UNIVERSITÉ PARIS 13 — MASTER 1 - ALGÈBRE II — Décembre 2015

CORRIGÉ DE L'EXAMEN

DURÉE 3 HEURES

INSTRUCTIONS. La présentation, la lisibilité, l'orthographe, la qualité de la rédaction, la clarté et la précision des raisonnements entreront pour une part importante dans l'appréciation des copies.

Toute réponse non justifiée ne recevra aucun point.

Exercice 1 (Diagonalisabilité)**.**

Soit $M \in \mathcal{M}_n(\mathbb{F}_q)$ un matrice carrée à coefficients dans un corps finis. Montrer que M est diagonalisable si et seulement si $M^q = M$.

CORRECTION. Comme le groupe multiplicatif $(\mathbb{F}_q^*, \times)$ a $q-1$ éléments, le théorème de Lagrange donne $x^{q-1} = 1$ pour tout $x \in \mathbb{F}_q^*$, soit $x^q = x$ pour tout $x \in \mathbb{F}_q$. Comme $\mathbb{F}_q$ est un corps, c'est un anneau intégre et donc le polynôme $Q := X^q - X$ a au plus q racines. L'argument précédent montre qu'il en a en fait exactement q qui sont tous les éléments de $\mathbb{F}_q$:

$$Q = X^q - X = \prod_{x \in \mathbb{F}_q} (X - x) \ .$$

Si M est diagonalisable, alors le polynôme $P = \prod_{i=1}^{k} (X - \lambda_i)$, où les λ_i sont les valeurs propres de M, annule M. Comme le polynôme P divise le polynôme Q, alors $M^q = M$. Dans l'autre sens, si $M^q = M$, alors Q est un polynôme annulateur de M. Or ce dernier est scindé à racines simples, donc la matrice M est diagonalisable.

Exercice 2 (Corps finis)**.**

(1) Montrer que le polynôme $P := X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.

CORRECTION. La seule manière de factoriser (non trivialement) un polynôme de degré 3 consiste en l'écrire comme le produit de deux polynômes de degrés 2 et 1 respectivement. Or le polynôme P n'admet aucune racine dans $\mathbb{F}_2$: $P(0) = P(1) = 1$. Donc, le polynôme P est irréductible dans $\mathbb{F}_2[X]$.

On en conclut que

$$\mathbb{F}_8 \cong \frac{\mathbb{F}_2[X]}{(X^3+X+1)}$$

est un modèle du corps à 8 éléments. Dans ce modèle, on note x la classe de X.

(2) Calculer l'inverse de x^2.

CORRECTION. Dans $\mathbb{F}_2[X]$, les polynômes X^2 et X^3+X+1 sont premiers entre eux. On utilise l'algorithme d'Euclide pour trouver des coefficients de Bézout. On trouve

$$(X^2+X+1)X^2 + (X+1)(X^3+X+1) = 1 \ .$$

Donc l'inverse de x^2 dans $\mathbb{F}_8$ est x^2+x+1.

Exercice 3 (Exponentielle de matrices)**.**

Montrer que la matrice réelle

$$M := \begin{pmatrix} -1 & 0 \\ 0 & -2 \end{pmatrix} \ \in \ \mathcal{M}_n(\mathbb{R})$$

n'est pas dans l'image de l'exponentielle des matrices réelles.

CORRECTION. Supposons par l'absurde qu'il existe une matrice $N \in \mathcal{M}_n(\mathbb{R})$ telle que $\exp(N) = M$. Vue dans $\mathcal{M}_n(\mathbb{C})$, la matrice N est trigonalisable, c'est-à-dire qu'il existe une matrice $P \in \mathrm{GL}_n(\mathbb{C})$ et $\lambda, \mu \in \mathbb{C}$ tels que

$$N = P \begin{pmatrix} \lambda & * \\ 0 & \mu \end{pmatrix} P^{-1} \ .$$

Donc, $M = P \begin{pmatrix} e^\lambda & * \\ 0 & e^\mu \end{pmatrix} P^{-1}$ et on en conclut que la matrice $\begin{pmatrix} e^\lambda & * \\ 0 & e^\mu \end{pmatrix}$ est diagonalisable avec pour valeurs propres $e^\lambda = -1$ et $e^\mu = -3$. D'où $\lambda = i(\pi + 2k\pi)$ et $\mu = \ln 3 + i(\pi + 2l\pi)$ avec $k, l \in \mathbb{Z}$. On aurait alors

$$\lambda\mu = -(\pi+2k\pi)(\pi+2l\pi) + i\underbrace{(\pi+2k\pi)\ln 3}_{\neq 0} = \det N \in \mathbb{R} \ ,$$

d'où la contradiction.

Problème 1 (Sous-groupes compacts de $\mathrm{GL}_n(\mathbb{R})$)**.**

OBJECTIF. Le but de cet exercice est de donner une autre démonstration, par une méthode de point fixe, du théorème affirmant que tout sous-groupe compact $\mathrm{G} \subset \mathrm{GL}_n(\mathbb{R})$ est un sous-groupe d'un conjugué du groupe orthogonal $\mathrm{O}_n(\mathbb{R})$.

Soit $\mathcal{V}$ un $\mathbb{R}$-espace vectoriel de dimension finie, $\dim \mathcal{V} = N$, et soit K un compact convexe (non vide) de $\mathcal{V}$.

(1) Soit f un endomorphisme de $\mathcal{V}$ préservant K, $f(K) \subset K$. Montrer que f admet un point fixe dans K :

$$\exists\, x \in K,\ f(x) = x\ .$$

INDICATION. On pourra considérer une suite de la forme

$$x_k := \frac{1}{k+1} \sum_{i=0}^{k} f^i(x_0), \quad \text{où} \quad x_0 \in K\ .$$

CORRECTION. Comme K est non vide, on considère $x_0 \in K$ et la suite définie par

$$x_k := \frac{1}{k+1} \sum_{i=0}^{k} f^i(x_0)\ .$$

Comme K est convexe, on a $x_k \in K$ et comme K est compact, il existe une suite extraite $\varphi(k)$ telle que $x_{\varphi(k)}$ converge vers x dans K. On montre ensuite que

$$f(x_{\varphi(k)}) = x_{\varphi(k)} + \frac{1}{\varphi(k)+1} \left(f^{\varphi(k)+1}(x_0) - x_0 \right)\ .$$

Comme f est une application linéaire en dimension finie, elle est continue. Comme K est compact donc borné, en passant à la limite $k \to +\infty$ dans l'équalité précédente, on trouve $f(x) = x$.

Soit $\mathcal{G}$ un sous-groupe compact de $\mathrm{GL}(\mathcal{V})$ préservant K, i.e. $\forall\, f \in \mathcal{G},\ f(K) \subset K$.

(2) Après choix d'une base de $\mathcal{V}$, on l'identifie à $\mathbb{R}^N$ pour lequel on considère la norme euclidienne $||X|| = \sqrt{x_1^2 + \cdots + x_N^2}$, pour $X = (x_1, \ldots, x_N)$. Montrer que

$$||X||_{\mathcal{G}} := \mathrm{Max}_{f \in \mathcal{G}}\, ||f(X)||$$

définit une norme $\mathcal{G}$-invariante sur $\mathcal{V}$. (Il est équivalent de montrer que $X \mapsto ||X||_{\mathcal{G}}^2$ est une forme quadratique définie positive.)

CORRECTION. Pour tout $X \in \mathbb{R}^N$, la quantité $\mathrm{Max}_{f \in \mathcal{G}}\, ||f(X)||$ est bien définie : il s'agit du maximum du compact $\mathcal{G}$ par l'application continue $f \mapsto ||f(X)||$, il existe et est atteint. Les axiomes d'une norme sont facilement vérifiés, voir la question suivante par exemple. L'invariance par $\mathcal{G}$ vient de la bijection $\mathcal{G} \to \mathcal{G},\ f \mapsto fg$, pour tout $g \in \mathcal{G}$.

(3) Décrire le cas d'égalité pour son inégalité triangulaire.

CORRECTION. Soit $X, Y \in \mathbb{R}^N$ et soit $f_0 \in \mathcal{G}$ tel que $||X+Y||_{\mathcal{G}} = ||f_0(X+Y)||$. Donc

$$||X+Y||_{\mathcal{G}} = ||f_0(X+Y)|| = ||f_0(X) + f_0(Y)|| \leqslant ||f_0(X)|| + ||f_0(Y)|| \leqslant ||X||_{\mathcal{G}} + ||Y||_{\mathcal{G}}\ .$$

Le cas d'égalité $||X+Y||_{\mathcal{G}} = ||X||_G G + ||Y||_{\mathcal{G}}$ impose alors $||f_0(X) + f_0(Y)|| = ||f_0(X)|| + ||f_0(Y)||$. On a donc que $f_0(X)$ et $f_0(Y)$ sont positivement liés, il en va donc de même de X et Y. (On dit que la norme $||-||_{\mathcal{G}}$ est strictement convexe).

(4) Montrer qu'il existe, dans K, un point fixe commun à tous les éléments de $\mathcal{G}$, c'est-à-dire

$$\exists\, x \in K,\ \forall f \in \mathcal{G}, \quad f(x) = x\ .$$

CORRECTION. Pour tout $f \in \mathcal{G}$, on considère

$$F_f := \{x \in K, f(x) = x\}\ ,$$

l'ensemble des points fixes de f dans K. La question (1) donne $F_f \neq \emptyset$ et montrons que

$$\bigcap_{f \in \mathcal{G}} F_f \neq \emptyset\ .$$

Comme il s'agit là, d'une famille de fermés d'un compact, il suffit de montrer que tout nombre fini d'éléments $f_1, \ldots, f_k$ de $\mathcal{G}$ vérifient

$$\bigcap_{1 \leqslant i \leqslant k} F_{f_i} \neq \emptyset \ .$$

On considère

$$f := \frac{1}{k} \sum_{1 \leqslant i \leqslant k} f_i \ .$$

Il s'agit d'un endomorphisme de $\mathcal{V}$ qui préserve le compact convexe K, donc, par la question (1), il admet un point fixe $x \in K$, i.e. $f(x) = x$. En identifiant $\mathcal{V}$ à $\mathbb{R}^N$ et en considérant la norme euclidienne, comme à la question (2), on a

$$||x||_{\mathcal{G}} = ||f(x)||_{\mathcal{G}} \leqslant \frac{1}{k} \sum_{1 \leqslant i \leqslant k} ||f_i(x)||_{\mathcal{G}} = \frac{1}{k} \sum_{1 \leqslant i \leqslant k} ||x||_{\mathcal{G}} = ||x||_{\mathcal{G}} \ .$$

Comme la norme $||-||_{\mathcal{G}}$ est strictement convexe, on en conclut que les $f_i(x)$ sont positivement liés et même égaux car $||f_i(x)||_{\mathcal{G}} = ||x||_{\mathcal{G}}$. Et comme leur moyenne est égale à x, ils sont tous égaux à x, ce qui conclut la question.

Pour pouvoir conclure en utilisant ce théorème de point fixe, nous allons en outre avoir besoin du théorème de Carathéodory, qui est l'affirmation suivante, ainsi que de son corollaire.

(5) Soit $\mathcal{E} \subset \mathcal{V}$ un sous-ensemble de $\mathcal{V}$. Montrer que tout élément de l'enveloppe convexe de $\mathcal{E}$ peut s'écrire comme combinaison convexe d'au plus $N+1$ éléments de $\mathcal{E}$, c'est-à-dire

$$\mathrm{Conv}(\mathcal{E}) = \left\{ \sum_{i=1}^{N+1} \lambda_i x_i \mid \sum_{i=1}^{N+1} \lambda_i = 1 \text{ et } \forall i,\ \lambda_i \in \mathbb{R}^+, x_i \in \mathcal{E} \right\} \ .$$

Correction. Posons

$$\mathrm{C}_n(\mathcal{E}) := \left\{ \sum_{i=1}^{n} \lambda_i x_i \mid \sum_{i=1}^{n} \lambda_i = 1 \text{ et } \forall i,\ \lambda_i \in \mathbb{R}^+, x_i \in \mathcal{E} \right\}$$

et montrons que pour $n \geqslant N+2$, $\mathrm{C}_n(\mathcal{E}) \subset \mathrm{C}_{n-1}(\mathcal{E})$. Soit $n \geqslant N+2$ et soit $x = \sum_{i=1}^n \lambda_i x_i$. Comme la dimension de $\mathcal{V}$ est N, on peut trouver des réels μ_i non tous nuls et de somme nulle tels que $\sum_{i=1}^n \mu_i x_i = 0$. (On peut considérer une sous-famille libre maximale de $\{x_i\}$, soit par exemple $x_1, \ldots, x_N$. On écrit ensuite X_{N+1} et X_{N+2} comme combinaisons linéaires de ces derniers :

$$\alpha_1 x_1 + \cdots + \alpha_N x_N - X_{N+1} = 0 \quad \text{et} \quad \beta_1 x_1 + \cdots + \beta_N x_N - X_{N+2} = 0 \ .$$

Si la somme des coefficients d'une des deux est nulle, alors, il n'y a rien à faire. Sinon, en posant a et b ces deux sommes respectivement, on considère

$$b(\alpha_1 x_1 + \cdots + \alpha_N x_N - X_{N+1}) - a(\beta_1 x_1 + \cdots + \beta_N x_N - X_{N+2}) = 0$$

qui fait le job.) Pour tout réel $t \in \mathbb{R}$, on a $x = \sum_{i=1}^n (\lambda_i + t\mu_i) x_i$. Soit l'ensemble non vide $I := \{1 \leqslant i \leqslant n \mid \mu_i > 0\}$ et posons

$$t := \operatorname*{Min}_{i \in I} \frac{\lambda_i}{\mu_i} = \frac{\lambda_k}{\mu_k} \geq 0 \ ,$$

pour un certain $k \in I$. Par construction, tous les $\lambda_i + t\mu_i$ sont positifs et $\lambda_k + t\mu_k = 0$. De plus, on a

$$\sum_{i=1}^{n} \lambda_i + t\mu_i = \sum_{i=1}^{n} \lambda_i = 1 \ .$$

Soit au final,

$$\boxed{x = \sum_{\substack{i=1 \\ i \neq k}}^{n} (\lambda_i + t\mu_i) x_i} \ .$$

(6) En déduire que l'enveloppe convexe d'un compact de $\mathcal{V}$ est encore un compact.

CORRECTION. Le théorème de Carathéodory de la question précédente montre que l'enveloppe convexe d'un compact K de $\mathcal{V}$ est l'image de $H \times K^{N+1}$ par la fonction continue

$$(\lambda_1, \ldots, \lambda_{N+1}, x_1, \ldots, x_{N+1}) \mapsto \sum_{i=1}^{N+1} \lambda_i x_i \ ,$$

où

$$H := \left\{ (\lambda_1, \ldots, \lambda_{N+1}) \in (\mathbb{R}^+)^{N+1} \mid \sum_{i=1}^{N+1} \lambda_i = 1 \right\} \ .$$

Or H puis $H \times K^{N+1}$ sont des compacts, donc l'enveloppe convexe $\mathrm{Conv}(K)$ de K est encore compact.

On va maintenant pouvoir démontrer le résultat principal. Soit $\mathrm{G} \subset \mathrm{GL}_n(\mathbb{R})$ sous-groupe compact.

(7) Pour $A \in \mathrm{G}$ et pour $S \in \mathcal{S}_n(\mathbb{R})$, une matrice symétrique, on pose

$$\rho_A(S) := {}^tASA \ .$$

Montrer que ceci définit une application continue de la forme $\rho : \mathrm{G} \to \mathrm{GL}(\mathcal{V})$, où on précisera $\mathcal{V}$, telle que

$$\forall \ (A, B) \in \mathrm{G}^2, \ \rho(BA) = \rho(A) \circ \rho(B) \ .$$

CORRECTION. Posons l'espace vectoriel $\mathcal{V} := \mathcal{S}_n(\mathbb{R})$ (de dimension $N = \frac{n(n+1)}{2}$) et considérons l'application

$$\begin{cases} \rho \ : & \mathrm{G} \to \mathrm{GL}(\mathcal{V}) \\ & A \mapsto (S \mapsto {}^tASA) \ . \end{cases}$$

Pour tout $A \in \mathrm{G}$, on a bien que $\rho(A)$ est une application linéaire inversible (d'inverse $\rho(A^{-1})$). En tant que composée d'applications continues, l'application ρ est continue. Pour tout $(A, B) \in \mathrm{G}^2$ et pour tout $S \in \mathcal{S}_n(\mathbb{R})$, on a

$$\boxed{\rho(BA)(S) = {}^t(BA)SBA = {}^tA({}^tBSB)A = \rho(A) \circ \rho(B)(S)} \ .$$

(8) Conclure en considérant l'enveloppe convexe de l'ensemble $\{{}^tMM \mid M \in \mathrm{G}\}$.

CORRECTION. Posons $\mathcal{G} := \rho(\mathrm{G})$; il s'agit d'un sous-groupe compact de $\mathrm{GL}(\mathcal{V})$, par continuité de la fonction ρ. Comme G est compact, l'ensemble $\{{}^tMM \mid M \in \mathrm{G}\}$ est un compact de $\mathcal{V} = \mathcal{S}_n(\mathbb{R})$. La question (6) montre que son enveloppe convexe K est compact. Par construction, l'ensemble K est $\mathcal{G}$-stable car $\rho(A)(K) \subset K$ pour tout $A \in \mathrm{G}$. (En effet, $\rho(A)({}^tMM) = {}^t(AM)AM$ et on conclut par la linéarité de $\rho(A)$.) Le théorème de point fixe "global" de la question (4) montre qu'il existe un élément $S \in K$ fixé par tous les éléments de $\mathcal{G}$, c'est-à-dire

$$\forall A \in \mathrm{G}, \quad \rho(A)(S) = {}^tASA = S \ .$$

Il se trouve que l'ensemble $\{{}^tMM \mid M \in \mathrm{G}\}$ vit dans le convexe $\mathcal{S}_n^{++}(\mathbb{R})$, il en est donc de même de K, son enveloppe convexe. Donc S est dans $\mathcal{S}_n^{++}(\mathbb{R})$.
Au final, on a montré que tout élément $A \in \mathrm{G}$ est dans $\mathrm{O}(q_S)$, pour S symétrique définie positive.