

DM n° 22 : Balbutiements d'algèbre linéaire

Corrigé du problème 1 –

1. • Soit F un sous-espace de E . Il est donc non vide, et stable par combinaisons linéaires à coefficients complexes ; il est donc *a fortiori* stable également par combinaisons linéaires à coefficients réels, et est donc un sous-espace sur $\mathbb{R}$ de E . Tout sous-espace vectoriel (sur $\mathbb{C}$) de E est donc un sous-espace vectoriel sur $\mathbb{R}$.
- La réciproque n'est pas vraie ; un sous-ensemble stable par combinaisons linéaires à coefficients réels n'a pas de raison en général d'être stable par combinaisons linéaires à coefficients complexes. Donnons un contre-exemple. Soit $E = \mathbb{C}$. Alors $F = \mathbb{R} \subset \mathbb{C}$ est un sous-espace sur $\mathbb{R}$ de $\mathbb{C}$, mais n'est pas un sous-espace de $\mathbb{C}$, car F n'est pas stable par combinaisons linéaires à coefficients complexes ; par exemple, $i \cdot 1 \notin \mathbb{R}$.

2. (a) • Pour commencer, pour tout $y \in iF$, il existe $x \in F$ tel que $y = ix$, et comme $x \in E$ et que E est un espace vectoriel sur $\mathbb{C}$, $ix \in E$. Ainsi, iF est un sous-ensemble de E .
- On a : $0 = i \cdot 0$, et comme $0 \in F$, on a donc $0 \in iF$.
- Soit $(x, y) \in (iF)^2$, et soit $\lambda \in \mathbb{R}$. Alors il existe x' et y' dans F tels que $x = ix'$ et $y = iy'$. Ainsi :

$$\lambda x + y = i(\lambda x' + y').$$

Comme F est un sous-espace sur $\mathbb{R}$ de E , il est stable par combinaisons linéaires à coefficients réels ; par conséquent, $\lambda x' + y' \in F$, puis $\lambda x + y \in iF$. Ainsi, iF est stable par combinaisons linéaires à coefficients réels.

- On en déduit que iF est un sous-espace vectoriel sur $\mathbb{R}$ de E .

- (b) De façon immédiate, par pseudo-associativité de la loi externe, $i(iF) = -F$, et par stabilité, par prise d'opposé on obtient $-F \subset F$, et puisque $-(-F) = F$, de même $F \subset -F$. Ainsi, $i(iF) = F$.

- (c) Soit $(b_1, \dots, b_n)$ une base de F . Alors $(ib_1, \dots, ib_n)$ est une base de iF . En effet, l'application $\varphi : F \rightarrow iF$ définie par $\varphi(x) = ix$ est linéaire, et c'est un isomorphisme, sa réciproque étant l'application $\psi : iF \rightarrow F$ définie par $\psi(y) = -iy$. Par conséquent, φ envoie une base de F sur une base de iF .

On en déduit que $\dim(F) = \dim(iF)$.

- (d) • Pour commencer, $F' = F \cap iF \subset F$, et $F \cap iF$ est un sous-espace de E . En effet, F' est un sous-ensemble de E contenant 0, stable par somme (car F et iF le sont). Il reste donc à montrer la stabilité par multiplication par un scalaire complexe $\lambda = a + ib$. Par stabilité de F et iF par somme et multiplication par un réel, il suffit de vérifier la stabilité par multiplication par i . Or, étant donné $x \in F'$, $x \in F$, donc $ix \in iF$, et de même, $x \in iF$, donc $ix \in i(iF) = F$. Ainsi, $x \in F'$.

Par conséquent, $F' = F \cap iF$ est un sous-espace vectoriel (sur $\mathbb{C}$) de E .

- Montrons que c'est le plus grand sous-espace de E contenu dans F . Soit G un sous-espace de E contenu dans F . On a alors, par stabilité, $iG \subset G$, et $G = i(iG) \subset iG$, donc $G = iG$. Comme $iG \subset iF$, on en déduit que $G \subset F \cap iF$.

Ainsi, $F \cap iF$ est le plus grand sous-espace (sur $\mathbb{C}$) de E contenu dans F .

- (e) Soit G un supplémentaire de $F \cap iF$ dans F . Puisque $G \subset F$ et $iG \subset iF$, on a $G \cap iG \subset F \cap iF$, et puisque $G \cap iG \subset G$, il vient

$$G \cap iG \subset G \cap (F \cap iF) = \{0\},$$

par définition d'un supplémentaire. L'inclusion réciproque étant évidente, il vient donc $G \cap iG = \{0\}$, donc

G est un sous-espace réel de E .

3. Soit F un sous-espace réel de E .

- (a) Soit $(x_j)_{j \in I}$ une famille d'éléments de F , libre sur $\mathbb{R}$. Soit $(\lambda_j)_{j \in \mathbb{C}}$ une famille d'éléments de $\mathbb{C}$ presque tous nuls, tels que

$$\sum_{j \in I} \lambda_j x_j = 0.$$

Écrivons pour tout $j \in I$, $\lambda_j = a_j + i b_j$, où a_j et b_j sont des réels. Alors les a_j et les b_j sont presque tous nuls, et $\sum_{j \in I} a_j x_j = - \sum_{j \in I} b_j (i x_j)$. La première somme est dans F , la seconde est dans iF . Ainsi, au vu de l'égalité, elles sont toutes les deux dans $F \cap iF$ qui est égal à $\{0\}$ (F est un sous-espace réel). Ainsi :

$$\sum_{j \in I} a_j x_j = 0 \quad \text{et} \quad \sum_{j \in I} b_j (i x_j) = 0.$$

Comme la famille $(x_j)_{j \in I}$ est libre (sur $\mathbb{R}$), la première somme (qui est à coefficients réels) amène : $\forall j \in I, a_j = 0$.

De plus, en multipliant la seconde somme par $-i$, on obtient $\sum_{j \in I} b_j x_j = 0$. En utilisant de nouveau la liberté de la famille $(x_j)_{j \in I}$ sur $\mathbb{R}$, on en déduit que pour tout $j \in I, b_j = 0$.

Ainsi, pour tout $j \in I, \lambda_j = 0$, et la famille $(x_j)_{j \in I}$ est libre sur $\mathbb{C}$.

- (b) • Si $\dim_{\mathbb{C}} E = n$, alors $\dim_{\mathbb{R}} E = 2n$. En effet, si $(b_j)_{j \in \llbracket 1, n \rrbracket}$ est une base de E sur $\mathbb{C}$, alors :
- * en séparant partie réelle et partie imaginaire des coefficients, toute combinaison à coefficients complexes de $(b_1, \dots, b_n)$ est combinaison linéaire à coefficients réels de $(b_1, \dots, b_n, i b_1, \dots, i b_n)$.
 - * toute combinaison linéaire à coefficients réels des vecteurs de $(b_1, \dots, b_n, i b_1, \dots, i b_n)$ est une combinaison linéaire à coefficients complexes des b_k (en regroupant les termes b_k et $i b_k$). Si elle est nulle, la liberté sur $\mathbb{C}$ de la famille (b_k) nous assure la nullité de tous ces coefficients complexes, donc de leur partie réelle et imaginaire, donc de tous les coefficients de la combinaison initiale.
- Ainsi, $(b_1, \dots, b_n, i b_1, \dots, i b_n)$ est une base de E sur $\mathbb{R}$.
- Soit F un sous-espace réel. Comme F et iF ont même dimension, et comme $F \cap iF = \{0\}$ (par définition d'un sous-espace réel), il vient $\dim F + \dim iF \leq 2n$, donc $\dim F \leq n$.
 - On a égalité si et seulement si $\dim_{\mathbb{R}}(F \oplus iF) = \dim_{\mathbb{R}}(E)$. L'inclusion, avec égalité des dimensions, amène l'égalité. Ainsi, $\dim F \leq n$ si et seulement si $F \oplus iF = E$.

4. Soit G un sous-espace de E de dimension finie. Soit $(b_1, \dots, b_\ell)$ une base sur $\mathbb{C}$ de G . Le même argument que pour E montre que $(b_1, \dots, b_\ell, i b_1, \dots, i b_\ell)$ est une base de G sur $\mathbb{R}$.

Soit alors $F = \text{Vect}_{\mathbb{R}}(b_1, \dots, b_\ell)$. On a $iF = \text{Vect}_{\mathbb{R}}(i b_1, \dots, i b_\ell)$, et le fait que $(b_1, \dots, b_\ell, i b_1, \dots, i b_\ell)$ soit une base de G amène alors :

$$\boxed{G = F \oplus iF}$$

(l'égalité provenant du caractère générateur, et la somme directe de la liberté).

Cet espace n'est bien sûr pas unique ; en effet, si F est un tel espace, alors iF convient aussi. D'autres contre-exemples : si $E = G = \mathbb{C}$, soit $z \in \mathbb{C}^*$, et soit $F = \mathbb{R}z$ (ainsi, F est n'importe quelle droite réelle dans le plan complexe). Alors $iF \cap F = \{0\}$, et $\mathbb{C} = F \oplus iF$. On a trouvé une infinité de sous-espaces F qui conviennent.

5. On considère $\mathcal{F}$ l'ensemble des sous-espaces vectoriels sur $\mathbb{R}$ de G tels que $F \oplus iF$ soit directe (et nécessairement inclu dans G , par stabilité de G par multiplication par un scalaire complexe), ordonné par l'inclusion.

Soit $(F_i)_{i \in I}$ un sous-ensemble totalement ordonné de $\mathcal{F}$. Alors :

- si $I = \emptyset, \{0\}$ est un majorant de (F_i)
- si $I \neq \emptyset$, soit $F = \bigcup_{i \in I} F_i$.
 - * Montrons que F est un sous-espace vectoriel sur $\mathbb{R}$ de E . Soit $x, y \in F$. Il existe $(i, j) \in I^2$ tels que $x \in F_i$ et $y \in F_j$. L'ordre étant total sur $(F_i)_{i \in I}$, on a $F_i \subset F_j$ ou $F_j \subset F_i$. Ainsi, x et y sont soit tous deux dans F_i , soit tous deux dans F_j . Pour se fixer les idées, supposons que x et y soient dans F_i . Alors pour tout $\lambda \in \mathbb{R}, x + \lambda y \in F_i$, donc $x + \lambda y \in F$. Comme de plus, F est de toute évidence inclus dans E , et contient 0 (car $I \neq \emptyset$), on en déduit que F est un sous-espace vectoriel sur $\mathbb{R}$ de E .
 - * F est inclus dans G . De plus, soit $x \in F \subset iF$. Il existe donc i et j tels que $x \in F_i$ et $x \in iF_j$. De même que précédemment, on peut supposer $i = j$ car l'ordre est total, donc $x \in F_i \cap iF_i = \{0\}$. Ainsi, $x = 0$. Par conséquent, $F \cap iF = \{0\}$, et la somme $F \oplus iF$ est directe.

Ainsi, F est un majorant dans $\mathcal{F}$ de (F_i) .

On en déduit que $\mathcal{F}$ est inductif. D'après le lemme de Zorn, il admet donc un élément maximal F . On a $F \oplus iF \subset G$. Si ce n'est pas une égalité, alors soit $x \in G \setminus (F \oplus iF)$.

Il n'est pas très dur de se convaincre que F est un sous-espace vectoriel (sur $\mathbb{C}$) de G . Ainsi, on obtient

$$(F \oplus iF) \oplus \mathbb{C}x \subset G.$$

Or, vu comme espace sur $\mathbb{R}$,

$$F \oplus iF \oplus \mathbb{C}x = F \oplus iF \oplus \mathbb{R}x \oplus \mathbb{R}ix = (F \oplus \mathbb{R}x) \oplus (iF \oplus \mathbb{R}ix) = (F \oplus \mathbb{R}x) \oplus i(F \oplus \mathbb{R}x).$$

Cela contredit la maximalité de F .

Ainsi, $\boxed{F \oplus iF = G.}$

6. Soit F un espace vectoriel sur $\mathbb{R}$ quelconque.

(a) On définit des opérations sur $F \times F$ par :

$$(x, y) + (x', y') = (x + x', y + y') \quad \text{et} \quad (a + ib) \cdot (x, y) = (ax - by, bx + ay).$$

Pour vérifier que cela définit une structure d'espace vectoriel, il faut vérifier toutes les propriétés d'un espace vectoriel (ici, ce n'est pas le sous-espace vectoriel de quelque chose!) :

- Structure de groupe abélien pour la somme : la définition donnée pour la somme n'est rien d'autre que la définition de la structure de groupe produit $G \times H$, abélien si les deux groupes G et H le sont.
- Compatibilité avec le neutre $1 \in \mathbb{C}$:

$$\forall x, y \in F \times F, 1 \cdot (x, y) = (1 + i \cdot 0) \cdot (x, y) = (1 \cdot x - 0 \cdot y, 0 \cdot x + 1 \cdot y) = (x, y).$$

- Le produit est associatif : pour tout $(x, y) \in F^2$, et tous $a, b, c, d \in \mathbb{R}$,

$$((a + ib)(c + id))(x, y) = (ac - bd + i(bd + ad))(x, y) = ((ac - bd)x - (ad + bc)y, (ad + bc)x + (ac - bd)y),$$

$$\begin{aligned} \text{et : } (a + ib)((c + id)(x, y)) &= (a + ib)(cx - dy, dx + cy) \\ &= (a(cx - dy) - b(dx + cy), b(cx - dy) + a(dx + cy)) = ((a + ib)(c + id))(x, y). \end{aligned}$$

- Distributivité du produit sur la somme de $\mathbb{C}$:

$$((a + ib) + (c + id))(x, y) = ((a + c) + i(b + d))(x, y) = (a + c)x - (b + d)y, (b + d)x + (a + c)y,$$

$$\begin{aligned} \text{et : } (a + ib)(x, y) + (c + id)(x, y) &= (ax - by, bx + ay) + (cx - dy, dx + cy) \\ &= ((a + c)x - (b + d)y, (b + d)x + (a + c)y). \end{aligned}$$

- Distributivité du produit sur la somme de $F \times F$: de même.

Au passage, remarquez à quel point c'est préférable de pouvoir définir un espace vectoriel comme un sous-espace d'un espace connu : il y a beaucoup moins de vérifications à faire !

- (b) • Tout d'abord, montrons que F est un sous-espace sur $\mathbb{R}$ de $F_{\mathbb{C}}$; pour cela, étudions la stabilité par combinaisons linéaires. Soit $X = (x, 0)$ et $Y = (y, 0)$ deux éléments de F , et $\lambda \in \mathbb{R}$. Alors $\lambda X + Y = (\lambda x + y, 0)$. Or, $\lambda x + y$ est dans F , par stabilité de F , donc $(\lambda x + y, 0) \in F$, d'après l'abus de notation précisé dans l'énoncé. Comme $(0, 0) \in F$, on en déduit que $\boxed{F \text{ est un sous-espace sur } \mathbb{R} \text{ de } F_{\mathbb{C}}}$.

Remarquez que l'abus de notation se justifie par le fait que l'application linéaire $F \longrightarrow F$ (de l'ancien F vers le nouveau) donnée par $x \mapsto (x, 0)$ est un isomorphisme.

- Soit maintenant $X = (x, 0)$ un élément de F . Alors $iX = (0, x)$, d'après la description de la loi externe. Ainsi, iF est le sous-espace sur $\mathbb{R}$ de $F_{\mathbb{C}}$ constitué des couples $(0, x)$, pour $x \in F$. En particulier, $F \cap iF = \{(0, 0)\} = \{0\}$. Par conséquent, $\boxed{F \text{ est un sous-espace réel de } F_{\mathbb{C}}}$.

(c) On sait déjà que F et iF sont en somme directe (question précédente). Montrons que $F + iF = F_{\mathbb{C}}$. Soit (x, y) un élément de $F_{\mathbb{C}}$. Alors $(x, y) = (x, 0) + (0, y)$, avec $(x, 0) \in F$, et $(0, y) \in iF$. Donc $F_{\mathbb{C}} \subset F + iF$. L'inclusion réciproque est évidente, puisque $F \subset F_{\mathbb{C}}$ et $iF \subset F_{\mathbb{C}}$. Ainsi, $F \oplus iF = F_{\mathbb{C}}$.

(d) Un sous-espace réel de $F_{\mathbb{C}}$ n'est pas forcément un sous-espace (sur $\mathbb{R}$) de F .

En effet, si $F = \mathbb{R}$, alors une vérification immédiate montre que $F_{\mathbb{C}} = \mathbb{C}$; l'élément i correspond à $(0, 1)$. Le produit et l'addition correspondent au produit et à l'addition dans $\mathbb{C}$. On a vu plus haut que toute droite réelle de $\mathbb{C}$ est un sous-espace réel de $\mathbb{C}$. Ainsi, $iF = i\mathbb{R}$ est un sous-espace réel de $\mathbb{R}$, aussi étrange que puisse paraître la terminologie!

C'est d'ailleurs le cas pour tout sous-espace réel F : iF est alors aussi un sous-espace réel de $F_{\mathbb{C}}$, mais n'est bien sûr pas contenu dans F , sauf dans le cas où $F = \{0\}$.

7. D'après la question 4, il existe un sous-espace sur $\mathbb{R}$ de E tel que $F \oplus iF = E$. Montrons que E est isomorphe à $F_{\mathbb{C}}$. On définit l'isomorphisme

$$\varphi : F_{\mathbb{C}} = F \times F \longrightarrow E = F \oplus iF$$

par $\varphi(x, y) = x + iy$. Cette application est clairement une bijection. En effet l'application définie pour tout $x \in F$ et $y \in iF$ par $\psi(x + y) = (x, -iy)$ en est clairement une réciproque.

Montrons que c'est un isomorphisme, c'est-à-dire que cette bijection est une application linéaire. Soit (x, y) et (x', y') deux éléments de $F \times F$, et $\lambda \in \mathbb{C}$. On écrit $\lambda = a + ib$, où a et b sont deux réels. Alors :

$$\begin{aligned} \varphi(\lambda(x, y) + (x', y')) &= \varphi(ax - by + x', bx + ay + y') = (ax - by + x') + i(bx + ay + y') \\ &= (a + ib)(x + iy) + (x' + iy') = \lambda\varphi(x, y) + \varphi(x', y'). \end{aligned}$$

Ainsi, φ est un isomorphisme de $F_{\mathbb{C}}$ sur E : E est isomorphe au complexifié de F .

Corrigé du problème 2 – Polynôme minimal irréductible

Question préliminaire :

Un polynôme annulateur non nul ne peut pas être constant. On écrit alors $P = a_0 + XQ(X)$, avec $Q \neq 0$. Si $a_0 = 0$, alors X divise P . Si $\deg(Q) = 0$, X serait polynôme annulateur de f , ce qui équivaut à dire que $f = 0$, ce qu'exclut l'énoncé (après rectification...)

Ainsi, $\deg(Q) > 0$, et P se factorise non trivialement, ce qui contredit son irréductibilité.

On en déduit que $a_0 \neq 0$. Par un argument classique, on peut alors montrer que f est bijectif, en exprimant une réciproque :

$$a_0 \text{id} = -f \circ Q(f) = -Q(f) \circ f,$$

donc $-\frac{1}{a_0}Q(f)$ est une réciproque de f . On en déduit que f est un isomorphisme, donc que $\text{Ker}(f) = \{0\}$.

Partie I – Polynôme minimal ponctuel

- Le polynôme nul est clairement dans I et J_x .
 - Soit P et Q dans I , alors $(P - Q)(f) = P(f) - Q(f) = 0_{\mathcal{L}(E)}$
 - Soit P et Q dans J_x , alors $(P - Q)(f)(x) = P(f)(x) - Q(f)(x) = 0_E$.
 - Soit $P \in I$ et $Q \in \mathbb{K}[X]$. Alors $(PQ)(f) = P(f) \circ Q(f) = 0 \circ Q(f) = 0$
 - Soit $P \in J_x$ et $Q \in \mathbb{K}[X]$, alors $(PQ)(f)(x) = Q(f) \circ P(f)(x) = Q(f)(0) = 0$.

Ainsi, I et J_x sont des idéaux de $\mathbb{K}[X]$.

- Comme $\mathbb{K}[X]$ est principal, on en déduit que I et J_x sont principaux, engendrés par des polynômes unitaires Q et Q_x . Tout autre polynôme de ces idéaux sont alors des multiples de ceux-là.
- En particulier, P étant un polynôme annulateur, P est un multiple du polynôme minimal Q . Comme P est irréductible, P et Q sont nécessairement associés. Les deux étant unitaires, on a donc $P = Q$.
- Soit $x \in E \setminus \{0\}$. D'après la question préliminaire $f(x) \neq 0$, donc Q_x n'est pas constant. Par ailleurs, P est un polynôme annulateur ponctuel en x , donc Q_x divise P . L'irréductibilité de P et le caractère unitaire des polynômes montre que $Q_x = P$.

Partie II – Endomorphisme induit

1. F étant stable, pour tout $x \in F$, $f(x) \in F$, et on peut donc définir $\tilde{f} : F \rightarrow F$ par :

$$\forall x \in F, \quad \tilde{f}(x) = f(x).$$

La linéarité de f se transfère de façon triviale à $\tilde{f}$.

Ainsi, $\boxed{\tilde{f} \in \mathcal{L}(F)}$.

On remarque dans un premier temps que par stabilité de F , pour tout $x \in F$ et $k \in \mathbb{N}$, $f^k(x) \in F$. Ainsi, à chaque itération, f correspond à $\tilde{f}$. On en déduit que $f^k(x) = \tilde{f}^k(x)$, puis que si P est un polynôme annulateur de f

$$0 = P(f)(x) = P(\tilde{f})(x).$$

Ceci étant vrai pour tout $x \in F$, $P(\tilde{f}) = 0$, donc $\boxed{P \text{ est un polynôme annulateur de } \tilde{f}}$.

2. Le polynôme minimal de $\tilde{f}$ est alors un diviseur de P (puisque P est annulateur de $\tilde{f}$). Puisque P est irréductible, ce polynôme minimal (unitaire) est donc 1 ou P . Le premier cas est impossible car id n'est pas nulle sur F (ayant été supposé distinct de $\{0\}$).

Ainsi, $\boxed{\text{le polynôme minimal de } \tilde{f} \text{ est } P}$.

Partie III – Dimension de E

1. Soit $e_1 \in E \setminus \{0\}$. Montrons que $(e_1, f(e_1), \dots, f^{d-1}(e_1))$ est une famille libre de E . Pour cela considérons une relation

$$\sum_{i=0}^{d-1} \lambda_i f^i(e_1) = 0.$$

Soit $R = \sum_{i=0}^{d-1} \lambda_i X^i$. Si $R \neq 0$, R est un polynôme annulateur ponctuel de f en e_1 , non divisible par P , ce qui contredit I-4.

Ainsi, $R = 0$ et les λ_i sont tous nuls.

On en déduit que $\boxed{(e_1, f(e_1), \dots, f^{d-1}(e_1)) \text{ est libre.}}$

Ayant trouvé dans E une famille libre de cardinal d , on peut affirmer que $\dim(E) \geq d$.

2. Notons $P = \sum_{k=0}^d a_k X^k$. Comme P est unitaire, on a $a_d = 1$. Soit $x \in E_1$. Il existe donc des coefficients $\lambda_0, \dots, \lambda_{d-1}$ tels que

$$x = \sum_{i=0}^{d-1} \lambda_i f^i(e_1).$$

En appliquant f , il vient :

$$\begin{aligned} f(x) &= \sum_{i=0}^{d-2} \lambda_i f^{i+1}(e_1) + \lambda_{d-1} f^d(e_1) \\ &= \sum_{i=0}^{d-2} \lambda_i f^{i+1}(e_1) - \lambda_{d-1} \sum_{i=0}^{d-1} a_i f^i(e_1), \end{aligned}$$

puisque P est annulateur de f . Ainsi, $f(x) \in E_1$, d'où la $\boxed{\text{stabilité de } E_1 \text{ par } f}$.

3. On suppose que $E_1 \neq E$, et on considère $e_2 \in E \setminus E_1$. On note $E_2 = \text{Vect}(e_2, f(e_2), \dots, f^{d-1}(e_2))$.
- (a) Tout comme E_1 , E_2 est stable par f . Soit alors $x \in E_1 \cap E_2$. Par stabilité de E_1 , $f(x) \in E_1$, et par stabilité de E_2 , $f(x) \in E_2$. Ainsi, $f(x) \in E_1 \cap E_2$. On en déduit que $\boxed{E_1 \cap E_2 \text{ est stable par } f}$.
- (b) Puisque $E_1 \cap E_2$ est stable par f , on peut considérer l'endomorphisme $\tilde{f}$ induit par f sur $E_1 \cap E_2$. Si $E_1 \cap E_2 \neq \{0\}$, d'après la partie II, $\tilde{f}$ admet P comme polynôme annulateur. Mais d'après III-1, cela implique que $\dim(E_1 \cap E_2) \geq d$.

Ainsi, $E_1 \cap E_2 \subset E_2$ et d'après la question III-1 (appliquée à e_2), $\dim(E_2) = d \leq \dim(E_1 \cap E_2)$. Ceci n'est possible que si $E_1 \cap E_2 = E_2$, donc $E_2 \subset E_1$. Ceci contredit le fait que $e_2 \notin E_1$.

On en déduit que $\boxed{E_1 \cap E_2 = \{0\}}$, donc que la somme $E_1 \oplus E_2$ est directe.

- (c) On continue cette construction tant que possible : supposons $e_1, \dots, e_\ell$ construits, et $E_1, \dots, E_\ell$ les sous-espaces vectoriels correspondants, qu'on être en somme directe.

Si leur somme est égale à E , on a ce qu'on veut.

Sinon, on considère $e_{\ell+1} \in E \setminus (E_1 \oplus \dots \oplus E_\ell)$ et on construit l'espace $E_{\ell+1}$ comme les précédents.

La question III-1 montre que $\dim(E_{\ell+1}) = d$. La question 2 montre que tous les E_i sont stables, donc la somme $E_1 \oplus \dots \oplus E_\ell$ aussi, et un argument similaire à la question 3a justifie la stabilité de $(E_1 \oplus \dots \oplus E_\ell) \cap E_{\ell+1}$.

Si cette intersection n'est pas réduite à $\{0\}$, f y induit un endomorphisme $\tilde{f}$ dont P est le polynôme minimal, d'après II-2. Ainsi, d'après III-1,

$$\dim((E_1 \oplus \dots \oplus E_\ell) \cap E_{\ell+1}) \geq d = \dim(E_{\ell+1}).$$

Comme de plus

$$(E_1 \oplus \dots \oplus E_\ell) \cap E_{\ell+1} \subset E_{\ell+1},$$

on en déduit que $(E_1 \oplus \dots \oplus E_\ell) \cap E_{\ell+1} = E_{\ell+1} \subset E_{\ell+1}$, puis que

$$E_{\ell+1} \subset E_1 \oplus \dots \oplus E_\ell,$$

ce qui contredit la définition de $e_{\ell+1}$.

Ainsi, $(E_1 \oplus \dots \oplus E_\ell) \cap E_{\ell+1} = \{0\}$, donc la somme suivante est directe :

$$E_1 \oplus E_2 \oplus \dots \oplus E_\ell \oplus E_{\ell+1}.$$

On peut donc continuer cette construction par récurrence, tant que la somme n'est pas égale à E . Cette construction finit par s'arrêter, car à chaque étape, la dimension de la somme augmente strictement, et doit rester bornée par $\dim(E)$. Ainsi il existe $k \in \mathbb{N}^*$ et une famille $(e_1, \dots, e_k)$ tels que les sous-espaces $E_1, \dots, E_k$ associés vérifient :

$$E = \bigoplus_{i=1}^k E_i.$$

4. D'après la question III-1, pour tout $i \in \llbracket 1, k \rrbracket$, $\dim(E_i) = d$. Ainsi, la propriété des dimensions des sommes directes amène

$$\dim(E) = kd, \quad \text{donc: } \boxed{d \mid \dim(E)}.$$

Les $(e_i, \dots, f^{d-1}(e_i))$ sont des bases des E_i , donc, par concaténation de ces bases, on obtient une base adaptée à la somme directe décrivant E . En particulier, c'est donc une base de E .