Ulm, maths I. *Soit E un espace vectoriel normé de dimension finie n, muni d'une base $(e_i)_{i=1\dots n}$ telle que $\|\sum_i \lambda_i e_i\| = \|\sum_i |\lambda_i| e_i\|$ pour tout $\lambda \in \mathbb{R}^n$. 1) Montrer que si $|\alpha_i| \leq |\beta_i|$ pour tout i alors $\|\sum_i \alpha_i e_i\| \leq \|\sum_i \beta_i e_i\|$. 2) Montrer qu'il existe $\lambda \in \mathbb{R}^n$ tel que $\|\sum_i \lambda_i e_i\| = 1$ et $\|\sum_i \frac{e_i^*}{\lambda_i}\|_* = n$ ($\|\cdot\|_*$ norme opératorielle dans le dual, n dimension de l'espace).*

Indications : 1) En deux dimensions, considérer la fonction $\mu \mapsto \|\lambda e_1 + \mu e_2\|$. 2) Poser $K = \{\lambda \in \mathbb{R}_+^n \colon \|\sum_i \lambda_i e_i\| = 1\}$ et $\varphi \colon \lambda \mapsto \prod_i \lambda_i$.

Résolution : 1) On peut supposer les α_i, β_i positifs. Il s'agit alors de montrer que pour tout i et tous $(\lambda_j)_{j \neq i}$ positifs, la fonction $\mu \mapsto \|\mu e_i + \sum_{j \neq i} \lambda_j e_j\|$ est croissante sur $\mathbb{R}_+$. Pour simplifier les écritures, on prendra $n = 2$ et $j = 2$, le cas général se traitant exactement de la même manière. On s'intéresse donc à la fonction $\psi \colon \mu \mapsto \|\lambda e_1 + \mu e_2\|$. Cette fonction est clairement continue. Par ailleurs, si $\mu, \mu' \in \mathbb{R}$, on a l'inégalité triangulaire

$$\|2\lambda e_1 + \mu e_2 + \mu' e_2\| \leq \|\lambda e_1 + \mu e_2\| + \|\lambda e_1 + \mu' e_2\|$$

soit en termes de ψ :

$$2\psi\left(\frac{\mu + \mu'}{2}\right) \leq \psi(\mu) + \psi(\mu')$$

On a donc montré $\psi(\frac{\mu+\mu'}{2}) \leq \frac{1}{2}(\psi(\mu) + \psi(\mu'))$. On en déduit que pour tout θ rationnel dont le dénominateur est une puissance de 2 (rationnel dyadique), compris entre 0 et 1, on a

$$\psi(\theta\mu + (1-\theta)\mu') \leq \theta\psi(\mu) + (1-\theta)\psi(\mu')$$

Comme ces rationnels sont denses dans $]0;1[$ et que ψ est continue, l'inégalité ci-dessus est valable pour tout $\theta \in]0;1[$. Autrement dit, ψ est convexe. De plus, d'après l'hypothèse sur la base, ψ est paire. Or une fonction convexe paire est croissante sur $\mathbb{R}_+$ (démonstration : si $0 \leq \mu \leq \mu'$, la corde reliant $-\mu'$ à μ', qui est horizontale, est au-dessus de la corde reliant μ à μ'). Donc ψ est croissante sur $\mathbb{R}_+$, ce qu'il fallait démontrer.

2) L'ensemble $K := \{\lambda \in \mathbb{R}_+^n \colon \|\sum_i \lambda_i e_i\| = 1\}$ est clairement fermé. Il est borné par l'équivalence des normes, et il est donc compact. La fonction $\varphi \colon \lambda \mapsto \prod_i \lambda_i$ est continue, et atteint donc sa borne supérieure sur K. Soit λ un point où cette borne est atteinte. L'idée serait d'utiliser le théorème des extrema liés appliqué à φ ; seulement, on ne sait pas que celle-ci est différentiable, et il faut ruser. On a déjà $\|\sum_i \lambda_i e_i\| = 1$, et comme $\langle \sum_i \lambda_i e_i, \sum_i \frac{e_i^*}{\lambda_i} \rangle = n$, on en tire $\|\sum_i \frac{e_i^*}{\lambda_i}\|_* \geq n$. Reste à montrer l'inégalité dans l'autre sens. Pour cela, on note que l'on a $\varphi(\mu) \leq \varphi(\lambda)$ pour tout $\mu \in K$; en homogénéisant, on en tire, pour tout $\mu \in \mathbb{R}_+^n$:

$$\prod_i \mu_i \leq \left\|\sum_i \mu_i e_i\right\|^n \varphi(\lambda)$$

Appliquons cette inégalité avec $\mu = \lambda + \varepsilon y_i$, où $y \in \mathbb{R}^n$ et $\varepsilon > 0$ est petit. On a $\prod_i (\lambda_i + \varepsilon y_i) = \varphi(\lambda)(1 + \varepsilon \sum_i \frac{y_i}{\lambda_i} + o(\varepsilon))$. L'inégalité triangulaire donne $\|\sum_i (\lambda_i + \varepsilon y_i) e_i\| \leq 1 + \varepsilon \|\sum_i y_i e_i\|$, d'où $\|\sum_i (\lambda_i + \varepsilon y_i) e_i\|^n \leq 1 + n\varepsilon \|\sum_i y_i e_i\| + o(\varepsilon)$. En appliquant l'inégalité de ci-dessus, on trouve $1 + \varepsilon \sum_i \frac{y_i}{\lambda_i} + o(\varepsilon) \leq 1 + n\varepsilon \|\sum_i y_i e_i\| + o(\varepsilon)$, qui est une inégalité entre polynômes de ε. On a donc $\sum_i \frac{y_i}{\lambda_i} \leq n \|\sum_i y_i e_i\|$. Ceci traduit précisément $\|\sum_i \frac{e_i^*}{\lambda_i}\|_* \leq n$, ce qu'il fallait démontrer.

Ulm, maths II. *Soit $S_n = \{\zeta^i, i = 0..n-1\}$ l'ensemble des racines n-ièmes de l'unité. On considère une application $f\colon S_n \to \mathbb{U}$ ($\mathbb{U}$ le cercle unité). Montrer que pour tout $1 \leq k \leq \frac{n}{2}$ entier il existe i, j tels que $|\zeta^i - \zeta^j| \geq |1 - \zeta^k| \geq |f(\zeta^i) - f(\zeta^j)|$.*

Indication : On prendra la longueur du cercle égale à n. Montrer qu'il existe alors un arc de cercle fermé de longueur k contenant au moins $k+1$ points $f(\zeta^i)$.

Résolution : Occupons-nous tout d'abord de la seconde inégalité. Dans ce qui suit, on notera les arcs sur le cercle par des intervalles, en rapportant la longueur du cercle à n ; autrement dit, l'intervalle $[a; b[$ correspondra à l'arc image de cet intervalle par $t \mapsto e^{\frac{2i\pi t}{n}}$. Considérons, sous cette convention, les arcs semi-ouverts $[\alpha+\ell k; \alpha+(\ell+1)k[$ pour $0 \leq \ell < n$ (α réel fixé pour l'instant). Ils recouvrent k fois le cercle ; ainsi, si on note N_ℓ le nombre de points $f(\zeta^i)$ dans $[\alpha + \ell k; \alpha + (\ell+1)k[$, on a $\sum_{\ell=0}^{n-1} N_\ell = kn$. Si (pour un certain α) il existe ℓ tel que $N_\ell > k$, alors on a trouvé un arc $[\alpha + \ell k; \alpha + (\ell+1)k]$ fermé de longueur k contenant au moins $k+1$ points $f(\zeta^i)$. Sinon, on a $N_\ell = k$ pour tout ℓ, et ce, pour tout α. Autrement dit, tout arc semi-ouvert de longueur k contient k points $f(\zeta^i)$. En particulier, si $f(1) = e^{\frac{2i\pi\alpha}{n}}$, l'arc $[\alpha; \alpha+k[$ contient k points $f(\zeta^i)$, et l'arc $[\alpha+\varepsilon; \alpha+\varepsilon+k[$ en contient aussi k pour tout $\varepsilon > 0$; c'est donc que $[\alpha+k; \alpha+\varepsilon+k[$ en contient un, et ce, pour tout $\varepsilon > 0$. C'est donc que $\alpha+k$ est un des points $f(\zeta^i)$. Et l'arc $[\alpha; \alpha+k]$ contient donc $k+1$ points $f(\zeta^i)$. Notons I l'arc finalement trouvé (fermé de longueur k contenant $k+1$ points de l'image de f), et $T = \{\xi \in S_n\colon f(\xi) \in I\}$. T est un sous-ensemble de S_n de cardinal au moins $k+1$, et si $\xi, \xi' \in T$ alors $f(\xi), f(\xi') \in I$ donc $|f(\xi) - f(\xi')| \leq |1 - \zeta^k|$. On a terminé avec la seconde inégalité.

Passons à présent à la première : on veut montrer qu'il existe $\xi, \xi' \in T$ tels que $|\xi - \xi'| \geq |1 - \zeta^k|$, et pour cela, on sait simplement que T à au moins $k+1$ éléments. Pour commencer, on peut supposer, quitte à effectuer une rotation, que $1 \in T$. Supposons par l'absurde que pour $\xi, \xi' \in T$ on ait toujours $|\xi - \xi'| < |1 - \zeta^k|$. Alors, puisque $1 \in T$, on a $T \subseteq \{\zeta^i\colon -k < i < k\} =: Z$. L'ensemble $Z^* := Z \setminus \{1\}$ a $2k-2$ éléments. Considérons la fonction

$$\psi\colon \zeta^i \mapsto \begin{cases} \zeta^{i+k} \text{ si } -k < i < 0 \\ \zeta^{i-k} \text{ si } 0 < i < k \end{cases}$$

Il est clair que ψ est une permutation de Z^*. Par ailleurs, si $T^* = T \setminus \{1\}$, les ensembles T^* et $\psi(T^*)$ doivent être disjoints puisqu'on a supposé que pour $\xi, \xi' \in T$ on a toujours $|\xi - \xi'| < |1 - \zeta^k|$. On a donc deux sous-ensembles disjoints, $T^*, \psi(T^*)$, ayant chacun au moins k éléments, d'un ensemble Z^*, qui en a $2k-2$. Ceci est une contradiction. C'est donc qu'il existe $\xi, \xi' \in T$ tels que $|\xi - \xi'| \geq |1 - \zeta^k|$. Et on sait déjà que $|f(\xi) - f(\xi')| \leq |1 - \zeta^k|$. Il existe donc i, j tels que $|\zeta^i - \zeta^j| \geq |1 - \zeta^k| \geq |f(\zeta^i) - f(\zeta^j)|$, ce qu'il fallait démontrer.

Lyon, maths I. *1) Soit $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ un homéomorphisme. Soit $a \in \mathbb{R}^2, r > 0$. On pose $M_f(a, r) = \sup\{\|f(x) - f(a)\|\colon \|x - a\| \leq r\}$: montrer que le $\sup$ en question n'est atteint que pour des points x tels que $\|x - a\| = r$. 2) Montrer que la fonction $r \mapsto M_f(a, r)$ est strictement croissante. 3) On pose maintenant $m_f(a, r) = \inf\{\|f(x) - f(a)\|\colon \|x - a\| \geq r\}$: montrer que l'$\inf$ en question est atteint, et n'est atteint que pour des points x tels que $\|x - a\| = r$. 4) Montrer que la fonction $r \mapsto m_f(a, r)$ est strictement croissante. 5) On a clairement $m_f(a, r) \leq M_f(a, r)$. On supposera désormais qu'il existe une constante $K_f \geq 1$ telle que pour tous a et r on ait $m_f(a, r) \leq M_f(a, r) \leq K_f m_f(a, r)$ (dans ces circonstances, on dit que l'homéomorphisme f est <u>quasi-conforme</u>). Montrer qu'alors $M_f(a, 2r) \leq (1 + K_f) M_f(a, r)$. 6) Montrer que $m_f(a, 2r) \geq (1 + K_f^{-1}) m_f(a, r)$. 7) Les homéomorphismes quasi-conformes forment un groupe pour la composition : montrer que du moins l'inverse d'un homéomorphisme quasi-conforme est un homéomorphisme quasi-conforme.*

Résolution : 1) Soit x tel que $\|x-a\| < r$, et soit $\varepsilon < r - \|x-a\|$. D'après la continuité de f^{-1}, il existe $\delta > 0$ tel que si $\|f(y) - f(x)\| < \delta$ alors $\|y - x\| < \varepsilon$, donc $\|y - a\| < r$. Or il existe certainement des z tels que $\|z - f(a)\| > \|f(x) - f(a)\|$ et $\|z - f(x)\| < \delta$; si $y = f^{-1}(z)$, on a alors $\|y - a\| < r$ et $\|f(y) - f(a)\| > \|f(x) - f(a)\|$. Ceci montre que le sup n'est pas atteint en x, ce qu'il fallait démontrer.

2) La fonction en question est clairement croissante. Supposons maintenant par l'absurde qu'on ait $r < r'$ et $M_f(a,r) = M_f(a,r')$. Soit x tel que $\|x - a\| = r$ et $\|f(x) - f(a)\| = M_f(a,r)$. On a alors $\|x-a\| < r'$ et $\|f(x) - f(a)\| = M_f(a,r')$, contredisant le 1). C'est donc que $M_f(a,\cdot)$ est strictement croissante, ce qu'il fallait démontrer.

3) $\{x\colon \|x - a\| \geq r\}$ est fermé, donc son image par f l'est aussi (puisque f^{-1} est continue), et elle ne contient pas $f(a)$. On peut alors aisément se ramener à un compact pour montrer que l'inf est atteint. La fin de la question se traite comme le 1).

4) Se traite comme le 2).

5) Soit y tel que $\|y - a\| = 2r$ et $\|f(y) - f(a)\| = M_f(a,2r)$, et soit $x = \frac{1}{2}(a + y)$ le milieu de $[ay]$. On a $M_f(a,2r) = \|f(y) - f(a)\| \leq \|f(x) - f(a)\| + \|f(y) - f(x)\| \leq M_f(a,r) + M_f(x,r) \leq M_f(a,r) + K_f m_f(x,r) \leq M_f(a,r) + K_f\|f(x) - f(a)\| \leq M_f(a,r) + K_f M_f(a,r) = (1 + K_f)M_f(a,r)$, d'où le résultat.

6) Soit y tel que $\|y - a\| = 2r$ et $\|f(y) - f(a)\| = m_f(a,2r)$. Lorsque z se déplace sur le segment entre $f(a)$ et $f(y)$, $\|f^{-1}(z) - a\|$ varie continuement de 0 à $2r$. Il passe donc par la valeur r : soit donc $z \in [f(a)\, f(y)]$ tel que $\|f^{-1}(z) - a\| = r$, et $x = f^{-1}(z)$. On a $m_f(a,2r) = \|f(y) - f(a)\| = \|z - f(a)\| + \|f(y) - z\| = \|f(x) - f(a)\| + \|f(y) - f(x)\| \geq m_f(a,r) + m_f(x,r) \geq m_f(a,r) + K_f^{-1}M_f(x,r) \geq m_f(a,r) + K_f^{-1}\|f(x) - f(a)\| \geq (1 + K_f^{-1})m_f(a,r)$, d'où le résultat.

7) Supposons par l'absurde que f^{-1} ne soit pas quasi-conforme. Alors pour tout ℓ il existe b et r tels que $M_{f^{-1}}(b,r) \geq 2^\ell m_{f^{-1}}(b,r)$; et il existe alors z, t tels que $\|z - b\| = \|t - b\| = r$ et $M_{f^{-1}}(b,r) = \|f^{-1}(t) - f^{-1}(b)\| \geq 2^\ell\|f^{-1}(z) - f^{-1}(b)\| = 2^\ell m_{f^{-1}}(b,r)$. Si on pose $a = f^{-1}(b)$, $x = f^{-1}(z)$ et $y = f^{-1}(t)$, on a alors $\|f(y) - f(a)\| = \|f(x) - f(a)\|$, et $\|y - a\| \geq 2^\ell\|x - a\|$. Or $\|f(y) - f(a)\| \geq m_f(a, \|y - a\|) \geq m_f(a, 2^\ell\|x - a\|) \geq (1+K_f^{-1})^\ell m_f(a,\|x-a\|) \geq K_f^{-1}(1+K_f^{-1})^\ell M_f(a,\|x-a\|) \geq K_f^{-1}(1+K_f^{-1})^\ell\|f(x)-f(a)\|$, et donc $(1 + K_f^{-1})^\ell \leq K_f$ pour tout ℓ. Ceci est clairement une contradiction, donc f^{-1} est quasi-conforme, ce qu'il fallait démontrer.

Lyon, maths II. *Soit $A \in \mathbb{M}_2(\mathbb{Z})$ une matrice 2×2 à coefficients entiers, telle que $A \neq I_2$ et $A^3 = I_2$. Montrer qu'alors A est semblable sur $\mathbb{Z}$ à la matrice $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ (c'est-à-dire qu'il existe une matrice P inversible à coefficients entiers d'inverse à coefficients entiers telle que $P^{-1}AP$ soit la matrice écrite ci-dessus).*

Indication : Montrer qu'on peut se ramener à prouver qu'il existe $x \in \mathbb{Z}^2$ tel que $\det(x, Ax) = \pm 1$.

Résolution : On cherche à trouver une $\mathbb{Z}$-base de $\mathbb{Z}^2$ sur laquelle (l'endomorphisme associé à) A prend la forme voulue. D'après la première colonne, on voit qu'une telle base sera formée d'un vecteur $x \in \mathbb{Z}^2$ et de son image Ax par A. La matrice de passage P étant alors celle dont la première colonne est x et la seconde Ax, il faut qu'elle soit inversible dans $\mathbb{M}_2(\mathbb{Z})$. Il faut pour cela que le déterminant de P soit entier, et que son inverse, le déterminant de P^{-1} le soit aussi, c'est-à-dire en fin de compte que $\det(x, Ax) = \pm 1$. Réciproquement, si on trouve un tel x, la matrice P dont la première colonne est x et la seconde Ax sera à coefficients entiers, et d'après les formules de Cramér, elle sera inversible. La matrice $P^{-1}AP$ aura pour première colonne $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Nous allons à présent montrer que la seconde colonne sera bien $\begin{pmatrix} -1 \\ -1 \end{pmatrix}$. Pour cela, on constate que le polynôme à racines simples $X^3 - 1$ annule A ; A est donc diagonalisable et ses valeurs propres sont incluses dans l'ensemble $\{1, j, j^2\}$. Or si j est valeur propre de A, $\bar{\jmath} = j^2$ est valeur propre de $\bar{A} = A$; ainsi, si 1 est valeur propre de A, elle est la seule, et donc $A = I_2$ puisque A est diagonalisable, contradiction. Les valeurs propres de A sont donc j, j^2, et on en déduit que la trace de A est $j + j^2 = -1$ et son déterminant, $jj^2 = 1$. Mais alors le polynôme caractéristique de A est $X^2 + X + 1$. D'après Cayley-Hamilton, on a $A^2 + A + 1 = 0$, et en particulier $A^2x = -Ax - x$, ce qui donne précisément la seconde colonne égale à $\begin{pmatrix} -1 \\ -1 \end{pmatrix}$.

Tout revient donc à montrer qu'il existe $x \in \mathbb{Z}^2$ tel que $\det(x, Ax) = \pm 1$. Soit $A = \begin{pmatrix} a & b \\ c & -1-a \end{pmatrix}$ (on sait que $\operatorname{tr} A = -1$), et $x = \begin{pmatrix} u \\ v \end{pmatrix}$. Alors on vérifie aussitôt que

$$Q(x) := \det(x, Ax) = cu^2 - (1 + 2a)uv - bv^2$$

Q est alors une forme quadratique sur $\mathbb{Z}^2$. Son discriminant sur la base canonique est $-bc - \frac{1}{4}(1 + 2a)^2 = -a - a^2 - bc - \frac{1}{4}$. Or le déterminant de A est $a(-1 - a) - bc = -a - a^2 - bc$, et on sait qu'il vaut 1. Par conséquent, le discriminant de Q est $\frac{3}{4}$. En particulier, Q garde un signe constant (celui de c) ; si ce signe est positif, on peut espérer atteindre la valeur 1, et s'il est négatif, la valeur -1. On supposera désormais que Q est positive, et on cherchera à montrer qu'elle prend la valeur 1. Puisque Q est à coefficients entiers, il suffit pour cela de montrer qu'elle prend en un point de $\mathbb{Z}^2 \setminus \{(0, 0)\}$ une valeur ≤ 1.

On peut désormais tout oublier sauf ceci : on a une forme quadratique $Q(u, v) = ru^2 + suv + tv^2$ de discriminant $rt - \frac{1}{4}s^2 = \frac{3}{4}$, avec $r, t > 0$, et on cherche à montrer qu'elle prend pour un couple $(u, v) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ une valeur ≤ 1. Commençons par décomposer Q suivant la méthode de Gauss :

$$\begin{aligned}
Q(u, v) &= ru^2 + suv + tv^2 \\
&= r\left(u^2 + \frac{s}{r}uv + \frac{t}{r}v^2\right) \\
&= r\left[\left(u + \frac{s}{2r}v\right)^2 - \frac{s^2}{4r^2}v^2 + \frac{t}{r}v^2\right] \\
&= \left(\sqrt{r}u + \frac{s}{2\sqrt{r}}v\right)^2 + \left(\sqrt{t - \frac{s^2}{4r}}v\right)^2 \\
&= \left(\sqrt{r}u + \frac{s}{2\sqrt{r}}v\right)^2 + \left(\sqrt{\frac{3}{4r}}v\right)^2 \\
&= X^2 + Y^2
\end{aligned}$$

avec $X(u, v) = \sqrt{r}u + \frac{s}{2\sqrt{r}}v$ et $Y(u, v) = \sqrt{\frac{3}{4r}}v$. Dans le plan (X, Y), l'ensemble des points dont les coordonnées (u, v) sont entières, autrement dit, l'image de $\mathbb{Z}^2$ par $(u, v) \mapsto (X(u, v), Y(u, v))$, est un réseau $\mathcal{R}$ de points, qui n'est autre que l'ensemble des translatés de l'origine par les vecteurs de la forme $m\vec{p} + n\vec{q}$ où $m, n \in \mathbb{Z}$ et

$$\vec{p} = \begin{pmatrix} \sqrt{r} \\ 0 \end{pmatrix}$$

$$\vec{q} = \begin{pmatrix} \frac{s}{2\sqrt{r}} \\ \sqrt{\frac{3}{4r}} \end{pmatrix}$$

c'est-à-dire le réseau engendré par $\vec{p}$ et $\vec{q}$. On a $|\det(\vec{p},\vec{q})| = \sqrt{\frac{3}{4}}$. Notons maintenant que les deux opérations suivantes ne modifient pas la valeur de $|\det(\vec{p},\vec{q})|$, ni le réseau engendré par $\vec{p}$ et $\vec{q}$:

- Échanger $\vec{p}$ et $\vec{q}$ de façon à avoir $|\vec{p}| \leq |\vec{q}|$.
- Remplacer $\vec{q}$ par $\vec{q} + k\vec{p}$ où $k \in \mathbb{Z}$ de façon à avoir $|\vec{p} \cdot \vec{q}| \leq \frac{1}{2}\|\vec{p}\|^2$.

En appliquant alternativement ces deux opérations, on arrive à deux nouveaux vecteurs $\vec{p}$ et $\vec{q}$ qui engendrent toujours le même réseau $\mathcal{R}$ et qui vérifient toujours $|\det(\vec{p},\vec{q})| = \sqrt{\frac{3}{4}}$, avec de plus les conditions $\|\vec{p}\| \leq \|\vec{q}\|$ et $|\vec{p}\cdot\vec{q}| \leq \frac{1}{2}\|\vec{p}\|^2$; le processus doit nécessairement aboutir, puisque chaque application de la première opération diminue la norme de $\vec{p}$ (et l'ensemble des valeurs qu'elle peut prendre est discret). Soit maintenant θ l'angle géométrique entre les (nouveaux) vecteurs $\vec{p}$ et $\vec{q}$: d'après les conditions imposées, on a $|\cos\theta| \leq \frac{1}{2}$, et donc $\sin\theta \geq \sqrt{\frac{3}{4}}$; la condition sur le déterminant donne alors $\|\vec{p}\|\,\|\vec{q}\| \leq 1$; On en déduit $\|\vec{p}\| \leq 1$. On a ainsi trouvé un point du réseau $\mathcal{R}$ dont la distance à l'origine est ≤ 1, donc enfin un couple $(u,v) \in \mathbb{Z}^2\backslash\{(0,0)\}$ tel que $Q(u,v) = X(u,v)^2 + Y(u,v)^2 \leq 1$, ce qu'il fallait démontrer.

Cachan, maths I. *On considère le système différentiel suivant :*

$$\begin{cases} \dot{x} = y - f(x) \\ \dot{y} = -x \end{cases}$$

où $f(x) = x^3 - x$. Montrer géométriquement qu'il existe une orbite périodique attractrice unique.

Note : L'examinateur a beaucoup insisté sur le fait qu'il n'était pas question de produire une démonstration rigoureuse. En particulier, "il ne faut pas commencer par "soit $\varepsilon > 0$"".

Indication : Si p est un point de l'axe des ordonnées, on notera $\sigma(p)$ le point de l'axe des ordonnées atteint "après un tour". Montrer que σ est bien définie et strictement croissante. Pour étudier son comportement en 0, on étudiera le système linéarisé.

Cachan, maths II. *Si P est un polynôme à coefficient entiers, on définit son contenu $c(P)$ comme le PGCD de ses coefficients. 1) Montrer que $c(PQ) = c(P)\,c(Q)$. 2) Montrer que les polynômes irréductibles sur $\mathbb{Z}[X]$ sont exactement les nombres premiers (et leurs opposés), et les polynômes à coefficients entiers irréductibles sur $\mathbb{Q}[X]$ et de contenu 1. 3) Montrer que $\mathbb{Z}[X]$ est un anneau factoriel.*

Résolution : 1) Commençons par remarquer que pour tout polynôme $P \in \mathbb{Z}[X]$ non nul on peut écrire $P = c(P)\,P_0$ où $P_0 \in \mathbb{Z}[X]$ est un polynôme de contenu 1 ; et réciproquement, si $P = \gamma P_0$ où $P_0 \in \mathbb{Z}[X]$ est un polynôme de contenu 1 alors $c(P) = \gamma$ (ces deux affirmations découlent des propriétés correspondantes du PGCD). On peut alors écrire $P = c(P)\,P_0$ et $Q = c(Q)\,Q_0$ avec les notations ci-dessus, et on a $PQ = c(P)\,c(Q)\,P_0Q_0$. On aura donc fini si on montre que $R := P_0Q_0$ est de contenu 1. On constate à présent que pour tout premier p, l'application $\varphi_p\colon \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ de réduction modulo p des coefficients, est un morphisme d'anneaux (vérification immédiate). Si p est un diviseur premier de $c(R)$, alors il divise tous les coefficients de R ; autrement dit $\varphi_p(R) = 0$. Puisque φ_p est un morphisme d'anneaux, on a $\varphi_p(P_0)\,\varphi_p(Q_0) = 0$.

Mais l'anneau $(\mathbb{Z}/p\mathbb{Z})[X]$ des polynômes sur le corps $\mathbb{Z}/p\mathbb{Z}$ est intègre. On a donc $\varphi_p(P_0) = 0$ ou $\varphi_p(Q_0) = 0$. Le premier implique $p|c(P_0)$ et le second, $p|c(Q_0)$. Dans tous les cas, une contradiction. C'est donc que $c(R)$ n'a pas de diviseurs premiers, soit $c(R) = 1$, ce qu'il fallait démontrer.

2) Les unités de $\mathbb{Z}[X]$ sont clairement $+1$ et -1. Cela étant dit, montrons tout d'abord que les nombres premiers (et donc aussi leurs opposés) sont irréductibles sur $\mathbb{Z}[X]$: si p est premier et qu'on a $p = PQ$ sur $\mathbb{Z}[X]$, alors $\deg P + \deg Q = 0$ (puisque $\mathbb{Z}$ est intègre), donc $\deg P = \deg Q = 0$, et P et Q sont des entiers, et alors l'un des deux doit être une unité puisque p est premier, donc p est irréductible sur $\mathbb{Z}[X]$. Soit maintenant R un polynôme irréductible sur $\mathbb{Q}[X]$, à coefficients entiers et de contenu 1 ; montrons qu'il est irréductible sur $\mathbb{Z}[X]$. Or si on a $R = PQ$ sur $\mathbb{Z}[X]$, puisque R est irréductible sur $\mathbb{Q}[X]$, on doit avoir P ou Q une unité de $\mathbb{Q}[X]$, c'est-à-dire, constant. Supposons donc $P = \gamma \in \mathbb{Z}$. Alors γ divise le contenu de R, donc $\gamma = \pm 1$, et R est bien irréductible.

Réciproquement, supposons que $R \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Z}[X]$, et écrivons $R = c(R)\, R_0$ avec les notations utilisées plus haut. L'un des deux facteurs doit être ± 1. Si c'est R_0, on a $R = \pm c(R)$, et $c(R)$ doit être premier, car si $c(R) = rs$ avec r, s entiers > 1, on a $R = \pm rs$ et R n'est pas irréductible. Si c'est $c(R)$, alors R est un polynôme à coefficients entiers de contenu 1, et il reste à montrer qu'il est irréductible sur $\mathbb{Q}[X]$. Or si on a $R = PQ$ sur $\mathbb{Q}[X]$, on peut trouver des rationnels α, β non nuls tels que $P = \alpha P_0$ et $Q = \beta Q_0$ avec P_0, Q_0 des polynômes à coefficients entiers de contenu 1. On a alors $R = \alpha\beta P_0 Q_0$, et donc $\alpha\beta$ est un entier (puisque $c(P_0 Q_0) = 1$). Enfin, puisque R est irréductible sur $\mathbb{Z}[X]$, un des polynômes P_0, Q_0 au moins est égal à ± 1, et donc un des polynômes P, Q au moins est constant. Donc R est irréductible sur $\mathbb{Q}[X]$, ce qu'il fallait démontrer.

3) Tout d'abord, il faut choisir un système de représentants irréductibles : on choisit pour cela les nombres premiers (positifs), et les polynômes irréductibles de contenu 1 de coefficient dominant positif. Montrons l'existence de la décomposition : si $P \in \mathbb{Z}[X]$, on peut le décomposer en facteurs irréductibles sur $\mathbb{Q}[X]$, de la forme : $P = \alpha P_1 \cdots P_k$ où $\alpha \in \mathbb{Q}$ et $P_1, \ldots P_k \in \mathbb{Q}[X]$ sont unitaires irréductibles. On peut alors écrire $P_i = \alpha_i P_{0i}$ pour chaque i, où $\alpha_i \in \mathbb{Q}$ et $P_{0i} \in \mathbb{Z}[X]$ est de contenu 1 à coefficient dominant positif. Dans ce cas, $P = \alpha\alpha_1 \cdots \alpha_k P_{01} \cdots P_{0k}$, et comme $c(P_{01} \cdots P_{0k}) = 1$, on a $\alpha\alpha_1 \cdots \alpha_k \in \mathbb{Z}$; et en décomposant en facteurs premiers $\alpha\alpha_1 \cdots \alpha_k = \pm p_1 \cdots p_\ell$, on a la décomposition de P recherchée :

$$P = \pm p_1 \cdots p_\ell P_{01} \cdots P_{0k}$$

Reste enfin à montrer l'unicité d'une telle décomposition : si $P = \pm q_1 \cdots q_n Q_{01} \cdots Q_{0m}$ en est une autre, avec $q_1, \ldots, q_\ell$ des nombres premiers, et $Q_{01}, \ldots, Q_{0k}$ des polynômes à coefficients entiers de contenu 1 et irréductibles sur $\mathbb{Q}[X]$, alors tout d'abord le signe est clairement le même. Comme on a $p_1 \cdots p_\ell = c(P) = q_1 \cdots q_n$, les p_i et les q_j sont égaux à permutation près d'après l'unicité de la décomposition en facteurs premiers. Enfin, d'après l'unicité de la décomposition sur $\mathbb{Q}[X]$, les P_{0i} et les Q_{0j} sont proportionnels à permutation près, et comme ils sont à coefficients entiers de contenu 1, ils sont en fait égaux à permutation près. La décomposition est donc unique, et $\mathbb{Z}[X]$ est factoriel, ce qu'il fallait démontrer.