrm{Tr}(u)$, on obtient l'équation :

$$u^2 - \mathrm{Tr}(u)u = 0$$

Ainsi, le polynôme $X^2 - \mathrm{Tr}(u)X$ est un polynôme annulateur de u. Cela veut donc dire que Π_u, le polynôme minimal de u, divise $X^2 - \mathrm{Tr}(u)X$. On a donc $\Pi_u \in \{1, X, X - \mathrm{Tr}(u), X(X - \mathrm{Tr}(u))\}$. On élimine les choix suivants :

— $\Pi_u \neq 1$ car $1(u) = \mathrm{id}_E \neq 0$.
— $\Pi_u \neq X$ car $u \neq 0$.
— $\Pi_u \neq X - \mathrm{Tr}(u)$ car $u \neq \mathrm{Tr}(u)\mathrm{id}_E$ (cela implique que $\mathrm{Tr}(u) = 0$ et même que $u = 0$).

On en déduit que $\Pi_u = X^2 - \mathrm{Tr}(u)X$.

Remarque

Le degré d'un polynôme minimal π_a vaut 1 si et seulement si la famille $(1_E, a)$ est liée, c'est-à-dire si et seulement si a est un multiple scalaire de l'élément unité 1_E (homothétie).

Dans ce cas, le polynôme minimal est $\pi_a = X - \lambda$ avec $\lambda \in \mathbb{K}$ tel que $a = \lambda 1_E$.

Dans le cas contraire où $a \neq \lambda 1_E$ pour tout $\lambda \in \mathbb{K}$, le polynôme minimal π_a est de degré $d \geq 2$ et la famille $(1_E, a)$ est libre. On résout alors $a^2 = \lambda_0 1_E + \lambda_1 a$ pour voir si elle admet des solutions pour $\lambda_0, \lambda_1 \in \mathbb{K}$. Si c'est le cas, on obtient $\pi_a = X^2 - \lambda_1 X - \lambda_0$ et $\dim(\mathbb{K}[a]) = 2$. Sinon, on continue avec a^3 et ainsi de suite **jusqu'à trouver un polynôme annulateur minimal**.

En effet, il faut trouver le plus petit $d \geq 1$ tel que $a^d \in \mathrm{Vect}(1_E, a, \ldots, a^{d-1})$. Le polynôme minimal π_a est alors de degré d et la famille $(1_E, a, \ldots, a^{d-1})$ est une base de $\mathbb{K}[a]$, car $a^d = \sum_{i=0}^{d-1} \lambda_i a^i$ implique $\pi_a = X^d - \sum_{i=0}^{d-1} \lambda_i X^i$.

Exemple 6

Prenons $E = \mathcal{M}_3(\mathbb{R})$.

Soit $a = \begin{pmatrix} 2 & -1 & 2 \\ -1 & 2 & -2 \\ 1 & -1 & 3 \end{pmatrix}$. Calculons π_a.

On a $a \neq \lambda I_3$ pour tout $\lambda \in \mathbb{R}$, donc $\deg(\pi_a) \geq 2$. On calcule :

$$a^2 = \begin{pmatrix} 7 & -6 & 12 \\ -6 & 7 & -12 \\ 6 & -6 & 13 \end{pmatrix},$$

On cherche $\lambda_0, \lambda_1 \in \mathbb{R}$ tels que $a^2 = \lambda_1 a + \lambda_0 I_3$.

$$\lambda_1 a + \lambda_0 I_3 = \begin{pmatrix} 2\lambda_1 + \lambda_0 & -\lambda_1 & 2\lambda_1 \\ -\lambda_1 & 2\lambda_1 + \lambda_0 & -2\lambda_1 \\ \lambda_1 & -\lambda_1 & 3\lambda_1 + \lambda_0 \end{pmatrix}$$

En comparant les coefficients, on obtient le système :

$$\begin{cases} 7 = 2\lambda_1 + \lambda_0 \\ -6 = -\lambda_1 \\ 12 = 2\lambda_1 \\ -6 = -\lambda_1 \\ 7 = 2\lambda_1 + \lambda_0 \\ -12 = -2\lambda_1 \\ 6 = \lambda_1 \\ -6 = -\lambda_1 \\ 13 = 3\lambda_1 + \lambda_0 \end{cases}$$

Donc $\lambda_1 = 6$ et $\lambda_0 = -5$. Ainsi, $a^2 = 6a - 5I_3$, et le polynôme minimal est $\pi_a(X) = X^2 - 6X + 5$. La dimension de $\mathbb{R}[a]$ est donc 2, et une base est donnée par (I_3, a).

Remarque

Si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, alors on peut considérer que $\mathbb{L}$ est une $\mathbb{K}$-algèbre. En particulier, $\mathbb{C}$ est une $\mathbb{R}$-algèbre et $\mathbb{R}$ est une $\mathbb{Q}$-algèbre.

Rappel 5

On dit que $(\mathbb{L}, +, \times)$ est un corps si $(\mathbb{L}, +, \times)$ est un anneau et que $\forall x \in L \setminus \{0_\mathbb{L}\}$, x est inversible pour la multiplication.

Un sous-corps est un sous-ensemble $\mathbb{K} \subset \mathbb{L}$ qui est un sous-anneau de $\mathbb{L}$ et qui est stable par l'inverse (pour un élément non nul).

Exercice 2

Prenons $E = \mathbb{R}$ une $\mathbb{Q}$-algèbre (ce qui est possible car $\mathbb{Q}$ est un sous-anneau et un sous-espace vectoriel de $\mathbb{R}$)

Soit $a = \sqrt{2} + \sqrt{3}$.

Montrer que le polynôme minimal π_a existe et donner son expression.

Correction **(Exercice 2)**

On doit construire un polynôme dont les racines sont $\sqrt{2} + \sqrt{3}$ mais à coefficients rationnels. On a :

$$\begin{aligned} a = \sqrt{2} + \sqrt{3} &\implies (a - \sqrt{2})^2 = 3 \\ &\implies a^2 - 2a\sqrt{2} + 2 = 3 \\ &\implies a^2 - 1 = 2a\sqrt{2} \\ &\implies (a^2 - 1)^2 = 8a^2 \end{aligned}$$

On en déduit que le polynôme $P(X) = (X^2 - 1)^2 - 8X^2 = X^4 - 10X^2 + 1$ est annulateur de a.

On a $P \in \mathbb{Q}[X] \setminus \{0\}$ (et il est annulateur), donc π_a existe et $\pi_a \mid P$.

Vérifions pour le cas $\deg \pi_a = 1$. On vérifie si P admet des racines dans $\mathbb{Q}$. Si $\frac{p}{q}$ est une racine de P avec $p \wedge q = 1$, alors $p \mid a_0 = 1$ et $q \mid a_4$ (résultat démontré en TD), donc $p \mid 1$ et $q \mid 1$, ce qui implique que $\frac{p}{q} = \pm 1$. Or, $P(\pm 1) = 1 - 10 + 1 = -8 \neq 0$, donc P n'admet pas de racines rationnelles. Par conséquent, $\deg \pi_a \geq 2$.

Si $\pi_a = D_1 D_2$ et $\deg D_1 = 3$, alors D_1 admet une racine rationnelle $\frac{p}{q}$ avec $p \wedge q = 1$. Par le même raisonnement que précédemment, on obtient que $\frac{p}{q} = \pm 1$, ce qui est impossible car $P(\pm 1) \neq 0$. Donc $\deg D_1 \neq 3$ et $\deg \pi_a \neq 3$.

On en déduit que $\deg \pi_a \in \{2, 4\}$.

Supposons par absurde que $\deg \pi_a = 2$. Cela implique que :

$$\pi_a(X) = (X - a)(X - b)$$

avec $a = \sqrt{2} + \sqrt{3} \in \mathbb{R}$ et $b \in \mathbb{R}$.

On a aussi $P(-X) = P(X)$, donc $-a$ est racine de P. DOnc les racines de P sont $\sqrt{2} \pm \sqrt{3}$ et $-\sqrt{2} \pm \sqrt{3}$.

Dans le cas où $b = -a$: On a $\pi_a(X) = (X - a)(X + a) = X^2 - a^2$. Or, $a^2 = 5 + 2\sqrt{6} \notin \mathbb{Q}$, donc $\pi_a \notin \mathbb{Q}[X]$ ce qui est absurde. Donc $b \neq -a$. Donc $\pi_a \neq X^2 - a^2$

Dans le cas où $b = \sqrt{3} - \sqrt{2}$ **:** On a $\pi_a(X) = (X-a)(X-b) = X^2 - (a+b)X + ab$. Or, $a + b = 2\sqrt{3} \notin \mathbb{Q}$, donc $\pi_a \notin \mathbb{Q}[X]$ ce qui est absurde. Donc $b \neq \sqrt{3} - \sqrt{2}$.

Dans le cas où $b = \sqrt{2} - \sqrt{3}$ **:** On a $\pi_a(X) = (X-a)(X-b) = X^2 - (a+b)X + ab$. Or, $a + b = 2\sqrt{2} \notin \mathbb{Q}$, donc $\pi_a \notin \mathbb{Q}[X]$ ce qui est absurde. Donc $b \neq \sqrt{2} - \sqrt{3}$.

Donc $\pi_a \neq X^2 - (a+b)X + ab$ pour $b \in \{-a, \sqrt{3} - \sqrt{2}, \sqrt{2} - \sqrt{3}\}$.

On en déduit que $\deg \pi_a \neq 2$.

Donc $\pi_a = P = X^4 - 10X^2 + 1$.

Une base de $\mathbb{Q}[a]$ est donc donnée par $(1, a, a^2, a^3)$ et $\dim(\mathbb{Q}[a]) = 4$.

On peut aboutir aux mêmes résultats en généralisant pour un certain couple (r_1, r_2) tels que $r_1^2 = 2$ et $r_2^2 = 3$ et en considérant $a = r_1 + r_2$. On obtient le même polynôme minimal $\pi_a = X^4 - 10X^2 + 1$.

Note

La division euclidienne est conservée dans $\mathbb{Q}[X]$ et même dans n'importe quel corps $\mathbb{K}$ (pour justifier la division $\pi_a = D_1 D_2$).

4 Éléments inversibles de $\mathbb{K}[a]$

Propriété 4

Lorsque l'idéal I_a est réduit à $\{0\}$, les seuls éléments inversibles de $\mathbb{K}[a]$ sont les multiples scalaires de 1_E.

$$\mathbb{U}(\mathbb{K}[a]) = \{\lambda 1_E \mid \lambda \in \mathbb{K}^*\}$$

Démonstration. En posant $u : \mathbb{K}[X] \to \mathbb{K}[a]$ avec $P \mapsto P(a)$ un isomorphisme. Comme u est un isomorphisme de $\mathbb{K}[X] \to \mathbb{K}[a]$, $u(P) = P(a)$ est inversible si et seulement si le polynôme antécédent P est inversible dans $\mathbb{K}[X]$. Or, les seuls polynômes inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls. Donc $P(a)$ est inversible si et seulement si $P = \lambda \cdot 1_E$ avec $\lambda \in \mathbb{K}^*$, ce qui donne le résultat. □

Propriété 5

Dans le cas où $I_a = \pi_a \mathbb{K}[X]$ avec $\deg(\pi_a) = d \geq 1$, les propriétés suivantes sont équivalentes :

1. $P(a)$ est inversible dans E.
2. $P(a)$ est inversible dans $\mathbb{K}[a]$.
3. $P \wedge \pi_a = 1$.

Démonstration. On décompose la démonstration en trois implications : de 3 à 2, de 2 à 1 et de 1 à 3.

- **3** $\implies$ **2 :** Si $P \wedge \pi_a = 1$, il existe $U, V \in \mathbb{K}[X]$ tels que $UP + V\pi_a = 1$. En évaluant en a, on obtient $U(a)P(a) + V(a)\pi_a(a) = U(a)P(a) = 1_E$, donc $P(a)$ est inversible dans $\mathbb{K}[a]$.
- **2** $\implies$ **1 :** Si $P(a)$ est inversible dans $\mathbb{K}[a]$, il existe $Q(a) \in \mathbb{K}[a]$ tel que $P(a)Q(a) = 1_E$. Comme $\mathbb{K}[a] \subset E$, $P(a)$ est inversible dans E.
- **1** $\implies$ **3 :** Supposons $P(a)$ inversible dans E. Posons $D = P \wedge \pi_a$, unitaire. Il existe $P_1, P_2 \in \mathbb{K}[X]$ unitaires tels que :

  $$P = DP_1 \quad \text{et} \quad \pi_a = DP_2$$

  En évaluant en a, comme $\mathbb{K}[a]$ est commutatif :

  $$0 = \pi_a(a) = D(a)P_2(a) = P_2(a)D(a)$$

  On multiplie à droite par $P_1(a)$:

  $$P_2(a)\underbrace{D(a)P_1(a)}_{=P(a)} = 0 \implies P_2(a)P(a) = 0$$

  $P(a)$ étant inversible dans E, on multiplie à droite par son inverse $P(a)^{-1}$ (comme on peut poser $\exists y \in E$ tel que $P(a)y = 1_E$) :

  $$P_2(a) = 0$$

  Par minimalité de π_a, il vient $\pi_a \mid P_2$, c'est-à-dire $DP_2 \mid P_2$. Comme $P_2 \neq 0$, cela impose :

  $$\deg(D) + \deg(P_2) \leq \deg(P_2) \implies \deg(D) = 0$$

  D étant unitaire, $D = 1$, d'où $P \wedge \pi_a = 1$.

□

Exemple 7

Prenons $E = \mathcal{M}_n(\mathbb{R})$.

Soit $M = \begin{pmatrix} \alpha & \cdots & \cdots & \cdots & \cdots \\ \vdots & \ddots & (1) & \cdots & \vdots \\ \vdots & (1) & \ddots & (1) & \vdots \\ \vdots & \cdots & (1) & \ddots & \vdots \\ \cdots & \cdots & \cdots & \cdots & \alpha \end{pmatrix}$ avec $\alpha \in \mathbb{R}$.

Déterminons quelles valeurs α de $\mathbb{R}$ permettent à M d'être inversible, et donnons son inverse.

On réécrit M comme un polynôme d'une matrice A :

$$M = (\alpha - 1)I_n + A \text{ avec } A = \begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots \\ \vdots & \ddots & (1) & \cdots & \vdots \\ \vdots & (1) & \ddots & (1) & \vdots \\ \vdots & \cdots & (1) & \ddots & \vdots \\ \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix}$$

On a donc $M = P(A)$ avec $P(X) = (\alpha - 1) + X$. On a vu dans l'exemple précédent que $\pi_A(X) = X^2 - nX$. $\pi_A \wedge P = 1$ si et seulement si P n'a pas de racines en commun avec π_A, c'est-à-dire si et seulement si $P(0) \neq 0$ et $P(n) \neq 0$. On a donc :

$$P(0) = \alpha - 1 \neq 0 \iff \alpha \neq 1, \quad P(n) = (\alpha - 1) + n \neq 0 \iff \alpha \neq 1 - n$$

Les conditions sur α pour que M soit inversible sont donc :

$$\alpha \neq 1 \quad \text{et} \quad \alpha \neq 1 - n$$

Pour déterminer la matrice inverse M^{-1}, on utilise le théorème de Bézout puis on évalue en A :

$$\pi_A \wedge P = 1 \implies \exists U, V \in \mathbb{R}[X] : U\pi_A + VP = 1$$

On effectue une division euclidienne de π_A par P pour déterminer les coefficients U et V. On trouve :

$$\pi_A(X) = P(X)(X - (n + \alpha - 1)) + (n + \alpha - 1)(\alpha - 1)$$

On peut donc réécrire :

$$U(X)\pi_A(X) + V(X)P(X) = 1 \quad \text{avec} \quad U(X) = \frac{1}{(n + \alpha - 1)(\alpha - 1)}, \quad V(X) = -\frac{X - (n + \alpha - 1)}{(n + \alpha - 1)(\alpha - 1)}$$

En évaluant en A, on obtient :

$$\cancel{U(A)\pi_A(A)} + V(A)P(A) = 1_E \implies V(A)\underbrace{P(A)}_{=M} = 1_E \implies M^{-1} = V(A)$$

D'où $M^{-1} = -\frac{A - (n+\alpha-1)I_n}{(n+\alpha-1)(\alpha-1)}$.

On peut aussi déterminer les conditions d'inversibilité en calculant le déterminant de M, puis déterminer la matrice inverse en résolvant le système $MX = I_n$.

Rappel 6

Deux polynômes $P, Q \in \mathbb{R}(X]$ sont premiers entre eux si et seulement s'ils n'ont aucune racines communes dans $\mathbb{C}$ (pas seulement dans $\mathbb{R}$).

Exercice 3

Montrer que l'inverse d'une matrice triangulaire supérieure $A \in \mathcal{M}_n(\mathbb{K})$ est triangulaire supérieure.

Rappel 7

Les matrices triangulaires supérieures forment une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$.

Correction **(Exercice 3)**

Comme $T_n^s(\mathbb{K})$ forme une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$, on a $\mathbb{K}[A] \subset T_n^s(\mathbb{K})$. Si A est inversible, alors $A^{-1} \in \mathbb{K}[A] \subset T_n^s(\mathbb{K})$, donc A^{-1} est triangulaire supérieure.

Remarque

Si π_a existe alors :

$$a \text{ inversible} \iff \pi_a(0) \neq 0$$

Démonstration. On écrit $a = P(a)$ tel que $P(X) = X$. Alors a est inversible $\iff P \wedge \pi_a = 1$ si et seulement si $\pi_a(0) \neq 0$. □

Exercice 4

Prenons E un $\mathbb{K}$-espace vectoriel et $u \in \mathcal{L}(E)$ tel que π_u existe (ce qui est toujours le cas si $\dim(E) < \infty$). Montrer que les propriétés suivantes sont équivalentes :

(i) u est injective.
(ii) u est surjective.
(iii) u est bijective.
(iv) $\pi_u(0) \neq 0$.

Avec π_u le polynôme minimal de u dans l'algèbre $(\mathcal{L}(E), +, \cdot, \circ)$.

Note

Même dans un espace vectoriel de dimension **infinie**, on peut trouver des endomorphismes qui admettent un polynôme minimal. Par exemple, les projections; qui vérifient $u^2 = u$ et donc $\pi_u(X) \mid X^2 - X$.

Correction **(Exercice 4)**

D'après l'exercice précédent, on sait que u est inversible si et seulement si $\pi_u(0) \neq 0$. Or, u est inversible si et seulement si u est bijective. L'équivalence (iii) et (iv) est donc démontrée.

(i) Supposons que u est injective. Montrons que $\pi_u(0) \neq 0$. Si $\pi_u(0) = 0$, alors 0 est une racine de $\pi_u(X)$, donc $\pi_u(X) = XQ(X)$ pour un certain polynôme $Q \in \mathbb{K}[X]$.

En évaluant en u, on obtient $\pi_u(u) = uQ(u) = 0$. Comme u est injective, on a $Q(u) = 0$ car $\mathrm{Im}(Q(u)) \subset \ker(u)$ et $\ker(u) = \{0\}$ avec $Q \neq 0$.

Cela veut dire Q annule u et $\deg Q < \deg \pi_u$, donc π_u n'est pas de degré minimal, ce qui est absurde. Donc $\pi_u(0) \neq 0$.

(ii) Supposons que u est surjective. Montrons que $\pi_u(0) \neq 0$. Si $\pi_u(0) = 0$, alors $\pi_u(X) = XQ(X)$ pour un certain polynôme $Q \in \mathbb{K}[X]$.

En évaluant en u, on obtient $\pi_u(u) = uQ(u) = 0$. On a alors $uQ(u) = 0 \implies Q(u)u = 0$. On a donc $\mathrm{Im}(u) \subset \ker(Q(u))$. Comme u est surjective, on a $\mathrm{Im}(u) = E$, donc $\ker(Q(u)) = E$ et $Q(u) = 0$. Comme $\deg Q < \deg \pi_u$, cela contredit le fait que π_u est de degré minimal. Donc $\pi_u(0) \neq 0$.

Il faut aussi démontrer que (iii) $\implies$ (i) et (ii), ce qui est évident ; si u est bijective, alors u est injective et surjective par définition.

Le reste des implications découle immédiatement de l'équivalence (iii) et (iv). On a donc montré que les quatre propriétés sont équivalentes.

Remarque

Si π_a n'existe pas, alors $\mathbb{K}[a]$ n'est pas un corps car $\mathbb{K}[a] \simeq \mathbb{K}[X]$ et que :

$$\begin{cases} X \text{ n'est pas inversible dans } \mathbb{K}[X] \\ a \text{ n'est pas inversible dans } \mathbb{K}[a] \\ a \neq 0 \text{ (parce que } \pi_a \text{ n'existe pas)} \end{cases}$$

Remarque

Si π_a existe, les propriétés suivantes sont équivalentes :

1. $\mathbb{K}[a]$ est un corps.
2. π_a est irréductible.
3. $\mathbb{K}[a]$ est intègre.

Démonstration. On démontre 1 $\implies$ 3 simplement parce que tout corps est intègre. Montrons 3 $\implies$ 2. On a $\pi_a \neq 1$. Soit D un diviseur unitaire de π_a, montrons que $D = 1$ ou $D = \pi_a$. On va supposer l'existence d'un D' unitaire tel que $\pi_a = DD'$

À RECOPIER

Pour finaliser la preuve, on montre que 2 $\implies$ 1. Soit $y \in \mathbb{K}[a] \setminus \{0\}$. Montrer que y est inversible. Il existe $P \in \mathbb{K}[X]$ tel que $y = P(a)$. Comme π_a est irréductible, on a $P \wedge \pi_a = 1$ ou $P \wedge \pi_a = \pi_a$. Si $P \wedge \pi_a = \pi_a$, alors $\pi_a \mid P$ et donc $P(a) = 0$, ce qui est absurde. Donc $P \wedge \pi_a = 1$, et par la propriété précédente, on en déduit que $y = P(a)$ est inversible. □

Remarque

Si l'algèbre E est intègre et π_a existe, alors :

$\mathbb{K}[a]$ est un corps et π_a est irréductible.

Démonstration. $\mathbb{K}[1] \subset E$ et E est intègre. Donc $\mathbb{K}[a]$ est aussi intègre et d'après la remarque précédente, $\mathbb{K}[a]$ est un corps et π_a est irréductible. □

Exercice 5

$\mathbb{R}$ est considéré comme une $\mathbb{Q}$-algèbre et il est intègre, donc $\forall a \in \mathbb{R}$, si π_a existe, alors $\mathbb{Q}[a]$ est un corps et π_a est irréductible.

En particulier pour $a = \sqrt{2} + \sqrt{3}$, on a déjà vu dans l'exercice 2 que $\pi_a = X^4 - 10X^2 + 1$ est irréductible dans $\mathbb{Q}[X]$ et que $\mathbb{Q}[a]$ est un corps.

Calculer les coordonnées de $(a-1)^{-1}$ dans la base $(1, a, a^2, a^3)$ de $\mathbb{Q}[a]$.

Indication : Utiliser les coefficients de Bézout.

Correction

Utilisons les propriétés énoncées précédemment en posant $P(X) = X - 1$. On a $P(a) = a - 1$. Comme π_a est irréductible, on a $P \wedge \pi_a = 1$. Il existe donc $U, V \in \mathbb{Q}[X]$ tels que :

$$U(X)P(X) + V(X)\pi_a(X) = 1$$

On effectue une division euclidienne pour obtenir les coefficients de Bézout. On trouve :

$$U(X) = \frac{1}{8}(X^3 + X^2 - 9X - 9) \text{ et } V(X) = -\frac{1}{8}$$

En évaluant en a, on obtient :

$$U(a)(a-1) + V(a)\pi_a(a) = U(a)(a-1) = 1 \implies (a-1)^{-1} = U(a) = \frac{1}{8}(a^3 + a^2 - 9a - 9)$$

D'où les coordonnées de $(a-1)^{-1}$ dans la base $(1, a, a^2, a^3)$ de $\mathbb{Q}[a]$ sont :

$$\left(\frac{-9}{8}, \frac{-9}{8}, \frac{1}{8}, \frac{1}{8}\right)$$

Fin du Chapitre 1.