ECOLE NORMALE SUPERIEURE PARIS SACLAY

CONCOURS D’ADMISSION 2022

VENDREDI 18 MARS 2022
13h00 - 18h00

CCM MATHEMATIQUES

MATHEMATIQUES

Durée : 5 heures

L’utilisation des calculatrices n’est pas autorisée pour cette épreuve

L'épreuve est constituée de deux problèmes indépendants, qui compteront chacun pour une part égale de la note globale. Il est sans doute très judicieux de répartir son temps à parts égales sur les deux problèmes qui peuvent être traiter dans l'ordre qui vous convient. Merci de veiller à ***traiter chaque problème sur une copie séparée****, en identifiant bien le problème auquel elle correspond.*

Le sujet comprend 5 pages.

- Problème A

Rappels et notations

- On appelle A un anneau unitaire commutatif intègre, dont l'unité est notée 1_A, et $\mathbb{K}$ un corps (tous les corps seront supposés commutatifs).
- On rappelle qu'un idéal $I \subset A$ est dit maximal si les seuls idéaux de A contenant I sont I et A (avec $I \neq A$). On rappelle qu'un élément $a \in A$ est dit irréductible s'il est non nul, non inversible et que pour toute décomposition $a = b_1 b_2$, l'un des b_i est inversible.
- La lettre p désignera toujours un nombre premier.

I : Préliminaires

(A.1) Soit I un idéal de A. Démontrer que A est un corps si ses seuls idéaux sont $\{0\}$ ou A, puis en déduire que A/I est un corps si et seulement si I est maximal.

(A.2) Pour P un élément de $\mathbb{K}[X]$, montrer que P est irréductible si et seulement si l'idéal (P) est maximal (où (P) est l'idéal engendré par P).

(A.3) Montrer que, sous réserve d'existence, $\min\{x \in \mathbb{N}^*; \varphi(x) = 0\}$ est premier, où $\varphi : \mathbb{Z} \to A$ est l'unique morphisme d'anneaux envoyant 1 sur 1_A. On appelle cet entier la caractéristique de A.

(A.4) Montrer que φ induit une injection de $\mathbb{Z}/\ker\varphi$ dans A puis montrer que si $A = \mathbb{K}$ est un corps, l'image de cette injection est le plus petit sous-corps de $\mathbb{K}$.

(A.5) Si un corps $\mathbb{K}$ est fini, montrer qu'il existe un nombre premier p et un entier naturel non nul n tel que le cardinal de $\mathbb{K}$ vaut p^n.
Indication : On pourra commencer par considérer le plus petit sous-corps de $\mathbb{K}$.

(A.6) On se place dans cette question sur $\mathbb{K} = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

- (a) Montrer que $X^2 + X + 1$ est le seul polynôme irréductible de degré 2.
- (b) Montrer que $P = X^3 + X + 1$ et $Q = X^4 + X + 1$ sont irréductibles.
- (c) En déduire des corps $\mathbb{F}_8$ et $\mathbb{F}_{16}$ à 8 et 16 éléments respectivement.

On admet dans la suite que pour tout entier q de la forme p^n avec p premier et $n \in \mathbb{N}^*$, il existe un corps $\mathbb{F}_q$ de cardinal q, unique à isomorphisme près, que l'on peut explicitement obtenir comme le quotient de $\mathbb{F}_p[X]$ par un idéal engendré par un polynôme irréductible. Le corps $\mathbb{F}_p$ s'injecte alors canoniquement dans chaque $\mathbb{F}_q$.

(A.7) On suppose dans cette question que A est de caractéristique p avec p premier. On appelle $Frob$ l'application de A dans A envoyant tout x sur x^p.

(a) Montrer que $Frob$ est un morphisme d'anneaux unitaires.

(b) Pour $A = \mathbb{F}_p$, montrer que $Frob$ est l'identité.

(c) Pour $A = \mathbb{F}_p[X]$, montrer que $Frob$ est linéaire et déterminer ses points fixes.

(d) Pour $A = \mathbb{F}_q$, montrer que l'ensemble des points fixes de $Frob$ est isomorphe à $\mathbb{F}_p$.

II : Irréductibilité de polynômes dans $\mathbb{F}_p[X]$

On fixe un polynôme unitaire $f = f_1^{\alpha_1} f_2^{\alpha_2} \dots f_r^{\alpha_r}$ dans $\mathbb{F}_p[X]$ de degré $n \geqslant 1$ (où les f_i sont irréductibles unitaires, distincts 2 à 2, et les α_i dans $\mathbb{N}^*$) et on souhaite tester s'il est irréductible ou non.

(A.8) (a) Montrer que si $f' \neq 0$, alors $f/pgcd(f, f') = \prod_{i \in I} f_i$ où I est un sous-ensemble de $\{1, \dots, r\}$.

(b) Montrer que si $f' = 0$, alors il existe un polynôme g tel que $f(X) = (g(X))^p$ (et donc dans ce cas f n'est pas irréductible).

Dans les questions suivantes, on suppose que les α_i sont tous égaux à 1 i.e. $f = f_1 \dots f_r$.

On pose $K_i = \mathbb{F}_p[X]/(f_i)$ et on appelle $\psi : \mathbb{F}_p[X]/(f) \to K_1 \times \dots \times K_r$ l'application envoyant $g \mod f$ sur $(g \mod f_1, \dots, g \mod f_r)$. On appelle $\varphi : \mathbb{F}_p[X]/(f) \to \mathbb{F}_p[X]/(f)$ l'application $Frob - id$.

(A.9) Montrer que l'application ψ est bien définie et est un isomorphisme d'anneaux.

(A.10) En déduire que $\ker \varphi$ est un espace vectoriel de dimension r.

(A.11) Pour $f = X^4 + X + 1$ dans $\mathbb{F}_2[X]$, prouver l'irréductibilité de f en calculant la matrice de φ relativement à la base des $(\overline{X^i})_{0 \leqslant i < n}$ de $\mathbb{F}_p[X]/(f)$.

(A.12) Pour $f = X^5 + X^4 + 1$ dans $\mathbb{F}_2[X]$, prouver que f n'est pas irréductible en calculant la matrice de φ.

- Problème B

Rappels et notations

On fixe dans toute la suite, n un entier strictement positif.

- On note $\|x\|$ la norme euclidienne canonique d'un vecteur x de $\mathbb{R}^n$.
- Pour $r > 0$ et x un point de $\mathbb{R}^n$, on note $B_r(x)$ la boule ouverte de rayon r centrée en x pour la norme euclidienne, et $\bar{B}_r(x)$ la boule fermée correspondante.
- Pour U ouvert de $\mathbb{R}^n$ et $f : U \to \mathbb{R}^d$ de classe au moins $\mathcal{C}^1$, on note $df_a : \mathbb{R}^n \to \mathbb{R}^d$ la différentielle de f en $a \in U$. Si df_a est bijective, on notera df_a^{-1} son inverse, c'est-à-dire l'application linéaire réciproque de df_a.
- Pour v dans $\mathbb{R}^n$, on note alors indifféremment $df_a(v)$ et $df_a \cdot v$ la dérivée directionnelle de f le long de v. On prendra également $df_a^{-1} \cdot v$ pour $df_a^{-1}(v)$.

Dans toute la suite, on considère une application $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ de classe $\mathcal{C}^2$ telle que :

i. Pour tout point x de $\mathbb{R}^n$, $d\varphi_x$ est inversible.

ii. $\lim\limits_{\|x\| \to +\infty} \|\varphi(x)\| = +\infty$.

Le but du problème est de montrer que φ est un difféomorphisme global de $\mathbb{R}^n$ dans $\mathbb{R}^n$.

Partie I

On montre dans cette partie que pour tout $y \in \mathbb{R}^n$, l'ensemble $\varphi^{-1}(\{y\})$ est fini non vide.

(B.1) Dans le cas $n = 1$, montrer, à l'aide de contre-exemples, des situations où φ n'est pas bijective lorsque une seule des deux conditions i. et ii. est vérifiée.

(B.2) Soit $f : \mathbb{R}^n \to \mathbb{R}^d$ continue. Montrer que les propriétés suivantes sont équivalentes :

- La pré-image par f d'un ensemble compact est un ensemble compact.
- $\lim\limits_{\|x\| \to +\infty} \|f(x)\| = +\infty$.

(B.3) Montrer que $\varphi(\mathbb{R}^n)$ est fermé.

(B.4) Montrer que $\varphi(\mathbb{R}^n)$ est ouverte.

(B.5) En déduire que φ est surjective.

(B.6) On considère un point $y \in \mathbb{R}^n$.

(a) Montrer que les éléments de $\varphi^{-1}(\{y\})$ sont isolés, c'est à dire que

$$\forall x \in \varphi^{-1}(\{y\}),\ \exists \varepsilon_x > 0 \text{ tel que } B_{\varepsilon_x}(x) \cap \varphi^{-1}(\{y\}) = \{x\}.$$

(b) En déduire que $\varphi^{-1}(\{y\})$ est un ensemble fini non vide.

Partie II

On note $\{p_1, \ldots, p_l\} = \varphi^{-1}(\{0\})$ avec $l \in \mathbb{N}^*$. On considère $F : \mathbb{R}^n \to \mathbb{R}^n$ définie par

$$F(x) = d\varphi_x^{-1} \cdot \varphi(x)\,.$$

(B.7) Fixons un point p dans $\mathbb{R}^n$. Montrer que le problème de Cauchy

$$\begin{cases} x(0) = p, \\ x'(t) = -F(x(t)),\ t \geqslant 0 \end{cases} \tag{1}$$

a une unique solution maximale $x_p : [0, b[\to \mathbb{R}^n$, avec $b \in [0, +\infty]$.

(B.8) (a) Montrer que pour tout temps $t \in [0, b[$,

$$\varphi(x_p(t)) = e^{-t}\varphi(p).$$

(b) En déduire que $b = +\infty$ et que $\lim_{t\to+\infty} \varphi(x_p(t)) = 0$.

(B.9) Montrer que pour tout $i = 1, \ldots, l$, il existe un voisinage V_i de p_i tel que :

- φ est un difféomorphisme de V_i sur un voisinage de 0.
- pour tout point p de V_i, on a

$$\lim_{t\to+\infty} x_p(t) = p_i.$$

Indication : On pourra montrer que pour tout p assez proche de p_i, et $t \geqslant 0$,

$$x_p(t) = \varphi^{-1}\left(e^{-t}\varphi(p)\right),$$

où φ^{-1} est la réciproque de la restriction de φ à V_i.

On note pour $i \in \{1, \cdots, l\}$,

$$W_i = \{p \in \mathbb{R}^n,\ x_p(t) \to p_i \text{ lorsque } t \to +\infty\},\ .$$

(B.10) (a) Montrer que pour tous $t, T \geqslant 0$, et pour tout $p \in \mathbb{R}^n$, on a

$$x_{x_p(T)}(t) = x_p(t+T).$$

(b) Soit p dans $\mathbb{R}^n$. Montrer qu'il existe $T \geqslant 0$ et $i \in \{1, \ldots, l\}$ tels que $x_p(T) \in V_i$, où V_i est défini à la question B.9.

(c) En déduire que $\mathbb{R}^n = \cup_{i=1}^{l} W_i$.

(B.11) (a) Soient $p \in \mathbb{R}^n$, $T > 0$ et $\delta > 0$. Montrer qu'il existe $\epsilon > 0$ tel que pour tout $q \in B_\epsilon(p)$ on a $\|x_p(t) - x_q(t)\| \leqslant \delta$ pour tout $t \in [0, T]$.

Indication : On pourra utiliser le lemme de Grönwall.

(b) Montrer que W_i est ouvert pour chaque $i \in \{1, \ldots, l\}$.

(c) En déduire que $l = 1$.

(B.12) Conclure.