

CONTRÔLE 4

Calculatrice et documents sont interdits.

Tous les résultats doivent être correctement rédigés et rigoureusement justifiés.

Durée de l'épreuve : 1h25.

Le barème est donné à titre indicatif : grosso modo un point par question.

I. Racines carrées de matrices

Soit $n \in \mathbf{N}^*$ et $A \in \mathcal{M}_n(\mathbf{C})$.

Une **racine carrée** de A est une matrice $J \in \mathcal{M}_n(\mathbf{C})$ telle que $J^2 = A$.

Le but de ce problème est d'étudier quelques propriétés des racines carrées de matrices.

1. Exemples

(a) Dans $\mathcal{M}_2(\mathbf{C})$, trouver trois racines carrées différentes de $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ dont au moins une n'est pas une matrice diagonale.

(b) Soit $D = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \in \mathcal{M}_2(\mathbf{C})$. Trouver une matrice K telle que $K^2 = D$.

Soient $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $P = \begin{pmatrix} -i & i \\ 1 & 1 \end{pmatrix}$.

(c) Montrer que P est inversible et calculer P^{-1} .

(d) Calculer $P^{-1}AP$.

(e) En déduire qu'on peut trouver une matrice $J \in \mathcal{M}_2(\mathbf{C})$ telle que $J^2 = A$.

(f) Interprétation : l'application $r : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \begin{pmatrix} x \\ y \end{pmatrix}$ est une transformation géométrique simple du plan. Décrire r et proposer une transformation s telle que $s \circ s = r$.

2. Existence

Nous allons montrer que certaines matrices n'ont pas de racine carrée.

Soit N une matrice de taille 2 non nulle nilpotente : $\exists k \geq 2, N^k = 0$. On note k_0 le plus petit entier satisfaisant cette propriété (k_0 est l'indice de nilpotence de N).

(a) Montrer que N est non inversible.

On a démontré en TD que cela impliquait qu'il existe $\alpha \in \mathbf{R}$ tel que $N^2 + \alpha N = 0$.

(b) Montrer que $\alpha = 0$ et donc $N^2 = 0$.

(c) Supposons qu'il existe une matrice L telle que $N = L^2$. Montrer que L est nilpotente.

(d) Appliquer le résultat de la question b et obtenir une contradiction. Conclure.

3. Décomposition polaire d'une matrice

On rappelle qu'une matrice est **symétrique** si elle est égale à sa transposée.

On admet le **théorème spectral** : si S est une matrice symétrique à coefficients réels, alors il existe deux matrices réelles P et D telles que

$$D \text{ est diagonale, } P^{-1} = {}^tP \text{ et } S = P^{-1}DP.$$

Soit $M \in \mathcal{M}_n(\mathbf{R})$. On suppose M inversible.

- (a) Soit $S = {}^tMM$. Montrer que S est une matrice symétrique.
- (b) À l'aide du théorème spectral, montrer que S admet une racine carrée $H \in \mathcal{M}_n(\mathbf{C})$ qui est également symétrique.
- (c) On pose $Q = HM^{-1}$. Montrer que ${}^tQQ = I_n$.

Remarque : Q est une matrice dite orthogonale. Cette dernière égalité permet d'écrire $M = HQ^{-1}$. C'est la décomposition polaire de M (qui est analogue à l'écriture polaire des complexes).

II. Code correcteur BCH

On souhaite envoyer un message en binaire de longueur 4. Pour garantir une transmission sans erreur, nous allons envoyer le message avec 3 chiffres supplémentaires qui vont permettre de détecter et corriger une éventuelle erreur lors de la transmission.

Nous travaillons en binaire : tous les calculs s'effectueront modulo 2.

Dans $\mathbf{Z}/2\mathbf{Z}[X]$, on considère le polynôme $P = X^3 + X + 1$.

On souhaite émettre le message $m = (a, b, c, d) \in \{0, 1\}^4$.

- On définit le polynôme $M = aX^6 + bX^5 + cX^4 + dX^3$.
- On calcule le reste $R = eX^2 + fX + g$ de la division euclidienne de M par P .
- On envoie le message $m_e = (a, b, c, d, e, f, g)$ et on note $M_e = M + R$ le polynôme qui lui est associé. On note également m_r le message reçu et M_r son polynôme associé (en l'absence d'erreur, $m_r = m_e$).

1. Quel est le message m_e correspondant à $m = (1, 1, 1, 0)$?
Ne pas oublier de réduire modulo 2 tous les coefficients obtenus.
2. Justifier que le polynôme P est irréductible dans $\mathbf{Z}/2\mathbf{Z}[X]$.
3. Montrer que le reste de la division de M_e par P est nul.
4. On note dans la suite R_k le reste de la division euclidienne de X^k par P .
Calculer les restes $R_0, R_1, \dots, R_6$. Quel ensemble obtient-on avec ces sept restes ?
On peut déduire sans trop de calculs les restes R_4, R_5, R_6 à partir des restes précédents.
5. Supposons qu'il y a une erreur sur le premier chiffre du message : $a+1$ a été reçu au lieu de a . Ainsi $m_r = (a+1, b, c, d, e, f, g)$. Montrer alors que le reste R_r de la division de M_r par P est égal à R_6 .
6. Montrer plus généralement que s'il y a une seule erreur dans la transmission, alors $R_r = R_k$ où $7-k$ désigne la position du chiffre erroné.
7. On a reçu le message $m_r = (1, 0, 0, 1, 0, 0, 1)$. Quel était le message m initial ?

Pour envoyer des messages plus longs et détecter/corriger plus d'erreurs, il suffit de travailler avec des polynômes irréductibles de degré plus élevé.