Composition de Mathématiques

Le 15 novembre 2017 – De 13 heures à 17 heures

Si, au cours de l'épreuve, un candidat repère ce qui lui semble être une erreur d'énoncé, il le signale sur sa copie et poursuit sa composition en expliquant les raisons des initiatives qu'il est amené à prendre.

Les calculatrices sont interdites.
Les téléphones portables doivent être éteints et rangés.

❖ I – Problème ❖

On compare ici deux algorithmes de calcul du pgcd de deux entiers naturels.

1. On *rappelle* que le pgcd de deux entiers naturels a et b est l'unique $d \in \mathbb{N}$ qui divise à la fois a et b et tel que tout entier δ qui divise à la fois a et b divise également d.

Étant donnés deux entiers naturels a et b (non nuls), on pose

$$\Omega = \left\{k \in \mathbb{N}^* \,:\, k \mid a \quad \text{et} \quad k \mid b\right\}$$

ainsi que

$$M = \max \Omega.$$

1.a. Démontrer que l'entier M est bien défini.
1.b. Démontrer que M est le pgcd de a et b.
1.c. Pour calculer M, on peut passer en revue tous les entiers compris entre 1 et a et retourner le dernier de ces entiers qui divise à la fois a et b.

Écrire *en langage Python* une fonction `gcd(a, b)` qui retourne le pgcd de a et b calculé selon la méthode qui vient d'être décrite.

2. La fonction Python `euclide(a,b)` retourne le pgcd de a et b calculé au moyen de l'algorithme d'Euclide.

```
def euclide(a, b):
  u, v = a, b
  while v!=0:
    u, v = v, u%v
  return u
```

2.a. Écrire *en langage Python* une fonction récursive `euclide_rec(a,b)` qui retourne le pgcd des entiers a et b calculé au moyen de l'algorithme d'Euclide.
2.b. En utilisant la fonction `euclide`, écrire *en langage Python* une fonction `gcd_trois(a,b,c)` qui retourne le pgcd des entiers a, b et c.

3. La suite de Fibonacci $(F_n)_{n\in\mathbb{N}}$ est définie par

$$F_0 = 0, \quad F_1 = 1 \quad \text{et} \quad \forall n \in \mathbb{N}, \quad F_{n+2} = F_{n+1} + F_n.$$

On *admet* que $(F_n)_{n\in\mathbb{N}}$ est une suite strictement croissante d'entiers naturels et que, lorsque n tend vers $+\infty$,

$$F_n \sim \frac{\varphi^n}{\sqrt{5}}$$

où $\varphi = (1+\sqrt{5})/2$.

3.a. Quel est le reste de la division euclidienne de F_{n+2} par F_{n+1} ?
3.b. En déduire le nombre u_n de divisions euclidiennes effectuées en calculant le pgcd de F_{n+2} et F_{n+1} avec la fonction `euclide`.
3.c. On note v_n, le nombre de divisions euclidiennes effectuées pour calculer le pgcd de F_{n+2} et F_{n+1} avec la fonction `gcd`. Comparer les ordres de grandeur de u_n et de v_n lorsque n tend vers $+\infty$.

4. Écrire *en langage Python* une fonction `fibo(n)` dont l'argument n est un entier naturel et qui retourne le nombre de Fibonacci F_n.

❖ II – Problème ❖

On considère la matrice carrée

$$A = \begin{pmatrix} 2 & -4 \\ 1 & 5 \end{pmatrix}$$

et les matrices colonnes

$$B_0 = \begin{pmatrix} 2 \\ 2 \end{pmatrix} \quad \text{et} \quad B_1 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}.$$

1. Le système $AX = B_0$ admet une, et une seule, solution

$$X \in \mathfrak{M}_{2,1}(\mathbb{Z}/11\mathbb{Z}).$$

Calculer cette solution et expliquer pourquoi elle est unique.

2. On considère ici la matrice A comme une matrice à coefficients dans $\mathbb{Z}/7\mathbb{Z}$.
2.a. Quel est le rang de A ?
2.b. Démontrer que le système $AX = B_0$ n'a pas de solution.
2.c. Expliquer pourquoi le système $AX = B_1$ admet exactement sept solutions

$$X \in \mathfrak{M}_{2,1}(\mathbb{Z}/7\mathbb{Z})$$

et donner la liste de ces sept solutions.

3.a. Calculer les solutions

$$X \in \mathfrak{M}_{2,1}(\mathbb{Z}/6\mathbb{Z})$$

du système $AX = B_0$.
3.b. Pourquoi la structure de l'ensemble des solutions est-elle différente de ce qu'on a l'habitude de trouver ?

❖ III – Problème ❖

On pose $E = \mathbb{R}^n$ où l'entier n est supérieur à 2. L'endomorphisme identiquement nul de E est noté ω_E.

1. (Question de cours) Soient u et v, deux endomorphismes de E. Démontrer que : si $u \circ v = v \circ u$, alors $\operatorname{Ker} u$ et $\operatorname{Im} u$ sont stables par v.

2. On considère un endomorphisme $u \in L(E)$ tel que $u^2 = \omega_E$.

2.a. Démontrer que $\operatorname{Im} u \subset \operatorname{Ker} u$.

2.b. En déduire une inégalité reliant n et $\operatorname{rg} u$.

3. Dans cette question, $n = 2$ et on suppose que $u \neq \omega_E$.

3.a. Démontrer qu'il existe une droite vectorielle D telle que

$$\operatorname{Ker} u = \operatorname{Im} u = D.$$

3.b. Soit $v \in L(E)$, tel que $v^2 = \omega_E$ et que

$$v \circ u = u \circ v.$$

En comparant $\operatorname{Im} u$ et $\operatorname{Im} v$, démontrer que

$$u \circ v = \omega_E.$$

3.c. Soit $w \in L(E)$ tel que $w^2 = \omega_E$ et que

$$w \circ u = u \circ w.$$

Démontrer que

$$w \circ v = v \circ w = \omega_E.$$

4. On revient au cas général : $E = \mathbb{R}^n$ et on considère m endomorphismes $u_1, \ldots, u_m$ de E tels que

$$\forall\, 1 \leqslant i \leqslant m, \quad u_i^2 = \omega_E$$

et que

$$\forall\, 1 \leqslant i < j \leqslant m, \quad u_i \circ u_j = u_j \circ u_i.$$

On pose $F_1 = \operatorname{Im} u_1$ et

$$\forall\, 2 \leqslant i \leqslant m, \quad F_i = \operatorname{Im}(u_1 \circ u_2 \circ \cdots \circ u_i).$$

4.a. Démontrer que, pour tout $1 \leqslant i < m$, le sous-espace F_i est stable par u_{i+1}.

4.b. En déduire que

$$\forall\, 1 \leqslant i \leqslant m, \quad \dim F_i \leqslant \frac{n}{2^i}.$$

4.c. Que peut-on en déduire lorsque $2^m > n$?

❖ IV – Problème ❖

On étudie ici la matrice

$$A = \begin{pmatrix} -1 & 1 & 0 \\ 1 & -2 & 1 \\ 0 & 1 & -1 \end{pmatrix}.$$

Partie A. Polynômes annulateurs

1. On calcule le polynôme minimal de A.

1.a. En vérifiant que

$$A^2 = \begin{pmatrix} 2 & -3 & 1 \\ -3 & 6 & -3 \\ 1 & -3 & 2 \end{pmatrix}$$

démontrer que la famille (I_3, A, A^2) est libre.

1.b. Exprimer A^3 en fonction de I_3, A et A^2.

1.c. En déduire le polynôme minimal de A.

2. Démontrer que

$$F = \operatorname{Vect}(I_3, A, A^2)$$

est un espace vectoriel de dimension 3 et qu'il est stable par produit.

3.a. Calculer le polynôme caractéristique χ_A de A.

3.b. Comparer χ_A au polynôme minimal de A.

Partie B. Diagonalisation

On note u, l'endomorphisme de $\mathbb{R}^3$ canoniquement associé à la matrice A et on considère les vecteurs ε_1, ε_2 et ε_3 de $\mathbb{R}^3$ respectivement représentés dans la base canonique par les matrices colonnes suivantes.

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

4. Démontrer que $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ est une base de $\mathbb{R}^3$ constituée de vecteurs propres de u.

5. Expliciter une matrice $Q \in GL_3(\mathbb{R})$ telle que

$$Q^{-1}AQ = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -3 \end{pmatrix}.$$

6. Démontrer que

$$Q^{-1}P(A)Q = \begin{pmatrix} P(0) & 0 & 0 \\ 0 & P(-1) & 0 \\ 0 & 0 & P(-3) \end{pmatrix}$$

pour tout polynôme $P \in \mathbb{R}[X]$.

7. On considère les trois matrices suivantes.

$$B_1 = Q\,\operatorname{Diag}(1,0,0)Q^{-1}$$
$$B_2 = Q\,\operatorname{Diag}(0,1,0)Q^{-1}$$
$$B_3 = Q\,\operatorname{Diag}(0,0,1)Q^{-1}$$

On ne demande pas de calculer explicitement ces trois matrices.

7.a. Calculer $B_1 + B_2 + B_3$.

7.b. Calculer les produits $B_i B_j$ en fonction des indices i et j.

7.c. Démontrer que

$$\forall\, n \geqslant 1, \quad A^n = (-1)^n B_2 + (-3)^n B_3.$$

Cette relation est-elle encore vraie pour $n = 0$?

7.d. Démontrer que

$$F = \operatorname{Vect}(B_1, B_2, B_3).$$

Partie C. Commutant de A

8. Soit $v \in L(E)$.

8.a. Démontrer que $u \circ v = v \circ u$ si, et seulement si, les vecteurs ε_1, ε_2 et ε_3 sont des vecteurs propres de v.

8.b. En déduire que $u \circ v = v \circ u$ si, et seulement si, il existe un polynôme P tel que

$$v = P(u) \quad \text{et} \quad \deg P \leqslant 2.$$

9. Quel est l'ensemble des matrices $B \in \mathfrak{M}_3(\mathbb{R})$ telles que $AB = BA$?

Solution I ❀ Nombres de Fibonacci

1. a. Le nombre d'entiers $k \in \mathbb{N}^*$ qui divisent à la fois a et b est inférieur au nombre d'entiers $1 \leqslant k \leqslant a$. Par conséquent, Ω est une partie finie de $\mathbb{N}$.

D'autre part, 1 divise a et b, donc $1 \in \Omega$. En tant que partie finie et non vide de $\mathbb{N}$, Ω admet un plus grand élément.

1. b. Soit d, le pgcd de a et b.

Comme $M \in \Omega$, l'entier M est un diviseur commun à a et b, donc M divise d : il existe $q \in \mathbb{N}^*$ tel que $d = q \times M$ et comme $q \geqslant 1$, alors $M \leqslant d$.

Réciproquement, en tant que diviseur commun à a et b, le pgcd d appartient à Ω et comme M est le plus grand élément de Ω, on a donc $d \leqslant M$.

Finalement, on a bien $M = d$.

1. c. Tout diviseur commun à a et b est inférieur à a et à b. Pour limiter les calculs, on pose $m = \min\{a, b\}$ et on parcourt la liste des entiers $2 \leqslant k \leqslant m$ (la boucle `for` doit s'achever avec $k = m$) : on sait que 1 est un diviseur commun à a et b.

Pour chaque entier k, on calcule les restes de la division euclidienne de a par k et de la division euclidienne de b par k : s'ils sont tous les deux nuls, c'est que k est un diviseur commun de a et b et dans ce cas, on affecte la valeur de k à la variable d.

On retourne la valeur finale de d, qui est le dernier (et donc le plus grand) diviseur commun trouvé.

```
def gcd(a, b):
  m = min(a, b)
  d = 1
  for k in range(2, m+1):
    if (a%k==0) and (b%k==0):
      d = k
  return d
```

2. a. L'algorithme d'Euclide repose sur la relation

$$\forall\, b > 0, \qquad \mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$$

où r est le reste de la division euclidienne de a par b et sur le cas particulier :

$$\forall\, a \in \mathbb{N}, \qquad \mathrm{pgcd}(a, 0) = a.$$

La version récursive de l'algorithme s'en déduit immédiatement.

```
def euclide_rec(a, b):
  if (b==0):
    d = a
  else:
    d = euclide_rec(b, a%b)
  return d
```

2. b. Il suffit de savoir que

$$\mathrm{pgcd}(a, b, c) = \mathrm{pgcd}(a, \mathrm{pgcd}(b, c))$$

(associativité du pgcd).

```
def gcd_trois(a, b, c):
  return euclide(a, euclide(b, c))
```

3. a. D'après la relation de récurrence :

$$F_{n+2} = F_{n+1} + F_n = 1 \times F_{n+1} + F_n$$

et comme la suite de Fibonacci est positive et strictement croissante, on en déduit que $0 \leqslant F_n < |F_{n+1}|$. La relation ci-dessus est donc bien la division euclidienne de F_{n+2} par F_{n+1} : le quotient est égal à 1 et le reste à F_n.

3. b. Dans la fonction `euclide`,

- Le couple `(u,v)` est initialement égal à (F_{n+2}, F_{n+1}) ;
- D'après la question précédente, à chaque étape, le couple (F_{k+1}, F_k) est remplacé par le couple (F_k, F_{k-1}) ;
- On sort de la boucle lorsque `v` devient nul et dans ce cas, le couple `(u,v)` a pour valeur $(F_1, F_0) = (1, 0)$.

On passe de F_{n+1} à $F_0 = F_{(n+1)-(n+1)}$ en effectuant $(n+1)$ itérations et une division euclidienne à chaque itération, donc on effectue $u_n = n + 1$ divisions euclidiennes en tout.

REMARQUE.— On a démontré au passage que F_{n+2} et F_{n+1} étaient premiers entre eux.

3. c. On parcourt la liste des entiers compris entre 1 et

$$F_{n+1} = \min\{F_{n+1}, F_{n+2}\}$$

et pour chacun de ces entiers, on effectue deux divisions euclidiennes. On effectue en tout $v_n = 2F_{n+1}$ divisions euclidiennes.

❀ Lorsque n tend vers $+\infty$,

$$u_n \sim n \quad \text{et} \quad v_n \sim \frac{2\varphi^n}{\sqrt{5}}$$

donc $u_n = o(v_n)$ (puisque $|\varphi| > 1$). La fonction `euclide` est donc sensiblement plus efficace que la fonction `gcd`.

4. On retourne à part la valeur F_0. Pour calculer F_n avec $n \geqslant 1$, on effectue une boucle.

Initialisation
$(u, v) = (F_0, F_1) = (0, 1)$
Itération $(1 \leqslant k < n)$
Entrée de boucle
$(u, v) = (F_{k-1}, F_k)$
Sortie de boucle
$(u, v) = (F_k, F_{k+1}) = (F_k, F_k + F_{k-1})$
Terminaison
$(u, v) = (F_{n-1}, F_n)$

- L'entrée de la première itération ($k = 1$) coïncide avec l'initialisation.
- La sortie de la k-ième itération coïncide avec l'entrée de la $(k+1)$-ième itération.
- La terminaison coïncide avec la sorte de la dernière itération ($k = n - 1$).

En retournant la valeur finale de v, la fonction `fibo` donne bien la valeur de F_n.

On insiste sur un détail essentiel : l'instruction

```
for k in range(1, n):
```

traduit exactement l'encadrement $1 \leqslant k < n$ qui figure sur le tableau.

```
def fibo(n):
  if (n==0):
    return 0
  else:
    u, v = 0, 1
    for k in range(1, n):
      u, v = v, u+v
    return v
```

☙ On calcule F_n en effectuant $(n-1)$ itérations de la boucle et chaque itération calcule une somme. Le nombre de sommes effectuées est donc équivalent à n : la complexité de la fonction `fibo` est donc linéaire.

REMARQUE.— On peut faire mieux ! En exploitant la relation de récurrence linéaire et l'algorithme d'exponentiation rapide, on peut écrire une fonction de complexité logarithmique.

Solution II ❁ Systèmes d'équations et arithmétique modulaire

1. On applique l'algorithme du pivot.

$$\begin{cases} 2x - 4y = 2 \\ x + 5y = 2 \end{cases} \sim \begin{cases} -3y = -2 \\ x + 5y = 2 \end{cases} \quad (L_1 \leftarrow L_1 - 2L_2)$$
$$\sim \begin{cases} x = 6 \\ y = 8 \end{cases}$$

car $(-3) \times (-4) = 1$ dans $\mathbb{Z}/11\mathbb{Z}$.

☙ On vient de *calculer* la solution et de *démontrer* qu'elle était unique. L'unicité de la solution s'*explique* ici par le fait que la théorie des systèmes linéaires s'applique sur tous les corps et en particulier pour $\mathbb{K} = \mathbb{Z}/11\mathbb{Z}$ (comme 11 est premier, l'anneau $\mathbb{Z}/11\mathbb{Z}$ est un corps).

Le déterminant de la matrice A est égal à $3 \neq 0$, donc la matrice A est inversible et le système étudié admet pour unique solution la colonne $X = A^{-1}B_0$. En appliquant les formules de Cramer, on trouve que

$$A^{-1} = 3^{-1} \cdot \begin{pmatrix} 5 & 4 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} -2 & 5 \\ -4 & -3 \end{pmatrix}$$

puisque l'inverse de 3 dans $\mathbb{Z}/11\mathbb{Z}$ est égal à 4.

2. Comme à la question précédente, on calcule sur des matrices à coefficients dans un corps ($\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$ est un corps car 7 est premier), donc la théorie habituelle du calcul matriciel s'applique.

2. a. Comme les coefficients de A appartiennent à $\mathbb{Z}/7\mathbb{Z}$,

$$A = \begin{pmatrix} 2 & -4 \\ 1 & -2 \end{pmatrix}.$$

La matrice A n'est pas nulle, donc son rang est supérieur à 1. Les deux colonnes de A sont proportionnelles, donc le rang de A est strictement inférieur à 2. Donc le rang de A est égal à 1.

2. b. L'image de A est engendrée par les colonnes de A, donc l'équation $AX = B$ admet une solution (au moins) si, et seulement si, la matrice colonne B est proportionnelle à la matrice colonne

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix},$$

qui engendre $\operatorname{Im} A$.

La matrice colonne B_0 n'est pas proportionnelle à cette matrice colonne, donc l'équation $AX = B_0$ n'a pas de solution.

2. c. On remarque cette fois que

$$B_1 = \begin{pmatrix} 3 \\ 5 \end{pmatrix} = 5 \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} \in \operatorname{Im} A,$$

donc l'équation $AX = B_1$ admet au moins une solution X_1.

On sait alors (principe de superposition) que $AX = B_1$ si, et seulement si, la différence $(X - X_1)$ appartient au noyau de A. D'après le théorème du rang, le noyau de A est un sous-espace vectoriel de dimension 1 du plan $\mathbb{K}^2$, donc il est isomorphe à $\mathbb{K}^1$. En particulier, le cardinal de $\operatorname{Ker} A$ est égal au cardinal de $\mathbb{K}^1 = \mathbb{Z}/7\mathbb{Z}$, c'est-à-dire à 7.

C'est donc le principe de superposition qui explique pourquoi le système $AX = B_1$ admet exactement sept solutions.

☙ La discussion précédente montre que le système $AX = B_1$ équivaut à l'équation

$$x + 5y = -2$$

(la deuxième ligne du système), c'est-à-dire à

$$x = -2 + 5y.$$

On fait varier y de 0 à 6 et on en déduit la valeur correspondante de x : les solutions du système sont donc

$$\begin{pmatrix} 5 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 2 \\ 2 \end{pmatrix} \quad \begin{pmatrix} 4 \\ 3 \end{pmatrix} \quad \begin{pmatrix} 6 \\ 4 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 5 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 3 \\ 6 \end{pmatrix}.$$

3. Dans cette dernière question, tout change : on calcule avec des matrices à coefficients dans l'anneau $\mathbb{Z}/6\mathbb{Z}$, *qui n'est pas un corps* (car 6 n'est pas premier). Dans ces conditions, il n'est pas possible d'appliquer la théorie classique des systèmes linéaires et du calcul matriciel.

Il faut donc faire tous les calculs à la main, sans pouvoir être guidé par une théorie.

3. a. On applique l'algorithme du pivot dans $\mathbb{Z}/6\mathbb{Z}$.

$$\begin{cases} 2x - 4y = 2 \\ x + 5y = 2 \end{cases} \sim \begin{cases} 2x + 2y = 2 \\ x - y = 2 \end{cases}$$
$$\sim \begin{cases} 4x = 0 \\ x - y = 2 \end{cases} \quad (L_1 \leftarrow L_1 + 2L_2)$$

D'après la table de multiplication dans $\mathbb{Z}/6\mathbb{Z}$:

x	0	1	2	3	4	5
$4x$	0	4	2	0	4	2

l'équation $4x = 0$ admet deux solutions : $x = 0$ et $x = 3$. On déduit alors la valeur de y de la seconde équation.

Le système $AX = B_0$ admet donc exactement deux solutions :

$$\begin{pmatrix} 0 \\ 4 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 3 \\ 1 \end{pmatrix}.$$

3. b. L'explication a été donnée en préambule ! Il n'y a pas d'application linéaire derrière cette matrice et si le principe de superposition s'applique, l'ensemble des solutions de l'équation homogène $AX = 0$ n'a pas une structure d'espace vectoriel...

Néanmoins, le déterminant de A est égal à 2 et n'est donc pas inversible dans $\mathbb{Z}/6\mathbb{Z}$ (puisque 2 et 6 ne sont pas premiers entre eux) : cela explique pourquoi il n'y a pas unicité de la solution.

Il n'est pas compliqué de vérifier les résultats précédents. On utilise trois paramètres : le module n (pour calculer dans $\mathbb{Z}/n\mathbb{Z}$) et les coefficients a_0 et b_0 du second membre.

La fonction `convient(x, y, n, a0, b0)` retourne `True` si, et seulement si, le couple (x, y) vérifie

$$A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$$

modulo n.

```
def convient(x, y, n, a0, b0):
  a = (2*x-4*y)%n
  b = (x+5*y)%n
  return ((a==a0) and (b==b0))
```

La fonction `calculer(n, a0, b0)` parcourt l'ensemble $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ avec une double boucle `for` et chaque solution (x, y) rencontrée est enregistrée dans la liste `solutions` (initialement vide).

```
def calculer(n, a0, b0):
  solutions = []
  for x in range(n):
    for y in range(n):
      if convient(x, y, n, a0, b0):
        solutions.append((x,y))
  return solutions
```

Solution III ❁ Familles d'endomorphismes nilpotents

1. Soit $x \in \operatorname{Ker} u$. Alors $u(x) = 0$ et

$$u\big(v(x)\big) = (u \circ v)(x) = (v \circ u)(x) = v\big(u(x)\big) = v(0) = 0$$

d'après l'hypothèse de commutativité et la linéarité de v. Cela signifie que le vecteur $v(x)$ appartient au noyau de u. On a démontré que le noyau de u était stable par v.

Soit $y \in \operatorname{Im} u$. Alors il existe $x \in E$ tel que $y = u(x)$ et

$$v(y) = (v \circ u)(x) = (u \circ v)(x) = u\big(v(x)\big) \in \operatorname{Im} u.$$

On a démontré que l'image de u était stable par v.

2. a. Soit $y \in \operatorname{Im} u$. Il existe $x \in E$ tel que $y = u(x)$ et

$$u(y) = (u \circ u)(x) = \omega_E(x) = 0_E$$

donc $y \in \operatorname{Ker} u$. On a démontré que $\operatorname{Im} u \subset \operatorname{Ker} u$.

2. b. Comme E est un espace vectoriel de dimension *finie*, on déduit du théorème du rang que

$$\operatorname{rg} u + \dim \operatorname{Ker} u = \dim E = n.$$

Or $\operatorname{Im} u \subset \operatorname{Ker} u$, donc $\operatorname{rg} u \leqslant \dim \operatorname{Ker} u$ et par conséquent

$$2 \operatorname{rg} u \leqslant n.$$

3. a. Comme $u \neq \omega_E$, alors $\operatorname{rg} u \geqslant 1$. D'après la question précédente, $\operatorname{rg} u \leqslant 2/2 = 1$. Donc le rang de u est égal à 1.

Autrement dit, le sous-espace vectoriel $D = \operatorname{Im} u$ est une droite vectorielle.

D'après le théorème du rang,

$$\dim \operatorname{Ker} u = \dim E - \operatorname{rg} u = 2 - 1 = 1$$

et d'après la question précédente, $\operatorname{Im} u \subset \operatorname{Ker} u$. On déduit de cette inclusion et de l'égalité des dimensions que les deux sous-espaces sont égaux :

$$\operatorname{Im} u = \operatorname{Ker} u.$$

3. b. On distingue trois cas.

Premier cas : $v = \omega_E$. Par linéarité de u, la composée $u \circ v$ est l'endomorphisme nul.

Deuxième cas : $v \neq \omega_E$ et dans ce cas, v vérifie les mêmes hypothèses que u. L'étude de u menée au **3.a.** montre qu'il existe une droite vectorielle D' telle que $\operatorname{Im} v = \operatorname{Ker} v = D'$.

Cas 2.a : $D = D'$. Dans ce cas, pour tout $x \in E$, on a

$$v(x) \in \operatorname{Im} v = D' = D = \operatorname{Ker} u$$

donc $(u \circ v)(x) = u\big(v(x)\big) = 0_E$ et donc : $u \circ v = \omega_E$.

Cas 2.b : $D \neq D'$. Dans ce cas, $D \cap D'$ est un sous-espace strict de la droite vectorielle D, donc $D \cap D' = \{0_E\}$. Pour tout $x \in E$, on sait que

$$D = \operatorname{Im} u \ni u\big(v(x)\big) = v\big(u(x)\big) \in \operatorname{Im} v = D'.$$

Le seul vecteur de $D \cap D'$ étant le vecteur nul, on a démontré que

$$\forall\, x \in E, \quad (u \circ v)(x) = 0_E$$

et donc que $u \circ v = \omega_E$.

En conclusion, dans tous les cas possibles, la composée $u \circ v$ est l'endomorphisme nul.

3. c. Comme la propriété à établir est évidente dans le cas où $w = \omega_E$ et dans le cas où $v = \omega_E$, on suppose dans ce qui suit que ni v, ni w n'est l'endomorphisme nul.

L'étude de u au **3.a.** montre alors que $\operatorname{Im} v$ et $\operatorname{Im} w$ sont deux droites vectorielles et comme

$$u \circ v = u \circ w = \omega_E,$$

on en déduit que ces deux droites vectorielles sont contenues dans la droite vectorielle $D = \operatorname{Ker} u$. On en déduit (inclusion des sous-espaces et égalité des dimensions) que

$$\operatorname{Im} v = \operatorname{Im} w = D$$

et comme on sait aussi que $\operatorname{Im} v = \operatorname{Ker} v$ et $\operatorname{Im} w = \operatorname{Ker} w$, on en déduit que

$$\operatorname{Im} v = \operatorname{Ker} w \quad \text{et que} \quad \operatorname{Im} w = \operatorname{Ker} v.$$

Par conséquent, $w \circ v = v \circ w = \omega_E$.

4. a. Comme les u_k commutent deux à deux, on sait que les endomorphismes u_{i+1} et $v_i = u_1 \circ \cdots \circ u_i$ commutent, donc le sous-espace F_i, en tant qu'image de l'endomorphisme v_i, est stable par u_{i+1} (cf question de cours).

4. b. Comme F_i est stable par u_{i+1}, on peut définir l'endomorphisme $w_{i+1} \in L(F_i)$ induit par restriction de u_{i+1} à F_i.

Pour tout $x \in F_i \subset E$,

$$w_{i+1}^2(x) = u_{i+1}^2(x) = \omega_E(x) = 0_E.$$

On peut alors déduire de **2.b.** que

$$\operatorname{rg} w_{i+1} \leqslant \frac{1}{2} \dim F_i.$$

- Si $y \in \operatorname{Im} w_{i+1}$, alors il existe $x \in F_i$ tel que

$$y = w_{i+1}(x) = u_{i+1}(x)$$

et comme $x \in F_i$, il existe $x_0 \in E$ tel que

$$x = (u_1 \circ \cdots \circ u_i)(x_0).$$

Comme les endomorphismes u_k commutent deux à deux,

$$y = u_{i+1} \circ (u_1 \circ \cdots \circ u_i)(x_0) = (u_1 \circ \cdots \circ u_i \circ u_{i+1})(x_0)$$

ce qui prouve que $y \in F_{i+1}$.

Réciproquement, si $y \in F_{i+1}$, alors il existe $x \in E$ tel que

$$\begin{aligned} y &= (u_1 \circ \cdots \circ u_i \circ u_{i+1})(x) \\ &= u_{i+1}\big(\underbrace{u_1 \circ \cdots \circ u_i(x_0)}_{\in F_i}\big) \\ &= w_{i+1}\big(u_1 \circ \cdots \circ u_i(x_0)\big) \in \operatorname{Im} w_{i+1}. \end{aligned}$$

On a ainsi démontré que

$$\forall\, 1 \leqslant i < m, \quad \operatorname{rg} w_{i+1} = \dim F_{i+1} \leqslant \frac{1}{2} \dim F_i.$$

- Par **2.b.** appliqué à $u_1 \in L(E)$, on sait que

$$\dim F_1 = \operatorname{rg} u_1 \leqslant n/2.$$

La relation de récurrence précédente permet d'en déduire que

$$\forall\, 1 \leqslant i \leqslant m, \quad \dim F_i \leqslant \frac{n}{2^i}.$$

4. c. Si $2^m > n$, alors $\dim F_m < 1$, ce qui prouve que $\dim F_m = 0$ (la dimension d'un espace vectoriel est un entier) et donc que

$$\operatorname{Im}(u_1 \circ \cdots \circ u_m) = F_m = \{0_E\}.$$

Autrement dit,

$$u_1 \circ \cdots \circ u_m = \omega_E.$$

Solution IV ❁ Réduction d'une matrice

Partie A. Polynômes annulateurs

1. a. Soient a, b et c, des réels tels que

$$aI_3 + bA + cA^2 = 0_3.$$

La matrice $aI_3 + bA + cA^2$, nulle, est de la forme

$$\begin{pmatrix} * & * & * \\ * & * & * \\ c & * & * \end{pmatrix}$$

donc $c = 0$. Comme la matrice $aI_3 + bA + 0 \cdot A^2$, toujours nulle, est de la forme

$$\begin{pmatrix} * & * & * \\ b & * & * \\ 0 & * & * \end{pmatrix},$$

alors $b = 0$. Il reste seulement $aI_3 = 0_3$, donc $a = 0$. On a ainsi démontré que la famille (I_3, A, A^2) était libre.

1. b. On trouve (normalement sans difficulté)

$$A^3 = \begin{pmatrix} -5 & 9 & -4 \\ 9 & -18 & 9 \\ -4 & 9 & -5 \end{pmatrix}.$$

En comparant les coefficients situés à l'intersection de la troisième ligne et de la première colonne, on pense à former la matrice $A^3 + 4A^2$ et on observe alors que

$$A^3 = -4A^2 - 3A.$$

1. c. Le polynôme minimal de A est le polynôme unitaire annulateur de A de plus bas degré possible.

D'après **1.a.**, il n'existe aucun polynôme annulateur unitaire de degré inférieur à 2.

D'après **1.b.**, le polynôme unitaire

$$X^3 + 4X^2 + 3X = X(X+1)(X+3)$$

est un polynôme annulateur de A. C'est donc lui le polynôme minimal de A.

2. Par définition, F est le sous-espace de $\mathfrak{M}_3(\mathbb{R})$ engendré par les matrices I_3, A et A^2. Comme cette famille est libre d'après **1.a.**, c'est une *base* de F, donc la dimension de F est égale à 3.

- Les matrices qui appartiennent à F sont des polynômes en A, donc le produit de deux matrices de F est encore un polynôme en A.

Soit $P \in \mathbb{K}[X]$. On peut diviser le polynôme P par le polynôme minimal de A : il existe $Q \in \mathbb{K}[X]$ et $R \in \mathbb{K}[X]$ tels que

$$P = X(X+1)(X+3)Q + R \quad \text{et} \quad \deg R < 3.$$

En substituant A à X, on obtient alors

$$P(A) = R(A) \in \operatorname{Vect}(I_3, A, A^2) = F$$

puisque le polynôme minimal de A est un polynôme annulateur de A. On en déduit que tout polynôme en A appartient à F et donc que F est stable par produit.

REMARQUE.— Le sous-espace F est en fait une sous-algèbre de $\mathfrak{M}_3(\mathbb{R})$.

3. a. Pour tout $\lambda \in \mathbb{R}$,

$$\begin{aligned}\det(A-\lambda I_3) &= \begin{vmatrix} -1-\lambda & 1 & 0 \\ -\lambda & -\lambda & -\lambda \\ 0 & 1 & -1-\lambda \end{vmatrix} \\ &\qquad \text{(opération de pivot } L_2 \leftarrow L_2+L_1+L_3\text{)} \\ &= (-\lambda)\begin{vmatrix} -1-\lambda & 1 & 0 \\ -1 & -1 & -1 \\ 0 & 1 & -1-\lambda \end{vmatrix} \\ &\qquad \text{(on factorise } L_2 \text{ par } (-\lambda)\text{)} \\ &= (-\lambda)\big[(1+\lambda)(1+\lambda+1)+(1+\lambda)\big] \\ &\qquad \text{(développement par la première ligne)} \\ &= (-\lambda)(1+\lambda)(3+\lambda).\end{aligned}$$

Comme 3 est impair,

$$\forall \lambda \in \mathbb{R}, \quad \chi_A(\lambda) = -\det(A-\lambda I_3) = \lambda(1+\lambda)(3+\lambda)$$

et comme $\mathbb{R}$ est infini, on en déduit enfin que

$$\chi_A = X(X+1)(X+3)...$$

3. b. ... et en particulier que le polynôme caractéristique est égal au polynôme minimal.

Partie B. Diagonalisation

4. On vérifie très facilement que

$$A\begin{pmatrix}1\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix} = 0\cdot\begin{pmatrix}1\\1\\1\end{pmatrix}$$
$$A\begin{pmatrix}1\\0\\-1\end{pmatrix} = (-1)\cdot\begin{pmatrix}1\\0\\-1\end{pmatrix}$$
$$A\begin{pmatrix}1\\-2\\1\end{pmatrix} = (-3)\cdot\begin{pmatrix}1\\-2\\1\end{pmatrix}.$$

Comme ces matrices colonnes ne sont pas nulles, on a ainsi démontré que ε_1, ε_2 et ε_3 sont des vecteurs propres de u.

Comme ces vecteurs propres sont associés à des valeurs propres deux à deux distinctes (0, -1 et -3), ils forment une famille libre de trois vecteurs de $\mathbb{R}^3$ et donc une *base* de $\mathbb{R}^3$.

5. **Analyse.** On doit savoir que

$$Q^{-1}AQ = \mathrm{Diag}(0,-1,-3)$$

si, et seulement si, la matrice Q est la matrice de passage de la base canonique à une base de vecteurs propres de u, respectivement associés aux valeurs propres 0, -1 et -3.

Synthèse. D'après la question précédente, la matrice de passage de la base canonique à la base $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ convient. La matrice

$$Q = \begin{pmatrix}1 & 1 & 1\\ 1 & 0 & -2\\ 1 & -1 & 1\end{pmatrix}$$

est donc une matrice inversible telle que

$$Q^{-1}AQ = \mathrm{Diag}(0,-1,-3).$$

6. On sait que

$$\forall k \in \mathbb{N}, \quad (Q^{-1}AQ)^k = Q^{-1}(A^k)Q$$

et comme $Q^{-1}AQ$ est diagonale, on sait que

$$\forall k \in \mathbb{N}, \quad (Q^{-1}AQ)^k = \mathrm{Diag}(0^k, (-1)^k, (-3)^k).$$

On en déduit par combinaison linéaire que

$$Q^{-1}P(A)Q = \mathrm{Diag}\big(P(0), P(-1), P(-3)\big)$$

pour tout polynôme $P \in \mathbb{K}[X]$.

7. a. Comme

$$\mathrm{Diag}(1,0,0) + \mathrm{Diag}(0,1,0) + \mathrm{Diag}(0,0,1) = I_3,$$

alors

$$B_1 + B_2 + B_3 = Q^{-1}I_3Q = I_3.$$

7. b. On *doit savoir* que

$$(QM_1Q^{-1}) \times (QM_2Q^{-1}) = Q(M_1 \times M_2)Q^{-1}$$

quelles que soient les matrices M_1 et M_2.

- Il est clair que

$$\mathrm{Diag}(1,0,0)^2 = \mathrm{Diag}(1,0,0).$$

Par conséquent,

$$B_1^2 = Q\,\mathrm{Diag}(1,0,0)Q^{-1} = B$$

et, de même, $B_2^2 = B_2$ et $B_3^2 = B_3$.

- Il est tout aussi clair que

$$\mathrm{Diag}(1,0,0) \times \mathrm{Diag}(0,1,0) = \mathrm{Diag}(1\times 0, 0\times 1, 0) = 0_3.$$

Par conséquent,

$$B_1B_2 = Q \times 0_3 \times Q^{-1} = 0_3$$

et, de même,

$$\forall i \neq j, \quad B_iB_j = 0_3.$$

7. c. On applique **6.** au monôme $P = X^n$:

$$\begin{aligned}Q^{-1}A^nQ &= \mathrm{Diag}\big(0^n, (-1)^n, (-3)^n\big) \\ &= (-1)^n\,\mathrm{Diag}(0,1,0) + (-3)^n\,\mathrm{Diag}(0,0,1)\end{aligned}$$

car $n \geqslant 1$. En multipliant à gauche par Q et à droite par Q^{-1}, on en déduit que

$$A^n = (-1)^nB_2 + (-3)^nB_3.$$

- Cette relation est *fausse* pour $n = 0$:

$$\begin{aligned}A^0 = I_3 &= B_1 + B_2 + B_3 \\ &\neq B_2 + B_3 = (-1)^0B_2 + (-3)^0B_3.\end{aligned}$$

En revanche, la relation

$$A^n = 0^nB_1 + (-1)^nB_2 + (-3)^nB_3$$

est vraie pour tout $n \in \mathbb{N}$, y compris $n = 0$.

7. d. D'après **7.a.** et **7.c.**, les matrices I_3, A et A^2 sont des combinaisons linéaires de B_1, B_2 et B_3, donc

$$F \subset \mathrm{Vect}(B_1, B_2, B_3).$$

En particulier, $\dim F \leqslant \dim \mathrm{Vect}(B_1, B_2, B_3)$. Or $\dim F = 3$ par **2.** et $\dim \mathrm{Vect}(B_1, B_2, B_3) \leqslant 3$ (la dimension est majorée par le cardinal d'une famille génératrice), donc

$$\dim \mathrm{Vect}(B_1, B_2, B_3) = 3$$

et $F = \mathrm{Vect}(B_1, B_2, B_3)$ (inclusion des sous-espaces et égalité des dimensions).

REMARQUE.— On peut aussi exploiter le résultat du **6.** En notant L_1, L_2 et L_3, les polynômes interpolateurs de Lagrange associés aux réels 0, -1 et -3, on déduit de **6.** que

$$L_1(A) = Q\,\mathrm{Diag}\big(L_1(0), L_1(-1), L_1(-3)\big)Q^{-1} = B_1$$
$$L_2(A) = Q\,\mathrm{Diag}\big(L_2(0), L_2(-1), L_2(-3)\big)Q^{-1} = B_2$$
$$L_3(A) = Q\,\mathrm{Diag}\big(L_3(0), L_3(-1), L_3(-3)\big)Q^{-1} = B_3$$

et comme tous les polynômes en A appartiennent à F d'après **2.**, on en déduit que les matrices B_1, B_2 et B_3 appartiennent à F et donc que

$$\mathrm{Vect}(B_1, B_2, B_3) \subset F.$$

REMARQUE.— Comme les matrices

$$\mathrm{Diag}(1,0,0), \quad \mathrm{Diag}(0,1,0) \quad \text{et} \quad \mathrm{Diag}(0,0,1)$$

sont linéairement indépendantes (de façon évidente !) et que l'application $\big[M \mapsto QMQ^{-1}\big]$ est injective, les matrices B_1, B_2 et B_3 sont aussi linéairement indépendantes, ce qui donne une nouvelle preuve de l'égalité

$$\dim \mathrm{Vect}(B_1, B_2, B_3) = \dim F$$

et donc une troisième manière de conclure.

Partie C. Commutant de A

8. a. On sait depuis **4.** que

$$u(\varepsilon_1) = 0 \cdot \varepsilon_1, \quad u(\varepsilon_2) = (-1) \cdot \varepsilon_2, \quad u(\varepsilon_3) = (-3) \cdot \varepsilon_3.$$

❧ Supposons que ε_1, ε_2 et ε_3 soient trois vecteurs propres de v :

$$v(\varepsilon_1) = \lambda_1 \cdot \varepsilon_1, \quad v(\varepsilon_2) = \lambda_2 \cdot \varepsilon_2, \quad v(\varepsilon_3) = \lambda_3 \cdot \varepsilon_3.$$

On a alors

$$(u \circ v)(\varepsilon_1) = u(\lambda_1 \cdot \varepsilon_1) = (\lambda_1 \times 0) \cdot \varepsilon_1 = 0_E$$

tandis que

$$(v \circ u)(\varepsilon_1) = v(0_E) = 0_E.$$

De même,

$$(u \circ v)(\varepsilon_2) = (v \circ u)(\varepsilon_2) = (-\lambda_2) \cdot \varepsilon_2$$
$$(u \circ v)(\varepsilon_3) = (v \circ u)(\varepsilon_3) = (-3\lambda_3) \cdot \varepsilon_3.$$

Les applications *linéaires* $(u \circ v)$ et $(v \circ u)$ sont égales sur la *base* $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$, donc elles sont égales *partout* :

$$\forall\, x \in E, \quad (u \circ v)(x) = (v \circ u)(x)$$

c'est-à-dire $(u \circ v) = (v \circ u)$.

❧ Réciproquement, supposons que $(u \circ v) = (v \circ u)$.

Si x est un vecteur propre de u associé à la valeur propre α, alors

$$u\big(v(x)\big) = v\big(u(x)\big) = v(\alpha \cdot x) = \alpha \cdot v(x)$$

donc le vecteur $v(x)$ appartient au sous-espace propre $\mathrm{Ker}(u - \alpha\, I_E)$. Or les trois sous-espaces propres de u sont des *droites* vectorielles, respectivement dirigées par ε_1, ε_2 et ε_3. Par conséquent, le vecteur x dirige le sous-espace propre auquel il appartient et $v(x)$ est proportionnel à x, ce qui prouve que x est bien un vecteur propre de v.

On en déduit que ε_1, ε_2 et ε_3 sont trois vecteurs propres de v.

❧ Conclusion : les endomorphismes u et v commutent si, et seulement si, les vecteurs ε_1, ε_2 et ε_3 sont des vecteurs propres de v.

8. b. On *sait* que la sous-algèbre des polynômes en u est commutative. Par conséquent, s'il existe un polynôme $P \in \mathbb{R}[X]$ dont le degré est inférieur à 2 et tel que $v = P(u)$, alors u et v commutent.

❧ Réciproquement, supposons que u et v commutent.

Notons B, la matrice de v relative à la base canonique. D'après **5.** et **8.a.**, les endomorphismes u et v commutent si, et seulement si, la matrice de v relative à la base $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ est diagonale, c'est-à-dire s'il existe trois réels α_1, α_2 et α_3 tels que

$$Q^{-1}BQ = \mathrm{Diag}(\alpha_1, \alpha_2, \alpha_3).$$

D'après **6.** et la théorie des polynômes interpolateurs de Lagrange, il existe un, et un seul, polynôme $P \in \mathbb{R}_2[X]$ tel que

$$P(0) = \alpha_1, \quad P(-1) = \alpha_2 \quad \text{et} \quad P(-3) = \alpha_3$$

(*rappel* : le degré de P peut être choisi inférieur à n quand on interpole sur $(n+1)$ points) et donc tel que

$$Q^{-1}P(A)Q = Q^{-1}BQ.$$

En multipliant à gauche par Q et à droite par Q^{-1}, on en déduit que $B = P(A)$ et donc que $v = P(u)$.

9. D'après la question précédente, la matrice B commute à la matrice A si, et seulement si, B est une combinaison linéaire de I_3, A et A^2.

L'ensemble des matrices B telles que $AB = BA$ est donc la sous-algèbre F.