Épreuve écrite d'analyse et probabilités

Le but du problème est de donner une preuve partielle du théorème de la variété stable.

Préliminaires et notations

Préliminaires généraux

Dans tout le problème, k désigne un entier strictement positif ; $\mathbb{R}$ est le corps des nombres réels, $\mathbb{C}$ celui des nombres complexes. Le complémentaire d'un sous-ensemble Y dans X est noté $X - Y$.

Si E et F sont des espaces vectoriels, $\mathcal{L}(E,\, F)$ désigne l'ensemble des applications linéaires de E dans F, $\mathrm{End}(E)$ l'ensemble des endomorphismes de E et $\mathrm{Aut}(E)$ celui des automorphismes de E. Le déterminant d'un endomorphisme A est noté $\det A$.

Dans $\mathbb{R}^k$, le produit scalaire canonique de deux vecteurs u et v est noté $< u, v >$.

Si f est un homéomorphisme d'un espace métrique $(X,\, d)$, on désigne par f^n la n-ième itérée de f. Si x est élément de X, la variété[1] stable pour f du point x est l'ensemble

$$W^s_x(f) = \big\{y \in X \;\big|\; \lim_{n\to\infty} d\big(f^n(x),\, f^n(y)\big) = 0\big\}.$$

De même, la variété instable pour f du point x est l'ensemble

$$W^u_x(f) = \big\{y \in X \;\big|\; \lim_{n\to\infty} d\big(f^{-n}(x),\, f^{-n}(y)\big) = 0\big\}.$$

Soit γ un réel strictement positif. On rappelle qu'une application f d'un espace métrique $(X,\, d)$ dans lui-même est lipschitzienne de rapport γ (ou γ-lipschitzienne) si

$$\forall (x, y) \in X^2,\quad d\big(f(y),\, f(x)\big) \leqslant \gamma\; d(x, y).$$

On note Li_γ l'ensemble des applications $f : \mathbb{R} \to \mathbb{R}$ γ-lipschitziennes s'annulant en 0.

Fonctions définies sur $\mathbb{R}^2$

Dans les parties 1, 4 et 5, $\mathbb{R}^2$ sera muni de la norme $|(x_1,\, x_2)| = \max\big\{|x_1|, |x_2|\big\}$.

Soit h une application bornée, élément de $C^1(\mathbb{R}^2,\, \mathbb{R})$ et dont la différentielle $\mathrm{d}h$ est bornée. On note :

- $|h|_\infty = \sup\limits_{x\in\mathbb{R}^2} |h(x)|$;
- $\mathrm{d}h_x$ la différentielle de h au point x $\big(\mathrm{d}h_x \in \mathcal{L}(\mathbb{R}^2,\, \mathbb{R})\big)$;
- $\|\mathrm{d}h_x\|$ la norme subordonnée dans $\mathcal{L}(\mathbb{R}^2,\, \mathbb{R})$ de $\mathrm{d}h_x$;
- $|\mathrm{d}h|_\infty = \sup\limits_{x\in\mathbb{R}^2} \|\mathrm{d}h_x\|$;

[1] **Dans ce problème, le mot variété est juste une notation.**

et on pose $|h|_{C^1} = \max(|h|_\infty, |\mathrm{d}h|_\infty)$.

Liens entre les différentes parties

- *la partie* 3 *utilise les résultats de la partie* 2 *;*
- *la partie* 4 *utilise les résultats des parties* 1 *et* 2 *;*
- *la partie* 5 *est indépendante du reste du problème.*

Les candidats peuvent admettre les résultats d'une question à condition de l'indiquer clairement et poursuivre le problème en respectant la numérotation des questions.

1. Introduction

1.1. Montrer que l'application $d_\gamma : (\varphi, \psi) \mapsto \sup_{x \in \mathbb{R}-\{0\}} \dfrac{|\psi(x) - \varphi(x)|}{|x|}$, définie sur $(Li_\gamma)^2$, est une distance.

1.2. Montrer que, pour la métrique définie par la distance d_γ, Li_γ est complet.

1.3. Soient $\mu > 0$, $h \in C^1(\mathbb{R}^2, \mathbb{R})$ et $\varphi \in Li_\gamma$ tels que $|h|_{C^1}(1+\gamma) < \mu$.
Montrer que l'application G_φ définie par

$$\forall x \in \mathbb{R},\ G_\varphi(x) = \mu x + h\big(x, \varphi(x)\big),$$

est strictement croissante. En déduire que G_φ un homéomorphisme de $\mathbb{R}$.

2. Partie linéaire

Soit A un endomorphisme de $\mathbb{R}^k$. Le rayon spectral $r(A)$ est par définition le maximum des modules des valeurs propres complexes de A.

2.1. Soit ε' un réel strictement positif. Justifier qu'il existe une base $\mathcal{B}$ de $\mathbb{C}^k$ dans laquelle la matrice

$$a = (a_{i,j})_{\substack{1 \leqslant i \leqslant k \\ 1 \leqslant j \leqslant k}}$$

de A est triangulaire supérieure et telle que pour tous i et j vérifiant $1 \leqslant i < j \leqslant k$, on ait $|a_{i,j}| \leqslant \varepsilon'$.

2.2. En déduire que pour tout réel ε strictement positif, il existe sur $\mathbb{R}^k$ une norme notée N dite ε-adaptée pour A, c'est-à-dire telle que pour la norme d'opérateur subordonnée $\|\cdot\|_N$:

$$\|A\|_N \leqslant r(A) + \varepsilon.$$

2.3. Montrer que, pour toute norme $\|\cdot\|$ sur $\mathbb{R}^k$ et tout réel ε strictement positif, il existe une constante C_ε strictement positive telle que, pour tout $v \in \mathbb{R}^k$ et tout $n \in \mathbb{N}^*$,

$$\|A^n v\| \leqslant C_\varepsilon (r(A) + \varepsilon)^n \|v\|.$$

On dira que $A \in \mathrm{End}(\mathbb{R}^k)$ est hyperbolique si toutes ses valeurs propres complexes ont un module différent de 1.

Dans toute la suite de cette partie, A désigne un endomorphisme hyperbolique de $\mathbb{R}^k$.

2.4. Montrer qu'il existe deux sous-espaces vectoriels supplémentaires E^+ et E^- de $\mathbb{R}^k$ stables par A tels que la restriction de A à E^+ (resp. E^-) ait toutes ses valeurs propres (dans $\mathbb{C}$) de module strictement supérieur (resp. inférieur) à 1.

On désigne par $A_{|E}$ la restriction de A au sous-espace E.

2.5. Montrer que $(A_{|E^+})$ est inversible.

2.6. Montrer qu'il existe une norme dite A-adaptée $\|\cdot\|$ telle que

$$\forall (x^+,\, x^-) \in E^+ \times E^-,\ \|x^+ + x^-\| = \max(\|x^+\|, \|x^-\|)$$

et de plus pour la norme subordonnée :

$$\|A_{|E^-}\| < 1 \quad \text{et} \quad \|(A_{|E^+})^{-1}\| < 1.$$

2.7. Montrer que, pour tout $v \in E^-$, la suite $(A^n(v))_{n\in\mathbb{N}}$ converge vers 0.

2.8. Montrer de même que, pour tout $v \in E^+$ non nul, la suite $\left(\|A^n(v)\|\right)_{n\in\mathbb{N}}$ tend vers $+\infty$.

Préliminaires pour les parties 3 et 4

Le tore $\mathbb{T}^k$ est par définition le groupe additif quotient du groupe $(\mathbb{R}^k, +)$ par le sous-groupe $(\mathbb{Z}^k, +)$. Tout élément x de $\mathbb{T}^k$ peut s'écrire de manière unique $x = (x_1, \ldots, x_k)$, avec $x_i \in \mathbb{T}^1$, pour $i = 1, \ldots, k$.
On définit la projection canonique $\Pi : \mathbb{R}^k \to \mathbb{R}^k/\mathbb{Z}^k = \mathbb{T}^k$.

3. Linéarité et topologie

On considére le sous-ensemble $E = \left\{L \in \mathrm{End}(\mathbb{R}^k) \;\middle|\; L(\mathbb{Z}^k) \subset \mathbb{Z}^k\right\}$ de $\mathrm{End}(\mathbb{R}^k)$ ainsi que le sous-ensemble $\mathcal{E} = \left\{L \in \mathrm{Aut}(\mathbb{R}^k) \;\middle|\; L \in E \text{ et } L^{-1} \in E\right\}$ de $\mathrm{Aut}(\mathbb{R}^k)$.

3.1. Montrer qu'un élément L de $\mathrm{End}(\mathbb{R}^k)$ appartient à E si, et seulement si, sa matrice dans la base canonique de $\mathbb{R}^k$ est à coefficients dans $\mathbb{Z}$.

3.2. Montrer qu'un élément L de E appartient à $\mathcal{E}$ si, et seulement si, $\det L$ vaut -1 ou 1.

3.3. Dans cette question, on se place dans $\mathbb{R}^2$ et on considère l'endomorphisme L défini, pour tout $(x,\, y) \in \mathbb{R}^2$, par $L(x,\, y) = (2x + y,\, x + y)$. Cet endomorphisme est-il hyperbolique ? Est-il dans l'ensemble $\mathcal{E}$?

Existe-t-il des exemples comparables sur $\mathbb{R}$?

Dans toute la suite de cette partie 3, L désigne un élément hyperbolique de $\mathcal{E}$. Les sous-espaces vectoriels E^+ et E^- sont deux sous-espaces vectoriels supplémentaires de $\mathbb{R}^k$ stables par L tels que la restriction de L à E^+ (resp. E^-) ait toutes ses valeurs propres (dans $\mathbb{C}$) de module strictement supérieur (resp. inférieur) à 1 ; l'existence de cette décomposition a été démontrée au 2.4.

On dit qu'un élément x de $[0,1]^k$ est un point périodique de L s'il existe un entier p strictement positif tel que $L^p(x)-x$ appartient à $\mathbb{Z}^k$. On désigne par Per$L$ l'ensemble des points périodiques de L.

3.4. Démontrer que l'ensemble des points périodiques de L est donné par

$$\mathrm{Per}L = \mathbb{Q}^k \cap [0,1]^k.$$

En déduire que Per$L$ est dense dans $[0,1]^k$.

3.5. Montrer que pour une distance donnant la topologie usuelle, les variétés stables et instables pour L d'un point a de $\mathbb{R}^k$ sont respectivement $W^s_a(L) = a + E^-$ et $W^u_a(L) = a + E^+$.

3.6. Soit N une norme sur $\mathbb{R}^k$. On définit une application d de $\mathbb{T}^k \times \mathbb{T}^k$ dans $\mathbb{R}$ en posant

$$d(y,\, y') = \inf\big\{N(x-x') \;\big|\; x,\, x' \in \mathbb{R}^k \text{ avec } \Pi(x) = y \text{ et } \Pi(x') = y'\big\}.$$

1. Montrer que $\inf\limits_{z\in\mathbb{Z}^k-\{0\}} N(z)$ est strictement positif.
2. Montrer que d définit une distance sur $\mathbb{T}^k$.
3. Prouver que l'application $\Pi : \mathbb{R}^k \to \mathbb{T}^k$ est continue.

Dans la suite, $\mathbb{T}^k$ est muni de la topologie associée à la distance d.

3.7. Montrer que L induit un homéomorphisme noté F_L du tore $\mathbb{T}^k$ satisfaisant la relation de commutation

$$F_L \circ \Pi = \Pi \circ L.$$

La suite de cette partie n'est pas utilisée dans le reste du problème.

3.8. On suppose que la distance d provient d'une norme N adaptée pour L. Montrer que :

1. $\Pi(0 + E^-) \subset W^s_0(F_L)$;
2. $\Pi(0 + E^+)$ est dense dans $\mathbb{T}^k$;
3. la variété stable pour F_L du point 0 est dense dans $\mathbb{T}^k$.

Une application continue $f : \mathbb{T}^k \to \mathbb{T}^k$ est dite topologiquement mélangeante si, pour toute paire d'ouverts non vides U et V de $\mathbb{T}^k$, il existe un entier n_0, tel que :

$$\forall n > n_0,\ f^n(U) \cap V \neq \varnothing.$$

3.9. Montrer qu'une isométrie de $\mathbb{T}^k$ n'est pas une application topologiquement mélangeante.

3.10. Montrer que F_L est une application topologiquement mélangeante.

Indication : *On pourra utiliser, outre le fait que 0 est un point fixe, la densité de la variété stable pour un automorphisme hyperbolique F_L du point 0 ainsi que la densité de la variété stable pour F_L^{-1} du point 0.*

4. Un exemple presque linéaire dans $\mathbb{R}^2$

Dans la partie 4, f est une application élément de $C^1(\mathbb{R}^2, \mathbb{R}^2)$, fixant l'origine et proche en C^1-topologie d'un automorphisme linéaire hyperbolique diagonal A défini, pour tout $(x, y) \in \mathbb{R}^2 \times \mathbb{R}^2$ par $A(x, y) = (\mu x, \lambda y)$ avec $0 < \lambda < 1 < \mu$. Ceci signifie que f est de la forme

$$f(x, y) = \big(\mu x + \alpha(x, y), \lambda y + \beta(x, y)\big)$$

avec α et β vérifiant $\alpha(0, 0) = 0$, $\beta(0, 0) = 0$ et il existe un réel δ, strictement positif, tel que $|\alpha|_{C^1} < \delta$ et $|\beta|_{C^1} < \delta$.

Dans la suite δ sera considéré comme petit, ce qui sera précisé par des inégalités.

4.1. Prouver que si $2\delta < \lambda$, f est un difféomorphisme de $\mathbb{R}^2$.

Indication : *On pourra montrer que pour tout $(x', y') \in \mathbb{R}^2$ l'application*

$$F_{(x',y')} : (x, y) \mapsto \left(\frac{x'}{\mu} - \frac{\alpha(x, y)}{\mu}, \frac{y'}{\lambda} - \frac{\beta(x, y)}{\lambda}\right)$$

est lipschitzienne de rapport a, avec $0 < a < 1$.

Inégalités (*)

Dans toute la suite de cette partie on suppose qu'il existe un nombre γ vérifiant les inégalités

$$(*) \begin{cases} 0 < \gamma < 1 \\ 0 < \delta < \dfrac{\gamma(\mu - \lambda)}{\gamma + 2} \end{cases}$$

Le graphe d'une application $\varphi : \mathbb{R} \to \mathbb{R}$ est la partie de $\mathbb{R}^2$ définie par

$$H\varphi = \big\{\big(x, \varphi(x)\big) \;\big|\; x \in \mathbb{R}\big\}.$$

Dans la suite, on considère l'application G_φ définie, pour tout x réel, par

$$G_\varphi(x) = \mu x + \alpha\big(x, \varphi(x)\big).$$

4.2. Montrer que si φ est élément de Li_γ il existe une fonction $\psi : \mathbb{R} \to \mathbb{R}$ telle que : $f(H\varphi) = H\psi$.

4.3. Montrer que $f_* : \varphi \mapsto \psi$, définie à la question précédente, est une application de Li_γ dans lui-même.

4.4. Prouver pour tous φ et φ' dans Li_γ et pour tout x dans $\mathbb{R}$, l'inégalité

$$\big|f_*(\varphi)\big(G_\varphi(x)\big) - f_*(\varphi')\big(G_\varphi(x)\big)\big| \leqslant \big(\lambda + \delta(1 + \gamma)\big)\big|\varphi'(x) - \varphi(x)\big|.$$

4.5. En déduire qu'il existe une application φ^+ dans Li_γ dont le graphe H_{φ^+} est invariant par f.

Prouver l'inégalité $\big|f\big(x, \varphi^+(x)\big)\big| \geqslant (\mu - \delta)\big|\big(x, \varphi^+(x)\big)\big|$.

4.6. Pourquoi, si $\gamma,\ \delta$ satisfont les inégalités (*) et si δ est suffisamment petit, peut-on dire que l'ensemble $\big\{\big(x,\, \varphi^+(x)\big) \ \big|\ x \in \mathbb{R}\big\}$ est contenu dans la variété instable pour f du point $(0,0)$?

Commentaires sur les variétés stables et instables

On prouverait avec les mêmes arguments l'existence d'une variété stable de l'origine qui est le "graphe vertical" d'une fonction lipschitzienne $\varphi^- \in Li_\gamma$ c'est-à-dire

$$W_0^s(f) = \big\{\big(\varphi^-(x),\, x\big) \ \big|\ x \in \mathbb{R}\big\}.$$

On pourrait aussi montrer que les variétés stables et instables sont en fait des graphes d'applications de classe C^1.

5. Différentiabilité des fonctions lipschitziennes

Soit $\varphi \in Li_\gamma$ et $x \in \mathbb{R}$; on introduit, pour $y \neq x$, $\quad \Delta_y\varphi = \dfrac{\big(y,\varphi(y)\big) - \big(x,\varphi(x)\big)}{\big|\big(y,\varphi(y)\big) - \big(x,\varphi(x)\big)\big|}$, on pose :

$$U_x\varphi = \big\{v \in \mathbb{R}^2 \ \big|\ \exists (x_n)_{n\in\mathbb{N}},\ \lim_{n\to\infty} x_n = x,\ \forall n \in \mathbb{N},\ x_n \neq x \text{ et } \lim_{n\to\infty} \Delta_{x_n}\varphi = v\big\}$$

et on définit l'ensemble tangent au graphe de φ au point x comme

$$T_x\varphi = \bigcup_{v\in U_x\varphi} \mathbb{R}v, \text{ avec } \mathbb{R}v = \{av \,|\, a \in \mathbb{R}\}.$$

5.1. Montrer que $\mathrm{pr}_1(T_x\varphi) = \mathbb{R}$ où pr_1 est la projection sur le premier facteur :

$$\text{pour } u = (u_1,u_2) \in \mathbb{R}^2,\ \mathrm{pr}_1(u) = u_1.$$

Indication : *On pourra remarquer que pour tout $y \neq x$, $|\Delta_y\varphi| = 1$.*

5.2. Le cône horizontal H^γ est l'ensemble $H^\gamma = \big\{(u_1,u_2) \in \mathbb{R}^2 \ \big|\ |u_2| \leqslant \gamma|u_1|\big\}$.
Montrer l'inclusion $T_x\varphi \subset H^\gamma$.

5.3. On considére la fonction continue sur $\mathbb{R}$ définie pour tout réel x non nul par

$$\phi(x) = \frac{x}{2} \cdot \sin\big(\ln|x|\big).$$

Appartient-elle à Li_γ pour un certain γ ? Expliciter $T_0\phi$.

5.4. On suppose que $\gamma \leqslant 1$. Montrer que, si $T_x\varphi$ est un sous-espace vectoriel de dimension 1 de $\mathbb{R}^2$, alors φ est dérivable en x.

Corrigé

1 Introduction

1. • d_γ est bien définie car le rapport est borné par 2γ, en remarquant que :
$$\frac{|\psi(x)-\varphi(x)|}{|x|}\leqslant\frac{|\varphi(x)-\varphi(0)|}{|x|}+\frac{|\psi(x)-\psi(0)|}{|x|}\leqslant 2\gamma.$$
   - Si $d_\gamma(\varphi,\psi)=0$, alors pour tout $x\in\mathbb{R}$, $\varphi(x)=\psi(x)$ donc $\varphi=\psi$.
   - La symétrie est évidente.
   - Si φ, ψ, θ sont trois éléments de Li_γ :
   $\forall x\in\ \mathbb{R}^*, \left|\frac{\theta(x)-\varphi(x)}{x}\right|\leqslant\left|\frac{\theta(x)-\psi(x)}{x}\right|+\left|\frac{\psi(x)-\varphi(x)}{x}\right|\leqslant d_\gamma(\theta,\psi)+d_\gamma(\psi,\varphi)$
   donc $d_\gamma(\theta,\varphi)\leqslant d_\gamma(\theta,\psi)+d_\gamma(\psi,\varphi)$.
   $\boxed{d_\gamma \text{ est une distance sur } Li_\gamma}$.
2. Soit $(\varphi_n)_{n\in\mathbb{N}}$ une suite de Cauchy de (Li_γ,d). Alors :
$$\forall\varepsilon>0,\exists N\in\ \mathbb{N},\forall n\geqslant p\geqslant N, d_\gamma(\varphi_n,\varphi_p)\leqslant\varepsilon. \tag{1}$$
   Pour $x\neq 0$ fixé, on a donc : $\forall n\geqslant p\geqslant N, |\varphi_n(x)-\varphi_p(x)|\leqslant\varepsilon\,|x|$.
   Ainsi, $(\varphi_n(x))_{n\in\mathbb{N}}$ est une suite de Cauchy de $\mathbb{R}$: elle converge vers une limite $\varphi(x)$.
   Comme φ_n appartient à Li_γ : $\forall n\in\mathbb{N},\varphi_n(0)=0$, donc $(\varphi_n(0))_{n\in\mathbb{N}}$ converge vers $\varphi(0)=0$ et $\forall(x,y)\in\ \mathbb{R}^2, |\varphi_n(x)-\varphi_n(y)|\leqslant\gamma\,|x-y|$ donc $|\varphi(x)-\varphi(y)|\leqslant\gamma\,|x-y|$.
   Ainsi, φ est encore élément de Li_γ.
   En passant à la limite lorsque n tend vers $+\infty$ dans (**??**) :
$$\forall x\in\ \mathbb{R}\setminus\{0\},\forall p\geqslant\ N, \left|\frac{\varphi(x)-\varphi_p(x)}{x}\right|\leqslant\varepsilon \text{ donc } \forall p\geqslant N, d_\gamma(\varphi_p,\varphi)\leqslant\varepsilon.$$
   Ainsi, la suite $(\varphi_n)_{n\in\mathbb{N}}$ converge vers φ dans (Li_γ,d_γ) : $\boxed{(Li_\gamma,d_\gamma) \text{ est complet}}$.
3. (a) Soit x, y des réels tels que $x<y$. Alors :
$$G_\varphi(y)-G_\varphi(x)=\mu(y-x)+h(y,\varphi(y))-h(x,\varphi(x)).$$
   On remarque que : $|\varphi(x)-\varphi(y)|\leqslant\gamma\,|x-y|$ donc $|(y,\varphi(y))-(x,\varphi(x))|\leqslant(1+\gamma)\,|x-y|$.
   D'après l'inégalité des accroissements finis :
$$|h(y,\varphi(y))-h(x,\varphi(x))|\leqslant|h|_{C^1}\,|(y,\varphi(y))-(x,\varphi(x))|\leqslant\ |h|_{C^1}\,(1+\gamma)\,|y-x|<\mu\,|y-x|$$
   donc $G_\varphi(y)-G_\varphi(x)>0$: $\boxed{G_\varphi \text{ est strictement croissante}}$.
   (b) G_φ est continue strictement croissante donc définit un homéomorphisme de $\mathbb{R}$ sur $\left]\lim\limits_{x\to-\infty}G_\varphi(x),\lim\limits_{x\to+\infty}G_\varphi(x)\right[$.
   Or, comme ci-dessus, pour $x>0$: $G_\varphi(x)-G_\varphi(0)\geqslant(\mu-(1+\gamma)\,|h|_{C^1})\,x\xrightarrow{x\to+\infty}+\infty$
   donc $\lim\limits_{x\to+\infty}G_\varphi(x)=+\infty$. De même, $\lim\limits_{x\to-\infty}G_\varphi(x)=-\infty$.
   Ainsi $\boxed{G_\varphi \text{ est un homéomorphisme de } \mathbb{R}}$.

2 Partie linéaire

1. Le polynôme caractéristique de A est scindé dans $\mathbb{C}$, donc il existe une base $\mathcal{B}' = (e'_i)_{1\leqslant i\leqslant k}$ de $\mathbb{C}^k$ dans laquelle la matrice de A prend la forme d'une réduite de Jordan.
   En prenant la base $\mathcal{B} = (e_i)_{1\leqslant i\leqslant k}$ définie par $e_i = \varepsilon'^{i-1}e'_i$, $i \in [|1,k|]$, on peut faire en sorte que cette réduite contienne des ε' au lieu de 1 au-dessus de la diagonale.
2. Soit $\varepsilon = \varepsilon'$, $\lambda_1, \ldots, \lambda_k$ les termes diagonaux de la matrice, N la norme infinie associée à la base $\mathcal{B}$. Alors $\|A\|_N \leqslant \max\{|\lambda_i| + \varepsilon', i \in [|1,k|]\} \leqslant r(A) + \varepsilon$.
   La restriction de N à $\mathbb{R}^k$ est alors encore une norme sur $\mathbb{R}^k$, qui vérifie toujours
   $$\boxed{\|A\|_N \leqslant r(A) + \varepsilon}.$$
   Deuxième méthode pour 2.1 et 2.2
   Notons $\lambda_1, \ldots, \lambda_k$ les valeurs propres complexes, éventuellement confondues, de A, rangées de façon à ce que :
   $$|\lambda_1| \leqslant |\lambda_2| \leqslant \ldots \leqslant |\lambda_k|.$$
   Comme le polynôme caractéristique est scindé sur $\mathbb{C}$, il existe une base $\mathcal{B} = (e_i)_{1\leqslant i\leqslant k}$ dans laquelle la matrice $(a_{i,j})_{1\leqslant i,j\leqslant k}$ de A est triangulaire supérieure.
   Soit $K = \max\{|a_{i,j}|\,; i\neq j\}$ et α un réel strictement positif tel que $0 < \dfrac{K}{\alpha - 1} \leqslant \varepsilon$.
   Soit, pour tout vecteur x de $\mathbb{C}^k$ de coordonnées $(x_i)_{1\leqslant i\leqslant k}$ dans $\mathcal{B}$: $N(x) = \max\left\{\left|\alpha^i x_i\right|\,; i \in [|1,k|]\right\}$.
   $A(x) = y$ est un vecteur de coordonnées $(y_i)_{1\leqslant i\leqslant k}$ dans $\mathcal{B}$ telles que :
   $$y_i = \lambda_i x_i + \sum_{j=i+1}^{k} a_{i,j}x_j$$
   donc $\left|\alpha^i y_i\right| \leqslant |\lambda_i|\left|\alpha^i x_i\right| + \displaystyle\sum_{j=i+1}^{k} K\frac{\alpha^i}{\alpha^j}\left|\alpha^j x_j\right|$ d'où
   $$\left|\alpha^i y_i\right| \leqslant r(A)N(x) + K\left(\sum_{j=i+1}^{k}\alpha^{i-j}\right)N(x) \leqslant r(A)N(x) + K\left(\sum_{j=1}^{k-i}\alpha^{-j}\right)N(x) \leqslant \left(r(A) + \frac{K}{\alpha-1}\right)N(x)$$
   et comme ceci est valable pour tout $i \in [|1,k|]$:
   $$N(y) \leqslant (r(A)+\varepsilon)N(x) \text{ donc } \|A\|_N \leqslant r(A) + \varepsilon$$
   en notant $\|\cdot\|_N$ la norme sur $\mathrm{End}(\mathbb{C}^k)$ subordonnée à la norme N sur $\mathbb{C}^k$.
   Il ne reste qu'à restreindre à $\mathbb{R}^k$.
3. Comme $\mathbb{R}^k$ est de dimension finie, $\|\cdot\|$ est équivalente à N.
   Il existe donc $\alpha > 0$ et $\beta > 0$ tels que :
   $$\forall v \in \mathbb{R}^k, \alpha N(v) \leqslant \|v\| \leqslant \beta N(v).$$
   Alors, pour tout $v \in \mathbb{R}^k$ et tout $n \in \mathbb{N}^*$:
   $$\|A^n v\| \leqslant \beta N(A^n v) \leqslant \beta \|A\|_N^n N(v) \leqslant \frac{\beta}{\alpha}(r(A)+\varepsilon)^n \|v\|.$$
   Ainsi : $\boxed{\forall v \in \mathbb{R}^k, \forall n \in \mathbb{N}^*, \|A^n v\| \leqslant C_\varepsilon (r(A)+\varepsilon)^n \|v\|}$ en posant $\boxed{C_\varepsilon = \dfrac{\beta}{\alpha}}$.

4. Soit P le polynôme caractéristique de A. Comme A est un endomorphisme de $\mathbb{R}^k$, il s'agit d'un polynôme à coefficients réels. P est scindé sur $\mathbb{C}$, et ses racines sont réelles ou complexes conjuguées deux à deux, de modules différents de 1. On peut donc décomposer P sous la forme $P = QR$, où Q (resp. R) n'a que des racines de module strictement supérieur (resp. inférieur) à 1. Comme les racines complexes non réelles sont conjuguées deux à deux, Q et R sont encore des polynômes à coefficients réels.
   Q et R sont premiers entre eux, donc le lemme des noyaux assure que :
   $$\mathrm{Ker}Q(A) \oplus \mathrm{Ker}R(A) = \mathrm{Ker}P(A) = \mathbb{R}^k.$$
   Soit $\boxed{E^+ = \mathrm{Ker}Q(A) \text{ et } E^- = \mathrm{Ker}R(A)}$.
   E^+ et E^- sont bien stables par A et supplémentaires dans $\mathbb{R}^k$.
   Les valeurs propres de $A_{|E^+}$ (resp. $A_{|E^-}$) sont les racines de Q (resp. R), donc sont de modules strictement supérieurs (resp. inférieurs) à 1.
5. Comme toutes les valeurs propres de $A_{|E^+}$ sont de module strictement supérieur à 1, 0 n'est pas valeur propre de $A_{|E^+}$ donc $\boxed{A_{|E^+} \text{ est inversible}}$.
6. Les valeurs propres de $A_{|E^+}^{-1}$ sont les inverses des valeurs propres de $A_{|E^+}$, donc sont toutes de module strictement inférieur à 1. Ainsi :
   $$r\left(A_{|E^+}^{-1}\right) < 1 \text{ et } r\left(A_{|E^-}\right) < 1.$$
   Soit $\varepsilon > 0$ tel que $r\left(A_{|E^+}^{-1}\right) + \varepsilon < 1$ et $r\left(A_{|E^-}\right) + \varepsilon < 1$.
   D'après 2.2, il existe sur E^+ et E^- des normes N_+ et N_- adaptées telles que, pour les normes subordonnées :
   $$\left\|A_{|E^+}^{-1}\right\| \leqslant r\left(A_{|E^+}^{-1}\right) + \varepsilon < 1 \text{ et } \left\|A_{|E^-}\right\| \leqslant r\left(A_{|E^-}\right) + \varepsilon < 1.$$
   La norme $\|\cdot\|$ définie sur $\mathbb{R}^k$ par :
   $\|x\| = \max\left(N_+(x^+), N_-(x^-)\right)$ si x admet la décomposition $x^+ + x^-$ dans $E^+ \oplus E^-$
   est alors bien une norme sur $\mathbb{R}^k$, et vérifie les conditions imposées.
7. On remarque que, pour tout $v \in E^-$:
   $$\|A^n(v)\| \leqslant \left\|A_{|E^-}\right\|^n \|v\| \xrightarrow{n\to+\infty} 0 \text{ car } \left\|A_{|E^-}\right\| < 1$$
   donc $\boxed{\text{la suite } (A^n(v))_{n\in\mathbb{N}} \text{ converge vers } 0}$.
8. Soit $v \in E^+ \setminus \{0\}$ et, pour tout $n \in \mathbb{N}$: $v_n = A^n(v)$.
   Alors $\|v\| = \left\|\left(A_{|E^+}^{-1}\right)^n (v_n)\right\| \leqslant \left\|A_{|E^+}^{-1}\right\|^n \|v_n\|$ donc $\|v_n\| \geqslant \dfrac{1}{\left\|A_{|E^+}^{-1}\right\|^n} \|v\|$.
   Comme $\left\|A_{|E^+}^{-1}\right\| < 1$, $\dfrac{1}{\left\|A_{|E^+}^{-1}\right\|^n}$ tend vers $+\infty$ et $\|v\|$ est non nulle, donc $\boxed{(\|A^n(v)\|)_{n\in\mathbb{N}} \text{ tend vers } +\infty}$.

3 Linéarité et topologie

1. Notons $\mathcal{B} = (e_i)_{1\leqslant i\leqslant k}$ la base canonique de $\mathbb{R}^k$.
   - Soit $L \in E$, ℓ sa matrice dans la base canonique. Chaque e_i est un élément de $\mathbb{Z}^k$, donc $L(e_i)$ appartient à $\mathbb{Z}^k$, donc les coefficients de la i-ème colonne de ℓ sont dans $\mathbb{Z}$.
     Ainsi, ℓ est à coefficients dans $\mathbb{Z}$.

- Réciproquement, soit $L \in \mathrm{End}(\mathbb{R}^k)$, dont la matrice ℓ dans la base canonique est à coefficients dans $\mathbb{Z}$. Alors, pour tout $x \in \mathbb{Z}^k$ de coordonnées $x_1, \ldots, x_k$ dans $\mathcal{B}$, $L(x)$ a pour coordonnées $y_1, \ldots, y_k$ dans $\mathcal{B}$ tels que :

$$\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} = \ell \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}.$$

Tous les coefficients y_i sont donc dans $\mathbb{Z}$: $L(\mathbb{Z}) \subset \mathbb{Z}$ et $L \in E$.

L appartient donc à E si et seulement si sa matrice dans la base canonique de $\mathbb{R}^k$ est à coefficients dans $\mathbb{Z}$.

2. Soit $L \in E$, ℓ sa matrice dans la base canonique de $\mathbb{R}^k$. L appartient à $\mathcal{E}$ si et seulement si L^{-1} appartient à E, i.e. si et seulement si ℓ^{-1} est à coefficients entiers.

Or $\ell^{-1} = \dfrac{1}{\det \ell}{}^t\mathrm{Com}\,(\ell)$ et $\mathrm{Com}\,(\ell)$ est à coefficients dans $\mathbb{Z}$ (car ses coefficients sont des déterminants à coefficients dans $\mathbb{Z}$).

Ainsi, si $\det \ell$ vaut $+1$ ou -1, ℓ^{-1} est à coefficients entiers, donc L appartient à $\mathcal{E}$.

Si L appartient à $\mathcal{E}$, ℓ et ℓ^{-1} sont à coefficients entiers, donc $\det \ell$ et $\det \ell^{-1}$ sont des entiers tels que :

$$1 = \det I_k = (\det \ell).(\det \ell^{-1}).$$

Ainsi, $\det \ell = \det L$ est égal à $+1$ ou -1.

$L \in E$ est donc un élément de $\mathcal{E}$ si et seulement si $\det L$ vaut $+1$ ou -1.

3. • La matrice de L dans la base canonique de $\mathbb{R}^k$ est : $\ell = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$.

Son polynôme caractéristique est :

$$P = (2-X)(1-X) - 1 = X^2 - 3X + 1 = \left(X - \frac{3+\sqrt{5}}{2}\right)\left(X - \frac{3-\sqrt{5}}{2}\right).$$

Les deux valeurs propres, $\dfrac{3+\sqrt{5}}{2}$ et $\dfrac{3-\sqrt{5}}{2}$, sont donc de module différent de 1 : L est hyperbolique.

- ℓ est à coefficients entiers et $\det \ell$ vaut 1, donc $L \in \mathcal{E}$.
- Sur $\mathbb{R}$, L ne peut être que de la forme $x \mapsto ax$, $a \in \mathbb{R}$.
Pour qu'il soit de déterminant $+1$ ou -1, il faudrait que a vaille $+1$ ou -1. Mais a est aussi l'unique valeur propre de L, donc L ne peut pas être hyperbolique dans ce cas. Il n'existe pas d'exemple comparable sur $\mathbb{R}$.

4. • Soit $x = (x_1, \ldots, x_k) \in \mathbb{Q}^k \cap [0,1]^k$.
En mettant tous les x_i au même dénominateur, il existe $q \in \mathbb{N}^*$ et $(p_1, \ldots, p_k) \in [|0, q|]^k$ tels que :

$$\forall i \in [|1, k|], x_i = \frac{p_i}{q}.$$

Soit $y = (p_1, \ldots, p_k)$ donc $x = \dfrac{1}{q} y$.

Comme $L(\mathbb{Z})$ est contenu dans $\mathbb{Z}$, $L^p(x)$ est, pour tout entier $p \in \mathbb{N}^*$, de la forme $z = \frac{1}{q}(z_1, \ldots, z_k)$, avec $z_i \in \mathbb{Z}$.

Le reste modulo q de z_i ne peut prendre que q valeurs (de 0 à $q-1$), donc les projetés par Π des $L^p(x)$, $p \in \mathbb{N}$, ne peuvent prendre que q^k valeurs distinctes. Ainsi, il existe deux entiers $i < j$ tels que :

$$\Pi\left(L^i(x)\right) = \Pi\left(L^j(x)\right) \text{ donc } L^j(x) - L^i(x) \in \mathbb{Z}^k.$$

De plus $L^{-1}(\mathbb{Z}) \subset \mathbb{Z}$ donc $L^{j-i}(x) - x = L^{-i}\left(L^j(x) - L^i(x)\right) \in \mathbb{Z}^k$
ce qui montre que x est périodique.

- Réciproquement, soit $x \in \operatorname{Per} L$.
Il existe $p \in \mathbb{N}^*$ tel que $L^p(x) - x = y$ soit élément de $\mathbb{Z}^k$.
L est hyperbolique, donc n'a aucune valeur propre de module 1 ; ainsi $L^p - Id_{\mathbb{R}^k}$ est inversible et :

$$x = \left(L^p - Id_{\mathbb{R}^k}\right)^{-1}(y).$$

De plus, la matrice ℓ de L dans la base canonique de $\mathbb{R}^k$ est à coefficients entiers, donc la matrice $\frac{1}{\det(\ell^p - I_k)}{}^t\mathrm{Com}\,(\ell^p - I_k)$ de $\left(L^p - Id_{\mathbb{R}^k}\right)^{-1}$ est à coefficients rationnels, et comme y est à coordonnées entières, x est à coordonnées rationnelles : $x \in \mathbb{Q}^k \cap [0,1]^k$.

Ainsi $\boxed{\operatorname{Per} L = \mathbb{Q}^k \cap [0,1]^k}$ et comme $\mathbb{Q} \cap [0,1]$ est dense dans $[0,1]$, $\boxed{\operatorname{Per} L \text{ est dense dans } [0,1]^k}$.

5. Comme toutes les normes sont équivalentes, on peut choisir une norme quelconque, et cela donnera la topologie usuelle. On prend donc une norme L-adaptée $\|\cdot\|$ comme en 2.6.
Soit $x \in \mathbb{R}^k$. Comme $\mathbb{R}^k = E^+ \oplus E^-$, il existe $(x^+, x^-) \in E^+ \times E^-$ tel que :

$$x - a = x^+ + x^-.$$

Alors : $\forall n \in \mathbb{N}, L^n(x) - L^n(a) = L^n(x-a) = L^n(x^+) + L^n(x^-)$.
On sait (cf. 2.7 et 2.8) que, lorsque n tend vers $+\infty$, $L^n(x^-)$ tend vers 0 et $\left\|L^n(x^+)\right\|$ tend vers $+\infty$ si x^+ est non nul.
Ainsi, x appartient à W_a^s si et seulement si x^+ est nul, i.e. si et seulement si $x-a$ appartient à E^- : $\boxed{W_a^s = a + E^-}$.
On remarque que, par définition, la variété instable de a pour L est la variété stable de a pour L^{-1}. Passer de L à L^{-1} revient à échanger E^+ et E^- donc $\boxed{W_a^u = a + E^+}$.

6. (a) Soit $z_0 = (1, 0, \ldots, 0)$, $\alpha = N(z_0)$ et $\eta = \inf_{z \in \mathbb{Z}^k \setminus \{0\}} N(z)$.
Comme N est une norme, α est non nul.
Soit $B = \left\{z \in \mathbb{R}^k \mid N(z) \leqslant \alpha\right\}$: B est un compact de $\mathbb{R}^k$.
Par définition $\eta = \inf\left\{N(z); z \in B \cap \left(\mathbb{Z}^k \setminus \{0\}\right)\right\}$. $B \cap \left(\mathbb{Z}^k \setminus \{0\}\right)$ est un fermé dans B, donc un compact de $\mathbb{R}^k$.
N, qui est une application continue sur $\mathbb{R}^k$, atteint ses bornes sur ce compact.
En particulier, η est atteint en un point non nul, donc

$$\boxed{\eta = \inf_{z \in \mathbb{Z}^k \setminus \{0\}} N(z) \text{ est strictement positif}}.$$

(b) • d est bien une application à valeurs positives.
• Soit $(y, y') \in (\mathbb{T}^k)^2$ tel que $d(y, y') = 0$.
Si x et x' sont des représentants dans $\mathbb{R}^k$ de y et y' respectivement, $x - x'$ appartient à $\mathbb{Z}^k$.
$d(y, y') = 0$ impose qu'il existe des représentants x et x' tels que $x - x' = 0$ donc $y = y'$.
• La définition de d est visiblement symétrique.
• On remarque que d peut aussi être définie par :

$$d(y, y') = \inf \left\{ N(z) \mid z \in \mathbb{R}^k \text{ et } \Pi(z) = y - y' \right\}.$$

Soit y, y', y'' des éléments de $\mathbb{T}^k$. Alors, pour tous représentants x_1 et x_2 de $y - y'$ et $y' - y''$ respectivement, $x_1 + x_2$ est un représentant de $y - y''$ et :

$$d(y, y'') \leqslant N(x_1 + x_2) \leqslant N(x_1) + N(x_2).$$

Pour tout x_2 représentant de $y' - y''$:
$N(x_2) \geqslant d(y, y'') - N(x_1)$ donc $d(y', y'') \geqslant d(y, y'') - N(x_1)$
puis, pour tout x_1 représentant de $y - y'$:
$N(x_1) \geqslant d(y, y'') - d(y', y'')$ donc $d(y, y') \geqslant d(y, y'') - d(y', y'')$.
Finalement : $d(y, y'') \leqslant d(y, y') + d(y', y'')$ et $\boxed{d \text{ est une distance sur } \mathbb{T}^k}$.

(c) Soit $(x, x') \in (\mathbb{R}^k)^2$, $y = \Pi(x)$, $y' = \Pi(x')$. Par définition :
$d(y, y') \leqslant N(x - x')$ donc $d(\Pi(x), \Pi(x')) \leqslant N(x - x')$.
$\boxed{\Pi \text{ est 1-lipschitzienne donc continue}}$.

7. • Soit $y \in \mathbb{T}^k$, x et x' deux représentants de y dans $\mathbb{R}^k$. Alors $x - x'$ appartient à $\mathbb{Z}^k$ donc $L(x - x') = L(x) - L(x')$ appartient à $\mathbb{Z}^k$: L induit bien une application Π_L sur $\mathbb{T}^k$.
• Par construction de F_L : $F_L(\Pi(x)) = F_L(y) = \Pi(L(x))$ donc $F_L \circ \Pi = \Pi \circ L$.
• Soit $y \in \mathbb{T}^k$, $(y_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{T}^k$ tendant vers y.
Par définition de d, il existe un représentant x de y et une suite de représentants x_n de y_n tels que $(x_n)_{n\in\mathbb{N}}$ converge vers x dans $\mathbb{R}^k$ pour N.
Comme L est continue, $(L(x_n))_{n\in\mathbb{N}}$ converge vers $L(x)$ dans $\mathbb{R}^k$, donc $(\Pi(L(x_n)) = F_L(y_n))_{n\in\mathbb{N}}$ converge vers $\Pi(L(x)) = F_L(y)$. Ainsi, F_L est continu.
• Enfin, pour tout $y \in \mathbb{T}^k$ de représentant x dans $\mathbb{R}^k$:

$$F_{L^{-1}}(F_L(y)) = F_{L^{-1}}(\Pi(L(x))) = \Pi\left(L^{-1}(L(x))\right) = \Pi(x) = y$$

et de même pour $F_L \circ F_{L^{-1}}$, donc F_L est bijective, de réciproque $F_{L^{-1}}$ également continue.
$\boxed{F_L \text{ est un homéomorphisme.}}$

8. (a) Soit $y \in \Pi(0 + E^-)$ et $x \in E^-$ tel que $y = \Pi(x)$.
On sait que $(L^n(x))_{n\in\mathbb{N}}$ tend vers 0, donc $(F_L^n(y))_{n\in\mathbb{N}}$ tend vers 0 dans $\mathbb{T}^k$, i.e. $d(F_L^n(y), F_L^n(0))$ tend vers 0 lorsque n tend vers $+\infty$: y appartient à $W^s(0)$.

(b) Soit $y \in \mathbb{T}^k$ et $x \in [0, 1]^k$ tel que $y = \Pi(x)$; soit $\varepsilon > 0$.
Comme $\operatorname{Per} L$ est dense dans $[0, 1]^k$, il existe $x_0 \in \operatorname{Per} L$ tel que :

$$N(x - x_0) \leqslant \frac{\varepsilon}{2} \text{ donc } d(y, y_0) \leqslant \frac{\varepsilon}{2} \text{ en posant } y_0 = \Pi(x_0).$$

Comme $\mathbb{R}^k = E^+ \oplus E^-$, il existe $(x^+, x^-) \in E^+ \times E^-$ tel que : $x_0 = x^+ + x^-$.
Puisque x_0 est périodique, il existe $p \in \mathbb{N}^*$ tel que $L^p(x_0) - x_0$ soit dans $\mathbb{Z}^k$.
Alors $F_L^p(y_0) = y_0$ donc, pour tout $n \in \mathbb{N}$: $y_0 = F_L^{np}(y_0) = \Pi\left(L^{np}(x^+)\right) + \Pi\left(L^{np}(x^-)\right)$.

Comme $(L^{np}(x^-))_{n\in\mathbb{N}}$ tend vers 0, $\left(z_n = \Pi\left(L^{np}(x^+)\right)\right)_{n\in\mathbb{N}}$ est une suite de points de $\Pi(0+E^+)$ qui converge vers y_0.

Pour n suffisamment grand : $d(y_0,z_n)\leqslant\dfrac{\varepsilon}{2}$ donc $d(y,z_n)\leqslant\varepsilon$.

Ainsi, $\boxed{\Pi(0+E^+) \text{ est dense dans } \mathbb{T}^k}$.

(c) En appliquant le résultat précédent à L^{-1}, on obtient que $\Pi(0+E^-)$ est dense dans $\mathbb{T}^k$ et donc que $\boxed{W^s(0) \text{ est dense dans } \mathbb{T}^k}$.

Grâce à $F_{L^{-1}}$ toujours, on en déduit que la variété instable de 0 est également dense dans $\mathbb{T}^k$.

9. Soit f une isométrie de $\mathbb{T}^k$, supposée topologiquement mélangeante.

Soit x et y deux points distincts de $\mathbb{T}^k$, $\varepsilon = \dfrac{d(x,y)}{5} > 0$.

Soit $z\in\mathbb{T}^k$, V la boule ouverte de centre z de rayon ε, U_1 (resp. U_2) la boule ouverte de centre x (resp. y) de rayon ε.

Comme f est mélangeante, il existe $N\in\mathbb{N}$ tel que :

$$\forall n\geqslant N, f^n(U_1)\cap V\neq\varnothing \text{ et } f^n(U_2)\cap V\neq\varnothing.$$

Soit donc $z_1\in f^n(U_1)\cap V$ et $z_2\in f^n(U_2)\cap V$.

Il doit exister $t_1\in U_1$ et $t_2\in U_2$ tels que $z_1=f^n(t_1)$ et $z_2=f^n(t_2)$.

Comme f est une isométrie, $d(t_1,t_2)=d(z_1,z_2)$ et V est de diamètre 2ε donc :

$$d(x,y)\leqslant d(x,t_1)+d(z_1,z_2)+d(t_2,y)\leqslant 4\varepsilon$$

ce qui est absurde. Ainsi, $\boxed{\text{une isométrie de } \mathbb{T}^k \text{ n'est pas mélangeante}}$.

10. Soit U et V deux ouverts non vides de $\mathbb{T}^k$. Soit $x\in U$, $z\in V$, $\varepsilon>0$ tel que la boule ouverte de centre z de rayon ε soit contenue dans V.

$\Pi(0+E^+)$ est dense dans $\mathbb{T}^k$, donc il existe z_0 dans $\Pi(0+E^+)\cap B(z,\varepsilon)$.

Soit, pour tout $n\in\mathbb{N}$, $u_n = F_L^{-n}(z_0)$: $(u_n)_{n\in\mathbb{N}}$ tend vers 0.

$\Pi(0+E^-)$ est dense dans $\mathbb{T}^k$, donc il existe t dans $\Pi(0+E^-)\cap U$.

Soit alors $v_n = t+u_n$. Comme U est ouvert, v_n appartient à U pour n suffisamment grand, et $F_L^n(v_n)=F_L^n(t)+z_0$ tend vers z_0 lorsque n tend vers $+\infty$.

Pour n suffisamment grand, $F_L^n(v_n)$ appartient donc à $F_L^n(U)\cap V$. $\boxed{F_L \text{ est mélangeante}}$.

4 Un exemple presque linéaire dans $\mathbb{R}^2$

1. Soit (x',y'), (u,v), (u',v') des éléments de $\mathbb{R}^2$. On a :

$$F_{(x',y')}(u',v') - F_{(x',y')}(u,v) = \left(\frac{\alpha(u,v)-\alpha(u',v')}{\mu}, \frac{\beta(u,v)-\beta(u',v')}{\lambda}\right).$$

L'inégalité des accroissements finis donne : $\begin{cases} |\alpha(u,v)-\alpha(u',v')|\leqslant\delta\,|(u,v)-(u',v')| \\ |\beta(u,v)-\beta(u',v')|\leqslant\delta\,|(u,v)-(u',v')| \end{cases}$

donc $\left|F_{(x',y')}(u',v') - F_{(x',y')}(u,v)\right|\leqslant\dfrac{\delta}{\lambda}\,|(u,v)-(u',v')|$.

$F_{(x',y')}$ est donc lipschitzienne de rapport $a=\dfrac{\delta}{\lambda}<1$.

Comme application contractante dans $\mathbb{R}^2$ complet, $F_{(x',y')}$ admet un unique point fixe (u,v), solution de :

$$(u,v)=\left(\frac{x'-\alpha(u,v)}{\mu},\frac{y'-\beta(u,v)}{\lambda}\right), \text{ i.e. de } (x',y')=f(u,v).$$

Ceci étant valable pour tout couple (x',y') de $\mathbb{R}^2$, f est bijective (existence et unicité du point fixe, i.e. de l'antécédent).
f est $\mathcal{C}^1$ comme composée d'applications $\mathcal{C}^1$.
Sa différentielle en (x,y) a pour matrice, dans la base canonique de $\mathbb{R}^2$:

$$M=\begin{pmatrix}\mu+\dfrac{\partial\alpha}{\partial x}(x,y) & \dfrac{\partial\alpha}{\partial y}(x,y)\\ \dfrac{\partial\beta}{\partial x}(x,y) & \lambda+\dfrac{\partial\beta}{\partial y}(x,y)\end{pmatrix}.$$

Son jacobien est donc :

$$J(x,y)=\left(\mu+\frac{\partial\alpha}{\partial x}(x,y)\right)\left(\lambda+\frac{\partial\beta}{\partial y}(x,y)\right)-\frac{\partial\alpha}{\partial y}(x,y)\frac{\partial\beta}{\partial x}(x,y)\geqslant(\mu-\delta)(\lambda-\delta)-\delta^2$$

car toutes les dérivées partielles sont bornées par δ.
De plus : $\delta<\dfrac{\lambda}{2}<\dfrac{\mu}{2}$ donc $J(x,y)\geqslant\dfrac{\mu}{2}\dfrac{\lambda}{2}-\left(\dfrac{\lambda}{2}\right)^2>0$.
Ainsi, f définit (localement ou globalement au choix vu qu'on a déjà l'injectivité) un $\mathcal{C}^1$ difféomorphisme, et comme on sait déjà que f est bijective, $\boxed{f \text{ est un } \mathcal{C}^1\text{-difféomorphisme de } \mathbb{R}^2}$.

2. On cherche ψ telle que : $\forall x\in\mathbb{R},\exists x'\in\mathbb{R},(\mu x+\alpha(x,\varphi(x)),\lambda\varphi(x)+\beta(x,\varphi(x))=(x',\psi(x')))$
ce qui est équivalent à : $\forall x\in\mathbb{R},\psi(G_\varphi(x))=\lambda\varphi(x)+\beta(x,\varphi(x))$.
(*) assure que $\delta(1+\gamma)<\mu$ donc, d'après 1.3, G_φ est un homéomorphisme de $\mathbb{R}$; il suffit de prendre l'application ψ définie par :
$$\boxed{\forall x\in\mathbb{R},\psi(x)=\lambda\varphi\left(G_\varphi^{-1}(x)\right)+\beta\left(G_\varphi^{-1}(x),\varphi\left(G_\varphi^{-1}(x)\right)\right)}.$$

3. $G_\varphi(0)=0$ donc $G_\varphi^{-1}(0)=0$ et $\psi(0)=0$.
Soit y, y' dans $\mathbb{R}$, $x=G_\varphi^{-1}(y)$ et $x'=G_\varphi^{-1}(y')$.
Comme φ est γ-lipschitzienne : $|\varphi(x)-\varphi(x')|\leqslant\gamma|x-x'|$
et $\gamma<1$ donc $|(x,\varphi(x))-(x',\varphi(x'))|=|x-x'|$.
D'après l'inégalité des accroissements finis :

$$|G_\varphi(x)-G_\varphi(x')|\geqslant\mu|x-x'|-\delta|(x,\varphi(x))-(x',\varphi(x'))|\geqslant(\mu-\delta)|x-x'|.$$

Alors $|\psi(y)-\psi(y')|\leqslant\lambda|\varphi(x)-\varphi(x')|+|\beta(x,\varphi(x))-\beta(x,\varphi(x'))|\leqslant(\lambda\gamma+\delta)|x-x'|\leqslant\dfrac{\lambda\gamma+\delta}{\mu-\delta}|y-y'|$.
Or : $\dfrac{\lambda\gamma+\delta}{\mu-\delta}\leqslant\gamma\Leftrightarrow\delta\leqslant\dfrac{(\mu-\lambda)\gamma}{1+\gamma}$ ce qui est bien vérifié ici.
Ainsi ψ est γ-lipschitzienne et $\boxed{f_* \text{ est bien une application de } Li_\gamma \text{ dans lui-même}}$.

4. Soit $x\in\mathbb{R}$, $y=G_\varphi(x)$, $y'=G_{\varphi'}(x)$, $\psi=f_*(\varphi)$ et $\psi'=f_*(\varphi')$. Alors :
$|f_*(\varphi)(G_\varphi(x))-f_*(\varphi')(G_\varphi(x))|=|\psi(y)-\psi'(y)|\leqslant|\psi(y)-\psi'(y')|+|\psi'(y')-\psi'(y)|$.
Comme ψ' est γ-lipschitzienne : $|\psi'(y')-\psi'(y)|\leqslant\gamma|y'-y|$
et $|y'-y|=|\alpha(x,\varphi'(x))-\alpha(x,\varphi(x))|\leqslant\delta|\varphi(x)-\varphi'(x)|$.
On a : $\psi(y)=\lambda\varphi(x)+\beta(x,\varphi(x))$ et $\psi'(y')=\lambda\varphi'(x)+\beta(x,\varphi'(x))$
donc $|\psi(y)-\psi'(y')|\leqslant\lambda|\varphi(x)-\varphi'(x)|+\delta|\varphi(x)-\varphi'(x)|$.
Ainsi : $\boxed{|f_*(\varphi)(G_\varphi(x))-f_*(\varphi')(G_\varphi(x))|\leqslant(\lambda+\delta+\gamma\delta)|\varphi(x)-\varphi'(x)|}$.

5. Lorsque x décrit $\mathbb{R}^*$, $G_\varphi(x)$ décrit également $\mathbb{R}^*$. Ainsi :

$$d_\gamma\left(f_*(\varphi), f_*(\varphi')\right) = \sup_{x\neq 0}\left|\frac{f_*(\varphi)(G_\varphi(x)) - f_*(\varphi')(G_\varphi(x))}{G_\varphi(x)}\right|.$$

Or, pour tout $x \in \mathbb{R}$: $|G_\varphi(x)| \geqslant (\mu-\delta)\,|x|$
donc $\dfrac{|f_*(\varphi)(G_\varphi(x)) - f_*(\varphi')(G_\varphi(x))|}{|G_\varphi(x)|} \leqslant \dfrac{\lambda+\delta(1+\gamma)}{\mu-\delta}\left|\dfrac{\varphi'(x)-\varphi(x)}{x}\right|$.
Ainsi : $d_\gamma\left(f_*(\varphi), f_*(\varphi')\right) \leqslant \dfrac{\lambda+\delta(1+\gamma)}{\mu-\delta} d_\gamma(\varphi,\varphi')$.
Or : $\dfrac{\lambda+\delta(1+\gamma)}{\mu-\delta} < 1 \Leftrightarrow \delta < \dfrac{\mu-\lambda}{2+\gamma}$ ce qui est bien le cas ici.
f_* est donc une application contractante dans l'espace complet (Li_γ, d_γ) : elle admet un unique point fixe φ^+, qui est une application dont **le graphe horizontal est invariant par f**.

6. φ^+ appartient à Li_γ donc $\left|\varphi^+(x)\right| \leqslant \gamma\,|x|$ d'où, puisque $\gamma < 1$: $\left|\left(x,\varphi^+(x)\right)\right| = |x|$.
De plus, $\left|f(x,\varphi^+(x))\right| \geqslant \left|\mu x + \alpha(x,\varphi^+(x))\right|$ (c'est le maximum des deux coordonnées donc supérieur à la première)
et $\left|\alpha(x,\varphi^+(x))\right| \leqslant \delta\left|\left(x,\varphi^+(x)\right)\right| \leqslant \delta\,|x|$ donc $\boxed{\left|f(x,\varphi^+(x))\right| \geqslant (\mu-\delta)\,|x| = (\mu-\delta)\left|(x,\varphi^+(x))\right|}$.

7. Pour δ suffisamment petit, $\mu - \delta > 1$.
Soit $x \in \mathbb{R}$. Comme le graphe horizontal de φ^+ est stable par f, $f(x,\varphi^+(x))$ est encore un élément de H_{φ^+} donc 4.6 donne par récurrence :

$$\forall n \in \mathbb{N}, \left|f^n(x,\varphi^+(x))\right| \geqslant (\mu-\delta)^n\left|(x,\varphi^+(x))\right|.$$

Comme f est bijective, ceci donne aussi, en l'appliquant à $f^{-n}(x,\varphi^+(x))$ qui est toujours un élément du graphe horizontal de φ^+ :

$$\forall n \in \mathbb{N}, \left|f^{-n}(x,\varphi^+(x))\right| \leqslant (\mu-\delta)^{-n}\left|(x,\varphi^+(x))\right|$$

qui tend vers 0 lorsque n tend vers $+\infty$ donc $\boxed{(x,\varphi^+(x)) \text{ est dans la variété instable de } (0,0)}$.

5 Différentiabilité des fonctions lipschitziennes

1. On prend $x_n = x + 2^{-n}$ donc $\Delta_{x_n}\varphi = \dfrac{(2^{-n}, \varphi(x+2^{-n}) - \varphi(x))}{|(2^{-n}, \varphi(x+2^{-n}) - \varphi(x))|}$.
$\Delta_{x_n}\varphi$ est de norme 1 par construction ; cette suite bornée admet une sous-suite convergente, et quitte à ne garder que la sous-suite, il existe donc $v \in \mathbb{R}^2$ tel que $\lim\limits_{n\to+\infty} \Delta_{x_n}\varphi = v$.
Comme φ est γ-lipschitzienne : $\left|\varphi(x+2^{-n}) - \varphi(x)\right| \leqslant \gamma 2^{-n}$
donc $2^{-n} \leqslant |(x_n,\varphi(x_n)) - (x,\varphi(x))| \leqslant \alpha 2^{-n}$ où $\alpha = \max(1,\gamma)$.
Ainsi la première coordonnée de $\Delta_{x_n}\varphi$ est comprise entre $\dfrac{1}{\alpha}$ et 1, mais ne peut pas tendre vers 0 : $pr_1(v)$ est non nul. Alors $pr_1(T_x\varphi)$ contient au moins $pr_1(\mathbb{R}v) = \mathbb{R}$ et c'est contenu dans $\mathbb{R}$ par construction donc : $\boxed{pr_1(T_x\varphi) = \mathbb{R}}$.

2. On note pr_2 la projection sur la deuxième coordonnée.
Pour tout (x,y) : $|\varphi(y)-\varphi(x)| \leqslant \gamma\,|x-y|$ donc pour toute suite $(x_n)_{n\in\mathbb{N}}$ de limite x telle que $\Delta_{x_n}\varphi$ ait une limite v :

$$|pr_2(\Delta_{x_n}\varphi)| \leqslant \gamma\,|pr_1(\Delta_{x_n}\varphi)|$$

donc, à la limite, v est élément de H^γ : $\boxed{T_x\varphi \subset H^\gamma}$.

3. ϕ peut être prolongée par continuité en 0 par $\phi(0)=0$.
ϕ est dérivable sur $\mathbb{R}^*$. Par parité, on peut limiter l'étude à $\mathbb{R}^+$. On a :

$$\phi'(x) = \frac{1}{2}\sin(\ln x) + \frac{1}{2}\cos(\ln x) = \frac{\sqrt{2}}{2}\sin(\ln x + \frac{\pi}{4})$$

donc ϕ' est bornée par $\dfrac{\sqrt{2}}{2}$.

D'après l'inégalité des accroissement finis, $\boxed{\phi \text{ est dans } Li_\gamma \text{ pour } \gamma = \dfrac{\sqrt{2}}{2}}$.

Soit $(x_n)_{n\in\mathbb{N}}$ une suite convergente vers 0 :

$$\Delta_{x_n}\phi = \frac{\left(x_n, \dfrac{x_n}{2}\sin(\ln|x_n|)\right)}{\left|\left(x_n, \dfrac{x_n}{2}\sin(\ln|x_n|)\right)\right|}.$$

Comme $\left|\dfrac{x_n}{2}\sin(\ln|x_n|)\right| \leqslant |x_n|$, la norme du dénominateur est $|x_n|$ et :

$$\Delta_{x_n}\phi = \pm(1, \frac{1}{2}\sin(\ln|x_n|)).$$

La limite si elle existe est donc dans $H^{1/2}$.
Pour tout $(u,v) \in H^{1/2}$ tel que $u\neq 0$, il existe θ tel que $\dfrac{1}{2}\sin\theta = \dfrac{v}{u}$.
Soit, pour tout $n \in \mathbb{N}$: $x_n = \exp(\theta - 2n\pi)$.
$(x_n)_{n\in\,\mathbb{N}}$ tend vers 0 et $(\Delta_{x_n}\phi)_{n\in\,\mathbb{N}}$ a pour limite $\left(1, \dfrac{v}{u}\right)$, donc $(u,v) \in T_0\phi$.
Ainsi, $\boxed{T_0\phi = H^{1/2}}$.

4. Pour $\gamma\leqslant 1$, la norme $|(x,\varphi(x)) - (y,\varphi(y))|$ du dénominateur est égale à $|x-y|$ donc :

$$\Delta_y\varphi = \pm\left(1, \frac{\varphi(y)-\varphi(x)}{y-x}\right)$$

le signe $\pm$ dépendant de la position relative de x et y.
Soit $(x_n)_{n\in\mathbb{N}}$ une suite convergente vers x par valeurs supérieures par exemple.
$(\Delta_{x_n}\phi)_{n\in\mathbb{N}}$ est bornée donc admet une sous-suite convergente.
La limite est alors le seul vecteur $(1,v)$ de $T_x\varphi$ de première coordonnée 1. La suite $(\Delta_{x_n}\phi)_{n\in\mathbb{N}}$ est donc une suite bornée ayant une unique valeur d'adhérence $(1,v)$: elle converge vers $(1,v)$, ce qui montre que, pour toute suite de $]x,+\infty[$ convergente vers x, $\left(\dfrac{\varphi(x_n)-\varphi(x)}{x_n-x}\right)_{n\in\mathbb{N}}$ converge vers v.

Le critère séquentiel assure alors que : $\lim_{h\to 0^+} \dfrac{\varphi(x+h)-\varphi(x)}{h} = v$.

φ est dérivable à droite, de dérivée v.

On fait la même chose à gauche : pour toute suite $(x_n)_{n\in\mathbb{N}}$ de $]-\infty, x[$ convergente vers x, $\dfrac{\varphi(x_n)-\varphi(x)}{|x_n-x|} = \dfrac{\varphi(x_n)-\varphi(x)}{x-x_n}$ converge vers $-v$, donc $\lim_{h\to 0^-} \dfrac{\varphi(x+h)-\varphi(x)}{h} = v$.

Alors $\boxed{\varphi \text{ est dérivable en } x}$, et $\varphi'(x) = v$.

Rapport des correcteurs

Ce problème présente une introduction aux systèmes dynamiques avec un comportement chaotique

- Étude des itérations d'une application, d'abord dans le cas d'une application linéaire hyperbolique sur $\mathbb{R}^k$ puis en compactifiant sur le tore lorsque l'application et son inverse préservent le réseau $\mathbb{Z}^k$

- Étude du mélange topologique et de la densité des orbites périodiques. La fin aborde le cas non linéaire et donne des outils pour contrôler la régularité.

La plupart des candidats ont été en mesure d'aborder plusieurs parties du problème. Le mélange analyse/algébre linéaire, topologie et calcul différentiel ne semble pas avoir soulevé de trop grandes difficultés comme en attestent les résultats. Les questions 2.5 et 3.1 et 3.3.a ont été correctement traitées par la quasi-totalité des candidats.

Partie 1

Dans la première question beaucoup de copies ne s'assurent pas de l'existence de cette distance et oublient de tester certaines des conditions. Dans la question 1.2 beaucoup pensent que l'existence d'une limite simple dans (Li_γ, d_γ) suffit pour prouver la complétude alors qu'il faut prouver la convergence pour la distance d_γ. Le jury a été surpris de constater que les fonctions lipschitziennes sont souvent considérées comme différentiables. Par ailleurs le théorème des accroissements finis ne semble pas d'un usage largement répandu.

Partie linéaire

Force est de constater que l'algèbre linéaire est mal maitrisée La notion de norme subordonnée n'est pas bien connue et les questions 2.2 et 2.3 sont assez rarement bien traitées.

Au 2.4, il est surprenant de lire assez souvent que évidemment E est la somme des sous-espaces propres (voire la réunion !). Les sous espaces stables d'un endomorphisme sont d'ailleurs souvent confondus avec les sous espaces propres. D'autre part les conséquences pour l'endomorphisme réel du travail effectué dans le corps des nombres complexes sont rarement explicités correctement.

Partie linéarité et topologie

Comme déjà mentionné, le début de cette partie est assez bien compris et largement traité . Le jury a été particulièrement attentif à la qualité des justifications présentées, appréciant peu les assertions de type « il est clair que l'endomorphisme est hyperbolique ». La question 3.4 des points périodiques était plus difficile mais certains ont correctement prouvé les deux inclusions. Dans la question 3.5 les distances (comme dans tout le problème) considérées proviennent de normes (le résultat se géné ralise à la classe de toutes les distances qui leur sont bilipschitz-équivalentes).

La question 3.6.2 a révélé que les candidats ont beaucoup de difficultés à manipuler les inf. On a vu des choses catastrophiques où les inf sont traités comme des sup. Les difficultés sont ici à des niveaux élémentaires. La fin du 3 était sans doute la partie la plus poussée du problème. Elle a cependant été abordée avec succès par quelques candidats.

Partie 4

Les candidats ont surtout étudié la première question. Plusieurs ont correctement utilisé le théorème d'inversion locale. Mais rares sont ceux qui ont vu que l'on pouvait appliquer le théorème du point fixe à F pour prouver que f est une bijection.

Partie 5

Cette partie a été construite de manière à être indépendante du reste du problème (bien qu'en fait il s'agit de techniques utilisées pour comprendre la régularité des variétés stables). Elle n'a été que minoritairement abordée ce qui est un peu dommage vu la relative simplicité de certaines questions.

Le début du 5.3 montre des difficultés surprenantes à ce niveau pour étudier une fonction assez simple d'une variable réelle.

Épreuve écrite de mathématiques générales

Préambule

Le but de ce problème est d'étudier le nombre de solutions modulo un entier naturel q d'une congruence quadratique matricielle

$$ {}^tXSX \equiv T \pmod{q} $$

où S et T sont des matrices symétriques données à coefficients entiers, de tailles respectives $m \times m$ et $n \times n$, q est un entier strictement positif et l'inconnue X est une matrice d'entiers de taille $m \times n$, ${}^tX$ désignant sa transposée.

Soit R un anneau commutatif ; dans ce préambule, on note 1_R son élément unité, mais on permet d'écrire 1 dans la rédaction. On note $R^\times$ le groupe des éléments inversibles de R.

Étant donnés deux entiers m et n strictement positifs, on note $M_{m,n}(R)$ l'ensemble des matrices à m lignes et n colonnes à coefficients dans R.

Pour tout entier n strictement positif, on note $[1,n] = \{i \in \mathbb{Z} \,|\, 1 \leqslant i \leqslant n\}$; pour simplifier, on note $M_n(R)$, au lieu de $M_{n,n}(R)$, l'anneau des matrices carrées de taille $n \times n$ à coefficients dans R. Le déterminant d'une matrice carrée X à coefficients dans R est défini par la formule habituelle et noté $\det A$. On rappelle qu'une matrice de $M_n(R)$ est inversible si et seulement si son déterminant est dans l'ensemble $R^\times$ des éléments inversibles de R. On note $GL_n(R)$ le groupe des éléments de $M_n(R)$ de déterminant dans le groupe $R^\times$.

On note 1_n la matrice unité de $M_n(R)$. On note $S_n(R)$ l'ensemble des matrices X de $M_n(R)$ symétriques, c'est-à-dire telles que ${}^tX = X$.

A. Solutions modulo un nombre premier impair

Dans cette partie **A.**, on fixe un nombre premier **impair** p et on considère deux matrices symétriques S et T, avec $S \in M_m(\mathbb{Z}/p\mathbb{Z})$ et $T \in M_n(\mathbb{Z}/p\mathbb{Z})$, de déterminants respectifs s et t non nuls. L'élément de la i-ème ligne et j-ème colonne de S (resp. T) est noté $s_{i,j}$ (resp. $t_{i,j}$).

On introduit l'ensemble $\mathcal{A}_p(S,T) = \left\{X \in M_{m,n}(\mathbb{Z}/p\mathbb{Z}) \;\middle|\; {}^tXSX = T\right\}$ et on note $A_p(S,T)$ son cardinal.

A.I Un cas particulier

Dans cette section **A.I**, on prend $m = 2$ et $n = 1$. Soit s et t deux éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$, $T = \begin{pmatrix} t \end{pmatrix}$ et $S = \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}$. La matrice T, de taille 1×1, est identifiée à t ; ainsi $A_p(S,t)$ est le nombre de couples (x,y) dans $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ tels que $x^2 + sy^2 = t$.

1) Supposons que $-s$ soit un carré dans $\mathbb{Z}/p\mathbb{Z}$. Calculer $A_p(S,t)$.

2) On suppose dans toute la suite de cette section **A.I** que $-s$ n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

2.a. Montrer que le polynôme X^2+s est irréductible sur $\mathbb{Z}/p\mathbb{Z}$. Soit K un corps de rupture. Quel est le cardinal de K ?

2.b. Soit $F : K \to K,\ z \mapsto z^p$. Montrer que F est un automorphisme involutif de corps ($F \circ F = Id_K$) et déterminer ses points fixes.

2.c. Soit α une racine de X^2+s dans K. Montrer que $F(\alpha) = -\alpha$.

3) Soit $N : K^\times \to K^\times,\ z \mapsto z^{p+1}$.

3.a. Montrer que N est un morphisme de groupes d'image contenue dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

3.b. Déterminer le cardinal du noyau et de l'image de N.

3.c. Calculer $N(x+y\alpha)$ pour x, $y \in \mathbb{Z}/p\mathbb{Z}$ non tous deux nuls.

4) Calculer $A_p(S,\, t)$.

A.II Préliminaires

Dans cette section **A.II**, *m est un entier strictement positif et V un espace vectoriel de dimension finie m sur le corps $\mathbb{Z}/p\mathbb{Z}$.*

1) Soit $b : V \times V \to \mathbb{Z}/p\mathbb{Z}$ une forme bilinéaire symétrique sur V.

1.a. Démontrer que si $b(x,x)$ est nul pour tout x dans V, alors la forme bilinéaire b est nulle.

1.b. Démontrer que V possède une base $(e_1,\ldots,e_m)$ orthogonale pour b, c'est-à-dire telle que pour tous i et j distincts dans $[1,m]$, $b(e_i,e_j)=0$.

1.c. En déduire qu'il existe une matrice diagonale $D \in M_m(\mathbb{Z}/p\mathbb{Z})$ et une matrice inversible $P \in GL_m(\mathbb{Z}/p\mathbb{Z})$ telles que $S = {}^tPDP$.

2) Dans cette question **2**, on prend $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$ et on considère la forme bilinéaire b définie pour X et Y dans V par $b(X,Y) = {}^tXSY$.

Montrer que pour tout n entier strictement positif et tout T élément de $S_n(\mathbb{Z}/p\mathbb{Z})$, $A_p(S,T)$ est le nombre de n-uplets $(v_1,\ldots,v_n)$ d'éléments de V vérifiant $b(v_i,v_j) = t_{i,j}$ pour tous i et j dans $[1,n]$.

3) Vérifier que pour toutes matrices P de $GL_m(\mathbb{Z}/p\mathbb{Z})$ et Q de $GL_n(\mathbb{Z}/p\mathbb{Z})$, on a

$$A_p(S,T) = A_p({}^tPSP, {}^tQTQ).$$

4) Soit ϕ la fonction indicatrice d'Euler qui à un entier r strictement positif associe le nombre d'entiers de $[1,r]$ premiers à r.

4.a. Montrer que pour tout entier r strictement positif, $\displaystyle\sum_{d|r} \phi(d) = r$, la somme étant étendue à tous les entiers strictement positifs d diviseurs de r.

4.b. Soit K un corps fini commutatif à q éléments. Démontrer que pour tout entier strictement positif d diviseur de $q-1$, l'ensemble des éléments de $K^\times$ d'ordre divisant d est de cardinal au plus d.

4.c. En déduire que pour tout entier strictement positif d diviseur de $q-1$, $K^\times$ possède 0 ou $\phi(d)$ éléments d'ordre exactement d.

4.d. En déduire que $K^\times$ est cyclique.

A.III Le cas $n = 1$

Soit $n = 1$; on a alors $T = t \in \mathbb{Z}/p\mathbb{Z}$ et $2st \neq 0$ où l'on rappelle que $s = \det S$.

Soit $\omega = \exp\left(\dfrac{2\mathrm{i}\pi}{p}\right)$ une racine primitive p-ième de l'unité (on a $\omega \in \mathbb{C}^\times$).

Pour $\alpha \in \mathbb{Z}$, le nombre complexe ω^α ne dépend que de la classe a de α modulo p ; on le note ω^a : on admettra que l'on définit ainsi un morphisme $a \mapsto \omega^a$ du groupe additif $\mathbb{Z}/p\mathbb{Z}$ dans le groupe multiplicatif $\mathbb{C}^\times$.

Pour $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, on pose $\left(\dfrac{a}{p}\right) = 1$ s'il existe $b \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $a = b^2$, et $\left(\dfrac{a}{p}\right) = -1$ sinon. Ces notations seront utilisées dans toute la suite de la partie **A.**

1.a. Montrer qu'il y a dans $(\mathbb{Z}/p\mathbb{Z})^\times$ autant de carrés que de non carrés et que $a \mapsto \left(\dfrac{a}{p}\right)$ est un morphisme de groupes multiplicatifs $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$.

1.b. Pour $b \in \mathbb{Z}/p\mathbb{Z}$ calculer $\displaystyle\sum_{a\in\mathbb{Z}/p\mathbb{Z}} \omega^{ab}$.

1.c. Pour $c \in (\mathbb{Z}/p\mathbb{Z})^\times$, on pose $G_c = \displaystyle\sum_{a\in\mathbb{Z}/p\mathbb{Z}} \omega^{ca^2}$ et $H_c = \displaystyle\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right)\omega^{ca}$.

Démontrer qu'on a $G_c = H_c = \left(\dfrac{c}{p}\right)\cdot G_1$.

Dans ce qui suit, G_1 sera noté G.

2.a. Montrer que $pA_p(S,\, t) = \displaystyle\sum_{a,X} \omega^{a({}^tXSX - t)}$ où a parcourt $\mathbb{Z}/p\mathbb{Z}$ et X parcourt $M_{m,1}(\mathbb{Z}/p\mathbb{Z})$.

2.b. Soit D une matrice diagonale inversible élément de $M_m(\mathbb{Z}/p\mathbb{Z})$, de termes diagonaux $s_1, \ldots, s_m$. Montrer que

$$pA_p(D,\, t) = p^m + \left(\frac{\det D}{p}\right)\cdot G^m \cdot \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right)^m \omega^{-at}$$

2.c. Montrer que $G^2 = \left(\dfrac{-1}{p}\right)\cdot p$.

Indication : *On pourra appliquer à un cas particulier le résultat démontré dans la question précédente.*

3) Pour $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ et k entier naturel on pose $\varepsilon_k^{(p)}(a) = \left(\dfrac{(-1)^{k/2}a}{p}\right)$ si k est pair et $\varepsilon_k^{(p)}(a) = 0$ sinon.

Cette notation sera utilisée dans la suite du problème.

3.a. Montrer qu'on a l'égalité :

$$A_p(S,\, t) = \begin{cases} p^{m-1}\left(1 - \varepsilon_m^{(p)}(s)\, p^{-m/2}\right) & \text{si } m \text{ est pair} \\ p^{m-1}\left(1 + \varepsilon_{m-1}^{(p)}(st)\, p^{(1-m)/2}\right) & \text{si } m \text{ est impair} \end{cases}$$

3.b. Préciser pour quelles valeurs de m, s et t la quantité $A_p(S,\, t)$ s'annule.

A.IV Le cas n quelconque

Dans cette section, on suppose $m \geqslant n$.

1) Soit $n \geqslant 2$; soit $T \in S_n(\mathbb{Z}/p\mathbb{Z})$ de déterminant $t \in (\mathbb{Z}/p\mathbb{Z})^\times$. Supposons $T = \begin{pmatrix} \delta & 0 \\ 0 & T_1 \end{pmatrix}$ avec $\delta \in (\mathbb{Z}/p\mathbb{Z})^\times$ et $T_1 \in S_{n-1}(\mathbb{Z}/p\mathbb{Z})$ inversible de déterminant t_1.

1.a. Montrer que l'application qui à $X \in \mathcal{A}_p(S, T)$ fait correspondre sa première colonne induit une application γ de $\mathcal{A}_p(S,\, T)$ dans $\mathcal{A}_p(S,\, \delta)$.

1.b. Soit $C_1 \in \mathcal{A}_p(S,\, \delta)$. Montrer qu'il existe une matrice symétrique inversible S_1 dans $M_{m-1}(\mathbb{Z}/p\mathbb{Z})$ dont le déterminant s_1 vérifie $\left(\dfrac{\delta s_1}{p}\right) = \left(\dfrac{s}{p}\right)$, et telle que $\gamma^{-1}(C_1)$ soit de cardinal $A_p(S_1,\, T_1)$.

Indication : *On pourra utiliser l'interprétation de la question 2 du Préliminaire en introduisant l'orthogonal W du vecteur C_1 pour la forme b de matrice S dans la base canonique de $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$.*

2.a. En procédant par récurrence sur n, montrer que

$$A_p(S, T) = p^{mn-n(n+1)/2}\psi_{p,m,n}(s,\, t) \prod_{m-n<2k<m} \left(1 - \frac{1}{p^{2k}}\right)$$

où

$$\psi_{p,m,n}(s,\, t) = \left(1 - \varepsilon_m^{(p)}(s)p^{-m/2}\right)\left(1 + \varepsilon_{m-n}^{(p)}(st)p^{(n-m)/2}\right)$$

2.b. À quelles conditions $A_p(S,\, T)$ est-il nul ?

B. Matrices à coefficients dans l'anneau $\mathbb{Z}/q\mathbb{Z}$

Soit q un entier naturel strictement positif ; on note π_q le morphisme canonique d'anneaux $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ et, si q' est un entier naturel strictement positif multiple de q, $\pi_{q,q'}$ le morphisme canonique d'anneaux $\mathbb{Z}/q'\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$. On pourra remarquer l'égalité $\pi_{q,q'} \circ \pi_{q'} = \pi_q$. Si n et m sont des entiers strictement positifs et M un élément de $M_{m,n}(\mathbb{Z})$, on note aussi $\pi_q(M)$ la matrice élément de $M_{m,n}(\mathbb{Z}/q\mathbb{Z})$ dont les coefficients sont les images par π_q des coefficients de M ; on définit de manière analogue $\pi_{q,q'}(M)$ si q' est un multiple de q et si M est élément de $M_{m,n}(\mathbb{Z}/q'\mathbb{Z})$. On considérera comme évidentes les propriétés des applications π_q et $\pi_{q,q'}$ relativement à la somme des matrices, au produit d'une matrice par un scalaire, au produit des matrices, à la transposition des matrices et au déterminant.

On dira que les matrices M_1 et M_2 de même taille et à coefficients dans $\mathbb{Z}$, resp. $\mathbb{Z}/q'\mathbb{Z}$, sont congrues modulo q si $\pi_q(M_1) = \pi_q(M_2)$, resp. si q divise q' et $\pi_{q,q'}(M_1) = \pi_{q,q'}(M_2)$; cette relation sera notée $M_1 \equiv M_2 \pmod{q}$.

Dans ce qui suit, m et n représentent deux entiers strictement positifs tels que $m \geqslant n$ et S et T deux matrices symétriques, $S \in S_m(\mathbb{Z})$ et $T \in S_n(\mathbb{Z})$, de déterminants respectifs s et t non nuls. Pour tout entier naturel impair q premier avec st, on pose

$$\mathcal{A}_q(S,\, T) = \left\{X \in M_{m,n}(\mathbb{Z}/q\mathbb{Z}) \;\middle|\; {}^tX\pi_q(S)X = \pi_q(T)\right\}$$

et on note $A_q(S,\, T)$ le cardinal de cet ensemble. Pour $a \in \mathbb{Z}$ et p premier impair, on pose $\chi_a(p) = 0$ si p divise a, $\chi_a(p) = 1$ si a est un carré non nul modulo p, et sinon $\chi_a(p) = -1$.

1) Soit q un entier strictement positif quelconque.

1.a. On suppose $q = q_1q_2$, où q_1 et q_2 sont premiers entre eux.
Montrer que l'application $X \mapsto (\pi_{q_1,q}(X), \pi_{q_2,q}(X))$ établit une bijection entre

$$M_{m,n}(\mathbb{Z}/q\mathbb{Z}) \text{ et } M_{m,n}(\mathbb{Z}/q_1\mathbb{Z}) \times M_{m,n}(\mathbb{Z}/q_2\mathbb{Z}).$$

1.b. Montrer que la bijection trouvée au 1.b induit une bijection entre

$$\mathcal{A}_q(S,T) \text{ et } \mathcal{A}_{q_1}(S,T) \times \mathcal{A}_{q_2}(S,T).$$

1.c. On suppose $q = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ où $p_1, \dots, p_r$ sont des nombres premiers impairs deux à deux distincts et $\alpha_1, \dots, \alpha_r$ sont des entiers strictement positifs. Pour tout i dans $[1, r]$, on pose $q_i = p_i^{\alpha_i}$. Démontrer que

$$A_q(S,T) = \prod_{i=1}^{r} A_{q_i}(S,T)$$

2) Dans cette question p désigne un nombre premier impair premier avec st et α est un entier naturel $\geqslant 1$. On considère une matrice $X \in M_{m,n}(\mathbb{Z})$ telle que $\pi_{p^\alpha}(X) \in \mathcal{A}_{p^\alpha}(S,T)$ et on pose $\widetilde{X} = \pi_p(X)$ et $\widetilde{S} = \pi_p(S)$.

2.a. Montrer que l'application $u : H \mapsto {}^t\widetilde{X}\widetilde{S}H$, est une application $\mathbb{Z}/p\mathbb{Z}$-linéaire surjective $M_{m,n}(\mathbb{Z}/p\mathbb{Z})$ dans $M_n(\mathbb{Z}/p\mathbb{Z})$.

2.b. Montrer que l'application $v : H \mapsto {}^t\widetilde{X}\widetilde{S}H + {}^tH\widetilde{S}\widetilde{X}$ est une application $\mathbb{Z}/p\mathbb{Z}$-linéaire surjective de $M_{m,n}(\mathbb{Z}/p\mathbb{Z})$ dans $S_n(\mathbb{Z}/p\mathbb{Z})$.

2.c. Montrer que le cardinal du noyau de l'application linéaire de la question précédente est $p^{mn-\frac{n(n+1)}{2}}$.

3) Montrer qu'il existe une matrice U dans $M_{m,n}(\mathbb{Z})$ telle que la matrice $Y = X + p^\alpha U$ de $M_{m,n}(\mathbb{Z})$ satisfasse $\pi_{p^{\alpha+1}}(Y) \in \mathcal{A}_{p^{\alpha+1}}(S,T)$.

4) Déduire de ce qui précède que l'application

$$\pi_{p^\alpha,p^{\alpha+1}} : M_{m,n}(\mathbb{Z}/p^{\alpha+1}\mathbb{Z}) \to M_{m,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$$

induit une application $r_\alpha : \mathcal{A}_{p^{\alpha+1}}(S,\, T) \to \mathcal{A}_{p^\alpha}(S,T)$ surjective, et que les cardinaux des images réciproques par r_α des singletons valent tous $p^{mn-\frac{n(n+1)}{2}}$.

5) Déterminer $A_{p^\alpha}(S,\, T)$ pour tout $\alpha \geqslant 1$.

6) Soit q un entier naturel impair $\geqslant 1$ premier avec st.

6.a. Exprimer $A_q(S,T)$ en fonction de m, n, s, t, q et des facteurs premiers de q.

6.b. À quelle condition $A_q(S,\,T)$ est-il nul ?

7) On note $\mathcal{P}$ l'ensemble des nombres premiers ne divisant pas $2st$; pour tout entier h strictement positif, on pose $\mathcal{P}_h = \mathcal{P} \cap [1,h]$ et on note q_h le produit des éléments de $\mathcal{P}_h$. On fixe $m \geqslant 1$ et $n \geqslant 1$ de sorte que $m > n+2$.

7.a. Montrer que la suite $\left(A_{q_h}(S,\,T) \Big/ q_h^{mn-\frac{n(n+1)}{2}} \right)_{h\geqslant 1}$ a une limite finie strictement positive.

7.b. Soit $Q_h = \prod_{p\in\mathcal{P}_h} p^h = q_h^h$.

Montrer que la suite $\left(A_{Q_h}(S,T) \Big/ Q_h^{mn-\frac{n(n+1)}{2}} \right)_{h\geqslant 1}$ a une limite finie strictement positive.

Corrigé

A.I

1) Si $s = -\alpha^2$ avec $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a $x^2 + sy^2 = (x - \alpha y)(x + \alpha y)$. Comme p est impair, la matrice $\begin{pmatrix} 1 & -\alpha \\ 1 & \alpha \end{pmatrix}$ est inversible. Donc pour tout $t \in (\mathbb{Z}/p\mathbb{Z})^\times$, l'ensemble $\mathcal{A}_p(S,t)$ est en bijection avec $\{(u,v) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times ; uv = t\}$ par $(x,y) \mapsto (x - \alpha y, x + \alpha y)$. Ce dernier ensemble est de cardinal $p-1$; on a donc $A_p(S,t) = p - 1$.

2.a. Un polynôme de degré deux à coefficients dans un corps commutatif est irréductible si et seulement si il n'a pas de racine dans ce corps. Ici, $X^2 + s$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$. Le choix d'une racine de $X^2 + s$ dans K fournit un homomorphisme surjectif et injectif d'anneaux $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 + s) \to K$. Le terme de gauche est un espace vectoriel de dimension 2 sur $\mathbb{Z}/p\mathbb{Z}$ (de base $\{1, \overline{X}\}$ où $\overline{X}$ désigne la classe de X modulo $(X^2 + s)$). Le corps K est donc d'ordre p^2.

2.b. On a $F(0) = 0$, $F(1) = 1$ et $F : K^\times \to K^\times$ est un homomorphisme de groupes multiplicatifs. Pour voir que F est additif, il suffit de noter par la formule du binôme de Newton que les coefficients binomiaux $\begin{pmatrix} p \\ i \end{pmatrix}$ $(i = 1, \ldots, p-1)$ sont divisibles par p. C'est clair car $i! \cdot (p-i)! \begin{pmatrix} p \\ i \end{pmatrix} = p!$ est divisible par p. Comme les deux premiers facteurs sont premiers à p, c'est que p divise le troisième. Ainsi F est un homomorphisme de corps. Tout homomorphisme de corps est injectif. Comme K est fini, F est donc bijectif. On a $F \circ F(z) = z^{p^2}$. Comme $K^\times$ est un groupe d'ordre $p^2 - 1$, on a pour tout $z \in K^\times$, $z^{p^2-1} = 1$, donc $z^{p^2} = z$. Cette relation est aussi satisfaite par 0, donc on a $F \circ F = Id_K$.

Si $z^p = z$, z est racine du polynôme $X^p - X$ de degré p. Par le petit théorème de Fermat, ce polynôme a exactement p racines. Le noyau de $F - Id_K$ est donc $\mathbb{Z}/p\mathbb{Z}$.

2.c. Soit $\alpha \in K$ une racine de $X^2 + s$. $F(\alpha)$ est encore racine de $X^2 + s$ car $s \in \mathbb{Z}/p\mathbb{Z}$ est fixé par F. Comme $\alpha \notin \mathbb{Z}/p\mathbb{Z}$, on a $F(\alpha) \neq \alpha$. Comme l'autre racine est $-\alpha$, on a $F(\alpha) = -\alpha$.

3.a. On a $N(z) = zF(z)$. C'est donc un homomorphisme multiplicatif de $K^\times$ dans lui-même. De plus $(N(z))^p = z^{p^2+p} = z^{1+p} = N(z)$ car $F \circ F = Id_K$. Ainsi, $N(z) \in (Z/p\mathbb{Z})^\times$.

3.b. Si $N(z) = 1$, z est racine de $X^{p+1} - 1$; ainsi l'ordre de $\operatorname{Ker} N$ est au plus $p + 1$ et celui de $\operatorname{Im} N$ au plus $p - 1$. Comme celui de $K^\times$ est $(p-1)(p+1)$, on tire de l'isomorphisme $K^\times / \operatorname{Ker} N \cong \operatorname{Im} N$ que $\operatorname{Card} \operatorname{Ker} N = p + 1$ et $\operatorname{Card} \operatorname{Im} N = p - 1$.

3.c. On a $N(x + y\alpha) = (x + y\alpha)F(x + y\alpha) = (x + y\alpha)(x - y\alpha) = x^2 - y^2\alpha^2 = x^2 + sy^2$.

4) Notons qu'étant donnés deux éléments x, y de $\mathbb{Z}/p\mathbb{Z}$, on a $x + y\alpha \in K^\times$ si et seulement si x et y sont non-nuls. On peut donc écrire $\mathcal{A}_p(S,t) = \{z \in K^\times ; N(z) = t\}$. Choisissons $z_0 \in K^\times$ tel que $N(z_0) = t$. On a alors $N(z) = t$ si et seulement si $N(zz_0^{-1}) = 1$, c'est-à-dire $zz_0^{-1} \in \operatorname{Ker} N$. Ainsi $z \mapsto zz_0^{-1}$ est une bijection de $\mathcal{A}_p(S,t)$ vers $\operatorname{Ker} N$. L'ordre de $\mathcal{A}_p(S,t)$ est donc $p+1$ par 3.b.

A.II

1.a. On a $b(x,y) = \frac{1}{2}[b(x+y,x+y) - b(x,x) - b(y,y)]$. Si donc $b(t,t) = 0$ pour tout vecteur t, on a $b = 0$.

1.b. On raisonne par récurrence sur la dimension de V. Si $b = 0$ il n'y a rien à démontrer. Sinon, on prend $e_1 \in V$ tel que $b(e_1, e_1) \neq 0$. La relation $x = x - \frac{b(e_1,x)}{b(e_1,e_1)} \cdot e_1 + \frac{b(e_1,x)}{b(e_1,e_1)} \cdot e_1$ montre que V est somme directe de la droite engendrée par e_1 et de son orthogonal V_1. On applique alors l'hypothèse de récurrence à V_1 pour conclure.

1.c. On prend $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$ et $b(X,Y) = {}^tXSY$. Soit P l'inverse de la matrice d'une base orthogonale de b. On a $S = {}^tPDP$ où D est diagonale.

2) La relation ${}^tXSX = T$ signifie pour tout i, j $b(v_i, v_j) = t_{i,j}$.

3) L'application

$$\mathcal{A}_p(S,T) \to \mathcal{A}_p({}^tPSP, {}^tQTQ), \quad X \mapsto P^{-1}XQ$$

est bijective.

4.a. On partitionne l'intervalle $[1,r]$ de $\mathbb{Z}$ en les sous-ensembles $\Phi(d)$ constitués des entiers dont le plus grand commun diviseur avec r est r/d, d parcourant l'ensemble des diviseurs positifs de d. La multiplication par r/d établit une bijection de $\Phi(d)$ avec l'ensemble des entiers premiers à d dans $[1,d]$. Son ordre est $\phi(d)$. On a donc $r = \sum_{d|r} \phi(d)$.

4.b. Un élément $x \in K^\times$ est d'ordre divisant d si et seulement si il est racine du polynôme de degré d $X^d - 1$. Il y a donc au plus d tels éléments dans $K^\times$.

4.c. Si $K^\times$ possède un élément x d'ordre d (diviseur $q-1$), il possède au moins d éléments d'ordre divisant d. Il en possède au plus d par la question précédente, donc exactement d, qui forment un groupe cyclique engendré par x. L'ensemble $(K^\times)_d$ des éléments d'ordre exactement d est donc d'ordre $\phi(d)$.

4.d. Si pour un diviseur d de $q-1$ il n'y a pas d'élément d'ordre d(*i.e.* $(K^\times)_d = \emptyset$), on a $q - 1 = \operatorname{Card} K^\times = \sum_{\delta|q-1} \operatorname{Card}(K^\times)_\delta < \sum_{\delta|q-1} \phi(\delta) = q-1$, ce qui est une contradiction.

A.III

1.a. L'homomorphisme $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^2$ a pour noyau $\{\pm 1\}$. Son image est donc d'indice 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$. C'est dire qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$.Soit a un non carré, tout non carré peut sécrire ax^2. Ainsi le produit de deux non carrés est un carré (et le produit d'un carré par un non carré est un non-carré, et le produit de deux carrés est un carré). Ceci montre que $x \mapsto (\frac{a}{p})$ est un homomorphisme.

1.b. Si $b \in (\mathbb{Z}/p\mathbb{Z})^\times$, $a \mapsto ab$ est bijective, donc $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ab} = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^a = \frac{\omega^p - 1}{\omega - 1} = 0$. Si $b = 0$, on a $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ab} = p$.

1.c. On a $G_c = 1 + 2 \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ca}$. D'autre part, $H_c = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ca} - \sum_{a\notin(\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ca}$. Comme $c \in (\mathbb{Z}/p\mathbb{Z})^{\times}$, on a $\sum_{a\in\mathbb{Z}/p\mathbb{Z}} \omega^{ac} = 0 = 1 + \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} + \sum_{a\notin(\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac}$, donc $1 + \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} = -\sum_{a\notin(\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac}$. Ainsi, $H_c = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} + 1 + \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} = G_c$.

2.a. Par 1.b, la somme $\frac{1}{p}.\sum_{a\in(\mathbb{Z}/p\mathbb{Z})} \omega^{ab}$ vaut 1 ou 0 suivant que b est nul ou pas. Donc $pA_p(S,t) = \sum_{X\in M_{m,1}(\mathbb{Z}/p\mathbb{Z})} \frac{1}{p} \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \omega^{a({}^tXSX-t)}$. D'où la formule annoncée.

2.b. On a ${}^tXDX = \sum_{i=1}^{m} s_i x_i^2$ donc $\omega^{a({}^tXDX-t)} = \omega^{as_1x_1^2} \dots \omega^{as_mx_m^2}\omega^{-at}$ et

$pA_p(S,t) = \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \omega^{-at}(\sum_{x_1\in\mathbb{Z}/p\mathbb{Z}} \omega^{as_1x_1^2}) \cdot \dots \cdot (\sum_{x_m\in\mathbb{Z}/p\mathbb{Z}} \omega^{as_mx_m^2})$

La contribution du terme $a = 0$ vaut p^m. De plus, on a pour chaque $i = 1, \dots, m$. $\sum_{x_i\in\mathbb{Z}/p\mathbb{Z}} \omega^{as_ix_i^2} = G_{as_i} = (\frac{as_i}{p})G$. Donc $pA_p(S,t) = p^m + \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at}(\frac{as_1}{p}) \dots (\frac{as_m}{p})G)$ et comme $(\frac{s_1}{p})\cdot\dots\cdot(\frac{s_m}{p}) = (\frac{D}{p})$, on a : $pA_p(S,t) = p^m + G^m(\frac{D}{p}) \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at}(\frac{a}{p})^m$.

2.c. Prenons $m = 1$, $s_1 = 1$ et $t = 1$. On a $A_p(S,1) = 2$ donc comme $G_{-1} = (\frac{-1}{p})G$, on a $2p = p + G(\frac{-1}{p})G$, soit $p = G^2(\frac{-1}{p})$, ou encore $G^2 = (\frac{-1}{p})p$.

3.a. Pour S symétrique non-dégénérée quelconque, ,on applique A.II 1.c et 3 pour se ramener à S diagonale, de déterminant $s_1 \dots s_m = s$. On obtient donc $pA(S,t) = p^m + (\frac{s}{p})G^m \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at}(\frac{a}{p})^m$.

Si $m = 2r$, on a $G^m \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at}(\frac{a}{p})^m = -(\frac{-1}{p})^r p^r$, donc $pA(S,t) = p^m(1 - (\frac{(-1)^{m/2}s}{p})p^{-m/2})$ d'où la formule annoncée.

Si $m = 2r+1$, on a $G^m \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at}(\frac{a}{p})^m = (\frac{-t}{p})G^{m+1} = (\frac{-t}{p})(\frac{-1}{p})^{r+1}p^{r+1}$ donc $pA(S,t) = p^m(1 + (\frac{(-1)^{(m-1)/2}st}{p})p^{(1-m)/2})$. D'où la formule annoncée.

3.b. Le seul cas de nullité intervient lorsque $m = 1$ et lorsque st n'est pas un carré.

A.IV

1.a. On écrit $X = (C_1, X_1)$ où C_1 est un vecteur colonne et $X_1 \in M_{m,n-1}(\mathbb{Z}/p\mathbb{Z})$. Alors un calcul par blocs montre que ${}^tXSX = T$ équivaut à ${}^tC_1SC_1 = \delta$, ${}^tX_1SX_1 = T_1$ et ${}^tC_1SX_1 = 0$. L'application $X \mapsto C_1$ induit donc en particulier une application $\gamma : \mathcal{A}(S,T) \to \mathcal{A}(S,\delta)$.

1.b. Soit W l'orthogonal de C_1 dans l'espace quadratique $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$ muni de $b(v,w) = {}^tvSw$. Soit $(v_i)_{i=2,\dots,m}$ une base de W. Soit $S_1 = (b(v_i,v_j))_{2\leqslant i,j\leqslant m}$ la matrice de b dans cette base. Soit $T_1 = (t_{i,j})_{2\leqslant i,j\leqslant n}$. Par la question précédente, on peut réécrire l'ensemble $\gamma^{-1}(C_1)$ comme

$$\{(w_2,\dots,w_n) \in W^{n-1}; b(w_i,w_j) = t_{i,j} \quad \text{pour tout } i,j \in [2,m]\}$$

Soit $X_1' \in M_{m-1,n-1}(\mathbb{Z}/p\mathbb{Z})$ la matrice des coordonnées des vecteurs colonnes w_j dans la base des v_i. On peut réécrire l'ensemble $\gamma^{-1}(C_1)$ comme

$$\mathcal{A}(S_1,T_1) = \{X_1' \in M_{m-1,n-1}(\mathbb{Z}/p\mathbb{Z}); {}^tX_1'S_1X_1' = T_1\}$$

Soit P la matrice de la base $(v_1,\dots,v_m)$. On a

$$\begin{pmatrix} \delta & 0 \\ 0 & S_1 \end{pmatrix} = {}^tPSP$$

Donc si $s_1 = \det S_1$, on a $\delta s_1 = s(\det P)^2$ et $(\frac{\delta s_1}{p}) = (\frac{s}{p})$.

2.a. Pour $n = 1$, vue la convention sur les cas de nullité de $\varepsilon_k^{(p)}(a)$, les formules pour $A_p(S,t)$ distinguant m pair ou impair peuvent être synthétisées en la seule formule $A_p(S,t) = p^{m-1}\psi_{p,m,1}(s,t)$. Si le résultat est vrai pour $n-1$, soit $T \in S_n(\mathbb{Z}/p\mathbb{Z})$; quitte à remplacer T par ${}^tQTQ$), ce qui ne change pas $A_p(S,T)$ par A.II.3, on peut supposer T diagonale (et en particulier de la forme de la question 1.2 ci-dessus. Avec les notations de la question 1.b, on a $A_p(S,T) = A_p(S,\delta)A_p(S_1,T_1)$. Par hypothèse de récurrence, $A_p(S_1,T_1) = p^{(m-1)(n-1)-(n-1)n/2}\psi_{p,m-1,n-1}(s_1,t_1)\prod_{m-n+1<2k<m}(1-\frac{1}{p^{2k}})$. et $A_p(S,\delta) = p^{m-1}\psi_{p,m,1}(s,\delta)$. Traitons par exemple le cas où m et n sont pairs. On observe que

- $(m-1)(n-1) - n(n-1)/2 + (m-1) = mn - n(n+1)/2$
- $\psi_{p,m,1}(s,\delta) = 1 - (\frac{(-1)^{m/2}s}{p})p^{-m/2}$ et
- $\psi_{p,m-1,n-1}(s_1,t_1) = 1 + (\frac{(-1)^{(m-n)/2}s_1t_1}{p})p^{(n-m)/2}$, et comme par la question 1.2 on a $s_1t_1\delta^2 = stu^2$, on trouve $\psi_{p,m,1}(s,\delta)\psi_{p,m-1,n-1}(s_1,t_1) = \psi_{p,m,n}(s,t)$. Comme on a aussi
- $\prod_{m-n<2k<m}(1-\frac{1}{p^{2k}}) = \prod_{m-n+1<2k<m}(1-\frac{1}{p^{2k}})$

on voit donc en multipliant $A_p(S,\delta)$ et $A_p(S_1,T_1)$ que

$$A_p(S,T) = p^{mn-n(n+1)/2}\psi_{p,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p^{2k}})$$

comme annoncé. Les autres cas se traitent de même.

2.b. Le seul cas de nullité de $A_p(S,T)$ se produit lorsque $m = n$ et que st n'est pas un carré.

B.

1.a. et **1.b.** se traitent simultanément en observant que, lorsque q_1 et q_2 sont premiers entre eux, le lemme chinois induit un isomorphisme d'anneaux $M_{m,n}(\mathbb{Z}/q_1q_2\mathbb{Z}) \cong M_{m,n}(\mathbb{Z}/q_1\mathbb{Z}) \times M_{m,n}(\mathbb{Z}/q_2\mathbb{Z})$.

1.c. est immédiat à partir des questions ci-dessus.

2.a. Soit $\widetilde{T} = \pi_p(T)$. Soit $H_1 \in M_n(\mathbb{Z}/p\mathbb{Z})$. Soit $H_2 \in M_n(\mathbb{Z}/p\mathbb{Z})$ telle que $H_1 = \widetilde{T}H_2$; posons $H = \widetilde{X}H_2 \in M_{m,n}(\mathbb{Z}/p\mathbb{Z})$. On a ${}^t\widetilde{X}\widetilde{S}H = {}^tX\widetilde{S}\widetilde{X}H_2 = \widetilde{T}H_2 = H_1$.

2.b. Comme p est impair, toute matrice symétrique $H_1 \in S_n(\mathbb{Z}/p\mathbb{Z})$ s'écrit $H_2 + {}^tH_2$ pour une matrice $H_2 \in M_n(\mathbb{Z}/p\mathbb{Z})$; par la question précédente, il existe $H \in M_{m,n}(\mathbb{Z}/p\mathbb{Z})$ tel que ${}^t\widetilde{X}\widetilde{S}H = H_2$. Ceci montre la surjectivité de $H \mapsto {}^t\widetilde{X}\widetilde{S}H + {}^tH\widetilde{S}\widetilde{X}$.

2.c. Le noyau de l'application ci-dessus est de dimension $mn - n(n+1)/2$. Donc son cardinal est $p^{mn-n(n+1)/2}$.

3) On abrège $\pi_{p^\alpha}(X) = X_\alpha$. Si ${}^tX_\alpha S_\alpha X_\alpha = T_\alpha$, posons $Y = X + p^\alpha U$. Cherchons $U \in M_{m,n}(\mathbb{Z})$ de sorte que ${}^tYSY \equiv T \pmod{p^{\alpha+1}}$. On peut réécrire cette relation comme ${}^t(X + p^\alpha U)S(X + p^\alpha U) \equiv T \pmod{p^{\alpha+1}}$, ou encore, en posant ${}^tXSX = T + p^\alpha\Theta$: ${}^tUSX + {}^tXSU \equiv \Theta \pmod{p}$. Par la question 2.2, cette congruence a une solution $U \in M_{m,n}(\mathbb{Z})$.

4) Étant donnée $X \in M_{m,n}(\mathbb{Z})$ telle que ${}^tXSX \equiv T \pmod{p^\alpha}$, l'ensemble $\{\pi_p(U) \in M_{m,n}(\mathbb{Z}/p\mathbb{Z}); {}^tUSX + {}^tXSU \equiv \Theta \pmod{p}\}$ est une variété linéaire affine de direction de dimension $mn - n(n+1)/2$. C'est donc un ensemble d'ordre $p^{mn-n(n+1)/2}$. Ainsi, r_α est surjective et l'image inverse de chaque singleton est d'ordre $p^{mn-n(n+1)/2}$.

5) On en déduit que

$$A_{p^\alpha} = p^{(\alpha-1)(mn-n(n+1)/2)}p^{mn-n(n+1)/2}\psi_{p,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p^{2k}}) =$$

$$p^{\alpha(mn-n(n+1)/2}\psi_{p,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p^{2k}}).$$

6.a. On a

$$A_q(S,T) = A_{p_1^{\alpha_1}}(S,T)\dots A_{p_r^{\alpha_r}}(S,T) = q^{\alpha(mn-n(n+1)/2)}\prod_i \psi_{p_i,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p_i^{2k}})$$

6.b. La nullité de $A_q(S,T)$ ne se produit que lorsque $m = n$ et que st n'est pas un carré modulo l'un des facteurs premiers de q.

7.a. On a $A_{q_h}(S,T)/q_h^{mn-n(n+1)/2} = \prod_i \psi_{p_i,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p_i^{2k}})$ On a $m > n+2$ donc en particulier $m/2 > 3/2$ et $(m-n)/2 > 1$; donc les produits infinis $\prod_i(1-(\frac{(-1)^{m/2}s}{p_i})p_i^{-m/2})$ et $\prod_i(1-(\frac{(-1)^{(m-n)/2}st}{p_i})p_i^{-(m-n)/2})$ sont absolument convergents.

A fortiori les produits $\prod_i(1-\frac{1}{p_i^{2k}})$ pour $2k \in]m-n, m[$. Leur limite sont des nombres strictement positifs. Il en va donc de même pour leur produit fini.

7.b. L'argument est identique car $A_{Q_h}(S,T)/Q_h^{mn-n(n+1)/2} = A_{q_h}(S,T)/q_h^{mn-n(n+1)/2}$

Rapport des correcteurs

Le problème portait sur l'étude, pour deux matrices symétriques S et T à coefficients dans $\mathbb{Z}$ données de tailles respectives m et n, des nombres $A_q(S,T)$ de solutions $X \in M_{m,n}(\mathbb{Z}/q\mathbb{Z})$ de la congruence ${}^tXSX \equiv T \pmod q$. On faisait l'hypothèse simplificatrice que les matrices sont définies positives et que q est premier à $2\det S \cdot \det T$.

La partie A concernait le cas où q est premier ; la partie B consistait à déduire le cas général du cas A. La partie $A.I$ proposait de calculer le nombre $A_p(S,T)$ pour $m = 2$ et $n = 1$ en distinguant selon que $-\det S$ est un carré ou non modulo p.

La première question de cette partie a semble-t'il posé problème à de nombreux candidats. Elle reposait sur l'identité remarquable $a^2-b^2 = (a-b)(a+b)$. Elle a occasionné les dénombrements les plus variés, conduisant parfois à des résultats absurdes. Pour les écrire, il a fallu que le candidat renonce au bon sens dont il aurait fait preuve en physique : une erreur de calcul peut conduire à trouver un cardinal égal à $\frac{p}{2}$ (pour p premier impair), ou à l'infini, pour un ensemble fini. Mais alors, le "bon sens physique", valable aussi en algèbre, aurait pu suggérer une relecture du calcul...

La confusion entre (auto)morphisme de corps, de groupes et d'espaces vectoriels a conduit certains candidats à ne pas vérifier la multiplicativité de F ainsi que la condition $F(1) = 1$, et inversement, elle en a conduit d'autres à vérifier l'additivité de N et à chercher son noyau comme l'ensemble des z tels que $N(z) = 0$.

Il faut essayer de dégager les structures algébriques concernées par les questions avant de se lancer dans les vérifications.

Atention dans $2.c$, on ne peut écrire sans précaution $\alpha = i\sqrt{-s}$ (vu que $i \in \mathbb{C}$ et $s \in \mathbb{F}_p$).

Dans $A.I$ et dans $B.1$, on a beaucoup vu d'énoncés de questions recopiés. C'est une remarque générale : recopier ou plagier l'énoncé ne rapporte rien !

La première question de $A.II$ a également surpris les correcteurs.On a vu des formes quadratiques définies et positives sur $\mathbb{F}_p$. La méthode de Gram-Schmidt ne s'applique que dans le contexte d'une forme quadratique réelle définie positive. C'est cependant souvent la méthode choisie pour montrer l'existence d'une base orthogonale dans le cadre du corps $\mathbb{F}_p$! Une erreur du même ordre a souvent été le recours à une "diagonalisation" de la forme quadratique avec matrice de passage orthogonale. Cette confusion classique dans le cadre réel de la réduction d'une forme quadratique avec la diagonalisation d'une matrice symétrique devient vraiment absurde sur $\mathbb{F}_p$ car une matrice symétrique n'est même plus nécessairement diagonalisable (comme le montre l'exemple de $\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$ sur $\mathbb{F}_5$).

En fait, on traite la question $1.b$ de $A.I$ par récurrence sur la dimension. Il faut cependant rédiger les récurrences et non se contenter de les amorcer en finissant par un "et ainsi de suite".

Une erreur courante, moins grave certes, est de penser que dans l'écriture $S = {}^tPDP$, la matrice P est la matrice de passage de la base canonique de K^n à la base orthogonale construite, alors que c'est l'inverse.

La cyclicité de $K^\times$ a souvent été mal traitée ; les questions $4.a$-$4.d$ occasionnent des réponses floues voire fausses alors que les candidats peuvent penser les avoir traitées correctement.

Certains ont tenté d'adapter une démonstration différente de celle demandée, en général sans succès. Encore une remarque générale : pour obtenir les points d'une question, il s'agit de répondre exactement à la question telle qu'elle est posée, y compris s'il s'agit d'une question de cours.

Le simple bon sens montre qu'on ne répond pas à $A.II.1.b$ en citant le théorème du cours affirmant qu'il existe une base orthogonale, de même qu'on ne répond pas à $4.a$-$4.d$ en citant celui qui affirme que $K^\times$ est cyclique !

$A.III$ Le symbole de Legendre et les sommes de Gauss semblaient connus des candidats, mais trop souvent les calculs proposés se sont bornés à une suite d'égalités non justifiées (et parfois erronées, conduisant malgré tout au résultat). Les formules écrites laissent souvent entendre que l'ensemble dans lequel vivent les sommes de Gauss n'est pas clair : on lit souvent que si p divise b, $\sum_a \omega^{ab} = p = 0$ et que $e^{2i\pi/p} \in \mathbb{F}_p$ (!) La réalité est que les sommes de Gauss sont des nombres complexes !

La partie $A.III.3$ n'a été abordée que par très peu de candidats.

Dans $A.IV$, seule la première question a été souvent abordée.

Pour la partie $B1$, de nombreuses copies proposaient une démonstration très pénible de l'injectivité. Certains candidats ont montré qu'ils n'avaient pas compris le théorème chinois, qu'ils pouvaient néanmoins citer, puisqu'ils affirmaient que la surjectivité sur le produit résultait de la surjectivité sur chacun des facteurs. En général, seules les questions évidentes du $B.II$ ont été abordées. Les autres questions n'ont concerné que quelques candidats.
