DM 15, corrigé

PROBLÈME
Commutant des endomorphismes cycliques

Partie I. Étude du commutant d'un endomorphisme

1) Tous les endomorphismes commutent avec l'identité. On en déduit que $Z(\mathrm{Id}_E) = \mathcal{L}(E)$.

2)

a) $\mathcal{L}(E)$ est bien un espace vectoriel (stable par combinaisons linéaires). Soient $v, w \in Z(u)$ et $\lambda, \mu \in \mathbb{K}$. On a alors, en utilisant la linéarité des différentes applications que :

$$\begin{array}{rcll} (\lambda v + \mu w) \circ u & = & \lambda v \circ u + \mu w \circ u & \\ & = & \lambda u \circ v + \mu u \circ w & \quad (\text{car } v, w \in Z(u)) \\ & = & u \circ (\lambda v + \mu w). & \end{array}$$

On en déduit que $\lambda v + \mu w \in Z(u)$. $Z(u)$ est donc un sous-espace vectoriel de $\mathcal{L}(E)$.

b) Soient $v, w \in Z(u)$. On a alors, par associativité de la loi $\circ$, que :

$$\begin{array}{rcll} u \circ (v \circ w) & = & (u \circ v) \circ w & \\ & = & (v \circ u) \circ w & \quad (\text{car } v \in Z(u)) \\ & = & v \circ (u \circ w) & \\ & = & v \circ (w \circ u) & \quad (\text{car } w \in Z(u)) \\ & = & (v \circ w) \circ u. & \end{array}$$

On a bien $v \circ w \in Z(u)$. De plus, $Z(u)$ contient l'application nulle et l'identité (qui commutent avec tous les éléments de $\mathcal{L}(E)$ donc en particulier avec u). Enfin, si $v \in Z(u)$, on a également $-v \in Z(u)$ (puisque d'après la question 1 on a une structure d'espace vectoriel). On en déduit que $Z(u)$ est un sous-anneau de l'anneau $(\mathcal{L}(E), +, \circ)$.

3) Soit $v \in Z(u)$. Montrons que le noyau et l'image de u sont stables par v.

Soit $x \in \ker(u)$. Montrons que $v(x) \in \ker(u)$. On a :

$$\begin{array}{rcll} u(v(x)) & = & v(u(x)) & \\ & = & v(0) & \\ & = & 0 & \quad (\text{puisque } v \text{ est linéaire}). \end{array}$$

On en déduit que $\forall x \in \ker(u),\ v(x) \in \ker(u)$. On a bien montré que $v(\ker(u)) \subset \ker(u)$.

Soit $y \in \mathrm{Im}(u)$. Montrons que $v(y) \in \mathrm{Im}(u)$. Il existe $x \in E$ tel que $y = u(x)$. On a alors :

$$\begin{array}{rcl} v(y) & = & v(u(x)) \\ & = & u(v(x)). \end{array}$$

On a bien $v(y) \in \mathrm{Im}(u)$. On a bien montré que $v(\mathrm{Im}(u)) \subset \mathrm{Im}(u)$.

4) Soit $v \in Z(u) \cap GL(E)$. Puisque $v \in Z(u)$, on a alors $u \circ v = v \circ u$. Puisque v est inversible, on peut composer cette relation à gauche et à droite par v^{-1}. On obtient alors après simplification que $v^{-1} \circ u = u \circ v^{-1}$. On a bien $v^{-1} \in Z(u)$.

5) Supposons $u \in GL(E)$. Montrons par double inclusion que $Z(u) = Z(u^{-1})$.

($\subset$) Soit $v \in Z(u)$. On a alors $v \circ u = u \circ v$. Puisque u est inversible, on peut composer à gauche et à droite par u^{-1} (comme à la question précédente). On a donc $u^{-1} \circ v = v \circ u^{-1}$. On a donc bien $v \in Z(u^{-1})$.

($\supset$) On procède exactement de la même manière en replaçant u par u^{-1} et en composant à gauche et à droite par u. On a donc l'inclusion inverse.

On a montré par double inclusion que si u est inversible, alors $Z(u) = Z(u^{-1})$.

6) Soient $u, v \in \mathcal{L}(E)$. Soit $w \in Z(u) \cap Z(v)$. On a alors, toujours par associativité de la loi $\circ$ et puisque w commute avec v et avec w, que :

$$\begin{aligned}(u \circ v) \circ w &= u \circ (v \circ w)\\ &= u \circ (w \circ v)\\ &= (u \circ w) \circ v\\ &= (w \circ u) \circ v\\ &= w \circ (u \circ v).\end{aligned}$$

On a donc $w \in Z(u \circ v)$. De la même manière, on montre que $w \in Z(v \circ u)$ en faisant commuter w avec u puis avec v. On a donc bien $Z(u) \cap Z(v) \subset Z(u \circ v) \cap Z(v \circ u)$.

7) Soit $P \in \mathbb{R}[X]$. On note $P = \sum_{k=0}^{p} a_k X^k$ où $p = \deg(P)$. On définit alors un endomorphisme de E, noté $P(u)$, en posant :

$$P(u) = a_0 \mathrm{Id}_E + a_1 u + \ldots + a_p u^p.$$

On note $\mathcal{P}_u = \{P(u),\ P \in \mathbb{R}[X]\}$.

a) Soit $v \in \mathcal{P}_u$. On a montré en 2.b que $\mathrm{Id}_E \in Z(u)$. De plus, $u \in Z(u)$. En effet, on a bien $u \circ u = u \circ u$! Puisque d'après le 2.b $Z(u)$ est stable par $\circ$, on en déduit par récurrence que $\forall n \in \mathbb{N}^*,\ u^n \in Z(u)$. Puisque $Z(u)$ est un espace vectoriel d'après 2.a, il est stable par combinaisons linéaires finies. On en déduit, puisque $v = \sum_{k=0}^{p} a_k u^k$ est bien une combinaison linéaire finie des u^n que $v \in Z(u)$. On a bien $\mathcal{P}_u \subset Z(u)$.

b) Remarquons tout d'abord que $\mathcal{P}_u$ est bien un espace vectoriel (puisque $\mathbb{K}[X]$ est un espace vectoriel). On suppose que $u \neq \mathrm{Id}_E$, $u \neq 0$ et que u est un projecteur. Montrons que la famille (Id_E, u) est une base de $\mathcal{P}_u$.

- (famille génératrice) Soit $v \in \mathcal{P}_u$. Il existe alors $p \in \mathbb{N}$ et $a_0, \ldots, a_p \in \mathbb{K}$ tels que $v = \sum_{k=0}^{p} a_k u^k$. Or, puisque u est un projecteur, on a $u^2 = u$. On en déduit que $\forall k \in \mathbb{N}^*,\ u^k = u$. On a donc :

  $$v = a_0 \mathrm{Id}_E + \left(\sum_{k=1}^{p} a_k \right) u.$$

  On a donc bien une famille génératrice de $\mathcal{P}_u$.

- (famille libre) Soient $\lambda_1, \lambda_2 \in \mathbb{K}$ tels que $\lambda_1 \mathrm{Id}_E + \lambda_2 u = 0$ (ici 0 est bien l'application nulle). Puisque $u \neq \mathrm{Id}_E$, il existe $x_0 \in E$ tel que $u(x_0) \neq x_0$. On peut alors évaluer la relation précédente en x_0 pour trouver que $\lambda_1 x_0 + \lambda_2 u(x_0) = 0$. Séparons alors plusieurs cas :

  — Si la famille $(x_0, u(x_0))$ est libre, on a alors directement que $\lambda_1 = \lambda_2 = 0$.

— Si la famille $(x_0, u(x_0))$ est liée, alors, puisque $x_0 \neq 0$ (sinon on aurait $u(x_0) = 0 = x_0$), on en déduit qu'il existe $\mu \in \mathbb{K}$ tel que $u(x_0) = \mu x_0$ avec $\mu \neq 1$. En appliquant u dans cette égalité, on a alors que $u^2(x_0) = \mu u(x_0)$. Or, u est un projecteur donc $u^2 = u$. On a donc $u(x_0) = \mu u(x_0)$. Puisque $\mu \neq 1$, on en déduit que $u(x_0) = 0$. On a alors en revenant dans la relation de liaison que $\lambda_1 x_0 = 0$. Puisque $x_0 \neq 0$, on a donc $\lambda_1 = 0$, ce qui entraine que $\lambda_2 u = 0$. Puisque u n'est pas l'application nulle, ceci entraine que $\lambda_2 = 0$. La famille (Id_E, u) est donc libre.

On a donc montré que si u était un projecteur différent de l'application nulle et de l'identité que $\mathcal{P}_u$ admettait une base à 2 éléments. On en déduit que $\dim(\mathcal{P}_u) = 2$.

c) Il n'y a pas toujours égalité entre $\mathcal{P}_u$ et $Z(u)$ dans l'inclusion $\mathcal{P}_u \subset Z(u)$. En effet, si on prend par exemple $u = \mathrm{Id}_E$, on a montré au 1 que $Z(\mathrm{Id}_E) = \mathcal{L}(E)$. On a de plus que $\mathcal{P}_{\mathrm{Id}_E}$ est de dimension 1 (toutes les applications doivent être proportionnelles à l'identité). On en déduit que si $n \geq 2$, n'importe quelle application linéaire qui n'est pas une homothétie n'est pas dans $\mathcal{P}_{\mathrm{Id}_E}$ (par exemple, si on fixe une base $e_1, \dots e_n$ de E, le projecteur p_1 sur e_1 parallèlement à $\mathrm{Vect}(e_2, \dots, e_n)$ n'est pas une homothétie et n'est donc pas dans $\mathcal{P}_{\mathrm{Id}_E}$). Si $n = 1$ par contre, toutes les applications linéaires étant des homothéties, on a alors toujours $\mathcal{P}_u = Z(u)$.

Partie II. Étude de $E_u(x)$

Soit $x \in E$ et $u \in \mathcal{L}(E)$.

8) Soit F un sous-espace vectoriel de E stable par u contenant x. Puisque $x \in F$ et que F est stable par u, on a $u(x) \in F$. Puisque l'on a déjà admis une récurrence « directe » dans ce devoir, poser celle-ci proprement pour montrer au correcteur que l'on sait poser une récurrence. Posons donc pour $k \in \mathbb{N}$ l'hypothèse $\mathcal{P}(k)$: « $u^n(k) \in F$. »

- $\mathcal{P}(0)$ est vraie (on a $x \in F$ par hypothèse).
- Soit $k \in \mathbb{N}$. Supposons $\mathcal{P}(k)$ vraie. On a alors $u^k(x) \in F$. Puisque F est stable par u, on a alors $u(u^k(x)) \in F$ donc $u^{k+1}(x) \in F$. $\mathcal{P}(k+1)$ est donc vraie.
- La propriété étant héréditaire et initialisée, on en déduit qu'elle est vraie pour tout $k \in \mathbb{N}$.

On en déduit que $\forall k \in \mathbb{N},\ u^k(x) \in F$. Puisque F est un espace vectoriel, on en déduit qu'il contient l'espace vectoriel engendré par tous ces vecteurs. On a donc $E_u(x) \subset F$. On a bien montré la propriété voulue.

9) On a une famille $(x, u(x), \dots, u^n(x))$ de $n+1$ vecteurs dans un espace vectoriel de dimension n. Elle est donc liée.

10) On suppose que $x \neq 0$. Posons $A = \{k \in \mathbb{N} \ / \ (x, u(x), \dots, u^k(x))$ est une famille libre.$\}$. A est non vide (il contient 0 car il n'y a que le vecteur x dans la famille et $x \neq 0$ par hypothèse). A est majoré. En effet, d'après la question précédente, si $k = n$, la famille est liée et si $k \geq n$, puisqu'une famille contenant une sous-famille liée est liée, la famille est encore liée. On en déduit que A est majoré par n. On a une partie non vide majorée de $\mathbb{N}$. Elle admet donc un maximum k_0. Il existe donc un entier k_0 maximal pour lequel la famille $(x, u(x), \dots, u^{k_0}(x))$ soit libre.

11) On a déjà que $(x, u(x), \dots, u^p(x))$ est une famille libre par construction. Montrons qu'elle est génératrice de $E_u(x)$. Pour cela, montrons que $\mathrm{Vect}(x, u(x), \dots, u^p(x))$ est stable par u. Ceci montrera d'après la question 1 qu'il contient $E_u(x)$ ce qui entrainera que la famille $(x, u(x), \dots, u^p(x))$ est génératrice.

Soit $y \in \mathrm{Vect}(x, u(x), \dots, u^p(x))$. Il existe donc $\lambda_0, \dots, \lambda_p \in \mathbb{K}$ tels que $y = \displaystyle\sum_{k=0}^{p} \lambda_k u^k(x)$. On a alors par linéarité de u que :

$$u(y) = \sum_{k=0}^{p} \lambda_k u^{k+1}(x).$$

Pour montrer que $u(y) \in \mathrm{Vect}(x, u(x), \dots, u^p(x))$, il suffit donc de vérifier que :

$$u^{p+1}(x) \in \mathrm{Vect}(x, u(x), \dots, u^p(x)).$$

Or, par maximalité de p, on sait que la famille $(x, u(x), \dots, u^{p+1}(x))$ est liée. Il existe donc des coefficients $a_0, \dots, a_{p+1}$ dans $\mathbb{K}$ non tous nuls tels que :

$$\sum_{k=0}^{p+1} a_k u^k(x) = 0.$$

Si $a_{p+1} = 0$, puisque la famille $(x, \dots, u^p(x))$ est libre, on aurait alors $a_0 = \dots = a_p = 0$ ce qui est absurde. On en déduit que $a_{p+1} \neq 0$, ce qui implique que :

$$u^{p+1}(x) = -\frac{1}{a_{p+1}} \sum_{k=0}^{p} a_k u^k(x).$$

On en déduit que $u^{p+1}(x) \in \mathrm{Vect}(x, u(x), \dots, u^p(x))$. Cet espace vectoriel est donc stable par u, ce qui entraine que la famille $(x, u(x), \dots, u^p(x))$ est génératrice de $E_u(x)$. Elle forme donc une base de $E_u(x)$. On a alors $E_u(x)$ de dimension finie égale à $p+1$.

12) Procédons par double implication.

($\Rightarrow$) Supposons $\dim(E_u(x)) = 1$. On a alors $x \neq 0$ (sinon il n'y aurait que 0 dans $E_u(x)$ et $E_u(x)$ serait de dimension 0). De plus, $u(x)$ et x sont liés. Il existe donc λ_1, λ_2 dans $\mathbb{K}$ non tous les deux nuls tels que $\lambda_1 x + \lambda_2 u(x) = 0$. Puisque $x \neq 0$, on a $\lambda_2 \neq 0$. Ceci entraine qu'il existe $\lambda \in \mathbb{K}$ tel que $u(x) = \lambda x$.

($\Leftarrow$) Réciproquement, supposons $x \neq 0$ et qu'il existe $\lambda \in \mathbb{K}$ tel que $u(x) = \lambda x$. Puisque la famille $(x, u(x))$ est liée, on en déduit que $E_u(x)$ est de dimension au plus 1 (d'après la question 4, on a $p \leq 0$). Puisque $x \neq 0$, on a au moins un vecteur non nul dans $E_u(x)$. On a donc $\dim(E_u(x)) = 1$.

13) Supposons que u est cyclique. On a alors qu'il existe $x \in E$ tel que $E_u(x) = E$. On en déduit que $(x, u(x), \dots, u^p(x))$ forme une base de E. On a alors $n = \dim(E_u(x)) = 1 + \dim(\mathrm{Vect}(u(x), \dots, u^p(x)))$ d'après la formule de Grassmann. Or, l'espace vectoriel $\mathrm{Vect}(u(x), \dots, u^p(x))$ est inclus dans $\mathrm{Im}(u)$. On en déduit que $\dim(\mathrm{Vect}(u(x), \dots, u^p(x))) \leq \mathrm{rg}(u)$. On a donc bien $n - 1 \leq \mathrm{rg}(u)$.

14) La réciproque n'est pas vraie. Par exemple Id_E est de rang n mais n'est pas cyclique si $n \geq 2$ (puisque pour tout vecteur x est envoyé sur lui même par l'identité, $E_u(x)$ est de dimension 1 (ou 0 si $x = 0$) et ne peut donc pas être égal à E). Si $n = 1$, alors toutes les applications linéaires sont cycliques (il suffit de prendre au départ un vecteur $x \neq 0$).

Partie III. Commutant d'un endomorphisme cyclique

Soit $u \in \mathcal{L}(E)$ un endomorphisme cyclique et $x_0 \in E$ tel que $E_u(x_0) = E$.

15) Soit le p défini à la question II.3 tel que $(x_0, \dots, u^p(x_0))$ soit une base de $E_u(x_0)$. On a alors qu'elle forme aussi une base de E. Or, E est de dimension n donc toutes les bases sont de cardinal n. On en déduit que $p + 1 = n$ d'où $p = n - 1$. On en déduit que $(x_0, u(x_0), \dots, u^{n-1}(x_0))$ est une base de E.

16) Soient $\lambda_0, \dots, \lambda_{n-1} \in \mathbb{K}$ tels que $\displaystyle\sum_{k=0}^{n-1} \lambda_k u^k = 0$. Évaluons cette relation en x_0. On obtient alors $\displaystyle\sum_{k=0}^{n-1} \lambda_k u^k(x_0) = 0$. Puisque la famille $(x_0, \dots u^{n-1}(x_0))$ est libre (c'est une base de E), on en déduit que tous les λ_i sont nuls. La famille $(\mathrm{Id}_E, u, \dots, u^{n-1})$ est donc une famille libre de $\mathcal{L}(E)$.

17) Soit $(v,w) \in Z(u)^2$. Procédons par double implication.

($\Rightarrow$) Si $v = w$, on directement $v(x_0) = w(x_0)$.

($\Leftarrow$) Supposons que $v(x_0) = w(x_0)$. En appliquant u dans cette égalité, on obtient $u(v(x_0)) = u(w(x_0))$ et en utilisant le fait que u et v et u et w commutent, on obtient $v(u(x_0)) = w(u(x_0))$. On montre alors par récurrence, en utilisant le fait que v et w commutent avec tous les u^k (on a déjà détaillé une récurrence « directe » proprement donc on peut se permettre de ne pas poser la seconde) que $\forall k \in [\![0, n-1]\!]$, $v(u^k(x_0)) = w(u^k(x_0))$. Les deux applications linéaires v et w sont donc égales sur une base. On en déduit qu'elle sont égales.

On a bien montré que $v = w \Leftrightarrow v(x_0) = w(x_0)$.

18) Soit $v \in Z(u)$. $v(x_0) \in E$ donc puisque $(x_0, \ldots, u^{n-1}(x_0))$ est une base de E d'après la question 1, il existe $\lambda_0, \ldots, \lambda_{n-1} \in \mathbb{K}$ tels que $v(x_0) = \sum_{k=0}^{n-1} \lambda_k u^k(x_0)$. Posons alors $w = \sum_{k=0}^{n-1} \lambda_k u^k$. On a par construction $v(x_0) = w(x_0)$ donc $v = w$ d'après la question précédente. On en déduit que :

$$v = \sum_{k=0}^{n-1} \lambda_k u^k.$$

On a alors montré que v est combinaison linéaire de $\mathrm{Id}_E, u, \ldots, u^{n-1}$. On a donc montré que $Z(u) \subset \mathcal{P}_u$ (toute application qui commute avec u s'écrit comme un polynôme en u). D'après la question 2 de cette partie, la famille $(\mathrm{Id}_E, u, \ldots, u^{n-1})$ est libre et d'après ce que l'on vient de montrer, elle est génératrice de $Z(u)$. Elle en forme donc une base, ce qui implique que $Z(u)$ est de dimension n.