DS6

Correction du devoir surveillé

Exercice 1 (Anneau des matrices circulantes)

Partie I. Étude du cas $n = 3$

1. Montrons que $\mathscr{C}$ est un sous-anneau commutatif de $\mathscr{M}_3(\mathbb{C})$:

   (i) $I_3 = C(1,0,0)$ est bien une matrice circulante.

   (ii) Soient $M, N \in \mathscr{C}$, qu'on note $M = C(x_0, x_1, x_2)$ et $N = C(y_0, y_1, y_2)$ avec $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{C}$. Calculons :
$$\begin{aligned} M - N &= \begin{pmatrix} x_0 & x_1 & x_2 \\ x_2 & x_0 & x_1 \\ x_1 & x_2 & x_0 \end{pmatrix} - \begin{pmatrix} y_0 & y_1 & y_2 \\ y_2 & y_0 & y_1 \\ y_1 & y_2 & y_0 \end{pmatrix} = \begin{pmatrix} x_0 - y_0 & x_1 - y_1 & x_2 - y_2 \\ x_2 - y_2 & x_0 - y_0 & x_1 - y_1 \\ x_1 - y_1 & x_2 - y_2 & x_0 - y_0 \end{pmatrix} \\ &= C(x_0 - y_0, x_1 - y_1, x_2 - y_2) \in \mathscr{C}. \end{aligned}$$

   (iii) Avec les notations introduites précédemment :
$$\begin{aligned} M \times N &= \begin{pmatrix} x_0y_0 + x_1y_2 + x_2y_1 & x_0y_1 + x_1y_0 + x_2y_2 & x_0y_2 + x_1y_1 + x_2y_0 \\ x_0y_2 + x_1y_1 + x_2y_0 & x_0y_0 + x_1y_2 + x_2y_1 & x_0y_1 + x_1y_0 + x_2y_2 \\ x_0y_1 + x_1y_0 + x_2y_2 & x_0y_2 + x_1y_1 + x_2y_0 & x_0y_0 + x_1y_2 + x_2y_1 \end{pmatrix} \\ &= C(x_0y_0 + x_1y_2 + x_2y_1, x_0y_1 + x_1y_0 + x_2y_2, x_0y_2 + x_1y_1 + x_2y_0) \in C. \end{aligned}$$

   Donc $\boxed{\mathscr{C} \text{ est un sous-anneau de } \mathscr{M}_3(\mathbb{C}).}$ Montrons qu'il est commutatif. En reprenant les notations et les calculs effectués plus haut :
$$\begin{aligned} M \times N &= C(x_0y_0 + x_1y_2 + x_2y_1, x_0y_1 + x_1y_0 + x_2y_2, x_0y_2 + x_1y_1 + x_2y_0) \\ &= C(y_0x_0 + y_1x_2 + y_2x_1, y_0x_1 + y_1x_0 + y_2x_2, y_0x_2 + y_1x_1 + y_2x_0) = N \times M. \end{aligned}$$

   Ainsi, $\boxed{\mathscr{C} \text{ est un anneau commutatif.}}$

2. Remarquons tout d'abord que $M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} = C(2,1,1)$ est bien une matrice circulante. Par l'algorithme du pivot de Gauss :
$$\left(\begin{array}{ccc|ccc} 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 1 & 1 & 2 & 0 & 0 & 1 \end{array}\right) \underset{L_3 \leftrightarrow L_1}{\overset{\mathscr{L}}{\sim}} \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 2 & 1 & 1 & 1 & 0 & 0 \end{array}\right) \underset{\substack{L_2 \leftarrow L_2 - L_1 \\ L_3 \leftarrow L_3 - 2L_1}}{\overset{\mathscr{L}}{\sim}} \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 & 1 & -1 \\ 0 & -1 & -3 & 1 & 0 & -2 \end{array}\right)$$
$$\underset{L_3 \leftarrow L_3 + L_2}{\overset{\mathscr{L}}{\sim}} \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 & 1 & -1 \\ 0 & 0 & -4 & 1 & 1 & -3 \end{array}\right)$$

   Puisque M est équivalente par lignes à $\begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & -4 \end{pmatrix}$ inversible car triangulaire supérieure sans 0 sur la diagonale, M est une matrice inversible. Effectuons la remontée pour obtenir M^{-1}.
$$\left(\begin{array}{ccc|ccc} 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 1 & 1 & 2 & 0 & 0 & 1 \end{array}\right) \underset{L_3 \leftarrow -\frac{1}{4}L_3}{\overset{\mathscr{L}}{\sim}} \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 & 1 & -1 \\ 0 & 0 & 1 & -\frac{1}{4} & -\frac{1}{4} & \frac{3}{4} \end{array}\right) \underset{\substack{L_2 \leftarrow L_2 + L_3 \\ L_1 \leftarrow L_1 - 2L_3}}{\overset{\mathscr{L}}{\sim}} \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 1 & 0 & -\frac{1}{4} & \frac{3}{4} & -\frac{1}{4} \\ 0 & 0 & 1 & -\frac{1}{4} & -\frac{1}{4} & \frac{3}{4} \end{array}\right)$$
$$\underset{L_1 \leftarrow L_1 - L_2}{\overset{\mathscr{L}}{\sim}} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{3}{4} & -\frac{1}{4} & -\frac{1}{4} \\ 0 & 1 & 0 & -\frac{1}{4} & \frac{3}{4} & -\frac{1}{4} \\ 0 & 0 & 1 & -\frac{1}{4} & -\frac{1}{4} & \frac{3}{4} \end{array}\right)$$

L'inverse de M est $M^{-1} = \begin{pmatrix} \frac{3}{4} & -\frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{3}{4} & -\frac{1}{4} \\ -\frac{1}{4} & -\frac{1}{4} & \frac{3}{4} \end{pmatrix} = C\left(\frac{3}{4}, -\frac{1}{4}, -\frac{1}{4}\right)$ et appartient bien à $\mathscr{C}$.

Ainsi, $\boxed{M \text{ est inversible dans l'anneau } \mathscr{C}.}$

Mise en garde.

Il faut ici se méfier un peu du vocabulaire et du sens du mot *inversible* :

- quand on dit généralement que la matrice M est inversible, on entend par là inversible dans l'anneau $\mathscr{M}_n(\mathbb{C})$, c'est-à-dire qu'il existe $N \in \mathscr{M}_n(\mathbb{C})$ tel que :

$$M \times N = N \times M = I_n.$$

- quand on dit que M est inversible dans l'anneau $\mathscr{C}$, cela signifie qu'il existe N **appartenant à** $\mathscr{C}$ tel que :

$$M \times N = N \times M = I_n.$$

En particulier, si M est inversible dans l'anneau $\mathscr{C}$, alors elle est inversible dans l'anneau $\mathscr{M}_n(\mathbb{C})$. La réciproque est fausse a priori : si M est une matrice circulante et inversible, rien ne dit que son inverse M^{-1} est encore une matrice circulante.

3. (a) Calculons les premières puissances de A :

$$A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad A^3 = I_3.$$

Dès lors, pour tout $p \in \mathbb{N}$:

$$A^{3p} = \left(A^3\right)^p = I_3^p = I_3, \quad A^{3p+1} = A^{3p} \times A = I_3 \times A = A, \quad A^{3p+2} = A^{3p} \times A^2 = I_3 \times A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Ainsi $\boxed{\text{pour tout } k \in \mathbb{N},\ A^k \text{ est égale à } I_3,\ A \text{ ou } A^2 \text{ selon que } k \text{ soit congru à } 0,\ 1 \text{ ou } 2 \text{ modulo } 3.}$

(b) Calculons :

$$P \times Q = \begin{pmatrix} 3 & 1 + j^2 + j & 1 + j + j^2 \\ 1 + j + j^2 & 3 & 1 + j + j^2 \\ 1 + j + j^2 & 1 + j + j^2 & 3 \end{pmatrix}.$$

Mais en se souvenant que $1 + j + j^2 = \sum_{\omega \in \mathbf{U}_3} \omega = 0$, on obtient $P \times Q = 3I_3$, et donc $\boxed{P \text{ est inversible, avec } P^{-1} = \frac{1}{3}Q.}$

(c) On calcule $P^{-1}A = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ j & 1 & j^2 \\ j^2 & 1 & j \end{pmatrix}$, puis $P^{-1}AP = \frac{1}{3}\begin{pmatrix} 3 & 0 & 0 \\ 0 & 3j & 0 \\ 0 & 0 & 3j^2 \end{pmatrix} \boxed{= \operatorname{diag}\left(1, j, j^2\right).}$

Partie II. L'anneau des matrices circulantes

4. Soient $\lambda, \mu \in \mathbb{C}$ et $M, N \in \mathscr{C}$, qu'on note $M = C(x_0, \ldots, x_{n-1})$ et $N = C(y_0, \ldots, y_{n-1})$ avec $x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1} \in \mathbb{C}$. Alors :

$$\lambda M + \mu N = \begin{pmatrix} \lambda x_0 + \mu y_0 & \lambda x_1 + \mu y_1 & \lambda x_2 + \mu y_2 & \cdots & \lambda x_{n-1} + \mu y_{n-1} \\ \lambda x_{n-1} + \mu y_{n-1} & \lambda x_0 + \mu y_0 & \lambda x_1 + \mu y_1 & \cdots & \lambda x_{n-2} + \mu y_{n-2} \\ \lambda x_{n-2} + \mu y_{n-2} & \lambda x_{n-1} + \mu y_{n-1} & \lambda x_0 + \mu y_0 & \cdots & \lambda x_{n-3} + \mu y_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda x_1 + \mu y_1 & \lambda x_2 + \mu y_2 & \lambda x_3 + \mu y_3 & \cdots & \lambda x_0 + \mu y_0 \end{pmatrix}.$$

Donc $\lambda M+\mu N = C(\lambda x_0+\mu y_0,\ldots,\lambda x_{n-1}+\mu y_{n-1}) \in \mathscr{C}$, et $\boxed{\mathscr{C} \text{ est stable par combinaison linéaire.}}$

5. Soient $x_0,\ldots,x_{n-1} \in \mathbb{C}$. Calculons :

$$\begin{aligned} C(x_0,\ldots,x_{n-1}) \times A &= \begin{pmatrix} x_0 & x_1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & x_1 & \cdots & x_{n-2} \\ x_{n-2} & x_{n-1} & x_0 & \cdots & x_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & x_3 & \cdots & x_0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix} \\ &= \begin{pmatrix} x_{n-1} & x_0 & x_1 & \cdots & x_{n-2} \\ x_{n-2} & x_{n-1} & x_0 & \cdots & x_{n-3} \\ x_{n-3} & x_{n-2} & x_{n-1} & \cdots & x_{n-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_0 & x_1 & x_2 & \cdots & x_{n-1} \end{pmatrix} \end{aligned}$$

Ainsi, $\boxed{C(x_0,\ldots,x_{n-1}) \times A \text{ est la matrice circulante } C(x_{n-1},x_0,x_1,\ldots,x_{n-2}).}$

6. Montrons par récurrence finie que pour tout $k \in [\![0,n-1]\!]$, $A^k = C(e_k)$.

I Puisque $C(e_0) = I_n = A^0$, la propriété est vraie au rang $k=0$.

H Soit $k \in [\![0,n-2]\!]$. Supposons que $A^k = C(e_k)$. À l'aide de l'identité obtenue à la question précédente :

$$A^{k+1} = A^k \times A = C(e_k) \times A = C(e_{k+1}).$$

D'où la propriété au rang $k+1$.

Par principe de récurrence, $\boxed{A^k = C(e_k) \text{ pour tout } k \in [\![0,n-1]\!].}$

En particulier, $A^{n-1} = C(e_{n-1})$ et toujours par l'identité obtenue à la question précédente :

$$A^n = A^{n-1} \times A = C(e_{n-1}) \times A = C(e_0) \boxed{= I_n.}$$

7. On procède par double inclusion.

$\subset$ Soit M une matrice circulante, qu'on écrit $M = C(x_0,\ldots,x_{n-1})$ avec $x_0,\ldots,x_{n-1} \in \mathbb{C}$. En utilisant l'identité observée à la question 4 :

$$\begin{aligned} M &= C(x_0e_0 + x_1e_1 + \ldots x_{n-1}e_{n-1}) = x_0C(e_0) + x_1C(e_1) + \cdots + x_{n-1}C(e_{n-1}) \\ &= x_0I_n + x_1A + \cdots + x_{n-1}A^{n-1} \end{aligned}$$

Donc M s'écrit comme un polynôme en A : elle appartient bien à $\mathbb{C}[A]$.

$\supset$ Par la question précédente, pour tout $k \in [\![0,n-1]\!]$, $A^k = C(e_k)$ appartient à $\mathscr{C}$.

Soit $k \in \mathbb{N}$. Notons q et r les quotient et reste de la division euclidienne de k par n :

$$k = nq = r \quad \text{avec} \quad r \in [\![0,n-1]\!].$$

Alors :

$$A^k = A^{nq+r} = (A^n)^q \times A^r = I_n^q \times A^r = C(e_r) \in \mathscr{C}.$$

Ainsi, toutes les puissances de A appartiennent à $\mathscr{C}$, et leur combinaison linéaires aussi par la question 4. Puisqu'un polynôme en A n'est autre qu'une combinaison linéaire de puissances de A, $\mathbb{C}[A]$ est bien inclus dans $\mathscr{C}$.

D'où l'égalité ensembliste $\boxed{\mathscr{C} = \mathbb{C}[A].}$

8. Montrons que $\mathscr{C} = \mathbb{C}[A]$ est un sous-anneau commutatif de $\mathscr{M}_n(\mathbb{C})$.

(i) $I_n = A^0$ appartient bien à $\mathbb{C}[A]$.

(ii) Soient M, N dans $\mathbb{C}[A]$: il existe $P, Q \in \mathbb{C}[X]$ des polynômes tels que $M = P(A)$ et $N = Q(A)$. Alors :

$$M - N = P(A) - Q(A) = (P - Q)(A)$$

est encore un polynôme en A.

(iii) Avec les mêmes notations :

$$M \times N = P(A) \times Q(A) = (P \times Q)(A)$$

est un polynôme en A.

Donc $\boxed{\mathscr{C} = \mathbb{C}[A] \text{ est un sous-anneau de } \mathscr{M}_n(\mathbb{C})}$, commutatif car deux polynômes en A commutent (c'est une propriété vue en cours).

La matrice $J = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix} = C(1, 1, \dots, 1)$ est non nulle et appartient à $\mathscr{C}$. En effectuant les opérations $L_i \leftarrow L_i - L_1$ pour tout $i \in [\![2, n]\!]$:

$$J \overset{\mathscr{L}}{\sim} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

qui n'est pas inversible (triangulaire supérieure avec des 0 sur la diagonale). Donc J n'est pas une matrice inversible, et a fortiori n'a pas d'inverse dans $\mathscr{C}$. Ainsi, $\boxed{\mathscr{C} \text{ n'est pas un corps.}}$

Partie III. Diagonalisation de la matrice A

9. Soit $\omega \in \mathbb{U}_n$. Calculons :

$$AX_\omega = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{n-1} \end{pmatrix} = \begin{pmatrix} \omega \\ \omega^2 \\ \omega^3 \\ \vdots \\ 1 \end{pmatrix} = \omega \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{n-1} \end{pmatrix} \boxed{= \omega X_\omega.}$$

10. (a) Soit $(k, \ell) \in [\![1, n]\!]^2$. Calculons :

$$\begin{aligned} [P\overline{P}]_{k,\ell} &= \sum_{p=1}^{n} [P]_{k,p} \left[\overline{P}\right]_{p,\ell} = \sum_{p=1}^{n} \zeta^{(p-1)(k-1)} \zeta^{-(p-1)(\ell-1)} \\ &= \sum_{p=1}^{n} \zeta^{(p-1)(k-\ell)} = \sum_{p=1}^{n} \left(\zeta^{(k-\ell)}\right)^{p-1} = \sum_{p=0}^{n-1} \left(\zeta^{(k-\ell)}\right)^{p}. \end{aligned}$$

Il s'agit de la somme des termes d'une suite géométrique de raison $\zeta^{k-\ell} \in \mathbb{U}_n$. Distinguons deux cas :

- si $\zeta^{k-\ell} = 1$, alors $[P\overline{P}]_{k,\ell} = \displaystyle\sum_{p=0}^{n-1} 1 = n$.
- si $\zeta^{k-\ell} \neq 1$, alors $[P\overline{P}]_{k,\ell} = \dfrac{1 - \left(\zeta^{(k-\ell)}\right)^n}{1 - \zeta^{k-\ell}} = \dfrac{1 - 1}{1 - \zeta^{k-\ell}} = 0$.

Reste à noter que $\zeta^{k-\ell}=1$ si, et seulement si, n divise $k-\ell$. Et puisque k et ℓ sont tous deux dans $[\![1,n]\!]$, $k-\ell$ est divisible par n si, et seulement si, $k=\ell$. Ainsi :

$$[P\overline{P}]_{k,\ell}=\begin{cases}0 & \text{si } k\neq\ell\\ n & \text{si } k=\ell\end{cases}\ ,\qquad \text{si bien que}\qquad \boxed{P\overline{P}=nI_n}.$$

Ainsi, $\boxed{P \text{ est inversible d'inverse } \dfrac{1}{n}\overline{P}.}$

(b) Pour faciliter le calcul demandé, souvenons nous que la $k^{\text{ème}}$ colonne de AP est égale au produit de A par la $k^{\text{ème}}$ colonne de P, qui ici est $X_{\zeta^{k-1}}$. Or, nous avons prouvé à la question 9 que $AX_{\zeta^{k-1}}=\zeta^{k-1}X_{\zeta^{k-1}}$.

Par le même argument, la $k^{\text{ème}}$ colonne de D étant égale à $\zeta^{k-1}E_k$, la $k^{\text{ème}}$ colonne de PD est $\zeta^{k-1}PE_k$. Et PE_k est la $k^{\text{ème}}$ colonne de P, c'est-à-dire $X_{\zeta^{k-1}}$. Et donc la $k^{\text{ème}}$ colonne de PD est $\zeta^{k-1}X_{\zeta^{k-1}}$.

Ainsi, toutes les colonnes de AP et de PD sont égales, si bien que $\boxed{AP=PD.}$

Partie IV. Étude des inversibles de $\mathscr{C}$

11. (a) En reprenant des calculs effectués à la question 7 :

$$\begin{aligned}C(x_0,x_1,\dots,x_{n-1})&=C(x_0e_0+x_1e_1+\dots x_{n-1}e_{n-1})=x_0C(e_0)+x_1C(e_1)+\cdots+x_{n-1}C(e_{n-1})\\&=x_0I_n+x_1A+\cdots+x_{n-1}A^{n-1}\boxed{=Q(A).}\end{aligned}$$

Par la question 10, $AP=PD$ et P est inversible, d'où $P^{-1}AP=D$. Et on montre par récurrence immédiate que $P^{-1}A^kP=(P^{-1}AP)^k=D^k=\operatorname{diag}(1,\zeta^k,(\zeta^2)^k,\dots,(\zeta^{n-1})^k)$ pour tout $k\in\mathbb{N}$.

Calculons alors :

$$\begin{aligned}P^{-1}C(x_0,\dots,x_{n-1})P&=P^{-1}(x_0I_n+x_1A+\cdots+x_{n-1}A^{n-1})P\\&=x_0I_n+x_1P^{-1}AP+\cdots+x_{n-1}P^{-1}A^{n-1}P\\&=x_0I_n+x_1P^{-1}AP+\cdots+x_{n-1}(P^{-1}AP)^{n-1}\\&=x_0I_n+x_1D+\cdots+x_{n-1}D^{n-1}\\&=\operatorname{diag}(x_0+x_1+\cdots+x_{n-1},\dots,x_0+x_1\zeta^{n-1}+\cdots+x_{n-1}(\zeta^{n-1})^{n-1})\\&\boxed{=\operatorname{diag}(Q(1),Q(\zeta),\dots,Q(\zeta^{n-1})).}\end{aligned}$$

(b) Par hypothèse, $C(x_0,\dots,x_{n-1})$ appartient à $\mathscr{U}(\mathscr{C})$. Cette matrice est donc en particulier inversible. Par produit de matrices inversibles :

$$\operatorname{diag}(Q(1),Q(\zeta),\dots,Q(\zeta^{n-1}))=P^{-1}C(x_0,\dots,x_{n-1})P$$

est également inversible. Or, une matrice diagonale est inversible si, et seulement si, tous ses coefficients diagonaux sont non nuls. Ainsi, $\boxed{Q(\zeta^k)\neq 0 \text{ pour tout } k\in[\![0,n-1]\!].}$

Notons D le PGCD des polynômes Q et X^n-1. Si $\deg(D)\geq 1$, D admettrait au moins une racine complexe α (c'est le théorème de d'Alembert-Gauss), qui serait donc racine commune de Q et X^n-1. Par conséquent, α serait une racine n-ème de l'unité et annulerait le polynôme Q, ce qui est faux d'après ce qu'on vient de montrer. Donc $\deg(D)=0$, et $\boxed{\text{les polynômes } Q \text{ et } X^n-1 \text{ sont bien premiers entre eux dans } \mathbb{C}[X].}$

12. Supposons Q et X^n-1 premiers entre eux dans $\mathbb{C}[X]$. Par le théorème de Bezout, il existe des polynômes $V,W\in\mathbb{C}[X]$ tels que :

$$1=QV+(X^n-1)W.$$

En évaluant cette égalité en la matrice A, on obtient :

$$I_n = Q(A)V(A) + \underbrace{(A^n - I_n)}_{=0_n} W(A) = C(x_0, \dots, x_{n-1})V(A).$$

Ainsi, $C(x_0, \dots, x_{n-1})$ est une matrice inversible d'inverse $V(A) \in \mathbb{C}[A] \overset{\text{quest. 7}}{=} \mathscr{C}$. Donc $\boxed{C(x_0, \dots, x_{n-1}) \text{ appartient bien à } \mathscr{U}(\mathscr{C}).}$

13. On déduit des résultats obtenus dans les questions 11 et 12 la description suivante des inversibles de $\mathscr{C}$:

$$\boxed{\mathscr{U}(\mathscr{C}) = \left\{ C(x_0, \dots, x_{n-1}) \mid (x_0 + x_1 X + \cdots + x_{n-1}X^{n-1}) \wedge (X^n - 1) = 1 \right\}.}$$

14. Considérons $M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} = C(2,1,1)$. On associe à M le polynôme $Q = 2 + X + X^2$. Pour établir que M appartient à $\mathscr{U}(\mathscr{C})$, montrons que Q est premier avec $X^3 - 1$. On utilise pour cela l'algorithme d'Euclide en effectuant les divisions successives :

$$X^3 - 1 = (X^2 + X + 2)(X - 1) + (-X + 1), \qquad \text{puis} \qquad X^2 + X + 2 = (-X + 1)(-X - 2) + 4.$$

Ainsi, $X^3 - 1 \wedge (X^2 + X + 2) = 1$ et M appartient bien à $\mathscr{U}(\mathscr{C})$.

Remarque. On aurait pu aussi remarquer que $Q(1)$, $Q(j)$ et $Q(j^2)$ sont tous non nuls, ce qui permettait aussi bien de conclure que $M \in \mathscr{U}(\mathscr{C})$. Mais on n'aurait alors pas été en mesure de calculer M^{-1}. On peut avec avec la méthode proposée remonter les calculs pour obtenir une identité de Bezout (c'est algorithme d'Euclide étendu).

En reprenant les calculs précédents :

$$\begin{aligned}
4 &= (X^2 + X + 2) - (-X + 1)(-X - 2) = (X^2 + X + 2) + (-X + 1)(X + 2) \\
&= (X^2 + X + 2) + \left[(X^3 - 1) - (X^2 + X + 2)(X - 1) \right] (X + 2) \\
&= (X^2 + X + 2)(1 - (X - 1)(X + 2)) + (X + 2)(X^3 - 1) \\
&= (X^2 + X + 2)(3 - X - X^2) + (X + 2)(X^3 - 1)
\end{aligned}$$

D'où en évaluant cette identité en la matrice A :

$$4I_3 = \underbrace{(A^2 + A + 2I_2)}_{=M}(3I_3 - A - A^2) + (A + 2I_3)\underbrace{(A^3 - I_3)}_{=0_3} = M\left(3I_3 - A - A^2\right).$$

On retrouve que M est inversible, et $\boxed{M^{-1} = \frac{3}{4}I_3 - \frac{1}{4}A - \frac{1}{4}A^2 = C\left(\frac{3}{4}, -\frac{1}{4}, -\frac{1}{4}\right).}$

Exercice 2 (Approximation d'une fonction $\mathscr{C}^n$ sur un segment par des polynômes)

Partie I. Résultats préliminaires

1. Considérons le polynôme $R = P - Q$. Il admet une infinité de racines puisque pour tout $t \in [-1,1]$, $R(t) = P(t) - Q(t) = 0$. Ainsi, $R = 0_{\mathbb{R}[X]}$, de sorte que $\boxed{P = Q.}$

2. La fonction $g = |f|$ est continue sur le segment $[-1,1]$ en tant que composée de fonctions qui le sont. Par le théorème des bornes atteintes, elle est bornée et atteint ses bornes. En particulier, elle admet un maximum sur $[-1,1]$, ce qui justifie $\boxed{\text{l'existence de } \max_{t \in [-1,1]} |f(t)|.}$

Partie II. Polynômes de Tchebychev

3. Pour tout $x \in [-1,1]$:

$$\boxed{T_0(x) = \cos(0) = 1 \quad \text{et} \quad T_1(x) = \cos(\arccos(x)) = x.}$$

4. Commençons par un rappel.

> **Rappel. Une formule de trigonométrie.**
> Pour tous $a, b \in \mathbb{R}$:
>
> $$\cos(a) + \cos(b) = 2\cos\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right).$$
>
> Cette formule peut par exemple se retrouver en passant par les complexes comme suit :
>
> $$\begin{aligned}\cos(a) + \cos(b) &= \mathrm{Re}\left(e^{ia} + e^{ib}\right) = \mathrm{Re}\left(e^{i\frac{a+b}{2}}\left(e^{i\frac{a-b}{2}} + e^{-i\frac{a-b}{2}}\right)\right)\\ &= \mathrm{Re}\left(e^{i\frac{a+b}{2}} 2\cos\left(\frac{a-b}{2}\right)\right) = 2\cos\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right).\end{aligned}$$

Soient $n \in \mathbb{N}$ et $x \in [-1,1]$. Calculons, à l'aide de la formule de trigonométrie ci-dessus :

$$\begin{aligned}T_{n+2}(x) + T_n(x) &= \cos((n+2)\arccos(x)) + \cos(\arccos(x))\\ &= 2\cos\left(\frac{(n+2)\arccos(x) + n\arccos(x)}{2}\right)\cos\left(\frac{(n+2)\arccos(x) - n\arccos(x)}{2}\right)\\ &= 2\cos((n+1)\arccos(x))\cos(\arccos(x)) \boxed{= 2xT_{n+1}(x).}\end{aligned}$$

5. Soit $x \in [-1,1]$. D'après la formule de récurrence précédente :

$$T_2(x) = 2xT_1(x) - T_0(x) \boxed{= 2x^2 - 1}$$

et

$$T_3(x) = 2xT_2(x) - T_1(x) = 2(2x^3 - x) - x \boxed{= 4x^3 - 3x.}$$

6. Montrons par récurrence (double) sur $n \in \mathbb{N}$ la propriété $\mathscr{P}(n)$: « T_n est une fonction polynomiale ».

I Puisque $T_0 : x \mapsto 1$ et $T_1 : x \mapsto x$ sont polynomiales, les propriétés $\mathscr{P}(0)$ et $\mathscr{P}(1)$ sont vraies.

H Soit $n \in \mathbb{N}$. Supposons $\mathscr{P}(n)$ et $\mathscr{P}(n+1)$ sont vraies.

Pour tout $x \in [-1,1]$:

$$T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x).$$

Donc T_{n+2} est bien une fonction polynomiale en tant que somme et produit de fonctions polynomiales. D'où la propriété $\mathscr{P}(n+2)$.

Par le principe de récurrence, $\boxed{T_n \text{ est une fonction polynomiale pour tout } n \in \mathbb{N}.}$

7. Montrons par récurrence (double encore) sur $n \in \mathbb{N}^*$ la propriété $\mathscr{Q}(n)$: « $\deg(T_n) = n$ et $\mathrm{CD}(T_n) = 2^{n-1}$ », où $\mathrm{CD}(P)$ désigne le coefficient dominant du polynôme non nul P.

I Puisque $T_1 = X$ et $T_2 = 2X^2 - 1$, on obtient $\deg(T_1) = 1$ et $\mathrm{CD}(T_1) = 1 = 2^0$, et $\deg(T_2) = 2$ et $\mathrm{CD}(T_2) = 2 = 2^{2-1}$. Ainsi les propriétés $\mathscr{Q}(1)$ et $\mathscr{Q}(2)$ sont vraies.

$\boxed{\mathbf{H}}$ Soit $n \in \mathbb{N}^*$. Supposons les propriétés $\mathscr{Q}(n)$ et $\mathscr{Q}(n+1)$ vraies.

Tout d'abord $\deg(T_{n+2}) = \deg(2XT_{n+1} - T_n)$ par la question 4. Or, $\deg(2XT_n) = \deg(X) + \deg(T_{n+1}) = n+2$ qui est strictement supérieur à $n = \deg(T_n)$. Ainsi :

$$\deg(T_{n+2}) = \deg(2XT_n) = n+2.$$

De plus, comme $\deg(T_n) < \deg(2XT_{n+1}))$:

$$\mathrm{CD}(T_{n+2}) = \mathrm{CD}(2XT_{n+1}) = 2\mathrm{CD}(XT_{n+1}) = 2CD(T_{n+1}) \overset{\mathrm{HR}}{=} 2 \times 2^n = 2^{n+1}.$$

D'où la propriété au rang $n+2$.

Par principe de récurrence, $\boxed{\deg(T_n) = n \text{ et } \mathrm{CD}(T_n) = 2^{n-1} \text{ pour tout } n \in \mathbb{N}^*.}$ Par ailleurs, on notera que $\deg(T_0) = 0$ et $\mathrm{CD}(T_0) = 1$.

8. Montrons par récurrence (double) sur $n \in \mathbb{N}$ la propriété $\mathscr{R}(n)$: « T_n est de même parité que n ».

$\boxed{\mathbf{I}}$ Comme $T_0 = 1$ et $T_1 = X$, $\mathscr{R}(0)$ et $\mathscr{R}(1)$ sont vraies.

$\boxed{\mathbf{H}}$ Soit $n \in \mathbb{N}$. Supposons $\mathscr{R}(n)$ et $\mathscr{R}(n+1)$ vraies.
Par hypothèse de récurrence, $T_{n+1}(-X) = (-1)^{n+1}T_{n+1}(X)$ et $T_n(X) = (-1)^n T_n(X)$, D'où :

$$T_{n+2}(-X) = 2(-X)(-1)^{n+1}T_{n+1}(X) - (-1)^n T_n(X) = (-1)^{n+2}(2XT_{n+1} - T_n) = (-1)^{n+2}T_{n+2}.$$

Donc T_{n+2} est de même parité que $n+2$, ce qui prouve $\mathscr{R}(n+2)$.

Par le principe de récurrence, $\boxed{T_n \text{ est de la parité de } n \text{ pour tout } n \in \mathbb{N}.}$

9. (a) Pour tout $\theta \in [0, \pi]$:

$$T_n(\cos(\theta)) = \cos(n \arccos(\cos(\theta))) \boxed{= \cos(n\theta).}$$

(b) Soit $\theta \in [0, \pi]$. Alors :

$$\begin{aligned} \cos(n\theta) = 0 \quad &\Leftrightarrow n\theta \equiv \frac{\pi}{2}[\pi] \Leftrightarrow \exists k \in \mathbb{Z},\ \theta = \frac{\frac{\pi}{2} + k\pi}{n} \Leftrightarrow \exists k \in \mathbb{Z},\ \theta = \frac{(2k+1)\pi}{2n} \\ &\underbrace{\Leftrightarrow}_{\theta \in [0,\pi]} \exists k \in [\![0, n-1]\!],\ \theta = \frac{(2k+1)\pi}{2n} \end{aligned}$$

L'ensemble des solutions de l'équation proposée est donc $\boxed{\left\{ \frac{(2k+1)\pi}{2n},\ k \in [\![0, n-1]\!] \right\}.}$

(c) Soit $n \in \mathbb{N}^*$. À l'aide des questions 9.(a) et 9.(b), pour tout $k \in [\![0, n-1]\!]$:

$$T_n\left(\cos\left(\frac{(2k+1)\pi}{2n}\right)\right) = \cos\left(n\frac{(2k+1)\pi}{2n}\right) = 0.$$

Les réels $\cos\left(\frac{(2k+1)\pi}{2n}\right)$ sont donc racines de T_n pour tout $k \in [\![0, n-1]\!]$. Ils sont de plus deux à deux distincts car $0 \le \frac{\pi}{2n} < \frac{3\pi}{2n} < \cdots < \frac{(2n-1)\pi}{2n} \le \pi$ et cos est injective sur $[0, \pi]$ (car strictement décroissante).

On vient ici d'expliciter $n = \deg(T_n)$ racines distinctes de T_n. Le polynôme T_n n'a donc pas d'autres racines, et ses racines sont exactement les $\boxed{\cos\left(\frac{(2k+1)\pi}{2n}\right) \text{ pour } k \in [\![0, n-1]\!]}$.

Comme elles sont toutes réelles, $\boxed{T_n \text{ est scindé sur } \mathbb{R}.}$

(d) Puisque T_n admet n racines réelles distinctes et est de degré n, toutes ses racines sont simples (de multiplicité égale à 1). Comme le coefficient dominant de T_n est 2^{n-1}, T_n se factorise en produits d'irréductibles dans $\mathbb{R}[X]$ sous la forme :

$$\boxed{T_n = 2^{n-1}\prod_{k=0}^{n-1}\left(X - \cos\left(\frac{(2k+1)\pi}{2n}\right)\right).}$$

(e) Par les relations coefficients-racines, en notant $p_0 = T_n(0)$ et $p_n = \mathrm{CD}(T_n)$:

$$\prod_{k=0}^{n-1}\cos\left(\frac{(2k+1)\pi}{2n}\right) = (-1)^n\frac{p_0}{p_n}.$$

On connait $p_n = 2^{n-1}$. Reste à calculer p_0 :

$$p_0 = T_n\left(\cos\left(\frac{\pi}{2}\right)\right) = \cos\left(\frac{n\pi}{2}\right) = \begin{cases}(-1)^{\frac{n}{2}} & \text{si } n \text{ est pair}\\ 0 & \text{sinon}\end{cases}.$$

Ainsi :

$$\boxed{\prod_{k=0}^{n-1}\cos\left(\frac{(2k+1)\pi}{2n}\right) = \begin{cases}\dfrac{(-1)^{\frac{n}{2}}}{2^{n-1}} & \text{si } n \text{ est pair}\\ 0 & \text{sinon}\end{cases}.}$$

Partie III. Minoration de la norme infinie sur $\mathbb{R}_n[X]$

10. Soit $n \in \mathbb{N}$. Pour tout $x \in [-1, 1]$:

$$|T_n(x)| = |\cos(n\arccos(x))| \leq 1, \qquad \text{et donc} \qquad \|T_n\|_\infty \leq 1.$$

D'autre part, $|T_n(1)| = |T_n(\cos(0))| = |\cos(n \times 0)| = 1$ et donc $\|T_n\|_\infty \geq 1$. Ainsi, $\boxed{\|T_n\|_\infty = 1.}$

11. Soit $n \in \mathbb{N}^*$. $\boxed{V_n = 2^{1-n}T_n \text{ est un polynôme unitaire de degré } n \text{ et à coefficients réels}}$ car T_n est de degré n à coefficients réels et $\mathrm{CD}(T_n) = 2^{n-1}$. De plus :

$$\|V_n\|_\infty = 2^{1-n}\|T_n\|_\infty \boxed{= 2^{1-n}.}$$

12. (a) Les polynômes V_n et P étant tous deux de degré n, $\deg(V_n - T) \leq n$. De plus, puisqu'ils sont unitaires, les termes dominants se simplifient par différence. Ainsi, $\boxed{\deg(V_n - P) \leq n - 1.}$

(b) Soit $k \in [\![0, n]\!]$. Calculons

$$(V_n - P)(x_k) = 2^{1-n}T_n(x_k) - P(x_k) = 2^{1-n}\cos(k\pi) - P(x_k) = 2^{1-n}(-1)^k - P(x_k).$$

Or, $|P(x_k)| \leq \|P\|_\infty < 2^{1-n}$ par hypothèse. Deux cas se présentent alors :

- si k est pair, $\boxed{(V_n - P)(x_k) = 2^{1-n} - P(x_k) > 0}$ car $P(x_k) < 2^{1-n}$;
- si k est impair, $\boxed{(V_n - P)(x_k) = -2^{1-n} - P(x_k) < 0}$ car $-P(x_k) < 2^{1-n}$.

(c) Soit $k \in [\![0, n-1]\!]$. Le polynôme $V_n - P$ change strictement de signe sur $[x_k, x_{k+1}]$. Comme la fonction polynomiale associée est continue sur $[x_k, x_{k+1}]$, par le théorème des valeurs intermédiaires, $V_n - P$ s'annule au moins une fois sur $]x_{k+1}, x_k[$. Ceci étant vraie pour tout $k \in [\![0, n-1]\!]$, $V_n - P$ s'annule donc au moins en n réels distincts.

Le polynôme $V_n - P$ admet au moins n racines distinctes et est de degré inférieur à $n - 1$. Donc $V_n - P = 0_{\mathbb{K}[X]}$ et $\boxed{V_n = P.}$

On aboutit à une contradiction puisque $\|P\|_\infty < 2^{1-n} = \|V_n\|_\infty$. Ainsi, pour tout polynôme à coefficients réels unitaire et de degré n, $\boxed{\|P\|_\infty \geq 2^{1-n} = \|V_n\|_\infty.}$

Partie IV. Majoration de l'erreur

13. Prouvons l'existence d'un tel polynôme. Notons pour cela, pour tout $i \in [\![1, n]\!]$:

$$L_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{X - a_j}{a_i - a_j}.$$

Rappelons que $(L_1, \dots, L_n)$ est la famille des polynômes de Lagrange associés aux réels deux à deux distincts $a_1, \dots, a_n$, et que ces polynômes vérifient, pour tout $(i, j) \in [\![1, n]\!]^2$:

$$L_i \in \mathbb{R}_{n-1}[X] \quad \text{et} \quad L_i(a_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} = \delta_{i,j} \quad \text{(symbole de Kronecker).}$$

Considérons le polynôme :

$$P = \sum_{i=1}^{n} f(a_i) L_i.$$

Ce polynôme est de degré au plus $n - 1$ en tant que combinaison linéaire de polynômes de $\mathbb{R}_{n-1}[X]$, et vérifie pour tout $j \in [\![1, n]\!]$:

$$P(a_j) = \sum_{i=1}^{n} f(a_i) \underbrace{L_i(a_j)}_{=\delta_{i,j}} = f(a_j) L_j(a_j) = f(a_j).$$

D'où l'existence d'un tel polynôme.

Pour montrer l'unicité, considérons P et Q des polynômes de $\mathbb{R}_{n-1}[X]$ tels que :

$$\forall i \in [\![1, n]\!], \quad P(a_i) = f(a_i) = Q(a_i).$$

Le polynôme $R = P - Q$ est de degré au plus $n - 1$ et admet $a_1, \dots, a_n$ pour racines distinctes. Donc $R = 0_{\mathbb{R}[X]}$ et $P = Q$.

Ainsi, $\boxed{\text{il existe un unique polynôme } P \text{ de } \mathbb{R}_{n-1}[X] \text{ tel que } P(a_i) = f(a_i) \text{ pour tout } i \in [\![1, n]\!].}$

14. (a) Puisque t n'appartient pas à $\{a_1, \dots, a_n\}$, $S(t)$ est non nul. Par suite, on peut poser $\boxed{\lambda = \dfrac{f(t) - P(t)}{S(t)}, \text{ de sorte que } \varphi(t) = 0.}$

(b) Pour tout $i \in [\![1, n]\!]$:

$$\varphi(a_i) = f(a_i) - P(a_i) - \lambda \underbrace{S(a_i)}_{=0} = f(a_i) - f(a_i) = 0.$$

Comme φ s'annule également en t et que tous les réels $a_i, \dots, a_n, t$ sont distincts, ceci nous donne $\boxed{n + 1 \text{ annulations de } \phi.}$

(c) Il s'agit d'appliquer le théorème de Rolle en cascade. Remarquons en préambule que φ est de classe $\mathscr{C}^n$ sur $[-1, 1]$ en tant que combinaison linéaire de telles fonctions.

Montrons par récurrence sur $i \in [\![0, n]\!]$ la propriété $\mathscr{P}(i)$: « φ s'annule (au moins) $n + 1 - i$ fois dans $[-1, 1]$ ».

$\boxed{\textbf{I}}$ La propriété au rang $i = 0$ a été établie à la question précédente : $\varphi^{(0)} = \varphi$ s'annule $n + 1$ fois sur $[-1, 1]$.

$\boxed{\textbf{H}}$ Soit $i \in [\![0, n - 1]\!]$. Supposons que $\varphi^{(i)}$ s'annule $n + 1 - i$ fois sur $[-1, 1]$. Notons les $c_1 < \cdots < c_{n+1-i}$.

Soit $j \in [\![1, n - i]\!]$. La fonction $\varphi^{(i)}$ est continue sur $[c_j, c_{j+1}]$, dérivable sur $]c_j, c_{j+1}[$, et s'annule en c_j et c_{j+1}. Par le théorème de Rolle, il existe $d_j \in \,]c_j, c_{j+1}[$ tel que $\varphi^{(i+1)}(d_j) = 0$.

On a montré l'existence de $n - i$ points d'annulation pour $\varphi^{(i+1)}$. D'où la propriété au rang $i + 1$.

Par principe de récurrence, la propriété $\mathscr{P}(i)$ est vraie pour tout $i \in [\![0, n]\!]$. En particulier, la propriété $\mathscr{P}(n)$ est vraie : $\boxed{\varphi^{(n)} \text{ s'annule au moins une fois dans } [-1, 1].}$

(d) Puisque P est de degré au plus $n-1$, sa dérivée n-ème est nulle.

D'autre part, la fonction polynomiale S est de degré n et unitaire. Par conséquent, $S^{(n)}$ est constante, égale à $n!$.

Ainsi, pour tout $x \in [-1, 1]$:

$$\boxed{\varphi^{(n)}(x) = f^{(n)}(x) - P^{(n)}(x) - \lambda S^{(n)}(x) = f^{(n)}(x) - \lambda n!.}$$

(e) Par la question 14.(c), il existe $a \in [-1, 1]$ tel que $\varphi^{(n)}(a) = 0$, soit avec l'expression obtenue à la question précédente :

$$f^{(n)}(a) - \lambda n! = 0, \qquad \text{d'où} \qquad \lambda = \frac{f^{(n)}(a)}{n!}.$$

Mais λ a été fixé de telle sorte que $\varphi(t) = 0$. Ainsi :

$$\boxed{f(t) - P(t) = \lambda S(t) = \frac{f^{(n)}(a)}{n!} S(t).}$$

15. Soit $t \in [-1, 1] \setminus \{a_1, \ldots, a_n\}$. Par la question précédente, il existe $a \in [-1, 1]$ tel que :

$$f(t) - P(t) = \lambda S(t) = \frac{f^{(n)}(a)}{n!} S(t).$$

En prenant les valeurs absolues puis en majorant :

$$\boxed{|f(t) - P(t)| \leq \frac{|f^{(n)}(a)|}{n!} |S(t)| \leq \frac{M_n}{n!} |S(t)|}$$

où $M_n = \|f^{(n)}\|_\infty$ (qui existe bien par continuité de $f^{(n)}$. Et cette inégalité est encore valable lorsque t est l'un des $a_1, \ldots, a_n$ puisqu'elle devient alors $0 \leq 0$.

16. La fonction S est polynomiale unitaire de degré n. D'après la question 12 :

$$\|S\|_\infty \geq 2^{1-n}$$

et cette borne est atteinte lorsque

$$S = 2^{1-n} T_n = \prod_{k=0}^{n-1} \left(X - \cos\left(\frac{(2k+1)\pi}{2n} \right) \right),$$

c'est-à-dire lorsque $\boxed{a_k = \cos\left(\frac{(2k-1)\pi}{n} \right) \text{ pour } k \in [\![1, n]\!].}$

Pour ce choix de $a_1, \ldots, a_n$, on obtient pour tout $t \in [-1, 1]$:

$$|f(t) - P(t)| \leq \frac{M_n}{n!} |S(t)| \leq \frac{M_n}{n!} 2^{1-n}.$$

Le réel $\frac{M_n}{n!} 2^{1-n}$ apparait comme un majorant de $\{|f(t) - P(t)|, \, t \in [-1, 1]\}$. Par comparaison d'un majorant au plus petit d'entre eux :

$$\boxed{\|f - P\|_\infty \leq \frac{M_n}{n!} 2^{1-n}.}$$