DS6

Exercice 1 : Cours

1. (*) Résoudre l'équation différentielle suivante :

$$(E) \qquad y'' + y \;=\; \cos(x)$$

Démonstration.

- On commence par résoudre l'équation homogène (H) associée à (E) :

$$y'' + y \;=\; 0$$

C'est une équation différentielle linéaire d'ordre 2 homogène à coefficients constants. On détermine donc les solutions de son équation caractéristique $r^2 + 1 = 0$.
Cette équation admet exactement 2 racines complexes : $r_1 = i = 0 + 1 \times i$ et $\overline{r_1}$.
L'ensemble des solutions de (H) est donc :

$$\begin{aligned} & \{x \mapsto \lambda_1 \,\mathrm{e}^{0\times x} \cos(1\times x) + \lambda_2 \,\mathrm{e}^{0\times x} \sin(1\times x) \mid (\lambda_1,\lambda_2) \in \mathbb{R}^2\} \\ = \;& \{x \mapsto \lambda_1 \cos(x) + \lambda_2 \sin(x) \mid (\lambda_1,\lambda_2) \in \mathbb{R}^2\} \end{aligned}$$

L'ensemble des solutions de (H) est : $\{x \mapsto \lambda_1 \cos(x) + \lambda_2 \sin(x) \mid (\lambda_1,\lambda_2) \in \mathbb{R}^2\}$.

- On cherche maintenant une solution particulière complexe de l'équation (E') :

$$y'' + y \;=\; \mathrm{e}^{ix}$$

Comme i est une racine simple de $Q(X) = X^2 + 1$, on cherche une solution particulière de (E') sous la forme $x \mapsto a\,x\,\mathrm{e}^{ix}$.
Soit $a \in \mathbb{C}$.
On pose $h : x \mapsto a\,x\,\mathrm{e}^{ix}$.

× La fonction h est deux fois dérivable sur $\mathbb{R}$ en tant que produit de fonctions deux fois dérivables sur $\mathbb{R}$.
Soit $x \in \mathbb{R}$.

$$h'(x) \;=\; a\left(1\times \mathrm{e}^{ix} + x \times i\,\mathrm{e}^{ix}\right) \;=\; a\,(1+ix)\,\mathrm{e}^{ix}$$

Ensuite :

$$h''(x) \;=\; a\left(i\times \mathrm{e}^{ix} + (1+ix)\times i\,\mathrm{e}^{ix}\right) \;=\; a\,(2i-x)\,\mathrm{e}^{ix}$$

× On obtient :

$$\begin{aligned} h \text{ solution de } (E') \quad & \Leftrightarrow \quad \forall x \in \mathbb{R},\; h''(x) + h(x) = \mathrm{e}^{ix} \\ & \Leftrightarrow \quad \forall x \in \mathbb{R},\; a\,(2i-x)\,\mathrm{e}^{ix} + a\,x\,\mathrm{e}^{ix} = \mathrm{e}^{ix} \\ & \Leftrightarrow \quad \forall x \in \mathbb{R},\; a\,(2i-x) + a\,x = 1 \qquad \textit{(car, comme } |e^{ix}| = 1\textit{,} \\ & \qquad\qquad\qquad\qquad\qquad\qquad\quad \textit{alors : } e^{ix} \neq 0\textit{)} \\ & \Leftrightarrow \quad \forall x \in \mathbb{R}, 2ia = 1 \\ & \Leftrightarrow \quad a = \frac{1}{2i} = -\frac{1}{2}\,i \end{aligned}$$

La fonction $g : x \mapsto -\dfrac{1}{2}\,i\,x\,\mathrm{e}^{ix}$ est donc une solution particulière de (E').

- On en déduit que la fonction $\mathrm{Re}\,(g)$ est une solution particulière de (E).
  Soit $x \in \mathbb{R}$.

$$\begin{aligned}\mathrm{Re}\,(g)\,(x) &= \mathrm{Re}\,(g(x)) \\ &= \mathrm{Re}\left(-\frac{1}{2}\,i\,x\,\mathrm{e}^{ix}\right) \\ &= -\frac{1}{2}\,x\,\mathrm{Re}\left(i\,\mathrm{e}^{ix}\right) \qquad \textit{(par linéarité de } \mathrm{Re}\,(\cdot)\textit{)}\end{aligned}$$

  Or :

$$i\,\mathrm{e}^{ix} = i\left(\cos(x) + i\,\sin(x)\right) = i\,\cos(x) - \sin(x)$$

  Ainsi : $\mathrm{Re}\left(i\,\mathrm{e}^{ix}\right) = -\sin(x)$. D'où :

$$\mathrm{Re}\,(g)\,(x) = -\frac{1}{2}\,x \times \left(-\sin(x)\right)$$

Une solution particulière de (E) est donc $x \mapsto \dfrac{1}{2}\,x\,\sin(x)$.

On en conclut que l'ensemble des solutions de (E) est :

$$\left\{x \mapsto \lambda_1\,\cos(x) + \lambda_2\,\sin(x) + \frac{1}{2}\,x\,\sin(x) \mid (\lambda_1, \lambda_2) \in \mathbb{R}^2\right\}$$

□

Exercice 2

On désigne par I la matrice identité de $\mathscr{M}_3(\mathbb{R})$ et on note : $A = \begin{pmatrix} -2 & 0 & 0 \\ -2 & -1 & -1 \\ -2 & 1 & -3 \end{pmatrix}$.

1. a) Calculer $(A+2\,I)^2$.

Démonstration.

- Tout d'abord :

$$A+2\,I \;=\; \begin{pmatrix} -2 & 0 & 0 \\ -2 & -1 & -1 \\ -2 & 1 & -3 \end{pmatrix} + \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \;=\; \begin{pmatrix} 0 & 0 & 0 \\ -2 & 1 & -1 \\ -2 & 1 & -1 \end{pmatrix}$$

- Ainsi :

$$(A+2\,I)^2 \;=\; \begin{pmatrix} 0 & 0 & 0 \\ -2 & 1 & -1 \\ -2 & 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ -2 & 1 & -1 \\ -2 & 1 & -1 \end{pmatrix} \;=\; \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\boxed{(A+2\,I)^2 = 0_{\mathscr{M}_3(\mathbb{R})}}$$

□

b) En déduire que A est inversible et déterminer A^{-1}.

Démonstration.

- D'après la question précédente : $(A+2\,I)^2 = 0_{\mathscr{M}_3(\mathbb{R})}$. Or :

$$(A+2\,I)^2 \;=\; A^2+4\,A+4\,I \qquad \textit{(car les matrices } A \textit{ et } I \textit{ commutent)}$$

- On en déduit :

$$\begin{aligned} & A^2+4\,A+4\,I = 0_{\mathscr{M}_3(\mathbb{R})} \\ \text{donc} \quad & A^2+4\,A = -4\,I \\ \text{et} \quad & A\,(A+4\,I) = -4\,I \\ \text{ainsi} \quad & A\left(-\frac{1}{4}\cdot(A+4\,I)\right) = I \end{aligned}$$

On en déduit que la matrice A est inversible, d'inverse $-\dfrac{1}{4}\cdot(A+4\,I)$.

$$\boxed{A^{-1} = -\frac{1}{4}\cdot A - I}$$

Commentaire

- L'écriture $\dfrac{A}{4}$ n'a pas de sens puisqu'il n'existe pas d'opérateur de division entre les matrices et les réels. Par contre, l'écriture $\dfrac{1}{4}\cdot A$ est bien autorisée : on multiplie une matrice par un scalaire à l'aide de l'opérateur de multiplication externe $\cdot : \mathbb{R}\times\mathscr{M}_n(\mathbb{R}) \to \mathscr{M}_n(\mathbb{R})$.
- On ne peut pas non plus diviser par une matrice. Rappelons que l'inverse d'une matrice A, si elle existe, est notée A^{-1} et pas $\dfrac{1}{A}$. L'écriture $\dfrac{A}{B}$ est elle aussi impropre car il n'y a pas d'opérateur de division entre deux matrices.

□

2. On note : $E_{-2}(A) = \{X \in \mathscr{M}_{3,1}(\mathbb{R}) \mid AX = -2X\}$.
Déterminer $E_{-2}(A)$.

Démonstration.

Soit $X \in \mathscr{M}_{3,1}(\mathbb{R})$. Alors il existe $(x, y, z) \in \mathbb{R}^3$ tel que : $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$.

$$\begin{aligned}
AX = -2\,X \quad &\iff \quad (A + 2\,I)\,X = 0_{\mathscr{M}_{3,1}(\mathbb{R})} \\
&\iff \quad \begin{pmatrix} 0 & 0 & 0 \\ -2 & 1 & -1 \\ -2 & 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \\
&\iff \quad \left\{ \begin{array}{rcl} 0 & = & 0 \\ -2\,x + y - z & = & 0 \\ -2\,x + y - z & = & 0 \end{array} \right. \\
&\iff \quad \left\{ \begin{array}{rcl} -2\,x + y - z & = & 0 \\ -2\,x + y - z & = & 0 \end{array} \right. \\
&\overset{L_3 \leftarrow L_3 - L_2}{\iff} \quad \left\{ \begin{array}{rcl} -2\,x + y - z & = & 0 \\ 0 & = & 0 \end{array} \right. \\
&\iff \quad \left\{ \begin{array}{rcl} z & = & -2\,x + y \end{array} \right.
\end{aligned}$$

On obtient alors :

$$\begin{aligned}
E_{-2}(A) &= \{\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathscr{M}_{3,1}(\mathbb{R}) \mid z = -2\,x + y\} = \{\begin{pmatrix} x \\ y \\ -2\,x + y \end{pmatrix} \mid (x, y) \in \mathbb{R}^2\} \\
&= \{x \cdot \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix} + y \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \mid (x, y) \in \mathbb{R}^2\} = \text{Vect}\left(\begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right)
\end{aligned}$$

$$\boxed{E_{-2}(A) = \text{Vect}\left(\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right)}$$

Commentaire

- Lors de la résolution du système, on choisit d'exprimer la variable z en fonction des variables x et y. Ces deux dernières variables sont alors appelées variables auxiliaires.
- Il était possible de faire d'autres choix. Par exemple :

$$AX = -X \quad \Leftrightarrow \quad y = 2\,x + z$$

On obtient alors l'expression de F suivante : $F = \text{Vect}\left(\begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right)$.

Notons au passage : $\text{Vect}\left(\begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right) = \text{Vect}\left(\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right)$.

(il suffit de remplacer le vecteur $\begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$ par la combinaison linéaire $\begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix} - 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$) □

3. On note $P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ -2 & -1 & -2 \end{pmatrix}$.

a) Démontrer que P est inversible et déterminer son inverse.

Démonstration.

- On applique l'algorithme du pivot de Gauss.

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 \\ -2 & -1 & -2 & 0 & 0 & 1 \end{array}\right)$$

On effectue l'opération $\{\, L_3 \leftarrow L_3 + 2\,L_1$. On obtient :

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 & 0 & 1 \end{array}\right)$$

On effectue l'opération $\{\, L_3 \leftarrow L_3 - L_2$. On obtient :

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & -1 & 1 \end{array}\right)$$

La réduite obtenue est triangulaire supérieure. De plus, ses coefficients diagonaux sont tous non nuls. Ainsi cette réduite est inversible et il en est de même de la matrice initiale P.

- On effectue les opérations $\left\{\begin{array}{l} L_1 \leftarrow L_1 - L_3 \\ L_2 \leftarrow L_2 + L_3 \end{array}\right.$. On obtient :

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & -1 & 1 & -1 \\ 0 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 2 & -1 & 1 \end{array}\right)$$

On effectue l'opération $\left\{\; L_1 \leftarrow L_1 - L_2 \;\right.$. On obtient :

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -3 & 1 & -2 \\ 0 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 2 & -1 & 1 \end{array}\right)$$

$$\boxed{\text{Finalement : } P^{-1} = \begin{pmatrix} -3 & 1 & -2 \\ 2 & 0 & 1 \\ 2 & -1 & 1 \end{pmatrix}.}$$

Commentaire

On remarque que les deux premières colonnes de la matrice P ne sont autres que les vecteurs de la famille $E_{-2}(A)$. C'est ce choix qui permet d'exprimer par la suite la matrice A sous une forme plus simple. On en parlera en $2^{\text{ème}}$ année dans le chapitre « Réduction ». □

b) Montrer que $P^{-1}AP = T$ où T est la matrice triangulaire supérieure $T = \begin{pmatrix} -2 & 0 & 1 \\ 0 & -2 & -1 \\ 0 & 0 & -2 \end{pmatrix}$.

Démonstration.

- Notons tout d'abord :

$$AP = \begin{pmatrix} -2 & 0 & 0 \\ -2 & -1 & -1 \\ -2 & 1 & -3 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ -2 & -1 & -2 \end{pmatrix} = \begin{pmatrix} -2 & -2 & -2 \\ 0 & -2 & 1 \\ 4 & 2 & 3 \end{pmatrix}$$

- Enfin :

$$P^{-1}AP = \begin{pmatrix} -3 & 1 & -2 \\ 2 & 0 & 1 \\ 2 & -1 & 1 \end{pmatrix}\begin{pmatrix} -2 & -2 & -2 \\ 0 & -2 & 1 \\ 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} -2 & 0 & 1 \\ 0 & -2 & -1 \\ 0 & 0 & -2 \end{pmatrix} = T$$

Ainsi : $P^{-1}AP = T$.

□

c) Démontrer : $\forall n \in \mathbb{N}$, $P^{-1}A^nP = T^n$.

Démonstration.
Démontrons par récurrence : $\forall n \in \mathbb{N}$, $\mathscr{P}(n)$ où $\mathscr{P}(n) : P^{-1}A^nP = T^n$.

▸ **Initialisation**

- D'une part : $P^{-1}A^0P = P^{-1}IP = P^{-1}P = I$.
- D'autre part : $T^0 = I$.

D'où $\mathscr{P}(0)$.

▸ **Hérédité** : soit $n \in \mathbb{N}$.
Supposons $\mathscr{P}(n)$ et démontrons $\mathscr{P}(n+1)$ (*i.e.* $P^{-1}A^{n+1}P = T^{n+1}$).

$$\begin{aligned} T^{n+1} &= T \times T^n \\ &= P^{-1}AP \times P^{-1}A^nP && \text{(d'après la question précédente et par hypothèse de récurrence)} \\ &= P^{-1}A(PP^{-1})A^nP \\ &= P^{-1}AIA^nP = P^{-1}A^{n+1}P \end{aligned}$$

D'où $\mathscr{P}(n+1)$.

Ainsi, par principe de récurrence : $\forall n \in \mathbb{N}$, $P^{-1}A^nP = T^n$.

□

4. a) Exhiber une matrice $N \in \mathscr{M}_3(\mathbb{R})$ telle que T s'écrit $T = -2I + N$.

Démonstration.

D'après l'énoncé, $N = T + 2I = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}$.

□

b) Calculer N^2 et en déduire N^k pour tout $k \in \mathbb{N}$.

Démonstration.

- Tout d'abord : $N^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.
- On en déduit, par une récurrence immédiate, que pour tout $k \geqslant 2$, $N^k = 0_{\mathscr{M}_3(\mathbb{R})}$.

En conclusion : $N^0 = I$, $N^1 = N$ et pour tout $k \geqslant 2$, $N^k = 0_{\mathscr{M}_3(\mathbb{R})}$.

Commentaire

- Au lieu de procéder par récurrence, il est aussi possible d'écrire, pour tout $k \geqslant 2$:
$$N^k = N^{k-2} \times N^2 = N^{k-2} \times 0_{\mathscr{M}_3(\mathbb{R})} = 0_{\mathscr{M}_3(\mathbb{R})}$$
- Insistons sur le fait que cette démonstration n'est valable que si $k \geqslant 2$ (si ce n'est pas le cas, alors $k - 2 < 0$).

□

c) Soit $n \in \mathbb{N}$. Déterminer T^n à l'aide de la formule du binôme de Newton.
Le résultat devra faire apparaître T^n comme combinaison linéaire de I et de N.

Démonstration.

- Les matrices $(-2\,I)$ et N commutent car la matrice identité commute avec toutes les matrices carrées du même ordre. On peut donc appliquer la formule du binôme de Newton.
- Soit $n \geqslant 1$.

$$\begin{aligned}
T^n &= (-2\,I + N)^n \\
&= \sum_{k=0}^{n} \binom{n}{k} (-2\,I)^{n-k}\, N^k \\
&= \sum_{k=0}^{n} \binom{n}{k} (-2)^{n-k}\, I^{n-k}\, N^k \\
&= \sum_{k=0}^{n} \binom{n}{k} (-2)^{n-k}\, I\, N^k && \textit{(car : } \forall j \in \mathbb{N},\ I^j = I\textit{)} \\
&= \sum_{k=0}^{1} \binom{n}{k} (-2)^{n-k}\, N^k + \sum_{k=2}^{n} \binom{n}{k} (-2)^{n-k}\, N^k && \textit{(ce découpage est valable car } n \geqslant 1\textit{)} \\
&= \sum_{k=0}^{1} \binom{n}{k} (-2)^{n-k}\, N^k && \textit{(car on a montré : } \forall k \geqslant 2,\ N^k = 0_{\mathscr{M}_3(\mathbb{R})}\textit{)} \\
&= \binom{n}{0} (-2)^n\, N^0 + \binom{n}{1} (-2)^{n-1}\, N^1 \\
&= (-2)^n\, I + n\,(-2)^{n-1}\, N \\
&= (-2)^{n-1}\,(-2\,I + n\,N)
\end{aligned}$$

- Enfin : $(-2)^{0-1}\,(-2\,I + 0 \cdot N) = I$ et $T^0 = I$.
La formule précédente reste valable pour $n = 0$.

Ainsi, pour tout $n \in \mathbb{N}$, $T^n = (-2)^{n-1}\,(-2\,I + n\,N)$.

Commentaire

- La relation de Chasles stipule que pour tout $(m,p,n) \in \mathbb{N}^3$ tel que $m \leqslant p \leqslant n$:

$$\sum_{k=m}^{n} u_k \;=\; \sum_{k=m}^{p} u_k + \sum_{k=p+1}^{n} u_k$$

  (la seconde somme est nulle si $p = n$)
  où (u_n) est une suite quelconque de réels ou de matrices de même taille.
- Dans cette question, on est dans le cas où $m = 0$ et $p = 1$.
  L'argument $n \geqslant 1$ est donc nécessaire pour découper la somme.
  Le cas $n = 0$ doit alors être traité à part.
- Ici, la matrice N vérifie : $\forall k \geqslant 2,\ N^k = 0_{\mathscr{M}_3(\mathbb{R})}$. Elle est dite nilpotente d'indice 2 (ce terme n'est pas au programme et il est préférable de ne pas l'utiliser dans une copie). Si elle avait été nilpotente d'ordre 3, il aurait fallu traiter à part les cas $n = 0$ mais aussi le cas $n = 1$.
- Cette question sur le binôme de Newton matriciel est extrêmement classique aux concours et il faut donc savoir parfaitement la traiter.

□

d) Soit $n \in \mathbb{N}$. Exprimer enfin T^n comme combinaison linéaire de I et de T.

Démonstration.
Comme $N = T + 2\,I$, on obtient :

$$\begin{aligned}(-2)^{n-1}\,(-2\,I + n\,N) &= (-2)^{n-1}\,\big(-2\,I + n\,(T + 2\,I)\big)\\ &= (-2)^{n-1}\,\big((-2+2n)\,I + n\,T\big)\\ &= (-2)^{n-1}\,\big(2(n-1)\,I + n\,T\big)\end{aligned}$$

Pour tout $n \in \mathbb{N}$, $T^n = (-2)^{n-1}\,\big(2(n-1)\,I + n\,T\big)$.

□

5. a) Expliquer pourquoi l'on a : $\forall n \in \mathbb{N},\ A^n = (-2)^{n-1}\,\big(2\,(n-1)\,I + n\,A\big)$.

Démonstration.
Soit $n \in \mathbb{N}$. D'après la question précédente, $T^n = (-2)^{n-1}\,\big(2\,(n-1)\,I + n\,T\big)$.
Or : $A^n = P\,T^n\,P^{-1}$. En combinant ces deux informations, on obtient :

$$\begin{aligned}A^n &= P\,T^n\,P^{-1} \;=\; P\,\Big((-2)^{n-1}\,\big(2\,(n-1)\,I + n\,T\big)\Big)\,P^{-1}\\ &= (-2)^{n-1}\,\big(2\,(n-1)\,PP^{-1} + n\,PTP^{-1}\big)\end{aligned}$$

Ainsi, pour tout $n \in \mathbb{N}$, $A^n = (-2)^{n-1}\,\big(2\,(n-1)\,I + n\,A\big)$.

□

b) Vérifier que la formule trouvée à la question ***5.a)*** reste valable pour $n = -1$.

Démonstration.
Si $n = -1$, on obtient :

$$\begin{aligned}(-2)^{n-1}\,\big(2\,(n-1)\,I + n\,A\big) &= (-2)^{-1-1}\,\big(2\,(-1-1)\,I + (-1)\,A\big)\\ &= \frac{1}{4}\,(-4\,I - A) \;=\; -\frac{1}{4}\,A - I\end{aligned}$$

Ainsi, la formule trouvée à la question ***5.a)*** reste valable pour $n = -1$.

□

Exercice 3

On note I l'intervalle $[0,1]$. Soient f et g deux fonctions continues sur I, **à valeurs dans** I.
On supposera dans tout le problème que f et g commutent, c'est-à-dire :

$$\forall x \in I, \quad (f \circ g)(x) \ = \ (g \circ f)(x)$$

Le but de ce problème est de répondre à la question suivante :

$$\text{(Q) : « } f \text{ et } g \text{ possèdent-elles un point fixe en commun dans } I \text{ ? »}$$

Dans tout le problème, on notera $h : x \mapsto f(x) - x$.

Partie I - Ensemble des points fixes

1. Montrer que la fonction f possède au moins un point fixe dans I.

Démonstration.

- Tout d'abord, on remarque, pour tout $x \in I$:

$$\begin{aligned} x \text{ point fixe de } f \quad &\Leftrightarrow \quad f(x) = x \\ &\Leftrightarrow \quad f(x) - x = 0 \\ &\Leftrightarrow \quad h(x) = 0 \end{aligned}$$

  On cherche donc à démontrer que la fonction h s'annule (au moins) une fois sur I.

- On remarque :
  - × d'une part :
  $$h(0) \ = \ f(0) - 0 \ = \ f(0)$$
  Or, f est à valeurs dans $I = [0,1]$. Donc : $f(0) \in [0,1]$. En particulier : $f(0) \geqslant 0$. D'où :
  $$h(0) \ = \ f(0) \ \geqslant \ 0$$
  - × d'autre part :
  $$h(1) \ = \ f(1) - 1$$
  Or, f est à valeurs dans I. Donc : $f(1) \in [0,1]$. En particulier : $f(1) \leqslant 1$. D'où :
  $$h(1) \ = \ f(1) - 1 \ \leqslant \ 0$$

- Ainsi, la fonction f est :
  - × continue sur $I = [0,1]$ en tant que somme de fonctions continues sur I,
  - × telle que : $h(0) \geqslant 0$ et $h(1) \leqslant 0$.

  D'après le théorème des valeurs intermédiaires, on en déduit qu'il existe $x_0 \in I$ tel que : $h(x_0) = 0$.

La fonction f possède donc au moins un point fixe dans I.

□

Pour les mêmes raisons, la fonction g possède également au moins un point fixe dans I.
On note F (resp. G) l'ensemble des points fixes de f (resp. de g) dans I.

2. Montrer que G est stable par f, c'est-à-dire : $\forall x \in G$, alors $f(x) \in G$.
On montrerait de même, et on l'admettra ici, que F est stable par g.

Démonstration.
Soit $x \in G$.
Démontrons : $f(x) \in G$. Autrement dit, montrons que $y = f(x)$ est un point fixe de g.
Il s'agit donc de vérifier : $g(y) = y$.

$$\begin{aligned} g(y) &= g\big(f(x)\big) && \textit{(par définition de } y\textit{)} \\ &= (g \circ f)(x) \\ &= (f \circ g)(x) && \textit{(car } f \textit{ et } g \textit{ commutent)} \\ &= f\big(g(x)\big) \\ &= f(x) && \textit{(car } x \in G \textit{ donc : } g(x) = x\textit{)} \\ &= y \end{aligned}$$

On en déduit que G est stable par f. □

3. Montrer que F possède une borne inférieure m et une borne supérieure M.

Démonstration.
L'ensemble F est l'ensemble des points fixes de f. Autrement dit :

$$F = \{x \in I \mid f(x) = x\}$$

En particulier : $F \subset I = [0, 1]$.

- L'ensemble F est donc :
  - × non vide, d'après ***1.***,
  - × minoré par 0, car : $F \subset [0, 1]$.

  L'ensemble F admet donc une borne inférieure.
- L'ensemble F est de plus :
  - × non vide, d'après ***1.***,
  - × majoré par 1, car : $F \subset [0, 1]$.

  L'ensemble F admet donc une borne supérieure.

□

4. Rappeler la caractérisation de la borne inférieure :

$$m = \inf(F) \quad \Leftrightarrow \quad \begin{cases} \cdots \\ \cdots \end{cases}$$

Démonstration.

$$\boxed{m = \inf(F) \quad \Leftrightarrow \quad \begin{cases} \forall x \in F,\ m \leqslant x \\ \forall \varepsilon > 0,\ \exists x_0 \in F,\ x_0 < m + \varepsilon \end{cases}}$$

□

5. En déduire qu'il existe une suite $(\ell_n)_{n\in\mathbb{N}^*}$ d'éléments de F telle que : $\forall n \in \mathbb{N}^*,\ \ell_n - m \leqslant \dfrac{1}{n}$.

Démonstration.
Soit $n \in \mathbb{N}^*$.
On sait : $m = \inf(F)$. Ainsi, d'après la question précédente, on a en particulier :

$$\forall \varepsilon > 0,\ \exists x_0 \in F,\ x_0 < m + \varepsilon$$

En appliquant cette proposition à $\varepsilon = \dfrac{1}{n} > 0$, on obtient qu'il existe $\ell_n \in F$ tel que :

$$\ell_n < m + \frac{1}{n} \quad \text{d'où} \quad \ell_n - m < \frac{1}{n}$$

On en déduit : $\ell_n - m \leqslant \dfrac{1}{n}$.

Comme ceci est valable pour tout $n \in \mathbb{N}^*$, il existe une suite (ℓ_n) d'éléments de F telle que :

$$\forall n \in \mathbb{N}^*,\ \ell_n - m \leqslant \frac{1}{n}.$$

□

6. En déduire : $\ell_n \underset{n\to+\infty}{\longrightarrow} m$. Puis : $m \in F$.
On montrerait de même, et on l'admettra ici, que $M \in F$.

Démonstration.

- Soit $n \in \mathbb{N}^*$.
  - × D'une part, d'après la question précédente :
  $$\ell_n - m \ \leqslant\ \frac{1}{n}$$
  - × d'autre part, comme $\ell_n \in F$ et $m = \inf(F)$, alors :
  $$m \ \leqslant\ \ell_n \quad \text{donc} \quad 0 \ \leqslant\ \ell_n - m$$
- On en déduit, pour tout $n \in \mathbb{N}^*$:
  $$0 \ \leqslant\ \ell_n - m \ \leqslant\ \frac{1}{n}$$
  De plus :
  × d'une part : $\lim\limits_{n\to+\infty} 0 = 0$,
  × d'autre part : $\lim\limits_{n\to+\infty} \dfrac{1}{n} = 0$.
  Par théorème d'encadrement, on en déduit : $\lim\limits_{n\to+\infty} \ell_n - m = 0$.

  Ainsi : $\lim\limits_{n\to+\infty} \ell_n = m$.
- Remarquons : $\forall n \in \mathbb{N}^*,\ 0 \leqslant \ell_n \leqslant 1$ (car $F \subset [0,1]$). Par passage à la limite : $0 \leqslant m \leqslant 1$.
  Soit $n \in \mathbb{N}^*$. Comme $\ell_n \in F$, alors ℓ_n est un point fixe de f. Ainsi :

$$\begin{array}{ccc} f(\ell_n) & = & \ell_n \\ \overset{u}{\underset{+\infty}{\downarrow}} & & \overset{u}{\underset{+\infty}{\downarrow}} \\ f(m) & = & m \end{array} \qquad \begin{array}{l} \\ \\ \textit{(car } f \textit{ continue sur } [0,1] \\ \textit{et donc en } m \in [0,1]\textit{)} \end{array}$$

On en déduit que m est un point fixe de f. Autrement dit : $m \in F$.

□

Partie II - Une condition suffisante : la stricte décroissance de f sur I

On suppose, **uniquement dans cette partie**, que la fonction f, en plus d'être continue sur I, est strictement décroissante sur I.

7. Montrer qu'il existe un unique élément $\ell \in F$.

Démonstration.

- On remarque tout d'abord que la fonction h est également strictement décroissante sur I. Démontrons le.
  Soit $(x, y) \in I^2$. Supposons : $x < y$. On obtient :
  - × tout d'abord, par stricte décroissance de f : $f(x) > f(y)$.
  - × ensuite : $-x > -y$.

  On en déduit :
$$\begin{array}{ccc} f(x) - x & > & f(y) - y \\ \shortparallel & & \shortparallel \\ h(x) & > & h(y) \end{array}$$
- Ainsi, la fonction h est :
  - × continue sur I (démontré en question ***1.***),
  - × strictement décroissante sur I.

  Elle réalise donc une bijection de I sur $h(I)$ où :
$$h(I) \;=\; h\big([0,1]\big) \;=\; \big[h(1), h(0)\big]$$
  Or : $0 \in \big[h(1), h(0)\big]$. En effet, on a déjà démontré en question ***1.*** :
$$h(1) \leqslant 0 \quad \text{et} \quad h(0) \geqslant 0$$
  On en déduit que l'équation $h(x) = 0$ admet une unique solution sur $[0, 1]$. Autrement dit, la fonction f admet un unique point fixe sur I.

  On en déduit qu'il existe un unique élément $\ell \in F$.

Commentaire

On prendra garde à ne pas inventer d'hypothèses. Par exemple, dans cette question, la fonction f n'est pas supposée dérivable sur I. Il n'y a donc aucune raison de penser que la fonction h l'est.
Pour démontrer la stricte décroissance de cette dernière sur I, il est donc nécessaire d'utiliser la définition de stricte décroissance (et non le signe de sa dérivée).

□

8. Démontrer : $g(\ell) \in F$.

Démonstration.
D'après la question ***2.***, l'ensemble F est stable par g. Autrement dit :
$$\forall x \in F, g(x) \in F$$
Or, d'après la question précédente : $\ell \in F$.

Ainsi : $g(\ell) \in F$.

□

9. Déduire des deux questions précédentes : $\ell \in G$.

Démonstration.

- D'après la question ***8.*** : $g(\ell) \in F$.
- Or, d'après la question ***7.*** : $F = \{\ell\}$. On en déduit : $g(\ell) \in \{\ell\}$, c'est-à-dire :

$$g(\ell) = \ell$$

Le réel ℓ est donc un point fixe de g.

Ainsi : $\ell \in G$.

□

10. Conclure quant à la question (Q) dans ce cas.

Démonstration.

- D'après la question ***7.*** : $\ell \in F$. Le réel ℓ est donc un point fixe de f.
- D'après la question précédente : $\ell \in G$. Le réel ℓ est donc un point fixe de g.

Les fonctions f et g possèdent donc au moins un point fixe commun dans I.

□

Partie III - Une condition suffisante (bis) : la stricte croissance de f sur I

On suppose, **uniquement dans cette partie**, que la fonction f, en plus d'être continue sur I, est strictement croissante sur I. On définit une suite $(x_n)_{n\in\mathbb{N}}$ de la manière suivante :

$$\begin{cases} x_0 \in G \\ \forall n \in \mathbb{N},\ x_{n+1} = f(x_n) \end{cases}$$

11. Montrer que la suite $(x_n)_{n\in\mathbb{N}}$ est bien définie et : $\forall n \in \mathbb{N},\ x_n \in G$.

Démonstration.

Démontrons par récurrence : $\forall n \in \mathbb{N},\ \mathscr{P}(n)$ où $\mathscr{P}(n) : \begin{cases} x_n \text{ existe} \\ x_n \in G \end{cases}$

▸ **Initialisation** :

- Tout d'abord, x_0 existe car, d'après ***1.***, la fonction g admet au moins un point fixe dans G. Ainsi : $G \neq \varnothing$.
- Ensuite : $x_0 \in G$.

D'où $\mathscr{P}(0)$.

▸ **Hérédité** : soit $n \in \mathbb{N}$.

Supposons $\mathscr{P}(n)$ et démontrons $\mathscr{P}(n+1)$ (*i.e.* $\begin{cases} x_{n+1} \text{ bien défini} \\ x_{n+1} \in G \end{cases}$).

- Par hypothèse de récurrence, x_n existe et : $x_n \in G$. Or : $G \subset [0,1]$.
  De plus, la fonction f est définie sur $[0,1]$. Ainsi, $x_{n+1} = f(x_n)$ existe.
- On sait :
  × d'une part : $x_n \in G$ (par hypothèse de récurrence),
  × d'autre part : G est stable par f (d'après ***2.***).
  On en déduit : $f(x_n) \in G$. Donc : $x_{n+1} \in G$.

D'où $\mathscr{P}(n+1)$.

Par principe de récurrence, la suite (x_n) est bien définie et : $\forall n \in \mathbb{N},\ x_n \in G$.

□

12. On suppose : $x_1 \geqslant x_0$. Démontrer : $\forall n \in \mathbb{N},\ x_{n+1} \geqslant x_n$. Que se passe-t-il si $x_1 \leqslant x_0$?

Démonstration.
Démontrons par récurrence : $\forall n \in \mathbb{N},\ \mathscr{P}(n)$ où $\mathscr{P}(n) : x_{n+1} \geqslant x_n$.

- **Initialisation** :
  Par hypothèse dans cette question : $x_1 \geqslant x_0$.
  D'où $\mathscr{P}(0)$.
- **Hérédité** : soit $n \in \mathbb{N}$.
  Supposons $\mathscr{P}(n)$ et démontrons $\mathscr{P}(n+1)$ (*i.e.* $x_{n+2} \geqslant x_{n+1}$).

  Par hypothèse de récurrence :

$$\begin{array}{lccll} & x_{n+1} & \leqslant & x_n & \\ \text{donc} & f(x_{n+1}) & \leqslant & f(x_n) & \text{(par croissance de } f \text{ sur } I\text{)} \\ \text{d'où} & x_{n+2} & \leqslant & x_{n+1} & \end{array}$$

  D'om $\mathscr{P}(n+1)$.

Par principe de récurrence : $\forall n \in \mathbb{N},\ x_{n+1} \geqslant x_n$.

Si $x_1 \leqslant x_0$, on démontrerait de même par récurrence : $\forall n \in \mathbb{N},\ x_{n+1} \leqslant x_n$.

□

13. En déduire que la suite $(x_n)_{n\in\mathbb{N}}$ converge vers un réel $\hat{\ell}$ et : $\hat{\ell} \in F$.

Démonstration.

- D'après la question précédente :
  - × si $x_1 \geqslant x_0$, alors la suite (x_n) est croissante,
  - × si $x_1 \leqslant x_0$, alors la suite (x_n) est décroissante.

  Finalement, dans tous les cas, la suite (x_n) est monotone.
- La suite (x_n) est donc :
  - × monotone,
  - × minorée par 0 et majorée par 1. En effet, d'après la question ***11.*** : $\forall n \in \mathbb{N},\ x_n \in G$.
    Or : $G \subset [0,1]$. Ainsi : $\forall n \in \mathbb{N},\ x_n \in [0,1]$.

  On en déduit que la suite (x_n) converge vers un réel $\hat{\ell}$ vérifiant : $0 \leqslant \hat{\ell} \leqslant 1$.
- De plus, pour tout $n \in \mathbb{N}$:

$$\begin{array}{ccc} x_{n+1} & = & f(x_n) \\ \overset{n\to+\infty}{\downarrow}{\scriptstyle u} & & \overset{n\to+\infty}{\downarrow}{\scriptstyle u} \\ \hat{\ell} & = & f(\hat{\ell}) \end{array} \quad \begin{array}{l} \\ \\ \text{(par continuité de } f \text{ sur } [0,1] \\ \text{et donc en } \hat{\ell} \in [0,1]\text{)} \end{array}$$

  Ainsi, $\hat{\ell}$ est un point fixe de f.

On en conclut : $\hat{\ell} \in F$.

□

14. Démontrer : $\hat{\ell} \in G$.

Démonstration.
Soit $n \in \mathbb{N}$. D'après ***11.*** : $x_n \in G$. Autrement dit, x_n est un point fixe de g. Ainsi :

$$\begin{array}{ccc} g(x_n) & = & x_n \\ \overset{u}{\underset{+\infty}{\downarrow}} & & \overset{u}{\underset{+\infty}{\downarrow}} \\ g(\hat{\ell}) & = & \hat{\ell} \end{array} \qquad \begin{array}{l} \textit{(par continuité de } g \textit{ sur } [0,1] \\ \textit{et donc en } \hat{\ell} \in [0,1]\textit{)} \end{array}$$

Ainsi, $\hat{\ell}$ est un point fixe de g.

On en conclut : $\hat{\ell} \in G$.

□

15. Conclure quant à la question (Q) dans ce cas.

Démonstration.

- D'après la question ***13.*** : $\hat{\ell} \in F$. Le réel $\hat{\ell}$ est donc un point fixe de f.
- D'après la question précédente : $\hat{\ell} \in G$. Le réel $\hat{\ell}$ est donc un point fixe de g.

Les fonctions f et g possèdent donc au moins un point fixe commun dans I.

□

Exercice 4

Soit $n \in \mathbb{N}^*$.

- On note $\mathbb{U}_n = \left\{ \mathrm{e}^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!] \right\}$ l'ensemble des racines $n^{\text{ème}}$ de l'unité, c'est-à-dire l'ensemble des complexes ω vérifiant : $\omega^n = 1$.
- On dit qu'un complexe ω est une racine **primitive** $n^{\text{ème}}$ de l'unité si :

  1) $\omega^n = 1$,

  2) $\forall q \in [\![1, n-1]\!]$, $\omega^q \neq 1$.

  En d'autres termes, une racine primitive $n^{\text{ème}}$ de l'unité est une racine $n^{\text{ème}}$ de l'unité pour laquelle n est la plus petite puissance q (non nulle) telle que : $\omega^q = 1$.
- On note P_n l'ensemble des racines primitives $n^{\text{ème}}$ de l'unité.
- On admet enfin le résultat suivant.

$$\forall (a,b,c) \in \mathbb{Z}^3, \quad \left.\begin{array}{l} a \mid bc \\ a \wedge b = 1 \end{array}\right\} \Rightarrow (a \mid c)$$

Partie I - Caractérisation des racines primitives $n^{\text{ème}}$ de l'unité

Soit $n \in \mathbb{N}^*$.

1. Expliciter sans démonstration les ensembles P_1, P_2, P_3 et P_4.

Démonstration.

- Tout d'abord, l'ensemble des racines $1^{\text{ère}}$ de l'unité est :

$$\mathbb{U}_1 = \{1\}$$

De plus, 1 est une racine primitive $1^{\text{ère}}$ de l'unité. En effet :

× d'une part : $1^1 = 1$,

× d'autre part : $\forall q \in [\![1, 0]\!] = \varnothing$, $1^q \neq 1$.

$$\boxed{\text{Ainsi : } P_1 = \{1\}.}$$

- Ensuite, l'ensemble des racines $2^{\text{ème}}$ de l'unité est :

$$\mathbb{U}_2 = \{1, -1\}$$

De plus :

× le complexe 1 n'est pas une racine primitive $2^{\text{ème}}$ de l'unité.
En effet, en choisissant $q = 1 \in [\![1, 2-1]\!]$: $1^q = 1$.

× le complexe -1 est une racine primitive $2^{\text{ème}}$ de l'unité. En effet :

- d'une part : $(-1)^2 = 1$,
- d'autre part : $\forall q \in [\![1, 2-1]\!] = \{1\}$, $(-1)^q \neq 1$.

$$\boxed{\text{Ainsi : } P_2 = \{-1\}.}$$

- Ensuite, l'ensemble des racines $3^{\text{ème}}$ de l'unité est :

$$\mathbb{U}_3 \;=\; \{1, j, j^2\}$$

De plus :

× le complexe 1 n'est pas une racine primitive $3^{\text{ème}}$ de l'unité.
En effet, en choisissant $q = 1 \in [\![1, 3-1]\!]$: $1^q \;=\; 1$.

× le complexe j est une racine primitive $3^{\text{ème}}$ de l'unité. En effet :
- d'une part : $j^3 = \left(\mathrm{e}^{\frac{2i\pi}{3}}\right)^3 = \mathrm{e}^{3\,\frac{2i\pi}{3}} = \mathrm{e}^{2i\pi} = 1$,
- d'autre part : $j^1 = \mathrm{e}^{\frac{2i\pi}{3}} \neq 1$ et $j^2 = \mathrm{e}^{\frac{4i\pi}{3}} \neq 1$.

× le complexe j^2 est une racine primitive $3^{\text{ème}}$ de l'unité. En effet :
- d'une part : $(j^2)^3 = \left(\mathrm{e}^{\frac{4i\pi}{3}}\right)^3 = \mathrm{e}^{3\,\frac{4i\pi}{3}} = \mathrm{e}^{4i\pi} = 1$,
- d'autre part : $(j^2)^1 = \mathrm{e}^{\frac{4i\pi}{3}} \neq 1$ et $(j^2)^2 = \mathrm{e}^{\frac{8i\pi}{3}} \neq 1$.

Ainsi : $P_3 = \{j, j^2\}$.

- Enfin, l'ensemble des racines $4^{\text{ème}}$ de l'unité est :

$$\mathbb{U}_4 \;=\; \{1, i, -1, -i\}$$

De plus :

× le complexe 1 n'est pas une racine primitive $4^{\text{ème}}$ de l'unité.
En effet, en choisissant $q = 1 \in [\![1, 4-1]\!]$: $1^q \;=\; 1$.

× le complexe i est une racine primitive $4^{\text{ème}}$ de l'unité. En effet :
- d'une part : $i^4 = \left(\mathrm{e}^{i\,\frac{\pi}{2}}\right)^4 = \mathrm{e}^{4\,i\,\frac{\pi}{2}} = \mathrm{e}^{2i\pi} = 1$,
- d'autre part : $i^1 \neq 1$, $i^2 = -1 \neq 1$ et $i^3 = -i \neq 1$.

× le complexe -1 n'est pas une racine primitive $4^{\text{ème}}$ de l'unité.
En effet, en choisissant $q = 2 \in [\![1, 4-1]\!]$: $(-1)^q \;=\; 1$.

× le complexe $-i$ est une racine primitive $4^{\text{ème}}$ de l'unité. En effet :
- d'une part : $(-i)^4 = i^4 = 1$,
- d'autre part : $(-i)^1 \neq 1$, $(-i)^2 = -1 \neq 1$ et $(-i)^3 = i \neq 1$.

Ainsi : $P_4 = \{i, -i\}$.

Commentaire

On a ici détaillé la réponse à cette question pour aider le lecteur. Néanmoins, comme le précise l'énoncé, aucun détail de démonstration n'est attendu sur la copie.

□

2. a) Soit $k \in [\![0, n-1]\!]$ tel que : $k \wedge n \neq 1$. Démontrer : $\mathrm{e}^{\frac{2ik\pi}{n}} \notin P_n$.

Démonstration.

- On note $d = k \wedge n$. Comme $d \neq 1$ et $d \mid k$ (et $k \leqslant n-1$), alors :

$$2 \;\leqslant\; d \;\leqslant\; n-1$$

- Comme $d = k \wedge n$, alors :
  - × d'une part : $d \mid n$. Il existe donc $q \in [\![2, n-1]\!]$ tel que : $n = d\,q$.
    (notons que $q \neq 1$ sinon $d = n$, et $q \neq n$ sinon $d = 1$)
  - × d'autre part : $d \mid k$. Il existe donc $p \in [\![2, n-1]\!]$ tel que : $k = d\,p$.
    (notons que $p \neq 1$ sinon $d = k$, et $p \neq n$ car $p \leqslant k < n$)
- On obtient :
$$\left(\mathrm{e}^{\frac{2ik\pi}{n}}\right)^q = \left(\mathrm{e}^{\frac{2i\,(dp)\,\pi}{n}}\right)^q = \mathrm{e}^{\frac{2i\,(qd)\,p\pi}{n}} = \mathrm{e}^{\frac{2i\,\cancel{n}\,p\pi}{\cancel{n}}} = \mathrm{e}^{2ip\pi} = 1 \qquad (\textit{car } p \in \mathbb{Z})$$
On a ainsi trouvé $q \in [\![1, n-1]\!]$ tel que : $\left(\mathrm{e}^{\frac{2ik\pi}{n}}\right)^q = 1$. Le complexe $\mathrm{e}^{\frac{2ik\pi}{n}}$ n'est pas une racine primitive $n^{\text{ème}}$ de l'unité.

On en déduit : $\mathrm{e}^{\frac{2ik\pi}{n}} \notin P_n$.

□

b) Réciproquement, soit $k \in [\![0, n-1]\!]$ tel que : $k \wedge n = 1$. En raisonnant par l'absurde, justifier : $\mathrm{e}^{\frac{2ik\pi}{n}}$ est une racine primitive $n^{\text{ème}}$ de l'unité.

Démonstration.
On procède par l'absurde.
Supposons que $\mathrm{e}^{\frac{2ik\pi}{n}}$ n'est pas une racine primitive $n^{\text{ème}}$ de l'unité. Alors :
- soit : $\left(\mathrm{e}^{\frac{2ik\pi}{n}}\right)^n \neq 1$.
  Absurde ! (car : $\left(\mathrm{e}^{\frac{2ik\pi}{n}}\right)^n = \mathrm{e}^{\cancel{n}\,\frac{2ik\pi}{\cancel{n}}} = \mathrm{e}^{2ik\pi} = 1$)
- soit il existe $q \in [\![1, n-1]\!]$ tel que : $\left(\mathrm{e}^{\frac{2ik\pi}{n}}\right)^q = 1$. On obtient : $\mathrm{e}^{\frac{2ikq\pi}{n}} = \mathrm{e}^{i\,0}$.
  Or deux nombres complexes ont même argument modulo 2π. Ainsi : $\dfrac{2kq\pi}{n} \equiv 0\ [2\pi]$.
  Il existe donc $p \in \mathbb{Z}$ tel que :
$$\begin{array}{rrcl} & \dfrac{2kq\pi}{n} & = & 2p\pi \\ \text{donc} & \dfrac{kq}{n} & = & p \\ \text{d'où} & kq & = & np \end{array}$$
  Ainsi :
  × d'une part : $n \mid kq$,
  × d'autre part : $n \wedge k = 1$
  D'après le résultat admis dans l'énoncé : $n \mid q$.
  Absurde ! (car $q \leqslant n - 1 < n$)

Finalement, si $k \wedge n = 1$, alors $\mathrm{e}^{\frac{2ik\pi}{n}}$ est une racine primitive $n^{\text{ème}}$ de l'unité.

□

On a donc prouvé :
$$P_n = \left\{\mathrm{e}^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!],\ k \wedge n = 1\right\}$$
En particulier, $\mathrm{e}^{\frac{2i\pi}{n}}$ est une racine primitive $n^{\text{ème}}$ de l'unité.

Soient z_1 et z_2 deux racines primitives $n^{\text{ème}}$. On admet qu'il existe $u \in \mathbb{Z}$ tel que :
$$\begin{cases} u \wedge n = 1 \\ {z_1}^u = z_2 \end{cases}$$

Partie II - Définition et premières propriétés des polynômes cyclotomiques

Dans la suite de ce problème, pour tout $n \in \mathbb{N}^*$, on définit le $n^{\text{ème}}$ polynôme cyclotomique par :

$$\Phi_n \;=\; \prod_{\omega \in P_n} (X-\omega) \;=\; \prod_{\substack{k\,=\,0 \\ k \wedge n \,=\, 1}}^{n-1} (X - \mathrm{e}^{\frac{2ik\pi}{n}})$$

3. Soit $n \in \mathbb{N}^*$. Factoriser sur $\mathbb{C}$ le polynôme $X^n - 1$.

Démonstration.

$$\boxed{X^n - 1 = \prod_{k=0}^{n-1} (X - \mathrm{e}^{\frac{2ik\pi}{n}})}$$

□

4. Écrire sous forme développée Φ_2, Φ_3, Φ_4.
Vérifier en particulier que ces polynômes sont à coefficients entiers.

Démonstration.

- D'après ***1.*** : $P_2 = \{-1\}$.

$$\boxed{\text{On en déduit : } \Phi(X) = \prod_{\omega \in P_2} (X-\omega) = X+1 \text{ (qui est bien à coefficients entiers).}}$$

- D'après ***1.*** : $P_3 = \{j, j^2\}$. On en déduit :

$$\begin{aligned}
\Phi_3(X) &= \prod_{\omega \in P_3} (X-\omega) \\
&= (X-j)\,(X-j^2) \\
&= \left(X - \mathrm{e}^{\frac{2i\pi}{3}}\right)\left(X - \mathrm{e}^{-\frac{2i\pi}{3}}\right) \\
&= X^2 - \left(\mathrm{e}^{\frac{2i\pi}{3}} + \mathrm{e}^{-\frac{2i\pi}{3}}\right) X + 1 \\
&= X^2 - 2\cos\left(\frac{2\pi}{3}\right) X + 1 \\
&= X^2 - 2\left(-\frac{1}{2}\right) X + 1
\end{aligned}$$

$$\boxed{\Phi_3(X) = X^2 + X + 1 \text{ (qui est bien à coefficients entiers)}}$$

- D'après ***1.*** : $P_4 = \{i, -i\}$. On en déduit :

$$\begin{aligned}
\Phi_4(X) &= \prod_{\omega \in P_4} (X-\omega) \\
&= (X-i)\,(X+i) \\
&= X^2 + 1
\end{aligned}$$

$$\boxed{\Phi_4(X) = X^2 + 1 \text{ (qui est bien à coefficients entiers)}}$$

□

5. a) Justifier : $\Phi_5(X) = \dfrac{X^5-1}{X-1}$.

Démonstration.

- D'une part, d'après ***3.*** :

$$\frac{X^5-1}{X-1} = \frac{\prod_{k=0}^{4}(X-\mathrm{e}^{\frac{2ik\pi}{5}})}{X-1} = \frac{\cancel{(X-1)}\prod_{k=1}^{4}(X-\mathrm{e}^{\frac{2ik\pi}{5}})}{\cancel{X-1}} = \prod_{k=1}^{4}(X-\mathrm{e}^{\frac{2ik\pi}{5}})$$

- D'autre part, par définition de Φ_5 :

$$\Phi_5(X) = \prod_{\substack{k=0 \\ k\wedge 5=1}}^{4}(X-\mathrm{e}^{\frac{2ik\pi}{5}})$$

Or les entiers $k \in [\![0,4]\!]$ vérifiant $k \wedge 5 = 1$ sont : 1, 2, 3, 4. Ainsi :

$$\Phi_5(X) = \prod_{k=1}^{4}(X-\mathrm{e}^{\frac{2ik\pi}{5}})$$

$$\boxed{\text{Finalement : } \Phi_5(X) = \frac{X^5-1}{X-1}.}$$

□

b) En déduire une forme développée de Φ_5.

Démonstration.
D'après la question précédente :

$$\Phi_5(X) = \frac{X^5-1}{X-1} = \frac{\cancel{(X-1)}\sum_{k=0}^{4}X^k\,1^{4-k}}{\cancel{X-1}}$$

$$\boxed{\text{Finalement : } \Phi_5(X) = \sum_{k=0}^{4}X^k.}$$

□

c) Plus généralement, si $p \in [\![2,+\infty[\![$ est un nombre premier, calculer Φ_p (on exprimera Φ_p sous forme de somme).

Démonstration.
Soit $p \in [\![2,+\infty[\![$.

- Par définition de Φ_p :

$$\Phi_p(X) = \prod_{\substack{k=0 \\ k\wedge p=1}}^{p-1}(X-\mathrm{e}^{\frac{2ik\pi}{p}})$$

Or les entiers $k \in [\![0,p-1]\!]$ vérifiant $k \wedge p = 1$ sont : 1, 2, …, $p-1$ car p est premier. Ainsi :

$$\Phi_p(X) = \prod_{k=1}^{p-1}(X-\mathrm{e}^{\frac{2ik\pi}{p}})$$

- On en déduit :

$$\begin{aligned}\Phi_p(X) &= \prod_{k=1}^{p-1}(X - \mathrm{e}^{\frac{2ik\pi}{p}}) \\ &= \frac{\prod_{k=0}^{p-1}(X - \mathrm{e}^{\frac{2ik\pi}{p}})}{X - \mathrm{e}^{\frac{2i0\pi}{p}}} \\ &= \frac{X^p - 1}{X - 1} \qquad \textit{(d'après 3.)} \\ &= \frac{\cancel{(X-1)}\sum_{k=0}^{p-1} X^k\, 1^{p-1-k}}{\cancel{X-1}}\end{aligned}$$

Finalement, si p est premier : $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$. □

6. Soit $n \in \mathbb{N}^*$.

a) Si d est un diviseur (positif) de n, on note :

$$E_d = \{k \in [\![0, n-1]\!] \mid k \wedge n = d\}$$

Justifier : $[\![0, n-1]\!] = \bigcup_{\substack{d=1 \\ d \mid n}}^{n} E_d$.

Démonstration.
On procède par double inclusion.

(⊂) Soit $k \in [\![0, n-1]\!]$.
On note : $d_0 = k \wedge n$. Alors :
× d'une part : $k \in E_{d_0}$,
× d'autre part : $d_0 \mid n$ et $d_0 \in [\![1, n]\!]$.
Ainsi : $k \in \bigcup_{\substack{d=1 \\ d \mid n}}^{n} E_d$.

$$[\![0, n-1]\!] \subset \bigcup_{\substack{d=1 \\ d \mid n}}^{n} E_d$$

(⊃) Soit $k \in \bigcup_{\substack{d=1 \\ d \mid n}}^{n} E_d$.
Alors il existe $d_0 \in [\![1, n]\!]$ tel que : $d_0 \mid n$ et $k \in E_{d_0}$.
Or : $E_{d_0} \subset [\![0, n-1]\!]$. Donc : $k \in [\![0, n-1]\!]$.

$$\bigcup_{\substack{d=1 \\ d \mid n}}^{n} E_d \supset [\![0, n-1]\!]$$

Finalement : $[\![0, n-1]\!] = \bigcup_{\substack{d=1 \\ d \mid n}}^{n} E_d$. □

b) Soit d un diviseur de n. On note :

$$F_d \;=\; \left\{k \in [\![0, \tfrac{n}{d} - 1]\!] \mid k \wedge \tfrac{n}{d} = 1\right\}$$

Démontrer que E_d et F_d sont en bijection.

Démonstration.
On pose f la fonction définie par :

$$\begin{array}{rccc} f & : & E_d & \mapsto & F_d \\ & & k & \mapsto & \dfrac{k}{d} \end{array}$$

- Démontrons que f est bien définie, c'est-à-dire que f est bien à valeurs dans F_d .
  Soit $k \in E_d$. Alors : $k \in [\![0, n-1]\!]$ et $k \wedge n = d$.
  × Démontrons tout d'abord $f(k) \in [\![0, \frac{n}{d} - 1]\!]$, c'est-à-dire : $\frac{k}{d} \in [\![0, \frac{n}{d} - 1]\!]$.
  Comme $d \mid k$, alors : $\dfrac{k}{d} \in \mathbb{Z}$.
  De plus $d \geqslant 1$ et $k \in [\![0, n-1]\!]$. Donc : $\dfrac{k}{d} \in \left[0, \dfrac{n-1}{d}\right] \cap \mathbb{Z}$. Or :

$$\left[0, \frac{n-1}{d}\right] \cap \mathbb{Z} \;=\; \left[0, \frac{n}{d} - \frac{1}{d}\right] \cap \mathbb{Z} \;=\; \left[\!\left[0, \frac{n}{d} - 1\right]\!\right]$$

  En effet, comme $d \mid n$, alors $\dfrac{n}{d} \in \mathbb{Z}$ et de plus $\dfrac{1}{d} \in]0, 1]$. Finalement : $f(k) = \dfrac{k}{d} \in \left[\!\left[0, \dfrac{n}{d} - 1\right]\!\right]$.
  × Montrons maintenant : $f(k) \wedge \frac{n}{d} = 1$, c'est-à-dire $\frac{k}{d} \wedge \frac{n}{d} = 1$.
  Comme $k \in E_d$, alors : $k \wedge n = d$. D'où, par définition du PGCD : $\frac{k}{d} \wedge \frac{n}{d} = 1$.
  Finalement : $f(k) \in F_d$.

  Ainsi, la fonction f est bien définie.

- Démontrons maintenant que la fonction f est injective.
  Soit $(k_1, k_2) \in \left(E_d\right)^2$. Supposons : $f(k_1) = f(k_2)$. Alors :

$$\frac{k_1}{d} \;=\; \frac{k_2}{d} \qquad \text{donc} \qquad k_1 = k_2$$

  La fonction f est donc injective.

- Démontrons enfin que la fonction f est surjective.
  Soit $p \in F_d$. Démontrons qu'il existe $k \in E_d$ tel que : $p = f(k)$.
  On note $k = dp$. Alors :
  × d'une part : $f(k) = \dfrac{k}{d} = \dfrac{d\,p}{d} = p$.
  × d'autre part, démontrons : $k \in E_d$.
  - Tout d'abord, comme $p \in F_d$, alors : $p \in [\![0, \frac{n}{d} - 1]\!]$. On en déduit : $k = dp \in [\![0, n-d]\!]$.
    Or : $[\![0, n-d]\!] \subset [\![0, n-1]\!]$ (car $d \geqslant 1$). Ainsi : $k \in [\![0, n-1]\!]$.
  - Ensuite, toujours comme $p \in F_d$, alors : $p \wedge \frac{n}{d} = 1$. Ainsi :

$$k \wedge n \;=\; (dp) \wedge \left(d\,\frac{n}{d}\right) \;=\; |d| \left(p \wedge \frac{n}{d}\right) \;=\; d \qquad (\textit{car } d \geqslant 0)$$

  Il existe donc $k \in E_d$ tel que : $p = f(k)$.

  La fonction f est donc surjective.

On en déduit que f est bijective. Ainsi E_d et F_d sont en bijection.

□

c) Démontrer :

$$\prod_{k\in E_d}(X-\mathrm{e}^{\frac{2ik\pi}{n}}) \;=\; \Phi_{\frac{n}{d}}(X)$$

Démonstration.

- Comme la fonction f définie en question précédent réalise une bijection de E_d sur F_d, alors on peut effectuer le changement d'indice $\boxed{p=\dfrac{k}{d}}$:

$$\begin{aligned}
\prod_{k\in E_d}(X-\mathrm{e}^{\frac{2ik\pi}{n}}) &= \prod_{p\in F_d}(X-\mathrm{e}^{\frac{2i\,dp\,\pi}{n}}) \\
&= \prod_{\substack{p=0\\ p\wedge\frac{n}{d}=1}}^{\frac{n}{d}-1}(X-\mathrm{e}^{\frac{2i\,dp\,\pi}{n}}) && \textit{(par définition de } F_d\textit{)} \\
&= \prod_{\substack{p=0\\ p\wedge\frac{n}{d}=1}}^{\frac{n}{d}-1}(X-\mathrm{e}^{\frac{2i\,p\,\pi}{\frac{n}{d}}}) \\
&= \Phi_{\frac{n}{d}}(X) && \textit{(par définition de } \Phi_{\frac{n}{d}}\textit{)}
\end{aligned}$$

□

d) En déduire :

$$X^n-1 \;=\; \prod_{\substack{d=1\\ d\mid n}}^{n}\Phi_d(X)$$

Démonstration.

- D'après la question ***3.*** :

$$\begin{aligned}
X^n-1 &= \prod_{k=0}^{n-1}(X-\mathrm{e}^{\frac{2ik\pi}{n}}) \\
&= \prod_{k\in[\![0,n-1]\!]}(X-\mathrm{e}^{\frac{2ik\pi}{n}}) \\
&= \prod_{k\in A_n}(X-\mathrm{e}^{\frac{2ik\pi}{n}}) && \textit{(d'après } \textbf{6.a)}\textit{, en notant : } A_n=\bigcup_{\substack{d=1\\ d\mid n}}^{n}E_d\textit{)} \\
&= \prod_{\substack{d=1\\ d\mid n}}^{n}\Big(\prod_{k\in E_d}(X-\mathrm{e}^{\frac{2ik\pi}{n}})\Big) && \textit{(par produit par paquets)} \\
&= \prod_{\substack{d=1\\ d\mid n}}^{n}\Phi_{\frac{n}{d}}(X) && \textit{(d'après la question précédente)}
\end{aligned}$$

- Or, en notant $\mathcal{D}(n)$ l'ensemble des diviseurs de n, on remarque que la fonction g suivante est bijective :
$$\begin{array}{rccc} g & : & \mathcal{D}(n) & \to & \mathcal{D}(n) \\ & & d & \mapsto & \dfrac{n}{d} \end{array}$$
En effet :
  - × elle est bien définie. Démontrons le.
    Soit $d \in \mathcal{D}(n)$. Comme d est un diviseur de n, alors il existe $k \in \mathbb{N}$ tel que : $n = dk$.
    En particulier : $k \mid n$. Or : $k = \dfrac{n}{d}$. Ainsi, $g(d)$ est un diviseur de n. Autrement dit : $f(d) \in \mathcal{D}(n)$.
  - × elle est bijective car, pour tout $(d, p) \in \left(\mathcal{D}(n)\right)^2$:
$$g(d) = p \ \Leftrightarrow\ \frac{n}{d} = p \ \Leftrightarrow\ \frac{n}{p} = d$$
    L'équation $g(d) = p$ d'inconnue $d \in \mathcal{D}(n)$ admet donc une unique solution. Ceci implique que g est bijective (de bijection réciproque $p \mapsto \dfrac{n}{p}$).
- On peut donc effectuer le changement d'indice $\boxed{p = \dfrac{n}{d}}$. On obtient :
$$\begin{aligned} X^n - 1 &= \prod_{d \in \mathcal{D}(n)} \Phi_{\frac{n}{d}}(X) \\ &= \prod_{p \in \mathcal{D}(n)} \Phi_p(X) \qquad \textit{(avec le changement d'indice } \boxed{p = \frac{n}{d}}\textit{)} \end{aligned}$$
$$\boxed{\text{Finalement : } X^n - 1 = \prod_{d \in \mathcal{D}(n)} \Phi_d(X) = \prod_{\substack{d=1 \\ d \mid n}}^{n} \Phi_d(X).}$$
□

7. Le but de cette question est de montrer par récurrence, pour tout $n \in \mathbb{N}^*$, $\mathscr{P}(n)$ où $\mathscr{P}(n) : \Phi_n \in \mathbb{Z}[X]$.

a) Démontrer l'initialisation.

Démonstration.
Par définition de Φ_1 :
$$\Phi_1(X) = \prod_{\omega \in P_1} (X - \omega) = \prod_{\omega \in \{1\}} (X - \omega) \qquad \textit{(d'après 1.)}$$
$$\boxed{\text{Ainsi : } \Phi_1(X) = X - 1. \text{ On a bien : } \Phi_1 \in \mathbb{Z}[X].}$$
□

Soit $n \in [\![2, +\infty[\![$. Supposons : $\forall k \in [\![1, n-1]\!]$, $\mathscr{P}(k)$. On cherche à démontrer $\mathscr{P}(n)$.

b) Énoncer (sans démonstration) le théorème de division euclidienne sur $\mathbb{K}[X]$.

Démonstration.
$$\boxed{\begin{array}{c}\text{Pour tout } (A, B) \in \left(\mathbb{K}[X]\right)^2, \text{ il existe un unique couple } (Q, R) \in \left(\mathbb{K}[X]\right)^2 \text{ tel que :} \\ \begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}\end{array}}$$
□

c) On admet que le théorème de division euclidienne est encore valable sur $\mathbb{Z}[X]$ si le polynôme diviseur est unitaire. Comparer la division euclidienne de X^n-1 par :

$$B \;=\; \prod_{\substack{d=1\\ d\mid n}}^{n-1} \Phi_d$$

avec la question ***6.d)***, et conclure.
(On justifiera bien qu'on peut appliquer le théorème de division euclidienne dans $\mathbb{Z}[X]$, et on précisera bien où on utilise l'hypothèse de récurrence)

Démonstration.

- Justifions que l'on peut appliquer le théorème de division euclidienne de $\mathbb{Z}[X]$ à $A(X)=X^n-1$ et $B=\prod_{\substack{d=1\\ d\mid n}}^{n-1}\Phi_d$.
  - × Tout d'abord : $A\in\mathbb{Z}[X]$.
  - × Ensuite :
    - pour tout $d\in\mathbb{N}$, par définition de Φ_d :

      $$\Phi_d(X) \;=\; \prod_{\omega\in P_d}(X-\omega)$$

      Le polynôme Φ_d est donc un produit de polynômes unitaires. Il est donc lui-même unitaire.
      Le polynôme $B=\prod_{\substack{d=1\\ d\mid n}}^{n-1}\Phi_d$ est alors un produit de polynômes unitaires. Il est donc lui-même unitaire.
    - par hypothèse de récurrence (forte), pour tout $d\in[\![1,n-1]\!]$: $\Phi_d\in\mathbb{Z}[X]$.
      Le polynôme B est donc un produit de polynômes à coefficients entiers. Il est donc également à coefficients entiers, c'est-à-dire : $B\in\mathbb{Z}[X]$.

  On a démontré : $(A,B)\in\big(\mathbb{Z}[X]\big)^2$ et B unitaire.

- Ainsi, par théorème de division euclidienne dans $\mathbb{Z}[X]$, il existe un unique couple $(Q,R)\in\big(\mathbb{Z}[X]\big)^2$ tel que :

  $$\begin{cases} X^n-1=B(X)\,Q(X)+R(X)\\ \deg(R)<\deg(B)\end{cases}$$

- Or, d'après la question ***6.d)***

  $$X^n-1 \;=\; \prod_{\substack{d=1\\ d\mid n}}^{n}\Phi_d(X) \;=\; \Big(\prod_{\substack{d=1\\ d\mid n}}^{n-1}\Phi_d(X)\Big)\times\Phi_n(X) \;=\; B(X)\times\Phi_n(X)$$

- On sait ainsi que :
  - × le polynôme Φ_n est le quotient de la division euclidienne de A par B **dans** $\mathbb{C}[X]$,
  - × le polynôme Q est le quotient de la division euclidienne de A par B dans $\mathbb{Z}[X]$. C'est donc également le quotient de la division euclidienne de A par B dans $\mathbb{C}[X]$.

  Or le quotient de la division euclidienne dans $\mathbb{C}[X]$ est unique. Ainsi : $\Phi_n=Q$. Or : $Q\in\mathbb{Z}[X]$.

  Donc : $\Phi_n\in\mathbb{Z}[X]$. Ceci démontre $\mathscr{P}(n)$.

Par principe de récurrence : $\forall n\in\mathbb{N}^*,\ \Phi_n\in\mathbb{Z}[X]$.

□