DM n$^{\text{o}}$11

Préparation aux oraux

Pour le 19 Mars

Pour le 18 Mars. Rédiger **huit** des exercices suivants dont obligatoirement les exercices 6, 7, 8 et 14. Les exercices marqués d'un astérisque sont plus difficiles, ceux marqués de deux réservés et destinés aux candidats X-ENS.

Exercice 1 $\star$ Des éléments A et B de $\mathcal{M}_n(\mathbf{Z})$ sont dit semblables dans $\mathcal{M}_n(\mathbf{Z})$ si il existe un élément P de $\mathcal{M}_n(\mathbf{Z})$ inversible d'inverse élément de $\mathcal{M}_n(\mathbf{Z})$ tel que $A = PBP^{-1}$. Pour tout entier a on note S_a l'élément de $\mathcal{M}_2(\mathbf{Z})$, $\begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}$

1. S_0 et S_1 sont elle semblables dans $\mathcal{M}_2(\mathbf{Q})$?
2. S_0 et S_1 sont elle semblables dans $\mathcal{M}_2(\mathbf{Z})$?
3. Soit A un élément de $\mathcal{M}_2(\mathbf{Z})$ ayant 1 et -1 comme valeurs propres. Montrer qu'il existe $a \in \mathbf{Z}$ tel que M soit semblable dans $\mathcal{M}_2(\mathbf{Z})$ à S_a.

Exercice 2$\star$ — Théorème de Cayley-Hamilton par la formule de Cauchy —
Soit A un élément de $\mathcal{M}_n(\mathbf{C})$. Montrer qu'il existe un réel $R \geq 0$ tel que, pour tout entier $k \geq 0$ et tout réel $r \geq R$,

$$A^k = \frac{1}{2\pi} \int_0^{2\pi} r^{k+1} e^{i(k+1)\theta} \left(re^{i\theta} I_n - A\right)^{-1} \mathrm{d}\theta.$$

En déduire le théorème de Cayley-Hamilton.

Exercice 3 — Soit Soit A un élément de $\mathcal{M}_n(\mathbf{K})$ diagonalisable. Nous noterons $\lambda_1, \lambda_2, \dots, \lambda_p$ ses p valeurs propres deux à deux distinctes et de multiplicité respectives $m_1, m_2, \dots, m_p$. Montrer que l'ensemble des éléments de $\mathcal{M}_n(\mathbf{K})$ qui commutent avec A est un espace vectoriel dont on déterminera la dimension.

Exercice 4 —

1. Déterminer les applications f de $\mathbf{R}$ dans $\mathbf{R}$ dérivables telles que $f'(x) = f(-x)$ pour tout réel x.
2. Déterminer les applications f de $\mathbf{R}_+^*$ dans $\mathbf{R}$ dérivables telles que $f'(x) = f\left(\frac{1}{x}\right)$ pour tout réel x.

Exercice 5 —

1. Soient A et A' et B des éléments de $\mathcal{M}_n(\mathbf{R})$ et M la matrice élément de $\mathcal{M}_{2n}(\mathbf{R})$, $\begin{pmatrix} A & B \\ 0_n & A' \end{pmatrix}$. Montrer que si M est diagonalisable alors A et A' le sont.
2. Déterminer les éléments A de $\mathcal{M}_n(\mathbf{R})$ tels que la matrice B suivante soit diagonalisable. $B = \begin{pmatrix} A & A \\ 0 & A \end{pmatrix}$

Exercices 6 — ÉQUATION DE MATHIEU —

Soit l'équation différentielle :

$$y'' + (1 + \gamma\, q)\, y = 0, \tag{1}$$

où q est une fonction continue réelle de période τ, γ un réel > 0. On pose $k = |q|$, et on note Q et K les fonctions définies par :

$$Q\,(t) = \int_0^t q\,(s)\;\mathrm{d}\,s,\;\; K\,(t) = \int_0^t k\,(s)\;\mathrm{d}\,s,$$

pour tout réel t.

Soit α et β des réels, on s'intéresse à la solution de (1) satisfaisant à la condition initiale :

$$y\,(0) = \alpha\;,\; y'\,(0) = \beta.$$

1. Soit g une fonction continue de $\mathbf{R}_+$ dans $\mathbf{C}$. Montrer que toute solution sur $\mathbf{R}_+$ de

$$y'' + y = g$$

est de la forme :

$$f\;: t \mapsto f\,(0)\cos t + f'\,(0)\sin t + \int_0^t \sin\,(t-s)\,g\,(s)\,\mathrm{d}\,s$$

2. On considère la suite d'applications de $\mathbf{R}_+$ dans $\mathbf{C}$, $(f_n)_{n\in\mathbf{N}}$, définie par :

$$f_0'' + f_0 = 0\,; f_0\,(0) = \alpha,\quad f_0'\,(0) = \beta,$$

pour tout $n \in \mathbf{N}^*$,

$$f_n'' + f_n = -q\, f_{n-1}; f_n\,(0) = 0,\; f_n'\,(0) = 0.$$

(a) Montrer que pour tout entier $n \geq 0$ et tout t élément de $\mathbf{R}_+$ on a :

$$|f_n\,(t)| \leq \sqrt{\alpha^2 + \beta^2}\,\frac{K^n\,(t)}{n\,!}.$$

En déduire que pour tout t élément de $\mathbf{R}_+$, la série entière de la variable complexe z, $\sum\limits_{n\geq 0} f_n\,(t)\,z^n$ a un rayon de convergence infini.

(b) Montrer que la fonction f définie par :

$$f\;:\;\mathbf{R}_+ \to \mathbf{R}\,;\; t \mapsto \sum_{n=0}^{\infty} f_n\,(t)\,\gamma^n$$

est l'unique solution sur $\mathbf{R}_+$ du problème de Cauchy :

$$y + (1 + \gamma\, q)\, y = 0,\; y\,(0) = \alpha\,,\; y'\,(0) = \beta.$$

Exercices 7 —
Stabilité asymptotique d'un système linéaire —
Soient $A \in \mathcal{M}_n(\mathbf{R})$ et $B \in \mathcal{M}_{n,1}(\mathbf{R})$ Soit X_0 une élément de $\mathcal{M}_{n,1}(\mathbf{R})$ tel que

$$AX_0 + B = 0_{n,1}.$$

On dira que X_0 est une position d'équilibre asymptotiquement stable du système différentiel

$$X' = AX + B, \tag{S}$$

si toute solution Φ sur $\mathbf{R}_+$ de ce système vérifie :

$$\Phi(t) \underset{t\to+\infty}{\to} X_0.$$

1. Montrer que X_0 est une position d'équilibre asymptotiquement stable de (S) si et seulement si
$$\exp(tA) \underset{t\to+\infty}{\to} 0_n.$$
2. On suppose que les parties réelles de toutes les valeurs propres complexes de A sont négatives. Montrer que X_0 est une position d'équilibre asymptotiquement stable de (S).
On utilisera une décomposition par blocs de Dundford de A.
3. On suppose qu'une valeur propre λ_0 de A a pour partie réelle un réel $r > 0$ et on note V_0 un vecteur propre de A associé à λ_0.
   (a) On suppose que la valeur propre λ_0 est réelle. Montrer que X_0 n'est pas une position d'équilibre asymptotiquement stable de (S).
   On pourra considérer la solution du système $X' = AX$ sur $\mathbf{R}_+$ qui prend en 0 la valeur V_0.
   (b) On suppose que la valeur propre λ_0 est non réelle. Montrer que X_0 n'est pas une position d'équilibre asymptotiquement stable de (S).
   On pourra considérer la solution du système $X' = AX$ sur $\mathbf{R}_+$ qui prend en 0 la valeur $\frac{1}{2}(V_0 + \bar{V}_0)$.

Exercice 8 — Cryptographie —
Le but de cet exercice est l'étude du principe de criptage RSA, qui permet de communiquer de façon sure des données. Ce résultat est à connaitre

Dans cet exercice φ désignera l'indicatrice d'Euler.

1. Chiffrement du message
On étudie le cryptage d'un message par un expéditeur. Soient p et q des nombres premiers distincts et n leur produit : $n = pq$. On appelle n *module de chiffrement*
   (a) Donner en fonction de p et q la valeur de $\varphi(n)$.
   (b) Soit e un entier premier avec $\varphi(n)$. On appele e *exposant de chiffrement.* Montrer qu'il existe un entier **naturel** d tel que $ed \equiv 1\,[\varphi(n)]$

   Le couple (n, e) est appelé clef publique (elle peut être transmise à l'expéditeur), le couple (n, d) est appelé clef privée, elle reste connue du seul destinataire du message.
   Dans la suite on considère un entier M (représentant le message) strictement inférieur à n. On note C l'élément de $\{0, 1, \dots, n-1\}$ congru à M^e modulo n. Cet entier représente le message codé qui est transmis.

2. DÉCHIFFREMENT DU MESSAGE
   On se propose de montrer que C^d est congru à M *modulo* n, ce qui permet au destinataire de trouver M, grâce à sa clef (n, d).
   (a) Montrer que M^{ed} est congru à M *modulo* p. On distinguera les deux cas M premier avec p et M non premiers avec p.
   (b) En déduire que $C^d \equiv M[n]$.

   pour trouver d à partir de e et n il faut savoir inverser e dans $\mathbf{Z}/\varphi(n)\mathbf{Z}$ ce qui nécessite de connaitre $\varphi(n)$ et donc le couple (p, q). La décomposition de n en facteurs premiers peut être très difficile si les nombres premiers p et q ont été choisis très grands.

Exercice 9 —

1. Donner une condition nécessaire portant sur la parité de l'élément n de $\mathbf{N}^*$, pour qu'il existe une matrice M élément de $\mathcal{M}_n(\mathbf{R})$ qui vérifie :
$$M^2 + 2M + 5I_n = 0_n.$$
2. Cette condition est-elle suffisante ?

Exercice 10 $\star$ —PROBLÈMES DE DIRICHLET —

1. Soient f et g des application de $[a, b]$ dans $\mathbf{R}$ continues telles que $f \leq 0$. Montrer que l'équation différentielle
$$y'' + f(t)y = g(t)$$
possède une solution unique φ sur $[a, b]$ telle que $\varphi(a) = \varphi(b) = 0$
2. Montrer que si f est positive alors l'équation précédente peut avoir aucune ou plusieurs solutions.

Exercice 11 $\star$ Soit X une variable aléatoire réelle admettant un moment d'ordre 2. Montrer pour tout réel $\lambda > 0$:

1. $$\mathbf{P}(X \geq \mathrm{E}(X) + \lambda) \leq \frac{\mathrm{V}}{\mathrm{V} + \lambda^2}.$$
   On pourra considérer poour tout $t \in \mathbf{R}_+^*$, $\{(X - \mathrm{E}(X) + t)^2 \geq (t + \lambda)^2\}$.
2. Soit $(X_n)_{n \in \mathbf{N}^*}$ une suite de variables aléatoires mutuellement indépendantes ayant un moment d'ordre 2. On suppose que tout $n \in \mathbf{N}^*$, on a :
$$\mathrm{E}(X_n) = 0 \text{ et } \mathrm{V}(X_n) = 1.$$
   On pose $N = \min\{n \in \mathbf{N}^*, X_n \leq 1\}$.
   (a) Soit un entier $n \geq 2$. Exprimer $\{N > n - 1\}$ grâce aux événements $\{X_i > 1\}$, pour $i = 1, ...n - 1$
3. En utilisant la question précédente, montrer :
$$P(N = n) \leq \frac{1}{2^{n-1}}.$$
   En déduire que N est presque sûrement finie.
4. Montrer que e^{aN} est d'espérance finie, pour tout $a \in [0, \ln 2[$

Exercice 12 $\star\star$ — Soit u un endomorphisme d'un $\mathbf{C}$-espace vectoriel $\mathbf{E}$ de dimension finie n, non nulle. Soit $Q \in \mathbf{C}[X]$. On suppose que $Q(u)$ est diagonalisable et que $Q'(u)$ est inversible. Montrer que u est diagonalisable.

Exercice 13 Soit M un élément de $\mathcal{M}_n(\mathbf{C})$.

— On suppose que pour tout entier m strictement positif, $\mathrm{Tr}(M^m) = 0$. Montrer que M est nilpotente.
— On suppose que $\mathrm{Tr}(M^m) \underset{m\to+\infty}{\to} 0$. Montrer que les valeurs propres de M sont toutes de module inférieur strictement à 1.

Exercice 14 —
Pour tout $n \in \mathbf{N}^*$ on les fonctions de la variable réelle x, u_n définies par :

$$u_n(x) = \frac{x^n}{1-x^n}\,;\, f(x) = \sum_{n=1}^{+\infty} u_n(x).$$

On considère également la fonction f de la variable réelle x, définie par :

$$f(x) = \sum_{n=1}^{+\infty} u_n(x).$$

1. Étudier le domaine de définition de f*.
2. Étudier la continuité et la dérivabilité de f.
3. Donner un équivalent de f en 1.
4. Démontrer que pour tout $x \in]-1,1[$, $f(x) = \sum\limits_{n=1}^{+\infty} d(n)x^n$, où $d(n)$ est le nombre de diviseurs positifs de n.

Exercice 15 ⋆⋆

1. Soit M un élément de $M_n(\mathbf{R})$. On note μ sont polynôme minimal et $\mu_{\mathbf{C}}$ sont polynôme minimal lorsqu'on considère M comme comme un élément de $\mathbf{C}$. Montrer que $\mu = \mu_{\mathbf{C}}$.
2. Soit M un élément de $M_n(\mathbf{Q})$. On note $\mu_{\mathbf{Q}}$ son polynôme minimal et $\mu_{\mathbf{R}}$ son polynôme minimal lorsqu'on considère M comme comme un élément de $\mathcal{M}_n(\mathbf{R})$. Montrer que $\mu_{\mathbf{Q}} = \mu_{\mathbf{R}}$.

Exercice 16 ⋆⋆ — Égalité des accroissements finis vectorielle —

1. Rappeler l'égalité des accroissements finis pour une application f d'un segment $[a,b]$ (non réduit à un point) à valeurs dans $\mathbf{R}$. Montrer que ce résultat est faux si l'on remplace « à valeurs dans $\mathbf{R}$ » par « à valeurs dans $\mathbf{R}^n$ ».
2. Soit F une application de $[a,b]$ dans $\mathbf{R}^p$ de classe $\mathcal{C}^1$. On note d la dimension de l'espace affine engendré par $F'([a,b])$, c'est-à-dire du plus petit sous-espace vectoriel de $\mathbf{R}^n$ contenant $F'([a,b])$.
   (a) Montrer que l'espace affine $\mathcal{A}$ engendré par $F'([a,b])$ est l'ensemble des barycentres d'un nombre quelconque de points de $F'([a,b])$. Que dire de $\mathcal{A}$ lorsque $0_{\mathbf{R}^n}$ appartient à $F'([a,b])$.
   (b) Montrer qu'il existe des éléments c_1, c_2,...,c_{d+1} de $[a,b]$, des réels $\lambda_1, \lambda_2, ..., \lambda_{d+1}$, positifs ou nuls, de somme 1 tels que :

$$\frac{F(b)-F(a)}{b-a} = \sum_{i=1}^{d+1} F'(c_i).$$

On pourra pour simplifier commencer par supposer que $0_{\mathbf{R}^n}$ est élément de $F'([a,b])$. On utilisera librement le théorème de Carathéodory, cf. colles