Lycée Louis-Le-Grand, Paris
MP2I – Mathématiques
A. Troesch

Pour le 07/05/2024

DM n° 23 : Algèbre linéaire : entraînement pour le DS

Ce devoir n'est pas à rendre. Il est donné en guise d'entraînement au DS du 07/05.

Corrigé du problème 1 – Sous-espaces stables par un endomorphisme

Partie I – Quelques résultats préliminaires sur les sous-espaces stables

1. **Intersection et somme de sous-espaces stables.** Soit $u \in \mathcal{L}(E)$.
   (a) $\boxed{E}$ est trivialement stable par u. On peut aussi considérer le sous-espace trivial $\{0\}$.
   (b) Soit $(F_i)_{i\in I}$ une famille de sous-espaces stables par u.
   - Soit $x \in \bigcap_{i\in I} F_i$. Pour tout $i \in I$, $x \in F_i$, donc par stabilité de F_i par u, $u(x) \in F_i$. Ainsi, ceci étant valable pour tout $i \in I$, $u(x) \in \bigcap_{i\in I} F_i$. On en déduit que $\boxed{\bigcap_{i\in I} F_i \text{ est stable par } u.}$
   - Soit $x \in \sum_{i\in I} F_i$. Il existe donc des $x_i \in I$ (presque tous nuls si I est infini) tels que $x = \sum_{i\in I} x_i$. Par linéarité, on a alors
   $$u(x) = \sum_{i\in I} u(x_i).$$
   Or, les $u(x_i)$ étant dans F_i (et presque tous nuls si I est infini), on en déduit que $u(x) \in \sum_{i\in I} F_i$, donc que $\boxed{\sum_{i\in I} F_i \text{ est stable par } u.}$

2. **Endomorphismes laissant stable un sous-espace donné.** Soit F un sous-espace de E.
   (a) Soit F stable par u et v.
   - Soit $x \in F$. On a $u(x) \in F$ et $v(x) \in F$. Comme F est un sous-espace vectoriel de E, il est stable par combinaison linéaire, donc $\lambda u(x) + v(x) \in F$. Ainsi, $\boxed{F \text{ est stable par } \lambda u + v.}$
   - Soit $x \in F$. Puisque F est stable par v, $v(x) \in F$, et puisque F est stable par u, $u(v(x)) \in F$, donc $u \circ v(x) \in F$. Ainsi, F est stable par $\boxed{u \circ v}$.

   (b) Soit $A = \{u \in \mathcal{L}(E) \mid u(F) \subset F\}$. Le sous-ensemble A de $\mathcal{L}(E)$ contient le neutre id_E, est stable par combinaison linéaire et par produit d'après la question précédente. Il s'agit donc d'une $\boxed{\text{sous-algèbre de } \mathcal{L}(E).}$
   (c) Une algèbre A sur un corps K étant stable par produit et par combinaison linéaire, pour tout $x \in A$, et tout polynôme P à coefficients dans K, $P(x)$ est un élément de A. Ainsi, avec les notations de la question précédente, si $u \in A$, pour tout $P \in K[X]$, $P(u) \in A$. En d'autres termes, si F est stable par u, alors $\boxed{F \text{ est stable par tout élément } P(u)}$ de $K[u]$ ($P \in K[X]$).

3. **Sous-espaces stables définis par des noyaux et images de polynômes en u.** Soit $u \in \mathcal{L}(E)$.
   (a)
   - Soit $x \in \mathrm{Ker}(u)$. On a $u(x) = 0$, donc $u(u(x)) = u(0) = 0$, donc $u(x) \in \mathrm{Ker}(u)$. Ainsi, $\boxed{\mathrm{Ker}(u) \text{ est stable par } u}$.
   - Soit $x \in \mathrm{Im}(u)$. On a évidemment $u(x) \in \mathrm{Im}(u)$ par définition de $\mathrm{Im}(u)$. Ainsi, $\boxed{\mathrm{Im}(u) \text{ est stable par } u}$.

   (b) Soit $P \in K[X]$.
   - Soit $x \in \mathrm{Ker}(P(u))$. On a donc $P(u)(x) = 0$, donc $u \circ P(u)(x) = 0$, et d'après la règle rappelée dans l'énoncé sur la commutation des polynômes d'endomorphisme, $P(u) \circ u(x) = 0$, c'est-à-dire $P(u)(u(x)) = 0$. Ainsi, $u(x) \in \mathrm{Ker}(P(u))$. Par conséquent, $\boxed{\mathrm{Ker}(P(u)) \text{ est stable par } u.}$

- Soit $x \in \operatorname{Im}(P(u))$. On fait de même : il existe y tel que $x = P(u)(y)$. On a alors

$$u(x) = u \circ P(u)(y) = P(u) \circ u(y) = P(u)(u(y)).$$

Ainsi, $u(x) \in \operatorname{Im}(P(u))$, donc $\boxed{\operatorname{Im}(P(u)) \text{ est stable par } u.}$

4. **Polynôme minimal ponctuel.** Soit $u \in \mathcal{L}(E)$ et $x \in E$.

(a) La famille $(u^k(x))_{k\in[\![0,n]\!]}$ est liée, car de cardinal $n+1$ alors que E est de dimension n. Ainsi, il existe une relation non triviale entre ces vecteurs, donc il existe des scalaires non tous nuls tels que

$$\boxed{0 = \sum_{k=0}^{n} \lambda_k u^k(x) = P(u)(x)},$$

avec $P = \sum_{k=0}^{n} \lambda_k X^k \neq 0$.

(b) Soit I_x l'ensemble des polynômes P tels que $P(u)(x) = 0$.

- On a évidemment $O \in I_x$
- Si P et Q sont dans I_x, $(P-Q)(u)(x) = P(u)(x) - Q(u)(x) = 0$, donc $P - Q \in I_x$;
- Ainsi, I_x est un sous-groupe additif de $K[X]$.
- Soit $P \in I_x$ et $Q \in K[X]$. On a alors

$$(PQ)(u)(x) = Q(u) \circ P(u)(x) = Q(u)(0) = 0.$$

Ainsi, $PQ \in I_x$.

- On en déduit que $\boxed{I_x \text{ est un idéal de } K[X]}$.

(c) L'idéal I_x n'est par réduit à $\{0\}$ d'après 4(a). Puisque K est un corps, $K[X]$ est principal, donc l'idéal I_x est engendré par un polynôme $\boxed{\pi_{u,x} \text{ qu'on peut choisir unitaire}}$. Ce polynôme divisant tout autre polynôme de I_x, il est de degré minimal parmi les polynômes non nuls de I_x.

5. **Sous-espaces cycliques.** Soit $u \in \mathcal{L}(E)$.

(a) Soit $\mathcal{F}$ l'ensemble des sous-espaces de E stables par u et tels que $X \subset F$. L'ensemble $\mathcal{F}$ n'est pas vide, puisqu'il contient trivialement E. On considère alors

$$\boxed{F_0 = \bigcap_{F\in\mathcal{F}} F}.$$

D'après 1(b), F_0 est stable par u. Il contient X car c'est le cas de chaque terme de l'intersection. Il est minimal pour cette propriété car par définition de l'intersection, pour tout $F \in \mathcal{F}$, $F_0 \subset F$.

(b)
- Puisque $< x >_u$ est stable par u, il est stable par u^k pour tout $k \in \mathbb{N}$ (question 2c), donc, puisque x en est un élément, $u^k(x) \in < x >_u$, pour tout $k \in \mathbb{N}$. S'agissant d'un espace vectoriel, on en conclut que $\operatorname{Vect}(u^k(x), k \in \mathbb{N}) \subset < x >_u$.
- Réciproquement, $F = \operatorname{Vect}(u^k(x), k \in \mathbb{N})$ est stable par u. En effet, soit $y = \sum_{k\in\mathbb{N}} \lambda_k u^k(x)$ un élément de F (les λ_k étant presque tous nuls). On a alors

$$u(y) = \sum_{k\in\mathbb{N}} \lambda_k u^{k+1}(x) \in F.$$

De plus, F contient x (prendre $k = 1$). Ainsi, par minimalité de $< x >_u$ pour ces propriétés, on a $< x >_u \subset \operatorname{Vect}(u^k(x), k \in \mathbb{N})$.

- Ainsi, $\boxed{< x >_u = \operatorname{Vect}(u^k(x), k \in \mathbb{N})}$
- La famille $(u^k(x))_{k\in[\![0,d-1]\!]}$ est libre, sinon on pourrait trouver une relation non triviale entre ces vecteurs, contredisant la minimalité du degré de $\pi_{u,x}$.
- Soit $y \in \operatorname{Vect}(u^k(x), k \in \mathbb{N})$. Il s'écrit donc sous la forme $y = P(u)(x)$, pour un certain polynôme P de $K[X]$. Soit $P = \pi_{u,x}Q + R$ la division euclidienne de P par $\pi_{u,x}$. On a alors $\deg(R) < \deg(\pi_{u,x})$. De plus

$$y = P(u)(x) = Q \circ \pi_{u,x}(u)(x) + R(u)(x) = R(u)(x).$$

Or, R étant de degré strictement plus petit que d, $R(u)(x)$ s'écrit comme combinaison linéaire des $u^k(x)$, pour $k \in [\![0, d-1]\!]$. Ainsi, $(u^k(x))_{kj\in[\![0,d-1]\!]}$ est génératrice de $\operatorname{Vect}(u^k(x), k \in \mathbb{N})$, donc de $< x >_u$.

- Par conséquent, $\boxed{\mathcal{B}_x = (u^k(x))_{k\in[\![0,d-1]\!]} \text{ est une base de } < x >_u.}$

(c) Soit $b_k = u^k(x)$, $k \in [\![0, d-1]\!]$. Pour tout $k \in [\![0, d-2]\!]$, on a $u(b_k) = b_{k+1}$, et de plus, en notant

$$\pi_{u,x} = X^d + \sum_{k=0}^{d-1} a_k X^k,$$

on a, puisque $\pi_{u,x}(u)(x) = 0$:

$$u(b_{d-1}) = u^d(x) = -\sum_{k=0}^{d-1} a_k u^k(x) = -\sum_{k=0}^{d-1} a_k b_k.$$

On obtient donc la matrice d'ordre d suivante :

$$\boxed{\mathrm{Mat}_{\mathcal{B}_x}(u_x) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d-2} \\ 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix}}$$

Soit u_x l'endomorphisme de $< x >_u$ induit par u sur le sous-espace stable $< x >_u$. Déterminer sa matrice dans la base $\mathcal{B}_x$ en fonction des coefficients du polynôme $\pi_{u,x}$.

Partie II – Sous-espaces stables par un projecteur ou une symétrie

Soit p un projecteur de E.

1. Soit F un sous-espace vectoriel de $\mathrm{Im}(p)$ et G un sous-espace vectoriel de $\mathrm{Ker}(p)$. Puisque p est un projecteur et que $F \subset \mathrm{Im}(p)$, pour tout $x \in F$, $p(x) = x \in F$. Donc F est stable par p. Par ailleurs, pour tout $x \in G$, $u(x) = 0 \in G$, donc G est stable par u. On en déduit que $\boxed{F + G \text{ est stable par } u}$ (question I-1(b))
2. Soit H un sous-espace vectoriel de E stable par p.
   - Puisque p est un projecteur, $\mathrm{Im}(p) \oplus \mathrm{Ker}(p) = E$. Donc $\mathrm{Im}(p) \cap \mathrm{Ker}(p) = \{0\}$, et donc

     $$(H \cap \mathrm{Im}(p)) \cap (H \cap \mathrm{Ker}(p)) = \{0\}.$$

     On en déduit que la somme $(H \cap \mathrm{Im}(p)) + (H \cap \mathrm{Ker}(p))$ est directe.
   - On a évidemment $(H \cap \mathrm{Im}(p)) + (H \cap \mathrm{Ker}(p)) \subset H$, les deux memebres de la somme vérifiant cette inclusion.
   - Soit $h \in H$. Comme $\mathrm{Im}(p) \oplus \mathrm{Ker}(p) = E$, on peut décomposer $h = x + y$, avec $x \in \mathrm{Im}(p)$ et $y \in \mathrm{Ker}(p)$. On a alors $p(x) = x$ et $p(y) = 0$, donc $p(h) = x$. Comme $h \in H$ et H stable par p, on en déduit que $x \in H$. Puis $y = h - x \in H$. Ainsi, $x \in \mathrm{Im}(p) \cap H$ et $y \in \mathrm{Ker}(p) \cap H$. On a bien obtenu

     $$h \in (H \cap \mathrm{Im}(p)) + (H \cap \mathrm{Ker}(p)),$$

     de quoi on déduit l'inclusion $H \subset (H \cap \mathrm{Im}(p)) + (H \cap \mathrm{Ker}(p))$.
   - Les deux inclusions amènent : $\boxed{H = (H \cap \mathrm{Im}(p)) \oplus (H \cap \mathrm{Ker}(p)).}$
3. La question 1 montre que la somme d'un sous-espace de $\mathrm{Im}(p)$ et d'un sous-espace de $\mathrm{Ker}(p)$ est stable par p. La question 2 montre que tout sous-espace stable est de cette forme.
   Ainsi, les sous-espaces stables sont exactement les sous-espaces s'écrivant sous la forme $\boxed{H = F + G}$, où F est un sev de $\mathrm{Im}(p)$ et G un sev de $\mathrm{Ker}(p)$.

Partie III – Diagonalisation

1. **Valeurs propres et espaces propres**

   (a) Le scalaire λ est valeur propre si et seulement s'il existe $x \in E$ non nul tel que $u(x) = \lambda x$, donc $(u - \lambda \mathrm{id})(x) = 0$, donc si et seulement si $\mathrm{Ker}(u - \lambda \mathrm{id})$ n'est pas réduit à 0. Cela équivaut à la non-injectivité de l'endomorphisme $u - \lambda \mathrm{id}$, donc à sa non bijectivité, puisque la dimension est finie.
   Ainsi, $\boxed{\lambda \text{ est valeur propre de } u \text{ si et seulement si } u - \lambda\mathrm{id} \text{ est pas un automophisme}}$.
   D'après ce qu'on vient de voir, les vecteurs propres associés à λ sont alors les vecteurs non nuls tels que $(u - \lambda \mathrm{id})(x) = 0$, c'est-à-dire tels que $\boxed{x \in \mathrm{Ker}(u - \lambda \mathrm{id})}$.

(b) Soit $\lambda_1, \dots, \lambda_k$ des valeurs propres de u et $F_1, \dots, F_k$ des sous-espaces vectoriels de $E_{\lambda_1}(u), \dots, E_{\lambda_k}(u)$. Pour tout $i \in [\![1,k]\!]$, et tout $x \in F_i$, on a $x \in E_{\lambda_i}(u)$, donc $u(x) = \lambda_i x \in F_i$, puisque F_i est stable par multiplication par un scalaire. Ainsi, pour tout $i \in [\![1,k]\!]$, F_i est stable par u. D'après la question I-1(b), $\boxed{F_1 + \cdots + F_k \text{ est stable par } u.}$

2. **Valeurs propres et polynôme annulateur**

(a) Soit P un polynôme, et x un vecteur propre de u, associé à une valeur propre λ. On a $u(x) = \lambda x$, puis $u^2(x) = \lambda u(x) = \lambda^2 x$, et par une récurrence immédiate, $u^k(x) = \lambda^k x$.
Notant $P = \sum_{k=0}^{d} a_k X^k$, on a alors

$$P(u)(x) = \sum_{k=0}^{d} a_k u^k(x) = \sum_{k=0}^{d} a_k \lambda^k x. = \boxed{P(\lambda)x}.$$

(b) Soit P un polynôme annulateur de u et $\lambda \in \mathrm{Sp}(u)$, et x un vecteur propre associé à λ. On a alors

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

Par définition d'un vecteur propre, $x \neq 0$, donc $P(\lambda) = 0$, donc $\lambda \in \mathrm{rac}(P)$. Ainsi, $\boxed{\mathrm{Sp}(u) \subset \mathrm{rac}(P).}$

(c) L'argument est à peu près le même que pour le polynôme minimal ponctuel, à part qu'on raisonne sur u au lieu de $u(x)$.

- I_u est non vide puisqu'il contient O le polynôme nul.
- Soit P et Q dans I_u. On a alors $P(u) = 0$ et $Q(u) = 0$, donc $(P - Q)(u) = P(u) - Q(u) = 0$. Donc $P - Q \in I_u$. On peut déjà conclure que I_u est un sous-groupe additif de $K[X]$.
- Soit P dans I_u et Q dans $K[X]$. On a alors

$$(PQ)(u) = Q(u) \circ P(u) = Q(u) \circ O_{\mathcal{L}(E)} = 0.$$

Ainsi, $PQ \in K[X]$. On en déduit que $\boxed{I_u \text{ est un idéal de } K[X].}$
- L'espace E étant de dimension finie n, $\mathcal{L}(E)$ est de dimension n^2, donc la famille $(u^0, u^1, \dots, u^{n^2})$ est liée, puisqu'on son cardinal est supérieur à la dimension de l'espace $\mathcal{L}(E)$ dans lequel sont les u^i. Une relation non triviale entre les objets de cette famille fournit un polynôme annulateur non nul de u. Ainsi, I_u n'est par réduit à $\{0\}$.
- Puisque $K[X]$ est principal, on en déduit que I_u est engendré par un polynôme π_u (qu'on peut choisir unitaire), de degré minimal parmi les polynômes non nul. On a alors $I_u = (\pi_u)$, donc par définition, tout P de I_u vérifie $\boxed{\pi_u \mid P.}$

(d) Soit λ une racine de π_u. On écrit $\pi_u = (X - \lambda)Q$, avec $Q \in K[X]$. On a alors

$$0 = \pi_u(u) = (u - \lambda \mathrm{id}) \circ Q(u).$$

Si λ n'est pas une valeur propre de u, d'après 1(a), $u - \lambda\mathrm{id}$ est un automorphisme, donc inversible dans l'anneau $\mathcal{L}(E)$, donc régulier. On en déduit que $Q(u) = 0$. Or, π_u étant non nul, $Q \neq 0$, et $\deg Q < \deg \pi_u$, donc π_u ne divise par Q, alors que Q est un polynôme annulateur de u. $\boxed{\text{Cela contredit la définition de } \pi_u}$.

(e) D'après la question précédente, toute racine de π_u est valeur propre de u, donc $\mathrm{rac}(\pi_u) \subset \mathrm{Sp}(u)$. Comme π_u annule u, l'inclusion réciproque est assurée par la question 2(b). Ainsi, $\boxed{\mathrm{rac}(\pi_u) = \mathrm{Sp}(u).}$

(f) Le polynôme π_u étant non nul, il admet un nombre fini de racines, donc d'après la question précédente, $\boxed{\text{l'ensemble } \mathrm{Sp}(u) \text{ est fini.}}$

3. **Lemme de décomposition des noyaux.** Soit $u \in \mathcal{L}(E)$.

(a) Soit P et Q deux polynômes de $K[X]$ premiers entre eux. D'après le théorème de Bezout, il existe deux polynômes U et V tels que

$$UP + BV = 1.$$

On a alors, en spécialisant à u :

$$U(u) \circ P(u) + B(u) \circ Q(u) = \mathrm{id}.$$

- Soit $x \in \mathrm{Ker}(P(u)) \cap \mathrm{Ker}(Q(u))$. On a alors, en appliquant l'identité précédente à x :

$$x = U(u)(P(u)(x)) + B(u)(Q(u)(x)) = U(u)(0) + B(u)(0) = 0.$$

Ainsi, $\mathrm{Ker}(P(u)) \cap \mathrm{Ker}(Q(u)) = \{0\}$, donc la somme est directe.

- On a trivialement $\mathrm{Ker}(P(u)) \subset \mathrm{Ker}(Q(u) \circ P(u)) = \mathrm{Ker}((PQ)(u))$, et de même pour $\mathrm{Ker}(Q(u))$. Par stabilité par somme, il vient alors
$$\mathrm{Ker}(P(u)) \bigoplus \mathrm{Ker}(Q(u)) \subset \mathrm{Ker}((PQ)(u)).$$
- Réciproquement, soit $x \in \mathrm{Ker}((PQ)(x))$. On applique l'identité obtenue ci-dessus à l'aide d'une relation de Bezout :
$$x = U(u) \circ P(u)(x) + V(u) \circ Q(u)(x).$$
Or,
$$Q(u)(U(u) \circ P(u)(x)) = Q(u) \circ U(u) \circ P(u)(x) = U(u) \circ P(u) \circ Q(u)(x) = U(u) \circ (PQ)(u)(x) = U(u)(0) = 0,$$
puisque $x \in \mathrm{Ker}((PQ)(x))$. Ainsi, $U(u) \circ P(u)(x) \in \mathrm{Ker}(Q(u)$. On montre de même que $V(u) \circ Q(u)(x) \in \mathrm{Ker}(P(u))$. Ainsi, on a bien décomposé x comme somme d'un élément de $\mathrm{Ker}(P(u))$ et d'un élément de $\mathrm{Ker}(Q(u))$. Par conséquent,
$$\mathrm{Ker}((PQ)(u)) \subset \mathrm{Ker}(P(u)) \bigoplus \mathrm{Ker}(Q(u)).$$
- Les deux inclusions amènent $\boxed{\mathrm{Ker}((PQ)(u)) \subset \mathrm{Ker}(P(u)) \bigoplus \mathrm{Ker}(Q(u)).}$

(b) On raisonne par récurrence sur $k \in \mathbb{N}^*$ pour montrer que si $P_1, \dots, P_k$ sont des polynômes deux à deux premiers entre eux, alors
$$\mathrm{Ker}((P_1 \cdots P_k)(u)) = \mathrm{Ker}(P_1(u)) \bigoplus \cdots \bigoplus \mathrm{Ker}(P_k(u)).$$
Le résultat est trivial pour $k = 1$. Il a été démontré dans la question précédente pour $k = 2$. Soit $k \geqslant 2$ tel que le résultat soit vrai pour k polynômes premiers entre eux 2 à 2, et considérons $P_1, \dots, P_{k+1}$ premiers entre eux deux à deux. On a alors $P_1 \cdots P_k$ et P_{k+1} qui sont premiers entre eux (les facteurs irréductibles de P_{k+1} n'étant facteur irréductible d'aucun autre P_i, donc par non plus du produit d'après le lemme d'Euclide). On utilise la question précédente, qui donne :
$$\mathrm{Ker}((P_1 \cdots P_{k+1})(u)) = \mathrm{Ker}((P_1 \cdots P_k)(u)) \bigoplus \mathrm{Ker}(P_{k+1}(u)).$$
L'hypothèse de récurrence amène alors :
$$\boxed{\mathrm{Ker}((P_1 \cdots P_{k+1})(u)) = \mathrm{Ker}(P_1(u)) \bigoplus \cdots \bigoplus \mathrm{Ker}(P_k(u)) \bigoplus \mathrm{Ker}(P_{k+1}(u))}.$$
Le principe de récurrence permet donc de conclure que la propriété est vraie pour tout $k \in \mathbb{N}^*$.

4. **Diagonalisabilité.**

(a) Considérons le polynôme $P = \prod_{i=1}^{k} (X - \lambda_i)$. Les λ_i étant deux à deux distincts, les polynômes $X - \lambda_i$ sont deux à deux premiers entre eux. D'après le lemme de décomposition des noyaux, il vient alors :
$$\boxed{\mathrm{Ker}(P(u)) = \bigoplus_{i=1}^{k} \mathrm{Ker}(u - \lambda_i \mathrm{id}) = \bigoplus E_{\lambda_i}(u).}$$
La propriété de somme directe fait partie du résultat fourni par le lemme de décomposition des noyaux.

(b) - Si u est diagonalisable, il existe une base $\mathcal{B} = (b_1, \dots, b_n)$ de E telle que $\mathrm{Mat}_{\mathcal{B}}(u)$ soit diagonale. Notons m_i son i-ième coefficient diagonal. On a donc, par définition de la matrice d'un endomorphisme, $u(b_i) = m_i b_i$ pour tout $i \in [\![1, n]\!]$, donc, b_i étant non nul, m_i est une valeur propre, et b_i est dans un espace propre, donc dans la somme des espaces propres. On a donc obtenu :
$$\forall i \in [\![1, n]\!], \quad b_i \in \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda(u).$$
Par stabilité par combinaison linéaire (ou par définition par minimalité de Vect), on a donc :
$$E = \mathrm{Vect}(b_1, \dots, b_n) \subset \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda(u).$$
L'incusion réciproque étant évidente, on a $\boxed{E = \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda(u).}$

- Réciproquement, si $E = \bigoplus_{\lambda\in \mathrm{Sp}(u)} E_\lambda(u)$, on obtient une base de E en juxtaposant des bases des $E_\lambda(u)$. Une telle base est constituée de vecteurs b_i appartenant chacun à l'un des espaces propres. Ainsi, pour tout $i \in [\![1, n]\!]$, il existe $\lambda_i \in \mathrm{Sp}(u)$ tel que $u(b_i) = \lambda_i$ Par définition de la matrice associée à u, la matrice $\mathrm{Mat}_{\mathcal{B}}(u)$ est donc diagonale, ses coefficients diagonaux étant les λ_i. L'endomorphisme $\boxed{u \text{ est donc diagonalisable.}}$

(c) On note $\lambda_1, \dots, \lambda_k$ les valeurs propres de u.

- Si u est diagonalisable, on a donc, en combinant 4a et 4b,

$$E = \mathrm{Ker}(\prod_{i=1}^{k}(u - \lambda_i \mathrm{id})).$$

Ainsi, en posant $P = \prod\limits_{i=1}^{k}(X - \lambda_i)$, $\mathrm{Ker}(P(u)) = E$, donc $P(u) = 0$, donc P est un polynôme annulateur de u. Ainsi, π_u divise P. Comme ce dernier est scindé à racines simples, $\boxed{\pi_u \text{ est aussi scindé à racines simples.}}$

- Réciproquement, supposons que π_u est scindé à racines simples. On a alors d'après 2(e) et le caractère unitaire de π_u,

$$\pi_u(X) = \prod_{i=1}^{k}(X - \lambda_k).$$

La question 4a amène alors

$$\mathrm{Ker}(\pi_u(u)) = \bigoplus_{i=1}^{k} E_{\lambda_k}(u).$$

Or, π_u étant un polynôme annulateur de u, $\mathrm{Ker}(\pi_u(u)) = E$, donc on est ramené à la question 4(b), nous permettant de conclure que $\boxed{u \text{ est diagonalisable}}$.

Partie IV – Description des sous-espaces stables

1. Les $P_i^{\alpha_i}$ sont deux à deux premiers entre eux. Le théorème de décomposition des noyaux amène donc :

$$\boxed{E = \mathrm{Ker}(\pi_u(u)) = \bigoplus_{i=1}^{k} \mathrm{Ker}(P_i^{\alpha_i}(u)).}$$

2. (a) Pour tout $P \in K[X]$, $P(u)$ laisse F stable (question I-2(c)) et coïncide clairement avec $P(v)$. Ainsi, $P(v)$ est l'endomorphisme induit par $P(u)$ sur F. En particulier, son noyau est obtenu en prenant l'intersection avec F du noyau de $P(u)$, d'après le cours. Ainsi, pour tout $i \in [\![1, k]\!]$,

$$\boxed{\mathrm{Ker}(P_i^{\alpha_i}(v)) = \mathrm{Ker}(P_i^{\alpha_i}(u)) \cap F.}$$

(b) Par ailleurs, $pi_u(u) = 0$, et comme dit dans la question précédente, $\pi_u(v)$ est l'endomorphisme induit sur F par π_u. On a donc aussi $\pi_u(v) = O_{\mathcal{L}(F)}$. Ainsi, en appliquen le lemme des noyaux à $\pi_u(v)$, on obtient cette fois :

$$F = \mathrm{Ker}(\pi_u(v)) = \bigoplus_{i=1}^{k} \mathrm{Ker}(P_i^{\alpha_i}(v)),$$

et en vertu de la question précédente,

$$\boxed{F = \bigoplus_{i=1}^{k} (\mathrm{Ker}(P_i^{\alpha_i}(u)) \cap F)}.$$

3. - D'après I-1(b), si F est somme de sous-espaces des $\mathrm{Ker}(P_i^{\alpha_i} u))$ chacun stable par u, alors $\boxed{F \text{ est stable par } u}$.
   - Réciproquement, si F est stable par u, la question précédente montre que $\boxed{F \text{ est somme de sous-espaces } F_i}$ des $\mathrm{Ker}(P_i^{\alpha_i}(u))$, chaque F_i étant défini par :

$$F_i = \mathrm{Ker}(P_i^{\alpha_i}(u)) \cap F.$$

De plus, F_i est intersection de sous-espaces stables par u (d'après I-3(b) pour le noyau), donc $\boxed{F_i \text{ est stable par } u}$ (d'après I-1(b)).

4. Comme on l'a déjà montré dans III-1(b) tout sous-espace F_i d'un espace propre de u est stable par u (car $x \in F_i$ vérifie $u(x) = \lambda x$). Ainsi, d'après la question précédente, les sous-espaces stables par u sont précisément les sous espaces obtenus comme $\boxed{\text{sommes de sev de chacun des espaces propres de } u.}$
   Cela complète la question III-1(b) en établissant la réciproque.
5. Pour un projecteur, un polynôme annulateur est donné par $X^2 - X$. D'après 2(b), les seules valeurs propres possibles sont 0 et 1 (éventuellement l'un seul des deux si $p = 0$ ou $p = \mathrm{id}$). D'après le cours, $\mathrm{Ker}(p) \oplus \mathrm{Im}(p) = E$, et $\mathrm{Im}(p) = \mathrm{Ker}(p - \mathrm{id})$. Cette décomposition correspond donc à celle de la question III-4(b). On en déduit que p est diagonalisable, et d'après ce qui précède, les sous-espaces stables sont bien obtenus comme $\boxed{\text{somme d'un sous-espace de } \mathrm{Ker}(p) \text{ et d'un sous-espace de } \mathrm{Im}(p).}$ C'est bien le résultat obtenu dans la partie II.
6. On suppose que u possède n valeurs propres distinctes, n étant la dimension de E.
   (a) Par définition, si λ est une valeur propre, $\mathrm{Ker}(u - \lambda \mathrm{id}) \neq \{0\}$, donc sa dimension est au moins 1. De plus, en notant $\lambda_1, \dots, \lambda_n$ les valeurs propres distinctes de u, d'après III-3b, on a une somme directe
   $$\bigoplus_{i=1}^{n} E_{\lambda_i}(u) \subset E.$$
   En passant aux dimensions,
   $$\dim(E) \geqslant \dim\left(\bigoplus_{i=1}^{n} E_{\lambda_i}(u)\right) = \sum_{i=1}^{n} \dim(E_{\lambda_i}(u)) \geqslant \sum_{i=1}^{n} 1 = n.$$
   Ceci implique que $\dim\left(\bigoplus_{i=1}^{n} E_{\lambda_i}(u)\right) = n$, donc que l'inclusion $\bigoplus_{i=1}^{n} E_{\lambda_i}(u) \subset E$ est une égalité donc d'après III-4(b), $\boxed{u \text{ est diagonalisable.}}$
   Par ailleurs, l'enchaînement des inégalités ci-dessus n'est possible que si toutes les inégalités considérées sont des égalités, ce qui nécessite, pour tout $i \in [\![1, n]\!]$, l'égalité $\boxed{\dim(E_{\lambda_i}(u)) = 1.}$ Ainsi, les sous-espaces propres sont tous des droites.
   (b) Les sous-espaces stables sont alors sommes de sous-espaces vectoriels des $E_{\lambda_i}(u)$. Or, chaque $E_{\lambda_i}(u)$ étant une droite, il n'a que deux sous-espaces possibles, $\{0\}$ et lui-même. On obtient donc une description simple des sous-espaces stables :
   $$\boxed{F_I = \bigoplus_{i \in I} E_{\lambda_i}(u)} \; I \in \mathcal{P}([\![1, n]\!]).$$
   Chaque choix de I fournit un sous-espace différent. En effet, si $I \neq I'$, il existe j tel que $j \in I$ et $j \in I'$ (ou l'inverse, qui se traite de même). Soit $x \in E_{\lambda_{j(u)}}$ non nul. On a alors $x \in F_I$, mais $x \notin F_{I'}$, car sinon, cela contredirait l'unicité de la décomposition de x dans la somme directe $\bigoplus_{i=1}^{n} E_{\lambda_i}(u)$, une première décomposition étant donnée par son appartenant à $F_{I'}$ ayant une composante nulle sur $E_{\lambda_j}(u)$, puisque $j \notin I'$, et une seconde étant donnée par lui-même sur $E_{\lambda_j}(u)$, et des 0 partout ailleurs.
   Ainsi, il y a autant de sous-espaces stables que de sous-ensembles I de $[\![1, n]\!]$, à savoir $\boxed{2^n}$.

Partie V – Endomorphismes semi-simples

1. Soit $y \in E$. On a par définition $\pi_u = 0_{\mathcal{L}(E)}$, donc en particulier $\pi_u(y) = 0$. L'ensemble des polynômes vérifiant cela étant par définition l'idéal engendré par $\pi_{u,y}$ (voir question I-4c), on en déduit que $\boxed{\pi_{u,y} \text{ divise } \pi_u.}$
2. On suppose dans cette question que π_u est irréductible. On souhaite montrer que u est semi-simple.
   (a) Soit y non nul dans E. Dans ce cas, $\pi_{u,y}$ n'est par constant. Comme il divise π_u qui est irréductible, on a nécessairement $\boxed{\pi_{u,y} = \pi_u}$.
   (b) Soit F un sous-espace stable par u tel que $F \neq E$, et soit $x \in E \backslash F$. Comme F et $< x >_u$ sont stables par u, $F \cap < x >_u$ est stable par u. On a alors
   De plus, supposons qu'il existe $y \neq 0$ dans cette intersection. Comme $F \cap < x >_u$ est un sous-espace vectoriel stable par u contenant y, on a, par minimalité de $< y >_u$, une inclusion $< y >_u \subset F \cap < x >_u \subset < x >_u$.

Par ailleurs x et y étant non nuls, ils ont, d'après 2a, même polynôme minimal ponctuel, égal à π_u. D'après I-5b, on en déduit que $< y >_u$ et $< x >_u$ ont même dimension. On déduit alors que les inclusions précédentes sont des égalités :

$$< y >_u = F\cap < x >_u = < x >_u .$$

La deuxième égalité contredit le fait que $x \notin F$. Ainsi, il n'existe pas d'élément non nul dans $F\cap < x >_u$, donc $\boxed{F\cap < x >_u = \{0\}}$.

(c) Soit F un sous-espace stable par u, et G un sous-espace stable par u de dimension maximale tel que $F \oplus G$ soit directe. Un tel sous-espace existe, car l'ensemble des sous-espaces stables en somme directe avec F est non vide (il constient $\{0\}$) et la dimension de ces espaces est bornée par la dimension de E.

Par I-1b, $F \oplus G$ est alors stable par u. Supposons que $F \oplus G \neq E$. Alors la question précédente donne l'existence de x tel que la somme $F \oplus G \oplus < x >_u$ soit directe. L'espace $G \oplus < x >_u$ est alors stable par u (toujours d'après I-1b), et de dimension strictement supérieur à G (car on a une inclusion stricte, obtenue en considérant x). De plus, sa somme avec F est directe. Cela contredit la maximalité du degré de G.

Ainsi, G est un supplémentaire de F, stable par u.

Pour tout sous-espace F stable par u, on a trouvé un supplémentaire de F stable par u, donc $\boxed{u \text{ est semi-simple.}}$

3. On suppose dans cette question que $\pi_u = P_1 \cdots P_k$, les P_i étant irréductibles unitaires distincts.

(a) Quitte à renuméroter les P_i, on peut se contenter de montrer que $\mathrm{Ker}(P_1(u)) \neq \{0\}$.

Si $\mathrm{Ker}(P_1(u)) = \{0\}$, $P_1(u)$ est un automorphisme, donc régulier dans $\mathcal{L}(E)$. L'égalité $P_1(u) \circ P_2(u) \circ \cdots \circ P_k(u) = 0$ se simplifie donc en $P_2(u) \circ \cdots \circ P_k(u) = 0$, ce qui contredit la minimalité du polynôme annulateur π_u. Ainsi, $\boxed{\mathrm{Ker}(P_1(u)) \neq \{0\}}$.

D'après la partie I, $\mathrm{Ker}(P_i(u))$ est stable par u. On peut donc considérer l'induit φ_i de u sur cet espace. On a alors, pour tout $x \in \mathrm{Ker}(P_i(u))$

$$P_i(v)(x) = P_i(u)(x) = 0.$$

Donc P_i est un polynôme annulateur de v. Le polynôme minimal π_v de v divise donc P_i qui est irréductible, donc $\pi_v = 1$ ou $\pi_v = P_i$. Le premier cas n'est pas possible (cela signifierait id $= 0$, ce qui contredit que $\mathrm{Ker}(P_i(u)) \neq \{0\}$). Ainsi, $\pi_v = P_i$.

Donc v_i a un polynôme minimal irréductible, donc d'après la question 2, $\boxed{v_i \text{ est semi-simple.}}$

(b) Soit F un sous-espace stable par u. On a alors, d'après IV-2b,

$$F = \bigoplus_{i=1}^{k} (\mathrm{Ker}(P_i^{\alpha_i}(u) \cap F)$$

Pour tout $i \in [\![1, k]\!]$, $\mathrm{Ker}(P_i^{\alpha_i}(u) \cap F$ est stable par v_i, qui est semi-simple. Cet espace admet donc un supplémentaire G_i dans $\mathrm{Ker}(P_i^{\alpha_i}(u)$, stable par v_i, donc aussi stable par u. On a alors

$$\begin{aligned} E = \bigoplus_{i=1}^{k} \mathrm{Ker}(P_i^{\alpha_i}(u)) &= \bigoplus_{i=1}^{k} (\mathrm{Ker}(P_i^{\alpha_i}(u) \cap F) \oplus G_i \\ &= \bigoplus_{i=1}^{k} (\mathrm{Ker}(P_i^{\alpha_i}(u) \cap F) \oplus \bigoplus_{i=1}^{k} G_i = F \oplus G, \end{aligned}$$

où on a posé $G = \bigoplus_{i=1}^{k} G_i$, stable par u d'après I-1b et la stabilité de chaque G_i.

Ainsi, on a bien trouvé un supplémentaire de F stable par u, donc $\boxed{u \text{ est semi-simple.}}$

4. On suppose inversement qu'il existe un irréductible unitaire P de $K[X]$ tel que P^2 divise π_u. On note $\pi_u = PQ$, avec $Q \in K[X]$. Soit $F = \mathrm{Ker}(P(u))$. Le sous-espace F est stable par u d'après I-3. Supposons qu'il existe un supplémentaire S de F stable par u.

(a) Soit $x \in S$. On a alors

$$0 = \pi_u(u)(x) = P(u) \circ Q(u)(x) = P(u)(Q(u)(x)).$$

Ainsi, $\boxed{Q(u)(x) \in \mathrm{Ker}(P(u)) = F}$. Or, S étant stable par u, il est stable par $Q(u)$ aussi (I-2). Comme $x \in S$, il vient donc $Q(u)(x) \in S$. On a donc $Q(u)(x) \in S \cap F = \{0\}$, ces deux espaces étant supplémentaires. Ainsi, $\boxed{Q(u)(x) = 0}$.

(b) Pour tout $x \in F$, $P(u)(x) = 0$, donc aussi $Q(u)(x) = 0$, puisque P est aussi encore facteur de Q par hypothèse. Pour tout $x \in S$, on a aussi $Q(u)(x) = 0$. Ainsi, par linéarité, pour tout $x \in E = F \oplus S$, on a $Q(u)(x) = 0$, donc Q est un polynôme annulateur de u. Cela contredit la minimalité de P.

Ainsi, $\mathrm{Ker}(P(u))$ est stable par u mais n'admet pas de supplémentaire stable par u. On en déduit que $\boxed{u \text{ n'est pas semi-simple.}}$

On a donc montré que u est semi-simple si et seulement si son polynôme minimale n'a pas de facteur irréductible multiple.

Partie VI – $K[u]$**-modules et sous-espaces stables**

1. L'application $\varphi_u : K[X] \to \mathcal{L}(E)$ définie par $\varphi_u(P) = P(u)$ est un morphisme d'anneau : on a en effet $\varphi_u(1) = \mathrm{id}_{\mathcal{L}(E)}$, $\varphi_u(P+Q) = (P+Q)(u) = P(u) + Q(u) = \varphi_u(P) + \varphi_u(Q)$ et $\varphi_u(PQ) = (PQ)(u) = P(u) \circ Q(u) = phi_u(P) \circ \varphi_u(Q)$.

   Ainsi, l'image de φ_u est un anneau. Or par définition, $\mathrm{Im}(\varphi_u) = K[u]$. Ainsi, $\boxed{K[u] \text{ est un anneau.}}$

   Par ailleurs, par définition, $\mathrm{Ker}(\varphi_u)$ est l'idéal des polynômes annulateurs de u, engendré par π_u. En quotientant par le noyau et en corestreingant à l'image, on obtient donc un isomorphisme d'anneaux $\boxed{K[X]/(\pi_u) \simeq K[u].}$

2. On a déjà la structure de groupe abélien provenant de la structure d'espace vectoriel sur K. Il reste à vérifier les propriétés relatives au produit externe :
   - $(P(u) \circ Q(u)) \cdot x = P(u) \circ Q(u)(x) = P(u)(Q(u)(x)) = P(u) \cdot Q(u)(x) = P(u) \cdot (Q(u) \cdot x)$.
   - $\mathrm{id} \cdot x = \mathrm{id}(x) = x$
   - $P(u) \cdot (x+y) = P(u)(x+y) = P(u)(x) + P(u)(y) + P(u) cdotx + P(u) \cdot y$
   - $(P(u) + Q(u)) \cdot x = (P+Q)(u)(x) = P(u)(x) + Q(u)(x) = P(u) \cdot x + Q(u) \cdot x$.

   Ainsi, toutes les propriétés requises sont satisfaites : $\boxed{E \text{ est un } K[u]\text{-module.}}$

3. Soit M un sous-$K[u]$-module de E. Alors M est par définition non vide, stable par somme, et stable par multiplication externe définie comme ci-dessus par un élément de $K[u]$. Les deux autres propriétés étant satisfaites, il suffit de vérifier que M est stable par multiplication par un scalaire λ de K.

   Considérons l'élément $\lambda \mathrm{id} \in K[u]$. Pour tout $x \in M$, on a alors $(\lambda \mathrm{id}) \cdot x \in M$, c'est-à-dire $\lambda x \in M$.

   Ainsi, M est non vide, stable par somme et par multiplication par un scalaire λ de K. Donc $\boxed{M \text{ est un sous-}K\text{-ev de } E.}$

   la réciproque n'est pas vraie en général. Supposons que tout sous-K espace vectoriel de u soit un sous-$K[u]$-module. En particulier, pour tout $x \in E$, la droite Kx est stable par $K[u]$. En prenant $u \in K[u]$, on obtient la stabilité de Kx par u. Ainsi, toute droite est stable par u. En d'autres termes, pour tout $x \in E$, x et $u(x)$ sont liés. Cela ne vous rappelle par quelque chose ?

   On en déduit que $\boxed{u \text{ est une homothétie}}$. Réciproquement, si u est une homothétie, on a un polynôme annulateur de degré 1 (de la forme $\pi_u = X - \lambda$). Ainsi, $K[u] = K/(X-\lambda) \simeq K$ (par division euclidienne). Via cet isomorphisme, la loi externe définie sur $K[u]$ coïncide avec celle définie sur K. Ainsi, les notions de $K[u]$-module et de K-ev coïncident dans cette situation.

4. Soit F un sous-espace vectoriel de E.
   - Si F est stable par u, il est stable par tout élément $P(u)$ de $K[u]$. Ainsi, il est stable par produit externe par un élément $P(u)$ de $K[u]$. Comme par ailleurs, il est aussi stable par somme (en tant que sev) et contient 0, il s'agit bien d'un $\boxed{\text{sous-}K[X]\text{-module de } E.}$
   - Récirpoquement si F est un sous-$K[X]$-module de E, il est stable par muliplication externe par tout $P(u)$ de $K[u]$, donc en particulier, il est stable par muliplication externe par u, ce qui équivaut à la $\boxed{\text{stabilité du sev } F}$ par l'endomorphisme u.

5. On suppose que π_u est irréductible.

   (a) L'anneau $K[u]$ est isomorphe à $K[X]/(\pi_u)$. On a déjà montré que cet anneau est un corps lorsque π_u est irréductible. En effet, si a est un élément non nul, représenté par un polynôme Q, ce polynôme est premier avec π_u (car leur pgcd divisant π_u, il est 1, ou π_u, par irréductibilité, ce dernier cas étant impossible, sinon a serait nul). Soit $UQ + V\pi_u = 1$ une relation de Bezout. On passe dans le quotient : $\overline{U}a = 1$. Cela prouve bien l'inversibilité de a.

   Donc $K[X]/(\pi_u)$ est un corps, donc $\boxed{K[u] \text{ est un corps}}$.

   (b) En particulier, puisque $K[u]$ est un corps, les $K[u]$-modules sont en fait des $K[u]$-ev. Soit alors F stable par u. F est donc un sous-$K[u]$-ev de E. Puisqu'on travaille ici avec des espaces vectoriels et non seulement des modules, F admet donc un supplémentaire G en tant que $K[u]$-ev (on est en dimension finie, et même sinon, on pourrait le faire avec l'axiome du choix). Ainsi, ce supplémentaire est un K-ev muni d'une structure de $K[u]$-ev donc stable par u et est un supplémentaire de F également au sens des K-ev.

On a bien montré que tout sous-espace stable admet un supplémentaire stable par u.

Ainsi, $\boxed{u \text{ est semi-simple.}}$

Partie VII – Endomorphismes cycliques et endomorphismes simples

1. On suppose dans cette question que u est cyclique, et on fixe $x \in E$ tel que $< x >_u = E$. Soit F un sous-espace stable par u.

   (a) C'est toujours pareil, il suffit de montrer que I est un idéal de $K[X]$. La stabilité de F par somme nous donne facilement la structure de groupe abélien. Si $P \in I$ et $Q \in K[X]$, $(QP)(u)(x) = Q(u)(P(u)(x))$. Comme $P(u)(x)$ est dans F qui est stable par u, donc aussi par $Q(u)$, on en déduit que $(QP)(u)(x) \in F$, donc $QP \in I$.

   Ainsi, I est un idéal de $K[X]$, non nul puisqu'il contient tout polynôme annulateur de u (donc en particulier π_u). Il est donc engendré par un polynôme unitaire D : $\boxed{I = (D).}$ De plus, puisque $\pi_u \in I$, on a alors $\boxed{D \mid \pi_u}$.

   (b)
   - Puisque $D(u)(x) \in F$ et F est stable par u, par minimalité de $< D(u)(x) >_u$ pour cette propriété, on a l'inclusion $< D(u)(x) >_u \subset F$.
   - Réciproquement, si $y \in F$, comme $< x >_u = E$, et par description de $< x >_u$ (I-5b), il existe P tel que $y = P(u)(x)$. Comme $y \in F$, par définition de I (question précédente), on a $P \in I$, et cet idéal étant engendré par D, il existe un polynôme Q tel que $P = QD$. On a alors $y = Q(u)(D(u)(x)) \in < D(u)(x) >_u$. Par conséquent, $F \subset < D(u)(x) >_u$.
   - Les deux inclusions donnent l'égalité $\boxed{< D(u)(x) >_u = F}$.

   (c) Puisque x est fixé, un sous-espace stable est entièrement déterminé par la seule donnée d'un diviseur unitaire D de π_u (en disant cela, on n'affirme pas que le choix de deux diviseurs distincts fournit deux sous-espaces stables distincts). Comme π_u admet un nombre fini de diviseurs unitaires (donné par le choix, pour chaque facteur irréductible intervenant dans π_u, de sa multiplicité, devant rester inférieur ou égal à la multiplicité totale dans π_u), on en déduit qu'il existe $\boxed{\text{un nombre fini de sous-espaces stables par } u.}$

2. On suppose que K est infini. Supposons que E n'admet qu'un nombre fini de sous-espaces stables par u. En particulier, E n'admet qu'un nombre fini de sous-espaces cycliques de la forme $< x >_u$. On note $F_1, \dots, F_k$ les sous-espaces de ce type. Chaque élément $x \in E$ appartient à l'un des F_i (car $x \in < x >_u$, et par définition $< x >_u$ est l'un des F_i). Ainsi, $E = F_1 \cup \cdots \cup F_n$.

   On a déjà vu en exercice que si K est infini, E n'est pas l'union de sous-espaces vectoriels stricts. En effet, supposons que les F_i sont des sev stricts. On peut alors considérer $x \in F_1 \cup \cdots \cup F_{n-1}$ tel que $x \notin F_n$ (sinon, on a une inclusion, et l'égalité de l'union à E amène F_n, ce qui contredit notre hypothèse). Quitte à supprimer certains des derniers termes de l'union, on peut supposer que $F_1 \cup \cdots \cup F_{n-1} \neq E$, et on peut faire le même raisonnement de façon symétrique : il existe $y \in F_n$ tel que $y \notin F_1 \cup \cdots \cup F_{n-1}$. Considérons alors les vecteurs $x + ty$, pour $t \in K$. Ces vecteurs sont en nombre infini (car K est infini), et sont chacun dans l'un des F_i, qui sont en nombre fini. Il existe donc au moins deux valeurs distinctes t_1 et t_2 tels que $x + t_1 y$ et $x + t_2 y$ sont dans le même F_i (principe des tiroirs). On a alors, par différence, $(t_2 - t_1)y \in F_i$, donc puisque $t_2 - t_1 \neq 0$, $y \in F_i$. Cela contredit la définition de y, sauf si $i = n$. Mais dans ce cas, puisque $x + t_1 y \in F_n$ et $y \in F_n$, on obtient $x \in F_n$, ce qui contredit cette fois la définition de x.

   Ainsi, E ne peut pas être une union finie de sous-espaces stricts. On en déduit que l'un des F_i est égal à E. Or, pour un tel i, par définition des F_i, il existe un vecteur x tel que $< x >_u = F_i = E$. On en déduit que $\boxed{u \text{ est cyclique.}}$

3. Dans cette question, on souhaite montrer que u est simple si et seulement si son polynôme minimal est irréductible de degré égal à $n = \dim(E)$.

   (a) Comme précédemment, π_u étant irréductible, $K[u]$ est un corps, isomorphe à $K[X]/(\pi_u)$. Nous avons déjà eu l'occasion de montrer que les classes de $1, X, \dots, X^{d-1}$ forment alors une base sur K de cet espace. Ainsi, $K[u]$ est un K-ev de dimension d. Soit F un sous-$K[u]$-espace vectoriel de E, de dimension k. Soit $c_1, \dots, c_k$ une base de F en tant que $K[u]$-ev. Soit $(b_1, \dots, b_d)$ une base de $K[u]$ en tant que K-ev. La famille $(b_i c_j)$ est alors une base de F en tant que K-ev. En effet,

- elle est génératrice : soit $x \in F$, il existe des éléments $\lambda_1, \ldots, \lambda_k$ de $K[u]$ tels que

$$x = \sum_{j=1}^{k} \lambda_j c_j.$$

Comme les λ_j sont dans $K[u]$ et que $(b_1, \ldots, b_d)$ est une base de $K[u]$ sur k, il existe, pour tout $j \in [\![1, k]\!]$, des scalaires $\mu_{1,j}, \ldots, \mu_{d,j}$ tels que

$$\lambda_j = \sum_{i=1}^{d} \mu_{i,j} b_i.$$

On a donc : $x = \displaystyle\sum_{j=1}^{k} \sum_{i=1}^{d} \mu_{i,j} b_i c_j$;

- elle est libre : en effet, soit $(m_{i,j})$ une famille de scalaires de K tels que

$$0 = \sum_{(i,j) \in [\![1,d]\!] \times [\![1,k]\!]} \mu_{i,j} b_i c_j. = \sum_{j=1}^{k} \left(\sum_{i=1}^{d} \mu_{i,j} b_i \right) c_j.$$

Les éléments $\displaystyle\sum_{i=1}^{d} \mu_{i,j} b_i$ étant dans $K[u]$, par liberté de la famille (c_j) sur $K[u]$, on obtient, pour tout $j \in [\![0, k]\!]$, $\displaystyle\sum_{i=1}^{d} \mu_{i,j} b_i = 0$, puis par liberté de (b_i), pour tout $j \in [\![0, k]\!]$, pour tout $i \in [\![0, d]\!]$, $\mu_{i,j} = 0$.

Ainsi, la dimension sur K de F est kd, donc $\boxed{\text{divisible par } d.}$

(b) Si π_u est irréductible de degré n, tout sous-espace stable F sera donc un sous-$K[u]$-ev de E, donc de K-dimension divisible par $n = \dim E$, ceci n'est possible que si $F = \{0\}$ ou $F = E$. Ainsi, u est simple.

(c) Réciproquement, si u est simple, il est en particulier semi-simple, donc π_u n'admet pas de facteur multiple dans sa décomposition irréductible. S'il admet plusieurs facteurs irréductibles, la décomposition en noyaux de la question IV-1 fournit une décomposition non triviale de E en somme directe de sous-espaces stables, ce qui conredit la simplicité de u. Ainsi, π_u est irréductible. D'après ce qui précède, son degré d va diviser n (car E est un $K[u]$-module). Si $d \neq n$, E est de $K[u]$-dimension strictement supérieure à 1, donc admet des sous-$K[u]$-ev stricts non triviaux, correspondant à des sous-ev stricts non triviaux de E stables par u. cela contredit la simplicité de u.

Ainsi, $\boxed{\text{le polynôme minimal de } u \text{ est irréductible de degré } n.}$

Corrigé du problème 2 – Dualité et théorème d'Erdös-Kaplansky

Partie I – Résultats préliminaires

1. **Famille duale d'une base, base duale**

(a) Soit $x \in E$, de coordonnées $(x_\beta)_{\beta \in \mathcal{B}}$ dans la base $\mathcal{B}$. Ainsi, par linéarité de b^*,

$$\begin{aligned} b^*(x) &= b^* \left(\sum_{\beta \in \mathcal{B}} x_\beta \beta \right) \\ &= \sum_{\beta \in \mathcal{B}} x_\beta b^*(\beta) \\ &= \sum_{\beta \in \mathcal{B}} x_\beta \delta_{b,\beta} \\ &= \boxed{x_b} \end{aligned}$$

Ces calculs sont justifiés par le fait que par définition d'une base, et de la décomposition d'un vecteur dans une base, la somme ne contient qu'un nombre fini de termes non nuls.

(b) Soit $(\lambda_b)_{b \in \mathcal{B}}$ une famille de scalaires à support fini. On suppose que

$$\sum_{b \in \mathcal{B}} \lambda_b b^* = 0.$$

Soit $\beta \in \mathcal{B}$. On a alors, en évaluant en β :

$$0 = \sum_{b \in \mathcal{B}} \lambda_b b^*(\beta) = \sum_{b \in \mathcal{B}} \lambda_b \delta_{b,\beta} = \lambda_\beta.$$

Ainsi, pour tout $\beta \in \mathcal{B}$, $\lambda_\beta = 0$. On en déduit que $\boxed{(b^*)_{b \in \mathcal{B}} \text{ est libre}}$.

(c) On suppose E de dimension finie n. Se servir de la dimension de E^* (vue dans le cours) est ici un peu abusif, car la démonstration du cours repose en fait sur l'étude de cette base (qui est un cas particulier de la base des $(u_{i,j})$ construite dans le cours pour $\mathcal{L}(E,F)$). On montre donc de façon directe le caractère générateur de $\mathcal{B}^*$, en remarquant que d'après la question 1(a),

$$\forall x \in E, \quad x = \sum_{i=1}^{n} b_i^*(x) b_i,$$

où on a noté $(b_1, \dots, b_n)$ la base $\mathcal{B}$. Ainsi, si $\varphi \in E^*$, on peut écrire, par linéarité :

$$\forall x \in E, \quad \varphi(x) = \sum_{i=1}^{n} b_i^*(x) \varphi(b_i),$$

et donc :

$$\varphi = \sum_{i=1}^{n} \varphi(b_i) b_i^* \in \mathrm{Vect}(b_1^*, \dots, b_n^*).$$

Cela montre que $\mathcal{B}^*$ est génératrice de E^*, et donc, d'après 1(b), $\boxed{\mathcal{B}^* \text{ est unne base de } E^*}$.

2. **Codimension d'un espace vectoriel**

(a) Un vecteur $x \in E$ est dans $\mathrm{Ker}(p_{|S})$ si et seulement s'il est dans le domaine de définition S et vérifie $p_{|S}(x) = p(x) = 0$. Ainsi

$$\mathrm{Ker}(p_{|S}) = S \cap \mathrm{Ker}(p) = S \cap F \qquad \text{donc:} \qquad \boxed{\mathrm{Ker}(p_{|S}) = \{0\}},$$

puisque S et F sont supplémentaires. On en déduit que $\boxed{p_{|S} \text{ est injective}}$.

(b)
- Soit $\mathcal{B}$ une base de S. Puisque $p_{|S}$ est injective, l'image par $p_{|S}$ est une famille libre $\mathcal{C}_0 = (p(b))_{b \in \mathcal{B}}$ de $\mathrm{Im}(p_{|S}) \subset T$. On peut donc la compléter en $\boxed{\text{une base } \mathcal{C} \text{ de } T}$.
- De plus, la construction de la base $\mathcal{C}$ montre que la restriction i de p à $\mathcal{B}$ est une bijection de $\mathcal{B}$ sur $\mathcal{C}_0 \subset \mathcal{C}$, donc une $\boxed{\text{injection } i : \mathcal{B} \to \mathcal{C}}$.

(c)
- On en déduit que $|\mathcal{B}| \leqslant |\mathcal{C}|$ (notation du préambule). Ainsi, $\dim(S) \leqslant \dim(T)$ (inégalité au sens des cardinaux)
- L'argument pouvant être symétrisé en intervertissant le rôle de S et T, on a aussi $\dim(T) \leqslant \dim(S)$. Donc, d'après le théorème de Cantor-Bernstein, $\boxed{\dim(S) = \dim(T)}$.
- Remarquez que pour que cet argument soit valide, il faut disposer du théorème de la dimension, nous assurant qu'on n'est pas obligé de garder les mêmes bases pour la réciproque, et donc que les dimensions sont bien définies au sens des cardinaux.

Partie II – Dualité en dimension finie

1.
- $(x, y) \mapsto \langle x, \varphi \rangle$ est bien une forme (à valeurs dans $\mathbb{K}$)
- Linéarité par rapport à la première variable. Soit $(x, y) \in E^2$, $\lambda \in \mathbb{K}$, et $\varphi \in E^*$. On a alors :

$$\langle x + \lambda y, \varphi \rangle = \varphi(x + \lambda y) = \varphi(x) + \lambda \varphi(y) = \langle x, \varphi \rangle + \lambda \langle y, \varphi \rangle,$$

car φ est linéaire.
- Linéarité par rapport à la deuxième variable. Soit $x \in E$, $(\varphi, \psi) \in E^*$, et $\lambda \in \mathbb{K}$. Alors :

$$\langle x, \varphi + \lambda \psi \rangle = (\varphi + \lambda \psi)(x) = \varphi(x) + \lambda \psi(x) = \langle x, \varphi \rangle + \lambda \langle x, \psi \rangle.$$

- Ainsi, $\boxed{(x, \varphi) \mapsto \langle x, \varphi \rangle \text{ est une forme bilinéaire}}$.

2. Soit $x \in E$. On a alors, pour tout $\varphi \in E^*$

$$\tilde{x}(\varphi) = \langle x, \varphi \rangle .$$

Ainsi, la linéarité de $\tilde{x}$ provient de la bilinéarité de $(x,\varphi) \mapsto \langle x, \varphi \rangle$. Il s'agit ici plus précisément de la linéarité par rapport à sa deuxième variable. Puisque $\tilde{x}$ va bien de E^* dans $\mathbb{K}$, on en déduit alors que $\boxed{\tilde{x} \in E^{**}}$.

3. • La linéarité de J équivaut à la linéarité par rapport à la première variable de $(x,y) \mapsto \langle x, y \rangle$, donc est acquise. En effet, si $(x,y) \in E^2$ et $\lambda \in \mathbb{K}$, pour tout $\varphi \in E^*$:

$$J(x+\lambda y)(\varphi) = \langle x+\lambda y, \varphi \rangle = \langle x, \varphi \rangle + \lambda \langle y, \varphi \rangle = J(x)(\varphi) + \lambda J(y)(\varphi).$$

• Soit $x \neq 0$. Montrons que $x \notin \mathrm{Ker}(J)$, donc qu'il existe $\varphi \in E^*$ tel que $\tilde{x}(\varphi) \neq 0$, i.e. $\varphi(x) \neq 0$.
Pour construire une telle forme linéaire φ, on considère S un supplémentaire de $\mathbb{K}x$ dans E. Soit alors $y \in E$, et $y = \lambda x + s$ sa décomposition dans la somme directe $E = \mathbb{K}x \oplus S$. On définit :

$$\varphi(y) = \varphi(\lambda x + s) = \lambda.$$

Une vérification sans difficulté montre que φ est linéaire (on peut aussi construire φ par rigidité en considérant une base de S complétée par x en une base de E), et $\varphi(x) = 1 \neq 0$.
Ainsi, $x \notin \mathrm{Ker}(J)$.

• On en déduit que $\mathrm{Ker}(J) = \{0\}$, donc que $\boxed{J \text{ est injective}}$.

• Si E est de dimension finie, la question 1(c) appliquée successivement à E et E^* montre que $\dim E = \dim E^* = \dim E^{**}$, donc, par caractérisation des isomorphismes en dimension finie, on en déduit que $\boxed{J \text{ est un isomorphisme}}$.

Partie III – Orthogonalité duale

1. **Propriétés élémentaires**

(a) • Étude de G°.

* Par définition $G^\circ \subset E^*$.
* Pour tout $x \in G$, $\langle x, 0 \rangle = 0(x) = 0$, donc $0 \in G^\circ$ (ici $0 = 0_{E^*}$, c'est donc l'application nulle).
* Soit $(\varphi, \psi) \in G^\circ$ et $\lambda \in \mathbb{K}$. Alors, pour tout $x \in G$,

$$\langle x, \varphi + \lambda\psi \rangle = \langle x, \varphi \rangle + \lambda \langle x, \psi \rangle = 0.$$

Donc $\varphi + \lambda\psi \in G^\circ$.

* Ainsi, $\boxed{G^\circ \text{ est un sous-espace vectoriel de } E^*}$.

• Étude de H°.

* Par définition $H^\circ \subset E$.
* Pour tout $\varphi \in H$, $\langle 0, \varphi \rangle = \varphi(0) = 0$, donc $0 \in H^\circ$.
* Soit $(x,y) \in H^\circ$ et $\lambda \in \mathbb{K}$. Alors, pour tout $\varphi \in H$:

$$\langle x + \lambda y, \varphi \rangle = \langle x, \varphi \rangle + \lambda \langle y, \varphi \rangle = 0.$$

Ainsi, $x + \lambda y \in H^\perp$.

* Par conséquent, $\boxed{H^\circ \text{ est un sous-espace vectoriel de } E}$

(b) • Soit $x \in G$. Pour tout $\varphi \in G^\circ$, on a $\langle x, \varphi \rangle = 0$ par définition de G°. Ceci étant vrai pour tout $\varphi \in G^\circ$, par définition de $(G^\circ)^\circ$, on obtient $x \in G^{\circ\circ}$. Ainsi, $\boxed{G \subset G^{\circ\circ}}$.

• Soit $\varphi \in H$. Pour tout $x \in H^\circ$, on a $\langle x, \varphi \rangle = 0$ par définition de H°. Ceci étant vrai pour tout $x \in H^\circ$, par définition de $(H^\circ)^\circ$, on obtient $\varphi \in H^{\circ\circ}$. Ainsi, $\boxed{H \subset H^{\circ\circ}}$.

(c) • Soit G_1 et G_2 sont deux sous-espaces de E tels que $G_1 \subset G_2$. Soit $\varphi \in G_2^\circ$. Ainsi, pour tout $x \in G_2$, $\langle x, \varphi \rangle = 0$. Comme $G_1 \subset G_2$, a fortiori, l'égalité $\langle x, \varphi \rangle = 0$ est aussi vraie pour tout $x \in G_1$, donc $\varphi \in G_1^\circ$. On en déduit que $\boxed{G_2^\circ \subset G_1^\circ}$.

• Soit H_1 et H_2 sont deux sous-espaces de E^* tels que $H_1 \subset H_2$. Soit $x \in H_2^\circ$. Ainsi, pour tout $\varphi \in H_2$, $\langle x, \varphi \rangle = 0$. Comme $H_1 \subset H_2$, a fortiori, l'égalité $\langle x, \varphi \rangle = 0$ est aussi vraie pour tout $\varphi \in H_1$, donc $x \in H_1^\circ$. On en déduit que $\boxed{H_2^\circ \subset H_1^\circ}$.

(d) Soit f l'application de E^* dans $G^* \times S^*$ définie par

$$f(\varphi) = (\varphi_{|G}, \varphi_{|S}).$$

- Linéarité. Soit $(\varphi, \psi) \in E^*$ et $\lambda \in \mathbb{K}$. Alors

$$\begin{aligned} f(\varphi + \lambda\psi) &= ((\varphi + \lambda\psi)_{|G}, (\varphi + \lambda\psi)_{|S}) \\ &= (\varphi_{|G} + \lambda\psi_{|G}, \varphi_{|S} + \lambda\psi_{|S}) \\ &= (\varphi_{|G}, \varphi_{|S}) + \lambda(\varphi_{|S}, \varphi_{|S}) \\ &= f(\varphi) + \lambda f(\psi). \end{aligned}$$

- Injectivité. Soit $\varphi \in \mathrm{Ker}(f)$. Alors $\varphi_{|G} = 0$ et $\varphi_{|S} = 0$. Soit $x \in E = G \oplus S$, et $x = x_G + x_S$ sa décomposition dans cette somme directe. On a alors

$$\varphi(x) = \varphi(x_G) + \varphi(x_S) = \varphi_{|G}(x_G) + \varphi_{|S}(x_S) = 0.$$

  Ainsi, $\mathrm{Ker}(f) = \{0\}$, donc f est injective.
- Surjectivité. N'étant pas en dimension finie, on est obligé de la vérifier. Soit $(\alpha, \beta) \in G^* \times S^*$. Avec les mêmes notations que ci-dessus pour la décomposition de x dans $G \oplus S$, on définit φ par :

$$\forall x \in E, \quad \varphi(x) = \alpha(x_G) + \beta(x_S).$$

  On vérifie facilement que φ est bien linéaire. En effet, si $(x, y) \in E^2$, $\lambda \in \mathbb{K}$, et $z = x + \lambda y$, on a

$$z = (x_G + \lambda y_G) + (x_S + \lambda y_S),$$

  et puisque $x_G + \lambda y_G \in G$ et $x_S + \lambda y_S \in S$, on obtient, du fait que la somme est directe :

$$z_G = x_G + \lambda y_G \qquad \text{et} \qquad z_S = x_S + \lambda y_S.$$

  Par conséquent,

$$\begin{aligned} \varphi(x + \lambda y) = \varphi(z) &= \alpha(z_G) + \beta(z_S) \\ &= \alpha(x_G + \lambda y_G) + \beta(x_S + \lambda y_S) \\ &= \alpha(x_G) + \lambda\alpha(y_G) + \beta(x_S) + \lambda\beta(y_S) \\ &= \varphi(x) + \lambda\varphi(y) \end{aligned}$$

  Ainsi, $\varphi \in E^*$, et de façon évidente, $\varphi_{|G} = \alpha$ et $\varphi_{|\beta} = \beta$. Ainsi, $f(\varphi) = (\alpha, \beta)$, ce qui prouve la surjectivité de φ.
- On en déduit que $\boxed{f \text{ est un isomorphisme}}$.

(e)
- - $*$ Soit $\varphi \in G^\circ$. Ainsi pour tout $x \in G$, $\varphi(x) = 0$, donc $G \subset \mathrm{Ker}(\varphi)$. Par conséquent,

$$G^\circ = \{\varphi \in E^* \mid G \subset \mathrm{Ker}(\varphi)\}.$$

  - $*$ Soit $\varphi \in \{\varphi \in E^* \mid G \subset \mathrm{Ker}(\varphi)\}$. Ainsi, $G \subset \mathrm{Ker}(\varphi)$, donc pour tout $x \in G$, $\varphi(x) = 0$. Par définition de G°, on en déduit que $\varphi \in G^\circ$.
  - $*$ Ainsi, $\boxed{G^\circ = \{\varphi \in E^* \mid G \subset \mathrm{Ker}(\varphi)\}}$
- Notons $T = \{0\} \times S^* \subset G^* \times S^*$. Clairement, T est isomorphe à S^*. Par ailleurs, l'application f étant celle introduite dans la question précédente,

$$f^{-1}(T) = \{\varphi \in E^* \mid \varphi_{|G} = 0\} = \{\varphi \in E^* \mid G \subset \mathrm{Ker}(\varphi)\} = G^\circ.$$

  Or, puisque f est un isomorphisme, $f^{-1}(T)$ est isomorphe à T, lui-même isomorphe à S^*.
  Donc $\boxed{G^\circ \text{ est isomorphe à } S^*}$. L'isomorphisme qu'on a établi consiste en la restriction à S.

2. **Cas de la dimension finie**

   On suppose dans cette question que E est de dimension finie.

   (a) D'après la question précédente,

$$\dim(G^\circ) = \dim(S^*).$$

   De plus, S étant de dimension finie, la question I-1(c) montre que $\dim S^* = \dim S$. Par ailleurs, S et G étant supplémentaires dans E,

$$\dim(E) = \dim G + \dim S \qquad \text{donc:} \qquad \boxed{\dim(E) = \dim G + \dim G^\circ}$$

(b) - La question 1(b) montre déjà que $G \circ G^{\circ\circ}$.
  - Réciproquement, on montre que $\dim(G) = \dim(G^{\circ\circ})$. On peut pour cela génnéraliser la question 2(a) à H, soit en refaisant un raisonnement similaire, soit en utilisant le principe de dualité, c'est-à-dire le fait que J soit un isomorphisme. En effet, en notant $\tilde{H}^\circ$ l'orthogonal de H dans E^{**},

$$\tilde{H}^\circ = \{\tilde{x} \in E^{**} \mid \tilde{x}(\varphi) = 0\} = \{\tilde{x} \in E^{**} \mid \varphi(x) = 0\} = J(H^\circ).$$

    Ainsi, $\tilde{H}^\circ$ et H° sont isomorphes, donc

$$\dim(H^\circ) = \dim(\tilde{H}^\circ).$$

    Or, d'après III-2(a) appliqué à H (dans le bon sens, en allant en direction du dual),

$$\dim H + \dim \tilde{H}^\circ = \dim E^{**} = \dim E,$$

    donc $\dim H + \dim H^\circ = \dim(E)$. Avec $H = G^\circ$, on obtient donc

$$\dim G^\circ + \dim G^{\circ\circ} = \dim(E).$$

    En combinant cette égalité et celle de la question III-2(a), on obtient bien

$$\dim G = \dim G^{\circ\circ}, \qquad \text{puis:} \qquad \boxed{G = G^{\circ\circ}}.$$

(c) - On a déjà montré que $\boxed{\dim H + \dim H^\circ = \dim(E)}$ dans la question précédente.
  - La question III-2(a) nous assure alors également que

$$\dim H^\circ + \dim H^{\circ\circ} = \dim E,$$

    et en combinant les deux, $\dim H = \dim H^{\circ\circ}$. La question 1(b) permet alors de conclurs que $\boxed{H = H^{\circ\circ}}$.

3. *Dans cette question, on ne suppose plus E de dimension finie, et on étudie $H^{\circ\circ}$, lorsque H est un sous-espace de dimension fini de E^*.*

   (a) Soit S un supplémentaire de G dans E. On a montré dans la question 1(e) que S^* et G° sont isomorphes. Or, S est de dimension finie (G de codimension finie), donc aussi S^*. On en déduit que G° est de dimension finie. De plus,

$$\boxed{\dim G^\circ = \dim(S^*) = \dim(S) = \mathrm{codim}_E(G)}.$$

   (b) Soit H un sous-espace vectoriel de dimension finie p de E^*, et $(\varphi_1, \dots, \varphi_p)$ une base de H. On pose $G = H^\circ$ son orthogonal dans E. Soit $u : E \longrightarrow \mathbb{K}^p$ définie pour tout $x \in E$ par

$$u(x) = (\varphi_1(x), \dots, \varphi_n(x)).$$

   - u est clairement linéaire.
   - Soit $x \in H^\circ$. Ainsi, pour tout $\varphi \in H$, $\varphi(x) = 0$. En particulier, pour tout $i \in [\![1, p]\!]$, $\varphi_i(x) = 0$, donc $u(x) = 0$. Par conséquent $x \in \mathrm{Ker}(u)$. On a donc l'inclusion $H^\circ \subset \mathrm{Ker}(u)$.
   - Réciproquement, soit $x \in \mathrm{Ker}(u)$. Ainsi,

$$(\varphi_1(x), \dots, \varphi_p(x)) = 0, \qquad \text{donc:} \qquad \forall i \in [\![1, p]\!], \quad \varphi_i(x) = 0.$$

     Soit $\varphi \in H$. Puisque $(\varphi_1, \dots, \varphi_p)$ est une base de H, il existe $\lambda_1, \dots, \lambda_p$ tels que

$$\varphi = \lambda_1\varphi_1 + \cdots + \lambda_p\varphi_p.$$

     Par conséquent

$$\varphi(x) = \lambda_1\varphi_1(x) + \cdots + \lambda_p\varphi_p(x) = 0.$$

     Ainsi, $x \in H^\circ$
   - Par principe de double-inclusion, $\boxed{H^\circ = \mathrm{Ker}(u)}$.

   (c) C'est une adaptation du théorème du rang (on revient en fait à la preuve, en introduisant un supplémentaire). Soit donc S un supplémentaire de $\mathrm{Ker}(u)$ dans E. Alors

$$\mathrm{Ker}(u_{|S}) = S \cap \mathrm{Ker}(u) = \{0\},$$

   donc $u_{|S}$ est injective. De plus $u_{|S} \in \mathcal{L}(S, \mathbb{K}^p)$. Ainsi, l'injectivité amène :

$$\mathrm{codim}(\mathrm{Ker}(u)) = \dim(S) = \dim(u(S)) \leqslant \dim(\mathbb{K}^p) = p = \dim H.$$

   La question précédente permet de conclure :

$$\boxed{\mathrm{codim}_E(H^\circ) = \mathrm{codim}(\mathrm{Ker}(u)) \leqslant \dim H}.$$

(d) On en déduit notamment que H° est de codimension finie, et on peut lui appliquer 3(a) :

$$\dim(H^{\circ\circ}) = \mathrm{codim}_E(H^\circ) \leqslant \dim H.$$

En particulier, $H^{\circ\circ}$ est aussi de dimension finie.

Or, on a déjà montré que $H \subset H^{\circ\circ}$ (1(b)). L'inégalité sur les dimensions qu'on vient de trouver (allant dans l'autre sens) montre alors que $\boxed{H = H^{\circ\circ}}$

Partie IV – Transposée d'une application linéaire

1. • Par propriété des composées d'applications linéaires, pour tout $\varphi \in F^*$, ${}^t f(\varphi)$ est bien dans E^*. Ainsi, ${}^t f$ est bien une application de F^* dans E^*.
   • Soit $(\varphi, \psi) \in (F^*)^2$, et $\lambda \in \mathbb{K}$. Alors

$$ {}^t f(\varphi + \lambda\psi) = (\varphi + \lambda\psi) \circ f = \varphi \circ f = \lambda\psi \circ f = {}^t f(\varphi) + \lambda\, {}^t f(\psi).$$

   Ainsi, $\boxed{{}^t f \in \mathcal{L}(F^*, E^*)}$.

2. • Soit $\varphi \in \mathrm{Ker}({}^t f)$. Ainsi, $\varphi \circ f = 0$. On en déduit que $\mathrm{Im}(f) \subset \mathrm{Ker}(\varphi)$, i.e. que φ s'annule sur $\mathrm{Im}(f)$. Par définition, on a alors $\varphi \in \mathrm{Im}(f)^\circ$.
   • Réciproquement, soit $\varphi \in \mathrm{Im}(f)^\perp$. Ainsi, pour tout $x \in \mathrm{Im}(f)$, $\varphi(x) = 0$, donc pour tout $x \in E$,

$$\varphi \circ f(x) = 0$$

   On en déduit que

$$ {}^t f(\varphi) = \varphi \circ f = 0,$$

   donc que $\varphi \in \mathrm{Ker}({}^t f)$.
   • Ainsi, $\boxed{\mathrm{Ker}({}^t f) = \mathrm{Im}(f)^\circ}$.

3. On suppose que E et F sont de dimension finie. D'après III-3(a) et la question précédente

$$\dim \mathrm{Ker}({}^t f) = \dim \mathrm{Im}(f)^\circ = \mathrm{codim}_F \mathrm{Im}(f) = \dim F - \mathrm{rg}(f).$$

   Par ailleurs, d'après le théorème du rang,

$$\dim \mathrm{Ker}({}^t f) = \dim(F^*) - \mathrm{rg}({}^t f) = \dim F - \mathrm{rg}({}^t f).$$

   En comparant les deux égalités ainsi obtenu, on en déduit que $\boxed{\mathrm{rg}(f) = \mathrm{rg}({}^t f)}$.

4. Soit $f \in \mathcal{L}(E, F)$ et $\mathcal{B} = (b_1, \dots, b_p)$, $\mathcal{C} = (c_1, \dots, c_n)$ des bases de E et F tels que $M = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$ (on peut prendre par exemple l'endomorphisme canoniquement associé). On note $M = (m_{i,j})$.
   Pour tout $j \in [\![1, n]\!]$,

$$f(b_j) = \sum_{i=1}^{n} m_{i,j} c_i,$$

   donc pour tout $i \in [\![1, p]\!]$, d'après I-1(a) :

$$c_i^*(f(b_j)) = m_{i,j}.$$

   Or, pour tout $x \in E$,

$$x = \sum_{j=1}^{n} b_j^*(x) b_j,$$

   donc

$$\begin{aligned} {}^t(f)(c_i^*)(x) &= c_i^* \circ f(x) \\ &= \sum_{j=1}^{n} b_j^*(x) c_i^* f(b_j) \\ &= \sum_{j=1}^{n} b_j^*(x) m_{i,j} \end{aligned}$$

Ainsi,

$$ {}^t(f)(c_i^*) = \sum_{j=1}^{n} m_{i,j} b_j^*. $$

par conséquent, en posant $N = \mathrm{Mat}_{\mathcal{C}*,\mathcal{B}*}({}^t f)$, le coefficient en position (j,i) de N est $m_{i,j}$. Cette description correspond à la description de la transposée de M. Ainsi,

$$ \mathrm{Mat}_{\mathcal{C}*,\mathcal{B}*}({}^t f) = {}^t M. $$

On déduit alors de la question 3 que

$$ \mathrm{rg}({}^t M) = \mathrm{rg}(\mathrm{Mat}_{\mathcal{C}*,\mathcal{B}*}({}^t f)) = \mathrm{rg}({}^t f) = \mathrm{rg}(f) = \mathrm{rg}(\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)), $$

et finalement, $\boxed{\mathrm{rg}(M) = \mathrm{rg}({}^t M)}$.

Partie V – Minoration de la dimension d'un sous-espace de $\mathbb{K}^A$

1. **Description du dual de $\mathbb{K}^{(A)}$.**
Soit A un ensemble quelconque
(a) Soit, pour tout $a \in A$, e_a l'application de $\mathbb{K}^{(A)}$ définie par

$$ \forall b \in A, \quad e_a(b) = \delta_{a,b}. $$

Le principe de la démonstration est à peu près le même que la question I-1(c).

- La famille est libre. En effet, soit $(\lambda_a)_{a\in A}$ une famille de scalaires presque tous nuls tels que

$$ 0 = \sum_{a\in A} \lambda_a e_a. $$

En évaluant en $b \in A$ quelconque, on obtient alors $\lambda_b = 0$. D'où la liberté.
- Soit $f \in \mathbb{K}^{(A)}$. Puisque f est à support fini, la famille $(f(a))_{a\in A}$ est à support fini, et une vérification simple montre que

$$ f = \sum_{a\in A} f(a) e_a. $$

Ainsi, $(e_a)_{a\in A}$ est génératrice.
- On en déduit que $\boxed{(e_a)_{a\in A} \text{ est une base}}$.

(b)
- Pour commencer, montrons la linéarité de Φ. Soit f et g dans $\mathbb{K}^A$, et $\lambda \in \mathbb{K}$. Alors $\Phi(f+\lambda g)$ est l'unique forme linéaire sur $\mathbb{K}^{(A)}$ telle que pour tout $a \in A$

$$ \Phi(f+\lambda g)(e_a) = (f+\lambda g)(a) = f(a) + \lambda g(a). $$

Or, $\Phi(f) + \lambda\Phi(g)$ vérifie aussi ces égalités. Par propriété de rigidité (coïncidence sur une base), on en déduit que $\Phi(f+\lambda g) = \Phi(f) + \lambda\Phi(g)$.
- Injectivité : soit $f \in \mathbb{K}^a$ dans $\mathrm{Ker}(\Phi)$. Ainsi, $\varphi_f = 0$, donc en particulier, pour tout $a \in A$,

$$ f(a) = \varphi_f(e_a) = 0. $$

On en déduit que $f = 0$, donc que $\mathrm{Ker}(\Phi) = \{0\}$, donc que Φ est injective.
- Surjectivité : Soit $\varphi \in (\mathbb{K}^{(A)})^*$. On définit $f \in \mathbb{K}^A$ par

$$ \forall a \in A, f(a) = \varphi(e_a). $$

Ainsi, φ_f et φ coïncident sur tous les vecteurs de la base (e_a), donc $\varphi_f = \varphi$, i.e. $\varphi = \Phi(f)$.
- Cela montre bien que $\boxed{\Phi \text{ est un isomorphisme de } \mathbb{K}^A \text{ dans } (\mathbb{K}^{(A)})^*}$.

2. **CNS de minoration de la dimension d'un sous-espace de $\mathbb{K}^A$.**

(a) Soit V un sous-espace vectoriel de $\mathbb{K}^A$. On suppose qu'il existe $a_1, \dots, a_p \in A$ et $f_1, \dots, f_p \in V$. Montrons que $(f_1, \dots, f_p)$ est une famille libre de V. On peut refaire le même raisonnement que plus haut pour la liberté de la famille des e_a, en évaluant une relation en chaque a_i, ou bien se ramener à cette propriété, en remarquant que si on définit $B = \{a_1, \dots, a_p\}$, la restriction $r : f \mapsto f_{|A}$ est une application linéaire de $\mathbb{K}^A$ dans $\mathbb{K}^B$. Or, l'image de la famille $(f_1, \dots, f_p)$ correspond alors exactement à la base canonnique de $\mathbb{K}^B = \mathbb{K}^{(B)}$ (cette dernière égalité résultant du fait que B est fini). On en déduit que la famille $(f_1, \dots, f_p)$ est envoyée par l'application linéaire r sur une famille libre. Elle est donc elle-même libre.

Puisqu'il existe dans V une famille libre de cardinal p, on en déduit que $\boxed{\dim V \geqslant p}$.

(b) Réciproquement, on suppose que $\dim V \geqslant p$, et on considère $V' = \Phi(V) \in (\mathbb{K}^{(A)})^*$. Soit H un sous-espace vectoriel de V' tel que $\dim H = p$.

i. • D'après III-3(d), H étant de dimension finie, $H^{\circ\circ} = H$, donc $\dim(H^{\circ\circ}) = \dim(H) = p$. Or, d'après III-3(c), H° est de codimension finie et donc $\dim(H^{\circ\circ}) = \operatorname{codim}_E(H) = p$, où $E = \mathbb{K}^{(A)}$. Soit $\mathcal{B}$ une base de H. D'après le théorème de la base incomplète (admis en dimension quelconque), on peut compléter la base $\mathcal{B}$ par ajout de vecteurs d'une famille génératrice $\mathcal{G}$ donnée. Prenons pour $\mathcal{G}$ la base canonique de $\mathbb{K}^{(A)}$.

• On peut donc compléter $\mathcal{B}$ en ajoutant des vecteurs formant une famille $\mathcal{B}'$ telle que $\mathcal{B}' \subset \mathcal{G}$.

• On a alors $E = \operatorname{Vect}(\mathcal{B}) \bigoplus \operatorname{Vect}(\mathcal{B}') = H^\circ \bigoplus \operatorname{Vect}(\mathcal{B}')$, donc $S = \operatorname{Vect}(\mathcal{B}')$ est un supplémentaire de H° dans E. D'après I-2, la dimension de ce supplémentaire est égal à la codimension de H°, donc p. Or, la famille génératrice $\mathcal{B}'$ de S est aussi une sous-famille de la famille libre $\mathcal{G}$, et est donc elle-même libre. Il s'agit donc d'une base de S, et son cardinal est donc égal à p.

• On peut donc écrire $\mathcal{B}' = \{e_{a_1}, \dots, e_{a_p}\}$, pour des éléments e_{a_i} de la base canonique, $a_i \in A$. On a montré que $\boxed{\operatorname{Vect}(e_{a_1}, \dots, e_{a_p}) \text{ est un supplémentaire de } H^\circ \text{ dans } \mathbb{K}^{(A)}}$.

ii. Soit pour tout $i \in [\![1, p]\!]$,

$$\tilde{f}_i = e_{a_i}^* \in (\mathbb{K}^{(A)})^* \qquad \text{et} \qquad f_i = \Phi^{-1}(\tilde{f}_i).$$

On a alors, pour tout $(i, j) \in [\![1, p]\!]^2$,

$$f_i(a_j) = \Phi^{-1}(\tilde{f}_i)(a_j) = \tilde{f}_i(e_{a_j}) = e_{a_i}^*(e_{a_j}) = \delta_{a_i, a_j},$$

et les a_i étant deux à deux distincts (nécessairement, sinon, la famille $(e_{a_1}, \dots, e_{a_p})$ ne serait pas libre et n'engendrerait pas un espace de dimension p), on en déduit que

$$\boxed{f_i(a_j) = \delta_{i,j}}.$$

Partie VI – Théorème d'Erdös-Kaplansky (partie difficile)

1. Soit $\mathbb{L}$ un sous-corps de $\mathbb{K}$, et $(f_1, \dots, f_p)$ une famille libre de $\mathbb{K}^A$ telle que pour tout $i \in [\![1, p]\!]$, et tout $a \in A$, $f_i(a) \in \mathbb{L}$. On pose $V = \operatorname{Vect}_{\mathbb{L}}(f_1, \dots, f_p) \subset \mathbb{L}^A$ et $W = \operatorname{Vect}_{\mathbb{K}}(f_1, \dots, f_p) \subset \mathbb{K}^A$

(a) La famille $(f_1, \dots, f_p)$ étant libre sur $\mathbb{K}$, elle l'est aussi sur $\mathbb{L}$. Ainsi, c'est une $\mathbb{L}$-base du $\mathbb{L}$-espace vectoriel V. On en déduit que V est de dimension p.

On peut donc appliquer V-2(b), nous donnant l'existence de $(a_1, \dots, a_p) \in A^p$ et $(g_1, \dots, g_p) \in V^p$ tels que

$$\forall (i, j) \in [\![1, p]\!]^2, \quad \boxed{g_i(a_j) = \delta_{i,j}}.$$

(b) D'après la preuve effectuée en V-2(a), $(g_1, \dots, g_p)$ est alors une famille libre de V. Comme $\dim(V) = p$, c'en est une base. On en déduit donc qu'elle est génératrice, et donc

$$\forall i \in [\![1, p]\!], \quad f_i \in \operatorname{Vect}_{\mathbb{L}}(g_1, \dots, g_p) \subset \operatorname{Vect}_{\mathbb{K}}(g_1, \dots, g_k).$$

Comme les f_i forment une famille $\mathbb{K}$-généatrice de W, les g_i aussi, et comme $\dim_{\mathbb{K}}(W) = p$, elle est minimale. Ainsi, $\boxed{(g_1, \dots, g_p) \text{ est une } \mathbb{K}\text{-base de } W.}$

(c) Soit $f \in W$. On décompose f dans la base $(g_1, \dots, g_p)$:

$$f = \sum_{i=1}^{p} \lambda_i g_i.$$

En évaluant en a_j, on obtient

$$f(a_j) = \sum_{i=1}^{p} \lambda_i \delta_{i,j} = \lambda_j.$$

Ainsi,

$$f = \sum_{i=1}^{p} f(a_j) g_i.$$

Pour tout $a \in A$, on a alors

$$f(a) = \sum_{i=1}^{p} f(a_j) g_i(a).$$

Or, les éléments $f(a_j)$ sont dans $\mathbb{L}[f(a_1), \ldots, f(a_p)]$ et les $g_i(a)$ sont dans $\mathbb{L}$, donc aussi dans $\mathbb{L}[f(a_1), \ldots, f(a_p)]$. Par stabilité de ce corps par somme et produit, on en déduit que

$$\boxed{f(a) \in \mathbb{L}[f(a_1), \ldots, f(a_p)]}.$$

2. (a)
- Pour commencer, $M \subset G'$, donc $|M| \leqslant |G'|$.
- On montre le lemme suivant : si X est infini, alors $|X| = |X^\bullet|$, où $X^\bullet$ est défini par

$$X^\bullet = \bigcup_{n \in \mathbb{N}} X^n.$$

L'ensemble M^0 est ici par convention $\{\varnothing\}$. En effet :
  - $*$ Pour tout $k \in \mathbb{N}^*$, $|X^k| = |X|$, par itération de la propriété admise dans le préambule.
  - $*$ En particulier, on dispose donc pour tout $k \in \mathbb{N}$ de surjections $\varphi_k : X \to X^k$ (y compris pour $k = 0$, en prenant la surjection constante de valeur $\varnothing$). L'application $\varphi : X \times \mathbb{N} \to X^\bullet$ définie par $\varphi(m,k) = \varphi_k(m)$ est alors surjective. On en déduit que $|X^\bullet| \leqslant |X \times \mathbb{N}|$.
  - $*$ Comme X est infini, $|\mathbb{N}| \leqslant |M|$, donc $|X \times \mathbb{N}| \leqslant |X \times X| = |X|$, d'après le préambule.
  - $*$ Ainsi, $|X^\bullet| \leqslant |X|$, et clairement $|X| \leqslant |X^\bullet|$ (X s'injectant dans $X^\bullet$ via les 1-uplets). Ainsi, d'après le théorème de Cantor-Bernstein, $|X| = |X^\bullet|$.
- Les éléments de G' s'écrivent (en notation multiplicative) sous la forme $x_1 \cdots x_n$, où $n \in \mathbb{N}$ et les x_i sont dans $M \cup M^{-1}$. Ainsi en posant $X = M \cup M^{-1}$, on dispose d'une surjection $s : X^\bullet \to G'$, définie par

$$s((x_1, \ldots, x_n)) = x_1 \cdots x_n.$$

Par conséquent, $|G'| \leqslant |X^\bullet| = |X|$. Par ailleurs, on dispose d'une surjection $M \times \{-1, 1\} \longrightarrow M \cup M^{-1}$ définie par $(m, \varepsilon) \mapsto m^\varepsilon$. Par conséquent,

$$|G'| \leqslant |X| \leqslant |M \times \{-1,1\}| \leqslant |M \times M| = |M|.$$

- On déduit du théorème de Cantor-Bernstein que $\boxed{|G'| = |M|}$.

(b) On montre par récurrence sur $n \in \mathbb{N}$ que A_n et P_n sont de même cardinal que M.
- $|A_0| = |M|$ d'après l'initialisation de la suite (A_n). De plus, $A_0 \cap \mathbb{K}^*$ diffère de A_0 d'au plus un élément. Comme A_0 est infini, $|A_0 \cap \mathbb{K}^*| = |A_0| = |M|$. On déduit de la question précédente, appliqué dans le groupe multiplicatif $(\mathbb{K}^*, \times)$, que $|P_0| = |M|$.
- Soit $n \in \mathbb{N}$. Supposons que $|A_n| = |P_n| = |M|$. Alors, en appliquant la question précédente dans le groupe additif $(\mathbb{K}, +)$, P_n étant infini, $|A_{n+1}| = |P_n| = |M|$. Montrer que $|P_{n+1}| = |A_{n+1}|$ se fait alors exactement comme dans l'initialisation, pour passer de A_0 à P_0.
- Ainsi, d'après le principe de récurrence, pour tout $n \in \mathbb{N}$, $|A_n| = |P_n| = |M|$.

(c) Montrons que $\mathbb{K}' = \bigcup_{n \in \mathbb{N}} A_n$.
- Montrons pour commencer que pour tout $n \in \mathbb{N}$, $A_n \subset \mathbb{K}'$. On le montre par récurrence.
  - $*$ L'initialisation $A_0 \subset \mathbb{K}'$ provient du fait que par définition, $M \subset \mathbb{K}'$.
  - $*$ Si $A_n \subset \mathbb{K}'$, alors le sous-groupe multiplicatif $\mathbb{K}'^*$ de $\mathbb{K}^*$ contient tous les éléments de $A_n \cap \mathbb{K}^*$. Par minimalité du groupe engendré, on a donc $P_n \subset \mathbb{K}'^*$.
  - $*$ On a donc $P_n \subset \mathbb{K}'$, qui est un sous-groupe additif de $\mathbb{K}$. Par minimalité du groupe (additif) engendré, on a donc $A_{n+1} \subset \mathbb{K}'$.
  - $*$ Ainsi, d'après le principe de récurrence, pour tout $n \in \mathbb{N}$, $A_n \subset \mathbb{K}'$, donc

$$\bigcup_{n \in \mathbb{N}} A_n \subset \mathbb{K}'.$$

- Posons $\mathbb{K}'' = \bigcup_{n\in\mathbb{N}} A_n \subset \mathbb{K}'$. Montrons que $\mathbb{K}''$ est un corps :
  * Pour commencer, $\mathbb{K}'' \subset \mathbb{K}$.
  * Pour tout $n \in \mathbb{N}$, $1 \in P_n$, donc $1 \in A_n$. Ainsi, $1 \in \mathbb{K}''$.
  * Soit $(x, y) \in (\mathbb{K}'')^2$. Les A_i formant une suite croissante (on enlève 0 pour construire P_n, mais on le remet ensuite, tous les autres éléments sont à chaque fois gardés), il existe $n \in \mathbb{N}$ tel que x et y soient dans A_n. Comme A_n est un groupe additif, $x - y \in A_n$, et donc $x - y \in \mathbb{K}''$.
  * Si de plus x et y sont non nuls x et y sont dans P_n qui est un groupe multiplicatif. Donc $xy^{-1} \in P_n \subset A_{n+1} \subset \mathbb{K}''$.
  * On en déduit que $\mathbb{K}''$ est un sous-corps de $\mathbb{K}$.
- D'après les deux points précédents, et la minimalité de $\mathbb{K}'$, on en déduit que $\mathbb{K}' = \mathbb{K}''$. Ainsi,

$$|\mathbb{K}'| = \left|\bigcup_{n\in\mathbb{N}} A_n\right|$$

  La question précédente, et le même argument qu'en question 2(a) pour faire l'union dénombrable montrent alors que $\boxed{|\mathbb{K}'| = |M|}$.

3. Soit $\mathbb{K}$ un corps, et C un ensemble infini tel que $|C| \geqslant |\mathbb{K}|$.

   (a) On construit une injection :

$$\imath : \mathbb{K}^{(C)} \to \mathcal{P}_f(C \times \mathbb{K}),$$

   qui à $f \in \mathbb{K}^{(C)}$ associe

$$\imath(f) = \{(c, f(c)) \mid f(c) \neq 0\}.$$

   Cette application est bien définie, puisque f est à support fini (donc $\imath(f)$ est bien une partie finie de $C \times \mathbb{K}$).
   Par ailleurs, supposons que $\imath(f) = \imath(g) = X$. Notons

$$C' = \{c \in C \mid \exists \lambda \in \mathbb{K},\ (c, \lambda) \in X\} = \pi_C(X),$$

   où π_C est la projection sur le premier facteur du produit cartésien $C \times \mathbb{K}$. On remarque d'abord que si $c \in C'$, alors par définition d'une application (unicité de l'image), $\pi_C^{-1}(c)$ ne contient qu'un élément λ, égal à la fois à $f(c)$ et à $g(c)$. On en déduit que pour tout $c \in C'$, $f(c) = g(c)$.
   Par ailleurs, si $c \in C \backslash C'$, par définition de $\imath(f)$ et $\imath(g)$, $f(c) = g(c) = 0$. Ainsi, pour tout $c \in C$, $f(c) = g(c)$, donc $f = g$.
   On a bien construit une application injective de $\mathbb{K}^{(C)}$ dans $\mathcal{P}_f(C \times \mathbb{K})$, d'où

$$\boxed{|\mathbb{K}^{(C)}| \leqslant |\mathcal{P}_f(C \times \mathbb{K})|}.$$

   (b)
   - D'après le lemme montré danns la question 2(a), si X est de cardinal infini, $|X| = |X^\bullet|$. Par ailleurs, on dispose d'une surjection (de façon évidente) de $X^\bullet \to \mathcal{P}_f(X)$, définie par

$$(x_1, \dots, x_n) \mapsto \{x_1, \dots, x_n\}.$$

     Ainsi,

$$|\mathcal{P}_f(X)| \leqslant |X^\bullet| = |X|.$$

     De façon évidente, $|X| \leqslant |\mathcal{P}_f(X)|$, puisque X s'identifie à l'ensemble des singletons. Ainsi, si X est de cardinal infini, $|\mathcal{P}_f(X)| = |X|$.
   - En appliquant cela à $C \times \mathbb{K}$, qui est infini, d'après nos hypothèses sur C (et le fait que $\mathbb{K}$ soit un corps, donc non vide), d'après la question précédente, on obtient

$$|\mathbb{K}^{(C)}| \leqslant |C \times \mathbb{K}| \leqslant |C \times C| \leqslant |C|,$$

     puisque $|C| \geqslant |\mathbb{K}|$, et d'après la propriété admise en préambule.
   - Réciproquement, $c \mapsto e_c$ fournit une injection de C dans $\mathbb{K}^{(C)}$, donc $|C| \leqslant |\mathbb{K}^{(C)}|$.
   - On en déduit que $\boxed{|\mathbb{K}^{(C)}| = |C|}$.

4. **Démonstration du théorème d'Erdös-Kaplansky**.

   (a) On va suivre l'indication assez détaillée donnée dans l'énoncé.

- On suppose qu'on n'a pas $|\mathbb{K}| \leqslant \dim(\mathbb{K}^{\mathbb{N}})$. Alors $|\mathbb{K}| > \dim(\mathbb{K}^{\mathbb{N}})$. Remarquez que cette propriété (le fait que la relation d'ordre définie par les cadinaux soit totale) n'est pas complètement triviale. Elle repose sur l'axiome du choix. Je n'en donne pas la preuve, utilisant le lemme de Zorn (elle est disponible dans un autre sujet, que je n'ai pas donné en DM cette année). Il existe donc une base $\mathcal{B}$ de $\mathbb{K}^{\mathbb{N}}$ telle que $|\mathcal{B}| < |\mathbb{K}|$. Soit
$$M = \{\beta(n), \quad (\beta, n) \in \mathcal{B} \times \mathbb{N}\},$$
l'ensemble de toutes les valeurs prises par les fonctions définissant la base $\mathcal{B}$.
- L'application $(\beta, n) \mapsto \beta(n)$ étant, par définition de M, une surjectionn de $\mathcal{B} \times \mathbb{N}$ sur M, on a l'inégalité :
$$|M| \leqslant |\mathcal{B} \times \mathbb{N}| \leqslant |\mathcal{B} \times \mathcal{B}| = |\mathcal{B}|.$$
En effet $\mathcal{B}$ est infini ($\mathbb{K}^{\mathbb{N}}$ n'est pas de dimension finie, pusique les $(e_a)_{a\in\mathbb{N}}$ en forment une famille libre), donc $|\mathbb{N}| \leqslant |\mathcal{B}|$ d'une part, et d'autre part on peut utiliser le résultat admis dans le préambule.
- Si M est fini, on peut lui ajouter des éléments de $\mathbb{K}$ en nombre dénombrable (c'est possible, car $\mathbb{K}$ lui-même est infini, du fait de l'hypothèse $|\mathbb{K}| > \dim(\mathbb{K}^{\mathbb{N}})$), on aura alors toujours
$$|M| \leqslant |\mathbb{N}| \leqslant |\mathcal{B}|.$$
Ainsi, on peut supposer M infini, vérifiant $|M| \leqslant |\mathcal{B}|$, et contenant toutes les valeurs des images de la base $\mathcal{B}$.
- On construit alors $\mathbb{L}$ le sous-corps de $\mathbb{K}$ engendré par M. Puisque M est infini, d'après la question 2(c),
$$|\mathbb{L}| = |M| \leqslant |\mathcal{B}| < |\mathbb{K}|.$$
- En particulier, $\mathbb{L} \subsetneq \mathbb{K}$, et il existe $\xi_0 \in \mathbb{K}\backslash\mathbb{L}$. On construit alors la suite $(\xi_n)_{n\in\mathbb{N}}$ par récurrence. On suppose $(\xi_0, \ldots, \xi_n)$ construits tels que pour tout $k \in [\![1, n]\!]$,
$$\xi_k \notin \mathbb{L}[\xi_0, \ldots, \xi_{k-1}].$$
Puisque $\mathbb{L}$ est infini (car de même cardinal que $|M|$), l'ensemble $\mathbb{L} \cup \{\xi_0, \ldots, \xi_n\}$ est de même cardinal que $\mathbb{L}$ à savoir $|M|$. Or, $\mathbb{L}[\xi_0, \ldots, \xi_n]$ est le sous-corps de $\mathbb{K}$ engendré par $\mathbb{L} \cup \{\xi_0, \ldots, \xi_n\}$. Ainsi, d'après la question 2(c),
$$|\mathbb{L}[\xi_1, \ldots, \xi_n]| = |M| < |\mathbb{K}|.$$
On a donc une inclusion stricte
$$\mathbb{L}[\xi_1, \ldots, \xi_n] \subsetneq \mathbb{K},$$
ce qui nous permet de trouver un élément ξ_{n+1} de $\mathbb{K}$ vérifiant
$$\xi_{n+1} \in \mathbb{K}\backslash\mathbb{L}[\xi_1, \ldots, \xi_n].$$
- On considère alors $f : \mathbb{N} \mapsto \xi_n$, élément de $\mathbb{K}^{\mathbb{N}}$. Puisque $\mathcal{B}$ est une base de $\mathbb{K}^{\mathbb{N}}$, f se décompose comme CL d'un nombre fini d'éléments de $\mathcal{B}$. On dispose donc d'un sous-ensemble fini $\mathcal{B}_0 = \{f_1, \ldots, f_p\}$ de $\mathcal{B}$ tel que $f \in \mathrm{Vect}(\mathcal{B}_0)$. De plus, $\mathcal{B}_0$ étant un sous-ensemble d'une base, c'est une famille libre. On est donc dans les conditions d'application de la question 1. Il existe donc $(a_1, \ldots, a_p) \in \mathbb{N}^n$ tels que
$$\forall g \in \mathrm{Vect}(f_1, \ldots, f_p), \quad \forall a \in A, \quad g(a) \in \mathbb{L}[g(a_1), \ldots, g(a_p)].$$
Sans perte de généralité, on peut supposer $a_1 < a_2 < \ldots, < a_p$ (quitte à renuméroter les f_i). Appliquons cela à la fonction f :
$$\forall a \in \mathbb{N}, \quad f(a) \in \mathbb{L}[f(a_1), \ldots, f(a_p)] = \mathbb{L}[\xi_{a_1}, \ldots, \xi_{a_p}] \subset \mathbb{L}[\xi_1, \ldots, \xi_{a_p}].$$
Mais par définition, pour $a = a_p + 1$,
$$\xi_{a_p+1} = f(a_p + 1) \notin \mathbb{L}[\xi_1, \ldots, \xi_{a_p}],$$
d'où une contradiction.
- On en déduit que l'hypothèse initiale est fausse. On en déduit in fine que $\boxed{|\mathbb{K}| \leqslant \dim \mathbb{K}^{\mathbb{N}}}$.

(b)
- Puisque A est infini, $|A| \geqslant |\mathbb{N}|$. Il existe donc une surjection $s : A \to \mathbb{N}$. On définit alors $\Phi : \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^A$ par $\Phi(f) = f \circ s$.

- On vérifie que Φ est injective. Soit en effet f et g dans $\mathbb{K}^{\mathbb{N}}$ tels que $f \circ s = g \circ s$. Soit $n \in \mathbb{N}$. Puisque s est surjective, il existe $a \in A$ tel que $s(a) = n$. On en déduit que

$$f(n) = f(s(a)) = g(s(a)) = g(n),$$

donc $f = g$. Ainsi, Φ est injective.
- Clairement, Φ est linéaire. L'injectivité nous assure alors que Φ envoie une base $\mathcal{B}$ de $\mathbb{K}^{\mathbb{N}}$ bijectivement sur une famille libre de $\mathbb{K}^A$, qu'on peut compléter en une base $\mathcal{C}$. Ainsi,

$$|\mathcal{B}| \leqslant |\mathcal{C}|, \qquad \text{donc:} \qquad \boxed{\dim(\mathbb{K}^A) \geqslant \dim(\mathbb{K}^{\mathbb{N}}) \geqslant |\mathbb{K}|}.$$

(c) Soit $\mathcal{B}$ une base de $\mathbb{K}^A$. Ainsi,

$$|\mathcal{B}| = \dim(\mathbb{K}^A) \geqslant |\mathbb{K}|.$$

Par ailleurs, $\mathbb{K}^A$ est isomorphe à $\mathbb{K}^{(\mathcal{B})}$. Ainsi, d'après la question 3(c),

$$|\mathbb{K}^A| = |\mathbb{K}^{(\mathcal{B})}| = |\mathcal{B}|, \qquad \text{soit:} \qquad \boxed{\dim(\mathbb{K}^A) = |\mathbb{K}^A|}.$$

(d) Soit E un espace vectoriel de dimension finie, et $\mathcal{B}$ une base de E. On a donc

$$E = \mathbb{K}^{(\mathcal{B})} \qquad \text{et} \qquad E^* \simeq \mathbb{K}^{\mathcal{B}}.$$

D'après ce qui précède,

$$\dim(E^*) = |\mathbb{K}^{\mathcal{B}}|.$$

Par ailleurs, $\mathbb{K}$ contient au moins 0 et 1, qui sont distincts. Ainsi, $|\mathbb{K}| \geqslant 2$, donc

$$|\mathbb{K}^{\mathcal{B}}| \geqslant |\{0,1\}^{\mathcal{B}}| = |\mathcal{P}(\mathcal{B})| > |\mathcal{B}|,$$

d'après le théorème de Cantor. On en déduit in fine que :

$$\dim \mathbb{K}^{\mathcal{B}} = |\mathbb{K}^{\mathcal{B}}| > |\mathcal{B}| = \dim E, \qquad \text{donc:} \qquad \boxed{\dim(E^*) > \dim(E)}.$$

On en déduit notamment que $\dim(E^{**}) > \dim E^* > \dim E$, donc que E^{**} ne peut jamais être isomorphe à E lorsque E est de dimension finie. Il est même beaucoup plus gros, puisqu'il y a au moins 2 cardinaux de différence entre les deux.

Question subsidiaire.
On montre dans cette question le théorème de la dimension dans le cas infini, à savoir l'égalité des cardinaux de toutes les bases d'un même espace vectoriel E de dimension infinie.
Soit $\mathcal{B}$ et $\mathcal{C}$ deux bases de E. Chaque vecteur $b \in \mathcal{B}$ se décompose sur un nombre fini de vecteurs de la base $\mathcal{C}$. Ainsi, pour tout $b \in \mathcal{B}$, on peut trouver un sous-ensemble fini $\gamma(b) \subset \mathcal{C}$ tel que

$$b \in \mathrm{Vect}(\gamma(b)).$$

Ainsi,

$$E = \mathrm{Vect}(\mathcal{B}) \subset \mathrm{Vect}\left(\bigcup_{b\in\mathcal{B}} \gamma(b)\right).$$

Si $\bigcup_{b\in\mathcal{B}} \gamma(b) \subsetneq \mathcal{C}$, cela contredit la minimalité de la famille génératrice $\mathcal{C}$. Ainsi,

$$\mathcal{C} = \bigcup_{b\in\mathcal{B}} \gamma(b).$$

Puisque pour tout $b \in \mathbb{N}$, $\gamma(b)$ est finis, il existe une surjection $s_b : \mathbb{N} \to \gamma(b)$. On peut alors construire une surjection

$$\sigma : \mathcal{B} \times \mathbb{N} \longrightarrow \bigcup_{b\in\mathcal{B}} \gamma(b) = \mathcal{C}$$

en posant $\sigma(b,n) = s_b(n)$. Comme de plus $|\mathcal{B} \times \mathbb{N}| \leqslant |\mathcal{B} \times \mathcal{B}| = |\mathcal{B}|$, on en déduit que $|\mathcal{B}| \geqslant |\mathcal{C}|$.
En intervertissant les rôles de $\mathcal{B}$ et $\mathcal{C}$, on obtient aussi $|\mathcal{C}| \leqslant |\mathcal{B}|$. Ainsi, $\boxed{|\mathcal{B}| = |\mathcal{C}|}$.

Remarquez que la démonstration donnée est indépendante (et assez différente) de celle donnée en dimension finie, et ne convient pas dans le cas de la dimension finie, les arguments utilisés nécessitant l'hypothèse d'infinitude. En revanche, elle n'est pas particulièrement plus dure (à condition de savoir manipuler un peu les cardinaux), presque au contraire, du fait que les cardinaux infinis donnent un peu plus de souplesse que les cardinaux finis, qui nécessitent de faire les choses de façon très précise, au vecteur près.
Remarquez tout de même la dépendance vis-à-vis de l'axiome du choix (comme une grande partie des arguments de ce DS), pour l'existence de bases d'une part et pour la comparaison entre $\mathcal{B} \times \mathcal{B}$ et $\mathcal{B}$ utilisée tout à la fin.

Sources :

Arnaudiès, Lelong-Ferrand, *Cours de mathématiques, 1. Algèbre* (Dunod)
Bourbaki, *Algèbre, chapitres 1 à 3,* (Springer), II-7.5 et exercice II-7.3 p II.193