Problème 1 : puissances de matrices

Rappels et notations

Étant donnés deux entiers naturels non nuls p et q, $\mathcal{M}_{p,q}(\mathbb{C})$ désigne l'ensemble des matrices à p lignes et q colonnes, à coefficients complexes.
L'ensemble $\mathcal{M}_{p,p}(\mathbb{C})$ est noté $\mathcal{M}_p(\mathbb{C})$ et I_p désigne la matrice identité de $\mathcal{M}_p(\mathbb{C})$.
On identifiera par la suite $\mathcal{M}_{p,1}(\mathbb{C})$ et $\mathbb{C}^p$.

Soit $(A_n)_{n\in\mathbb{N}}$ une suite de matrices de $\mathcal{M}_{p,q}(\mathbb{C})$. Pour tout entier n, on note $A_n = (a_{ij}(n))_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant q}}$.
On dit que la suite $(A_n)_{n\in\mathbb{N}}$ est convergente, si pour tout couple (i,j) tel que $i \in [\![1,p]\!]$ et $j \in [\![1,q]\!]$, la suite $(a_{i,j}(n))_{n\in\mathbb{N}}$ converge dans $\mathbb{C}$.
En posant $\lim\limits_{n\to+\infty}(a_{i,j}(n)) = l_{i,j}$ et $L = (l_{ij})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant q}}$, on dit alors que la matrice L est la limite de la suite $(A_n)_{n\in\mathbb{N}}$ et on note : $\lim\limits_{n\to+\infty} A_n = L$.

Soit A une matrice de $\mathcal{M}_p(\mathbb{C})$. Pour tout entier naturel n, on note A^n la puissance n-ième de la matrice A.
Ce problème a pour but de déterminer une condition nécessaire et suffisante pour que la suite $(A^n)_{n\in\mathbb{N}}$ converge dans $\mathcal{M}_p(\mathbb{C})$.

Partie A : étude d'un exemple

On considère les suites $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ définies par :

$$x_0 \in \mathbb{R}\,,\ y_0 \in \mathbb{R} \text{ et } \forall n \in \mathbb{N},\ \begin{cases} x_{n+1} = \dfrac{4}{5}x_n + \dfrac{2}{5}y_n \\ y_{n+1} = \dfrac{1}{5}x_n + \dfrac{3}{5}y_n \end{cases}$$

Dans cette partie, on pose $A = \dfrac{1}{5}\begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix}$.

1. Pour $n \in \mathbb{N}$, exprimer $\begin{pmatrix} x_n \\ y_n \end{pmatrix}$ en fonction de A^n et de $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$.
2. Montrer qu'il existe une matrice diagonale D de $\mathcal{M}_2(\mathbb{C})$ telle que A puisse s'écrire :

   $$A = PDP^{-1}$$

   où P désigne la matrice $\begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix}$.
3. Pour tout $n \in \mathbb{N}$, déterminer une expression de A^n en fonction de n.
4. Etablir que la suite $(A^n)_{n\in\mathbb{N}}$ est convergente et préciser sa limite.
5. Démontrer que les suites $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ convergent et déterminer les limites de ces suites en fonction de x_0 et y_0.

Partie B : résultats préliminaires

Soient p et q deux entiers naturels non nuls.

1. Soient $(A_n)_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$ deux suites de matrices de $\mathcal{M}_{p,q}(\mathbb{C})$ qui convergent respectivement vers L et M.
   1.1. Montrer que $\lim\limits_{n\to+\infty}(A_n + B_n) = L + M$.
   1.2. Soit $\alpha \in \mathbb{C}$. Montrer que $\lim\limits_{n\to+\infty}(\alpha A_n) = \alpha L$.

1.3. Soient $B \in \mathcal{M}_{p,q}(\mathbb{C})$ et $(\alpha_n)_{n\in\mathbb{N}}$ une suite de nombres complexes qui converge vers $\alpha \in \mathbb{C}$. Montrer que $\lim\limits_{n\to+\infty} \alpha_n B = \alpha B$.

2. Soit $(A_n)_{n\in\mathbb{N}}$ une suite de matrices de $\mathcal{M}_p(\mathbb{C})$ qui converge vers L.

2.1. Soit $X \in \mathcal{M}_{p,q}(\mathbb{C})$. Démontrer que $\lim\limits_{n\to+\infty} A_n X = LX$.

2.2. Énoncer sans démonstration un résultat analogue pour la multiplication à droite.

3. Soit $(A_n)_{n\in\mathbb{N}}$ une suite de matrices de $\mathcal{M}_p(\mathbb{C})$ telle que :

$$\forall X \in \mathbb{C}^p, \lim_{n\to+\infty} A_n X = 0$$

Montrer que $\lim\limits_{n\to+\infty} A_n = 0$.

Partie C : condition nécessaire

Dans la suite du problème, on note u l'endomorphisme de $\mathbb{C}^p$ représenté par la matrice A dans la base canonique.
On définit, pour tout entier naturel n, u^n par : $u^0 = \mathrm{Id}_{\mathbb{C}^p}$ et $u^{n+1} = u \circ u^n$.
On suppose dans cette partie que la suite $(A^n)_{n\in\mathbb{N}}$ converge.

1. Soit λ une valeur propre de u ($\lambda \in \mathbb{C}$).

1.1. Montrer que $|\lambda| \leqslant 1$.

1.2. On suppose que $|\lambda| = 1$.
Montrer qu'alors $\lambda = 1$. *On pourra considérer* $\left|\lambda^{n+1} - \lambda^n\right|$.

2. Montrer que $\mathrm{Ker}(u - \mathrm{Id}) \cap \mathrm{Im}(u - \mathrm{Id}) = \{0\}$.

Partie D : condition suffisante

On note $\chi_u(X) = \det(A - XI_p)$ le polynôme caractéristique de u, où det désigne le déterminant de la matrice considérée.

1. Énoncer le théorème de d'Alembert-Gauss.

2. En déduire que l'on peut écrire $\chi_u(X) = \det(A - XI_p) = \prod\limits_{i=1}^{p} (\alpha_i - X)$, avec $\alpha_i \in \mathbb{C}$ pour tout entier $i \in [\![1, p]\!]$.

3. Justifier le fait que u admet dans une certaine base $(e_1, ..., e_p)$ une matrice T de la forme :

$$T = \begin{pmatrix} \alpha_1 & \cdots & \cdots & \cdots \\ & \alpha_2 & \cdots & \cdots \\ & & \ddots & \cdots \\ 0 & & & \alpha_p \end{pmatrix}.$$

4. On suppose dans cette question que $|\alpha_i| < 1$ pour tout entier $i \in [\![1, p]\!]$.

4.1. Montrer que $\lim\limits_{n\to+\infty} u^n(e_1) = 0$.

4.2. Montrer par récurrence que pour tout entier $i \in [\![1, p]\!]$, $\lim\limits_{n\to+\infty} u^n(e_i) = 0$.

4.3. En déduire la limite de T^n, puis celle de A^n.

5. On note $\lambda_1, ..., \lambda_m$ les valeurs propres de u, deux à deux distinctes, avec $m \in \mathbb{N}^*$.
On suppose dans cette question que $\lambda_1 = 1$ et $|\lambda_i| < 1$ pour tout entier i tel que $2 \leqslant i \leqslant m$.
On suppose également que $\mathrm{Ker}(u - \mathrm{Id}) \cap \mathrm{Im}(u - \mathrm{Id}) = \{0\}$.

5.1. Montrer que $\mathrm{Ker}(u - \mathrm{Id})$ et $\mathrm{Im}(u - \mathrm{Id})$ sont deux sous-espaces supplémentaires dans $\mathbb{C}^p$ stables par u.

5.2. On note u_1 l'endomorphisme de $\mathrm{Im}(u - \mathrm{Id})$ induit par u. Montrer que toute valeur propre de u_1 est une valeur propre de u, distincte de λ_1.

5.3. En remarquant que u_1 vérifie les hypothèses de la question 4, en déduire que A^n converge et déterminer une matrice semblable à sa limite.

Partie E : conclusion et application

1. On note $\lambda_1, ..., \lambda_m$ les valeurs propres de A, deux à deux distinctes, avec $m \in \mathbb{N}^*$.
   Déduire des questions précédentes que la suite $(A^n)_{n\in\mathbb{N}}$ converge si et seulement si :
   $$\left\{\begin{array}{l} \forall i \in [\![1, m]\!], |\lambda_i| < 1 \\ \text{ou} \\ \lambda_1 = 1, \mathrm{Ker}\,(u - \mathrm{Id}) \cap \mathrm{Im}\,(u - \mathrm{Id}) = \{0\} \quad \text{et} \quad \forall i \in [\![2, m]\!], |\lambda_i| < 1 \end{array}\right.$$
2. Déterminer si la suite $(A^n)_{n\in\mathbb{N}}$ est convergente, dans chacun des cas suivants :

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

   2.2. $A = \begin{pmatrix} 1 & 1 & i \\ 0 & \dfrac{i}{2} & 1 \\ 0 & 0 & 1 \end{pmatrix}$

   2.3. $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -6 + \dfrac{i}{2} & 9 \\ 0 & -4 & 6 + \dfrac{i}{2} \end{pmatrix}$

Problème 2 : quelques théorèmes d'arithmétique

On démontre dans la partie A un théorème de Lagrange dont on utilise le résultat pour démontrer le théorème de Wilson (partie B) et le théorème de Wolstenholme (partie C).

Partie A : théorème de Lagrange

1. Montrer que pour tout entier $n \geqslant 1$ et tout entier $k \in [\![1, n]\!]$ on a :

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

2. Montrer que pour tout entier premier p et tout entier $k \in [\![1, p-1]\!]$, p divise $\dbinom{p}{k}$.

3. Soit p un entier premier impair. On considère la fonction f définie sur $\mathbb{R}$ par :

$$f(x) = \prod_{k=1}^{p-1}(x+k)$$

3.1. Montrer que pour tout réel x on a :

$$pf(x) = (x+1)f(x+1) - xf(x)$$

3.2. Justifier l'existence d'un p-uplet d'entiers $(a_0, a_1, \cdots, a_{p-1})$ tel que pour tout réel x on a :

$$f(x) = \sum_{k=0}^{p-1} a_k\, x^{p-1-k}$$

3.3. Montrer que $a_0 = 1$ et $a_{p-1} = (p-1)!$

3.4. À l'aide de la question 3.1 et en faisant intervenir le binôme de Newton, montrer que pour tout entier $k \in [\![0, p-1]\!]$ on a :

$$pa_k = \sum_{i=0}^{k}\binom{p-i}{k+1-i}a_i$$

3.5. En déduire que $a_1 = \dbinom{p}{2}$ et que pour tout entier $k \in [\![2, p-1]\!]$ on a :

$$k\,a_k = \binom{p}{k+1} + \sum_{i=1}^{k-1}\binom{p-i}{k+1-i}a_i$$

3.6. En déduire le théorème de Lagrange :

« Si p est un entier premier impair et si $f(x) = \displaystyle\prod_{k=1}^{p-1}(x+k) = \sum_{k=0}^{p-1} a_k\, x^{p-1-k}$ alors les coefficients $a_1, a_2, \cdots, a_{p-2}$ sont divisibles par p ». *On pourra raisonner par récurrence.*

Partie B : théorème de Wilson

On se propose de démontrer la propriété suivante, connue sous le nom de « théorème de Wilson » : si p est un entier premier alors $(p-1)! \equiv -1 \pmod{p}$.

1. Vérifier que la propriété est vraie pour $p = 2$.
2. p est maintenant un entier premier impair.
   2.1. Montrer que :
   $$p\,! = 1 + \sum_{k=1}^{p-2} a_k + (p-1)!$$
   (les entiers $a_i, i \in [\![1, p-2]\!]$, sont ceux définis à la question A.3.2)
   2.2. En déduire que $(p-1)! \equiv -1 \pmod{p}$.
3. Montrer que la réciproque du théorème de Wilson est vraie.
4. On se propose d'étudier ce que devient le théorème de Wilson pour les entiers non premiers strictement supérieurs à 4.
   4.1. On suppose que $n > 4$ et que la décomposition en produit de facteurs premiers de n comprend au moins deux facteurs premiers distincts. Montrer que $(n-1)! \equiv 0 \pmod{n}$.
   4.2. On suppose que $n > 4$ et que $n = p^\alpha$ où p est un entier premier et α est un entier strictement supérieur à 2. Montrer que $(n-1)! \equiv 0 \pmod{n}$.
   4.3. On suppose que $n > 4$ et que $n = p^2$ où p est un entier premier. Montrer que $1 < 2p < n$ et en déduire que $(n-1)! \equiv 0 \pmod{n}$.

Partie C : théorème de Wolstenholme

Pour tout entier $n \geqslant 1$, on considère le rationnel :

$$H_n = \sum_{k=1}^{n} \frac{1}{k}$$

On désigne par s_n et t_n les deux entiers naturels tels que :

$$H_n = \frac{s_n}{t_n} \qquad \text{et} \qquad \operatorname{pgcd}(s_n, t_n) = 1$$

1. Écrire un algorithme permettant d'obtenir pour n allant de 2 à 10 les entiers s_n et t_n (on supposera qu'on dispose d'une instruction *pgcd(a,b)* qui renvoie le plus grand commun diviseur de deux entiers a et b).
2. Calculer s_4, s_6 et s_{10} et vérifier que ces entiers sont divisibles respectivement par 5^2, 7^2 et 11^2.

Dans la suite, p désigne un nombre premier strictement supérieur à 3. On se propose de démontrer que l'entier s_{p-1} est divisible par p^2 (théorème de Wolstenholme).

3. Montrer que $H_{p-1} = \dfrac{a_{p-2}}{(p-1)!}$ où a_{p-2} est défini comme à la partie A. *On pourra utiliser une relation liant les racines d'un polynôme et l'un de ses coefficients.*
4. Déduire de l'écriture de $f(-p)$ que :
$$a_{p-2} = p^{p-2} - a_1 p^{p-3} + \cdots + a_{p-3}p$$
5. Conclure.