

DM : Algèbre Générale

Structure d'Algèbre

Samedi 03 Octobre 2026 (Durée : 2 heures)

Soit E un espace vectoriel de dimension finie $n \geq 1$ sur un corps $\mathbb{K}$.

Soit $u \in \mathcal{L}(E)$ un endomorphisme de E .

Dans tout le problème, 0 désigne 0_E .

Pour tout $x \in E \setminus \{0\}$. On pose $E_x = \{P(u)(x); \text{ tel que } P \in \mathbb{K}[X]\}$.

Partie A : Polynôme minimal d'un vecteur

- ① Montrer que E_x est un $\mathbb{K}$ -sev de E .
- ② Montrer que la famille $(x, u(x), u^2(x), \dots, u^n(x))$ est liée.
- ③ Montrer $\mathcal{I}_x = \{P \in \mathbb{K}[X]; \text{ tel que } P(u)(x) = 0\}$ est un idéal de $\mathbb{K}[X]$.
- ④ En déduire qu'il existe un unique polynôme unitaire non nul $\pi_x \in \mathbb{K}[X]$ tel que $\mathcal{I}_x = \langle \pi_x \rangle$.
- ⑤ Quel convention peut-proposer pour π_0 .
- ⑥ Justifier que π_x divise tout $P \in \mathbb{K}[X]$ tel que $P(u)(x) = 0$.
- ⑦ En déduire que π_x divise π_u .
- ⑧ En déduire que $\{\pi_x, \text{ tel que } x \in E \setminus \{0\}\}$ est fini.
- ⑨ Posons $d = \deg(P_x)$.

a Montrer que la famille $(x, u(x), \dots, u^{d-1}(x))$ est libre.

b Montrer que la famille $(x, u(x), \dots, u^d(x))$ est liée.

⑩ Démontrer que $E_x = \text{Vect}(x, u(x), \dots, u^{d-1}(x))$.

⑪ En déduire que $\dim E_x = \deg \pi_x$.

⑫ Soit $(x, y) \in E \setminus \{0\}$, tel que $\pi_x \wedge \pi_y = 1$.
Montrer alors que $\pi_{x+y} = \pi_x \cdot \pi_y$.

⑬ On pose $P = \text{PPCM}\{\pi_x, \text{ tel que } x \in E \setminus \{0\}\}$.

a Dire pourquoi P est bien défini et non constant.

On pose dans la suite $P = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r}$, où les Q_i sont des polynômes irréductibles distincts et $\alpha_i \geq 1$.

b Justifier que pour chaque $i \in \{1, \dots, r\}$, il existe un vecteur $y_i \in E$ tel que $P_i^{\alpha_i}$ divise π_{y_i} .

c On pose $\pi_{y_i} = P_i^{\alpha_i} \cdot R_i$ et $z_i = R_i(u)(y_i) \in E$.
Démontrer que $\pi_{z_i} = P_i^{\alpha_i}$.

⑭ En déduire d'après tout ce qui précède que $\exists x \in E$, tel que $\pi_u = \pi_x$.

⑮ Conclure enfin ce résultat (sans utiliser le théorème de Cayley-Hamilton) :

Degré du polynôme minimal

En dimension finie, le degré du polynôme minimal d'un endomorphisme est toujours inférieur à la dimension de l'espace vectoriel :

$$\forall u \in \mathcal{L}(E), \quad \deg(\pi_u) \leq \dim(E)$$

Partie B : Commutant d'un endomorphisme

Soit E un $\mathbb{K}$ -ev de dimension finie, on pose $\dim E = n \geq 2$. Soit $u \in \mathcal{L}(E)$.

☞ On pose $\mathbb{K}[u] = \{P(u), \text{ tel que } P \in \mathbb{K}[X]\}$.

☞ On pose $c(u) = \{v \in \mathcal{L}(E), \text{ tel que } u \circ v = v \circ u\}$, appelé le **commutant** de u .

① Montrer que $\mathbb{K}[u]$ est une sous algèbre de $(\mathcal{L}(E), +, \cdot, \circ)$.

② Montrer que $c(u)$ est une sous algèbre de $(\mathcal{L}(E), +, \cdot, \circ)$.

③ Dire pourquoi $\mathbb{K}[u] \subset c(u)$.

④ Soit $x_0 \in E$, et $k \in \mathbb{N}^*$.

a Montrer que si $(x_0, u(x_0), \dots, u^k(x_0))$ est libre, alors $(\text{Id}_E, u, \dots, u^k)$ est aussi libre.

b Á l'aide d'un contre-exemple, montrer que la réciproque de la question précédente n'est pas toujours vraie.

Endomorphisme Cyclique

Définition : On dit que u est un **endomorphisme cyclique** $\Leftrightarrow \exists x_0 \in E$, tel que $(x_0, u(x_0), \dots, u^{n-1}(x_0))$ est une base de E .

Dans toute la suite, on suppose que u est cyclique, et on considère $v \in c(u)$.

⑤ Dire pourquoi $(\text{Id}_E, u, \dots, u^{n-1})$ est libre.

⑥ Démontrer que $\deg \pi_u \geq n$, puis en déduire que $\deg \pi_u = n$.

⑦ Montrer que $\exists P \in \mathbb{K}_{n-1}[X]$, tel que $v(x_0) = P(u)(x_0)$.

⑧ En déduire que $v(u^j(x_0)) = P(u)(u^j(x_0))$, pour tout $0 \leq j \leq n-1$.

⑨ Conclure que $v = P(u)$, puis que $c(u) = \mathbb{K}[u] = \text{Vect}(\text{Id}_E, u, \dots, u^{n-1})$.

⑩ Montrer que $\exists Q \in \mathbb{K}_{n-1}[X]$, tel que $u^n(x_0) = Q(u)(x_0)$.

⑪ Démontrer alors que $\pi_u(X) = X^n - Q(X)$.

⑫ Démontrer que tout endomorphisme nilpotent d'indice n , est cyclique. Préciser alors son polynôme minimal.

FiN

Corrigé

Partie A : Polynôme minimal d'un vecteur

- ① $E_x = \{P(u)(x) \mid P \in \mathbb{K}[X]\}$.
- ☞ $E_x \subset E$ par définition de l'image d'un vecteur par un endomorphisme.
 - ☞ Pour $P = 0$, $0(u)(x) = 0_E \in E_x$, donc $E_x \neq \emptyset$.
 - ☞ Soient $y, z \in E_x$ et $\lambda \in \mathbb{K}$. Il existe $P, Q \in \mathbb{K}[X]$ tels que $y = P(u)(x)$ et $z = Q(u)(x)$. Alors $\lambda y + z = \lambda P(u)(x) + Q(u)(x) = (\lambda P + Q)(u)(x) \in E_x$ car $\lambda P + Q \in \mathbb{K}[X]$.
- Ainsi, E_x est un sous-espace vectoriel de E .
- ② La famille $(x, u(x), u^2(x), \dots, u^n(x))$ contient $n+1$ vecteurs. Comme $\dim E = n < n+1$, toute famille de $n+1$ vecteurs dans E est nécessairement liée.
- ③ Soit $\mathcal{I}_x = \{P \in \mathbb{K}[X] \mid P(u)(x) = 0\}$.
- ☞ Le polynôme nul $0 \in \mathcal{I}_x$, donc $\mathcal{I}_x \neq \emptyset$.
 - ☞ Soient $P, Q \in \mathcal{I}_x$. $(P-Q)(u)(x) = P(u)(x) - Q(u)(x) = 0 - 0 = 0$, donc $P-Q \in \mathcal{I}_x$.
 - ☞ Soient $P \in \mathcal{I}_x$ et $A \in \mathbb{K}[X]$. $(A \cdot P)(u)(x) = A(u)(P(u)(x)) = A(u)(0) = 0$, donc $A \cdot P \in \mathcal{I}_x$.
- $\mathcal{I}_x$ est donc un idéal de $\mathbb{K}[X]$.
- ④ Le corps $\mathbb{K}$ étant un corps commutatif, l'anneau $\mathbb{K}[X]$ est principal. Tout idéal de $\mathbb{K}[X]$ est donc engendré par un unique polynôme unitaire (ou nul). D'après la question 2, il existe une combinaison linéaire non nulle s'annulant en x , donc $\mathcal{I}_x \neq \{0\}$. Il existe donc un unique polynôme unitaire non nul $\pi_x \in \mathbb{K}[X]$ tel que $\mathcal{I}_x = \langle \pi_x \rangle$.

- ⑤ Pour $x = 0_E$, tout polynôme $P \in \mathbb{K}[X]$ vérifie $P(u)(0_E) = 0_E$. Ainsi $\mathcal{I}_0 = \mathbb{K}[X]$. Par convention de l'idéal engendré par l'élément unitaire de degré 0, on pose $\pi_0 = 1$.
- ⑥ Soit $P \in \mathbb{K}[X]$ tel que $P(u)(x) = 0$. Alors $P \in \mathcal{I}_x = \langle \pi_x \rangle$. Par définition d'un idéal principal, cela signifie exactement que π_x divise P .
- ⑦ Par définition du polynôme minimal global π_u , on a $\pi_u(u) = 0_{\mathcal{L}(E)}$. En particulier, $\pi_u(u)(x) = 0$. D'après la question 6, π_x divise π_u .
- ⑧ L'ensemble des diviseurs unitaires d'un polynôme fixés π_u est fini. Comme pour tout $x \in E \setminus \{0\}$, π_x est un diviseur unitaire de π_u , l'ensemble $\{\pi_x \mid x \in E \setminus \{0\}\}$ est fini.
- ⑨ **a** Posons $d = \deg(\pi_x)$. Supposons la famille $(x, u(x), \dots, u^{d-1}(x))$ liée. Il existerait des scalaires non tous nuls $(\lambda_0, \dots, \lambda_{d-1})$ tels que $\sum_{k=0}^{d-1} \lambda_k u^k(x) = 0$. Le polynôme $Q(X) = \sum_{k=0}^{d-1} \lambda_k X^k$ serait alors un polynôme non nul annulateur de x avec $\deg(Q) \leq d-1 < \deg(\pi_x)$, ce qui contredit la minimalité du degré de π_x . Donc la famille est libre.
- b** Par définition, $\pi_x(u)(x) = 0$. Comme π_x est unitaire de degré d , on a $u^d(x) + \sum_{k=0}^{d-1} a_k u^k(x) = 0$. Ainsi $u^d(x) = -\sum_{k=0}^{d-1} a_k u^k(x)$, ce qui démontre que la famille $(x, u(x), \dots, u^d(x))$ est liée.
- ⑩ Par récurrence, pour tout $k \geq d$, $u^k(x)$ s'exprime comme combinaison linéaire de $(x, u(x), \dots, u^{d-1}(x))$. Tout élément de $E_x = \{P(u)(x) \mid P \in \mathbb{K}[X]\}$ appartient donc

à $\text{Vect}(x, u(x), \dots, u^{d-1}(x))$. Réciproquement, la famille est clairement contenue dans E_x . D'où $E_x = \text{Vect}(x, u(x), \dots, u^{d-1}(x))$.

11 La famille $(x, u(x), \dots, u^{d-1}(x))$ est une famille libre (question 9.a) et génératrice de E_x (question 10). C'est donc une base de E_x . On en déduit que $\dim E_x = d = \deg \pi_x$.

12  $\pi_x \pi_y(u)(x+y) = \pi_y(u)(\pi_x(u)(x)) + \pi_x(u)(\pi_y(u)(y)) = 0+0=0$. Donc π_{x+y} divise $\pi_x \pi_y$.

 Inversement, $\pi_{x+y}(u)(x+y) = 0 \implies \pi_{x+y}(u)(x) = -\pi_{x+y}(u)(y)$. En composant par $\pi_x(u)$, on obtient $\pi_x \pi_{x+y}(u)(y) = 0$, donc $\pi_y \mid \pi_x \pi_{x+y}$. Comme $\pi_y \wedge \pi_x = 1$, d'après le lemme de Gauss, $\pi_y \mid \pi_{x+y}$. Par symétrie, $\pi_x \mid \pi_{x+y}$. Puisque $\pi_x \wedge \pi_y = 1$, leur produit $\pi_x \pi_y$ divise π_{x+y} .

Par unicité du polynôme unitaire, $\pi_{x+y} = \pi_x \pi_y$.

13 **a** L'ensemble $\{\pi_x \mid x \in E \setminus \{0\}\}$ est un ensemble fini non vide de polynômes unitaires. Le PPCM d'une famille finie de polynômes est donc bien défini et unitaire. P n'est pas constant car pour $x \neq 0$, $\deg(\pi_x) \geq 1$.

b Par définition du PPCM, pour chaque facteur irréductible $P_i^{\alpha_i}$, il existe au moins un vecteur dans la famille, noté $y_i \in E \setminus \{0\}$, tel que $P_i^{\alpha_i}$ divise π_{y_i} .

c Écrivons $\pi_{y_i} = P_i^{\alpha_i} R_i$ avec $P_i \nmid R_i$. Posons $z_i = R_i(u)(y_i)$.

 $P_i^{\alpha_i}(u)(z_i) = P_i^{\alpha_i} R_i(u)(y_i) = \pi_{y_i}(u)(y_i) = 0$, donc $\pi_{z_i} \mid P_i^{\alpha_i}$.

 Réciproquement, $\pi_{z_i}(u) R_i(u)(y_i) = 0 \implies \pi_{y_i} \mid \pi_{z_i} R_i \implies P_i^{\alpha_i} R_i \mid \pi_{z_i} R_i \implies P_i^{\alpha_i} \mid \pi_{z_i}$.

Par unicité du polynôme unitaire, $\pi_{z_i} = P_i^{\alpha_i}$.

14 Les polynômes $\pi_{z_i} = P_i^{\alpha_i}$ sont deux à deux premiers entre eux. D'après la question 12 généralisée par récurrence, en posant $x = z_1 + z_2 + \dots + z_r$, on a :

$$\pi_x = \prod_{i=1}^r \pi_{z_i} = \prod_{i=1}^r P_i^{\alpha_i} = P$$

Puisque $P(u)(y) = 0$ pour tout $y \in E$, $P(u) = 0$, donc $\pi_u \mid P$. Comme de plus $P = \pi_x \mid \pi_u$ (d'après q.7), on conclut par unitarité que $\pi_u = P = \pi_x$.

15 D'après la question 14, il existe $x \in E$ tel que $\pi_u = \pi_x$. En utilisant le résultat de la question 11 :

$$\deg(\pi_u) = \deg(\pi_x) = \dim E_x$$

Comme E_x est un sous-espace vectoriel de E , on a $\dim E_x \leq \dim E$. On en conclut que :

$$\forall u \in \mathcal{L}(E), \quad \deg(\pi_u) \leq \dim(E) \quad \blacksquare$$

Partie B : Commutant d'un endomorphisme

1 Montrons que $\mathbb{K}[u] = \{P(u) \mid P \in \mathbb{K}[X]\}$ est une sous-algèbre de $(\mathcal{L}(E), +, \cdot, \circ)$.

 $\text{Id}_E = X^0(u) \in \mathbb{K}[u]$, donc $\mathbb{K}[u] \neq \emptyset$.

 Soient $P(u), Q(u) \in \mathbb{K}[u]$ et $\lambda \in \mathbb{K}$.

 $\lambda P(u) + Q(u) = (\lambda P + Q)(u) \in \mathbb{K}[u]$ car $\lambda P + Q \in \mathbb{K}[X]$.

 $P(u) \circ Q(u) = (P \cdot Q)(u) \in \mathbb{K}[u]$ car $P \cdot Q \in \mathbb{K}[X]$.

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

2 Montrons que $c(u) = \{v \in \mathcal{L}(E) \mid u \circ v = v \circ u\}$ est une sous-algèbre de $(\mathcal{L}(E), +, \cdot, \circ)$.

 $\text{Id}_E \circ u = u = u \circ \text{Id}_E$, donc $\text{Id}_E \in c(u)$.

 Soient $v_1, v_2 \in c(u)$ et $\lambda \in \mathbb{K}$.

 $u \circ (\lambda v_1 + v_2) = \lambda(u \circ v_1) + u \circ v_2 = \lambda(v_1 \circ u) + v_2 \circ u = (\lambda v_1 + v_2) \circ u$, donc $\lambda v_1 + v_2 \in c(u)$.

 $u \circ (v_1 \circ v_2) = (u \circ v_1) \circ v_2 = (v_1 \circ u) \circ v_2 = v_1 \circ (u \circ v_2) = v_1 \circ (v_2 \circ u) = (v_1 \circ v_2) \circ u$, donc $v_1 \circ v_2 \in c(u)$.

Ainsi, $c(u)$ est une sous-algèbre de $\mathcal{L}(E)$.

③ Pour tout $P = \sum_{i=0}^d a_i X^i \in \mathbb{K}[X]$, on a $u \circ P(u) = u \circ \sum_{i=0}^d a_i u^i = \sum_{i=0}^d a_i u^{i+1} = \left(\sum_{i=0}^d a_i u^i \right) \circ u = P(u) \circ u$. Tout élément de $\mathbb{K}[u]$ commute donc avec u , ce qui prouve l'inclusion $\mathbb{K}[u] \subset c(u)$.

④ **a** Soient $\lambda_0, \dots, \lambda_k \in \mathbb{K}$ tels que $\sum_{i=0}^k \lambda_i u^i = 0_{\mathcal{L}(E)}$. En évaluant cette égalité d'endomorphismes en x_0 , on obtient :

$$\sum_{i=0}^k \lambda_i u^i(x_0) = 0_E$$

Comme la famille $(x_0, u(x_0), \dots, u^k(x_0))$ est libre par hypothèse, tous les coefficients λ_i sont nuls. La famille $(\text{Id}_E, u, \dots, u^k)$ est donc libre.

b Contre-exemple : Soit $E = \mathbb{R}^2$ et $u = \text{Id}_E$. La famille (Id_E) est une famille libre (composée d'un seul élément non nul) dans $\mathcal{L}(E)$ pour $k = 0$. Cependant, pour tout $x_0 \in E \setminus \{0\}$, $u(x_0) = x_0$, donc la famille $(x_0, u(x_0)) = (x_0, x_0)$ est liée. La réciproque est donc fautive.

⑤ Puisque u est cyclique, il existe $x_0 \in E$ tel que $\mathcal{B} = (x_0, u(x_0), \dots, u^{n-1}(x_0))$ soit une base de E . D'après la question 4.a appliquée à $k = n - 1$, la liberté de la famille de vecteurs $\mathcal{B}$ implique la liberté de la famille d'endomorphismes $(\text{Id}_E, u, \dots, u^{n-1})$.

⑥  Puisque la famille $(\text{Id}_E, u, \dots, u^{n-1})$ est libre (question 5), aucun polynôme non nul de degré strictement inférieur à n ne peut annuler u . Par conséquent, $\deg \pi_u \geq n$.

 D'autre part, d'après la Partie A (ou le théorème de Cayley-Hamilton), on a $\deg \pi_u \leq \dim E = n$.

Par double inégalité, on en déduit que $\deg \pi_u = n$.

⑦ Soit $v \in c(u)$. Puisque $\mathcal{B} = (x_0, u(x_0), \dots, u^{n-1}(x_0))$ est une base de E , le vecteur

$v(x_0) \in E$ se décompose de manière unique dans cette base :

$$v(x_0) = \sum_{i=0}^{n-1} a_i u^i(x_0)$$

En posant $P(X) = \sum_{i=0}^{n-1} a_i X^i \in \mathbb{K}_{n-1}[X]$, on a bien $v(x_0) = P(u)(x_0)$.

⑧ Pour tout $0 \leq j \leq n - 1$, comme $v \in c(u)$, v commute avec u^j , d'où $v \circ u^j = u^j \circ v$. On a donc :

$$v(u^j(x_0)) = (v \circ u^j)(x_0) = (u^j \circ v)(x_0) = u^j(v(x_0)) = u^j(P(u)(x_0)) = P(u)(u^j(x_0))$$

⑨ Les deux endomorphismes v et $P(u)$ coïncident sur tous les vecteurs de la base $\mathcal{B} = (x_0, u(x_0), \dots, u^{n-1}(x_0))$. Ils sont donc égaux : $v = P(u)$. On en déduit que $c(u) \subset \mathbb{K}[u]$. Avec la question 3, on conclut :

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

⑩ Le vecteur $u^n(x_0)$ appartient à E . Puisque $\mathcal{B} = (x_0, u(x_0), \dots, u^{n-1}(x_0))$ est une base de E , $u^n(x_0)$ s'exprime comme combinaison linéaire des éléments de $\mathcal{B}$:

$$\exists ! Q \in \mathbb{K}_{n-1}[X] \quad \text{tel que} \quad u^n(x_0) = Q(u)(x_0)$$

⑪ Posons $R(X) = X^n - Q(X)$. Pour tout $0 \leq j \leq n - 1$, on a :

$$R(u)(u^j(x_0)) = u^j(R(u)(x_0)) = u^j(u^n(x_0) - Q(u)(x_0)) = u^j(0_E) = 0_E$$

L'endomorphisme $R(u)$ s'annule sur tous les vecteurs de la base $\mathcal{B}$, donc $R(u) = 0_{\mathcal{L}(E)}$. Le polynôme $R(X)$ est unitaire, de degré n , et annule u . Puisque $\deg \pi_u = n$ (question 6) et que π_u est unitaire, on conclut par unicité :

$$\pi_u(X) = X^n - Q(X)$$

- 12 Soit u un endomorphisme nilpotent d'indice $n = \dim E$. Il existe $x_0 \in E$ tel que $u^{n-1}(x_0) \neq 0_E$. Montrons que la famille $(x_0, u(x_0), \dots, u^{n-1}(x_0))$ est libre. Soient $\lambda_0, \dots, \lambda_{n-1} \in \mathbb{K}$ tels que $\sum_{i=0}^{n-1} \lambda_i u^i(x_0) = 0_E$.
- En composant par u^{n-1} , on a $\lambda_0 u^{n-1}(x_0) = 0_E \implies \lambda_0 = 0$.
 - En composant successivement par $u^{n-2}, u^{n-3}, \dots$, on montre de proche en proche

que $\lambda_0 = \lambda_1 = \dots = \lambda_{n-1} = 0$.

La famille $(x_0, u(x_0), \dots, u^{n-1}(x_0))$ est une famille libre de n vecteurs en dimension n , c'est donc une base de E . u est donc **cyclique**.

Son polynôme minimal est unitaire, de degré n , annule u (car $u^n = 0$), d'où :

$$\pi_u(X) = X^n$$