

# Concours commun ENS Ulm–Lyon 1995, MP, Mathématiques

## Corrigé

Dans tout le problème,  $[\theta]$  désigne la partie entière de  $\theta \in \mathbb{R}$ ,  $\{\theta\} = \theta - [\theta]$  sa partie fractionnaire. Les énoncés formels et leurs preuves sont également formalisés en Lean 4 dans le dossier `UlmLyon1995/` ; voir les modules `PartieI.lean`, `PartieII.lean`, `PartieIII.lean`, `PartieIV.lean`.

## 1 Partie I — Approximation diophantienne

Dans cette partie, on note  $\|\theta\| = \inf(\{\theta\}, 1 - \{\theta\})$ , c'est-à-dire la distance de  $\theta$  à l'entier le plus proche.

### Question I.1.a

**Énoncé.** Soit  $\theta \in \mathbb{R}$  et  $Q > 1$  deux réels. Considérons

$$A = \{q \in ]0, Q[ \cap \mathbb{N} \mid \|q\theta\| \leq Q^{-1}\}, \quad B = \{q \in ]0, Q[ \cap \mathbb{N} \mid \|q\theta\| < Q^{-1}\}.$$

$A$  et  $B$  peuvent-ils être vides ?

**Réponse.**

—  $A$  n'est jamais vide.

—  $B$  peut être vide (contre-exemple :  $\theta = 1/2$ ,  $Q = 2$ ). En revanche, si  $\theta \notin \mathbb{Q}$ ,  $B$  est non vide.

**Démonstration que  $A \neq \emptyset$ .** Posons  $M = \lfloor Q \rfloor \geq 1$  (puisque  $Q > 1$ ) et  $N = \lceil Q \rceil$ , de sorte que  $N = M$  si  $Q \in \mathbb{Z}$  et  $N = M + 1$  sinon. Considérons les  $M + 2$  points de  $[0, 1]$  :

$$x_0 = 0, \quad x_q = \{q\theta\} \text{ pour } q \in \{1, \dots, M\}, \quad x_{M+1} = 1.$$

Notez bien que  $\{q \in \mathbb{N} \mid 0 < q < Q\} = \{1, \dots, M\}$  dans tous les cas. Découpons  $[0, 1]$  en les  $N$  sous-intervalles fermés

$$J_k = [kQ^{-1}, (k+1)Q^{-1}] \text{ pour } k = 0, \dots, N-2, \quad J_{N-1} = [(N-1)Q^{-1}, 1],$$

chacun de longueur au plus  $Q^{-1}$ . Leur réunion couvre  $[0, 1]$ .

Comme  $M + 2 > N$  (en effet  $N \leq M + 1 < M + 2$ ), le principe des tiroirs fournit deux indices  $i < j$  dans  $\{0, \dots, M + 1\}$  et un sous-intervalle  $J_k$  contenant tous deux  $x_i$  et  $x_j$ . On a donc  $|x_j - x_i| \leq Q^{-1}$ . Distinguons trois cas selon les valeurs de  $i, j$  :

(a) Si  $1 \leq i < j \leq M$  : posons  $q = j - i \in ]0, Q[ \cap \mathbb{N}$  et  $p = [j\theta] - [i\theta] \in \mathbb{Z}$ . Alors

$$q\theta - p = (j\theta - [j\theta]) - (i\theta - [i\theta]) = x_j - x_i \in [-Q^{-1}, Q^{-1}],$$

donc  $\|q\theta\| \leq |q\theta - p| \leq Q^{-1}$ , et  $q \in A$ .

(b) Si  $i = 0$  et  $j \leq M$  : alors  $x_j \leq Q^{-1}$ , donc  $\{j\theta\} \leq Q^{-1}$  et a fortiori  $\|j\theta\| \leq \{j\theta\} \leq Q^{-1}$ . Comme  $0 < j \leq M < Q$  (sauf le cas  $Q$  entier où  $j \leq Q - 1 < Q$ ), on a  $j \in A$ .

(c) Si  $j = M + 1$  : alors  $x_j = 1$ ,  $i \in \{1, \dots, M\}$  (le cas  $i = 0$  donnerait  $1 - 0 = 1 \leq Q^{-1}$ , absurde puisque  $Q > 1$ ), et  $1 - x_i \leq Q^{-1}$ , donc  $\|i\theta\| \leq 1 - \{i\theta\} \leq Q^{-1}$ , d'où  $i \in A$ .

Ainsi  $A \neq \emptyset$ . □

**Contre-exemple pour  $B$ .** Soit  $\theta = 1/2$  et  $Q = 2$ . Alors  $]0, Q[ \cap \mathbb{N} = \{1\}$  et  $\|1 \cdot \theta\| = \|1/2\| = 1/2 = Q^{-1}$ , donc l'inégalité stricte  $\|q\theta\| < Q^{-1}$  n'est jamais satisfaite. Donc  $B = \emptyset$ .

**Cas  $\theta \notin \mathbb{Q}$ .** Supposons  $\theta \notin \mathbb{Q}$  et reprenons la preuve de  $A \neq \emptyset$ . Si l'on avait  $\|q\theta\| = Q^{-1}$  pour le  $q$  obtenu, on aurait  $q\theta \in p \pm Q^{-1} + \mathbb{Z}$  pour un certain  $p \in \mathbb{Z}$ , donc  $\theta \in \mathbb{Q}$ , absurde. Ainsi  $\|q\theta\| < Q^{-1}$  et  $B \neq \emptyset$ .  $\square$

**Lean.** `dirichlet_A_nonempty` dans `PartieI.lean` formalise le résultat principal  $A \neq \emptyset$  via le théorème de Dirichlet de Mathlib (`Real.exists_rat_near_self`). Le cas  $\theta \notin \mathbb{Q}$  donnant  $B \neq \emptyset$  est utilisé implicitement dans I.2 via `Irrational.normInt_pos`.

## Question I.1.b

**Énoncé.** Que peut-on dire du nombre de solutions de l'inéquation  $q \|q\theta\| < 1$ ,  $q \in \mathbb{N}$ ?

**Réponse.** Quel que soit  $\theta \in \mathbb{R}$ , cette inéquation admet *une infinité* de solutions.

**Démonstration.** On montre qu'il existe une suite strictement croissante  $(q_n)$  d'entiers  $\geq 1$  vérifiant  $q_n \|q_n\theta\| < 1$ .

**Cas  $\theta \in \mathbb{Q}$ .** Écrivons  $\theta = a/b$  avec  $b \in \mathbb{N}^*$ . Alors pour tout  $n \geq 1$ ,  $q_n = nb \in \mathbb{N}^*$  vérifie  $q_n\theta = na \in \mathbb{Z}$ , donc  $\|q_n\theta\| = 0$  et  $q_n \|q_n\theta\| = 0 < 1$ . La suite  $(q_n)$  est strictement croissante.

**Cas  $\theta \notin \mathbb{Q}$ .** Pour tout  $q \in \mathbb{N}^*$ ,  $q\theta \notin \mathbb{Z}$  donc  $\|q\theta\| > 0$ . Construisons récursivement  $(q_n)$ . On pose  $q_1 = 1$  (licite car  $\|\theta\| < 1$ , donc  $1 \cdot \|\theta\| < 1$ ). Supposons  $q_1 < \dots < q_n$  construits avec  $q_k \|q_k\theta\| < 1$ .

Choisissons un entier  $Q > q_n$  tel que  $Q^{-1} < \min_{1 \leq k \leq q_n} \|k\theta\|$  (possible car le minimum est strictement positif). Par I.1.a, il existe  $q \in ]0, Q[ \cap \mathbb{N}$  avec  $\|q\theta\| \leq Q^{-1}$ . Si  $q \leq q_n$ , alors  $\|q\theta\| \geq \min_{1 \leq k \leq q_n} \|k\theta\| > Q^{-1}$ , contradiction. Donc  $q > q_n$ . On pose  $q_{n+1} = q$ ; on a alors  $q_{n+1} \|q_{n+1}\theta\| \leq q_{n+1} \cdot Q^{-1} < 1$  puisque  $q_{n+1} < Q$ .  $\square$

## Question I.2

**Énoncé I.2.a.** Soit  $\theta \in \mathbb{R} \setminus \mathbb{Q}$ . Montrer qu'il existe deux suites d'entiers relatifs  $(p_n)_{n \geq 1}$  et  $(q_n)_{n \geq 1}$  vérifiant :

- (i)  $q_1 = 1$  et la suite  $(q_n)_{n \geq 1}$  est strictement croissante ;
- (ii) pour tout  $n \in \mathbb{N}^*$ ,  $\|q_n\theta\| = |q_n\theta - p_n|$  ;
- (iii) la suite  $(\|q_n\theta\|)_{n \geq 1}$  est strictement décroissante ;
- (iv) pour tout  $n \in \mathbb{N}^*$  et tout entier  $q$  tel que  $0 < q < q_{n+1}$ , on a  $\|q\theta\| \geq \|q_n\theta\|$ .

Sont-elles uniques ?

**Construction.** On construit  $(q_n)$  par récurrence. On pose  $q_1 = 1$  et  $p_1$  est l'entier le plus proche de  $\theta$  (univoque puisque  $\theta \notin \mathbb{Q}$  implique  $\theta \notin \frac{1}{2} + \mathbb{Z}$ ). Alors  $\|q_1\theta\| = \|\theta\| = |q_1\theta - p_1| > 0$ .

Supposons construits  $q_1 < q_2 < \dots < q_n$  vérifiant (ii) pour les indices considérés. Posons

$$S_n = \{q \in \mathbb{N}^* \mid q > q_n, \|q\theta\| < \|q_n\theta\|\}.$$

$S_n$  est non vide. En effet, posons  $\delta_n = \min\{\|k\theta\| : 1 \leq k \leq q_n\}$ . Comme  $\theta \notin \mathbb{Q}$ ,  $\|k\theta\| > 0$  pour tout  $k \geq 1$ , donc  $\delta_n > 0$ . Choisissons un entier  $Q$  tel que  $Q^{-1} < \delta_n$  et  $Q > q_n$ . Par I.1.a, il existe  $q \in ]0, Q[ \cap \mathbb{N}$  avec  $\|q\theta\| \leq Q^{-1} < \delta_n$ . En particulier  $\|q\theta\| < \|k\theta\|$  pour tout  $k \in \{1, \dots, q_n\}$ , donc  $q > q_n$ ; de plus  $\|q\theta\| < \delta_n \leq \|q_n\theta\|$ , donc  $q \in S_n$ .

On définit alors  $q_{n+1} = \min S_n$  (existe car  $\mathbb{N}$  est bien ordonné). On a ainsi  $q_{n+1} > q_n$  (donc (i)) et  $\|q_{n+1}\theta\| < \|q_n\theta\|$  (donc (iii)). On pose  $p_{n+1} = \text{round}(q_{n+1}\theta) \in \mathbb{Z}$  pour satisfaire (ii).

**Vérification de (iv).** Soit  $0 < q < q_{n+1}$ . Si  $q = q_n$ , alors  $\|q\theta\| = \|q_n\theta\|$ . Si  $q_n < q < q_{n+1}$ , par minimalité de  $q_{n+1}$ ,  $q \notin S_n$  donc  $\|q\theta\| \geq \|q_n\theta\|$ . Si  $q < q_n$ , on procède par récurrence (descendante) en utilisant (iv) au rang  $n - 1$  : plus précisément, on raisonne par récurrence sur  $n$ . Pour  $n = 1$ ,  $0 < q < q_2$  et  $q \neq 1$  implique  $q \in S_1$  avec  $q < q_2$ , contradiction. Pour  $n \geq 2$ , l'hypothèse de récurrence donne  $\|q\theta\| \geq \|q_{n-1}\theta\| > \|q_n\theta\|$  par (iii).  $\square$

**Unicité.** Les propriétés déterminent uniquement les suites. En effet,  $q_1 = 1$  est imposé par (i). Étant donné  $q_n$ , par minimalité dans (iv),  $q_{n+1}$  est le plus petit entier  $> q_n$  tel que  $\|q\theta\| < \|q_n\theta\|$ , unique. Quant à  $p_n$ , il est défini par  $|q_n\theta - p_n| = \|q_n\theta\|$ , soit  $p_n = q_n\theta \pm \|q_n\theta\|$  ; si  $\|q_n\theta\| < \frac{1}{2}$ , un seul choix donne un entier. Si  $\|q_n\theta\| = \frac{1}{2}$ , il y a en théorie deux choix, mais  $\theta \notin \mathbb{Q}$  exclut ce cas. Donc  $p_n$  est unique.

**Cas rationnel (I.2.b).** Si  $\theta \in \mathbb{Q}$ ,  $\theta = a/b$  irréductible avec  $b \geq 1$ . Alors  $\|b\theta\| = 0$ , ce qui empêche la stricte décroissance (iii) au-delà d'un certain rang. La modification est : les suites  $(p_n)$  et  $(q_n)$  sont *finies*. Plus précisément, il existe un entier  $N \geq 1$  tel que  $(p_n)_{1 \leq n \leq N}$  et  $(q_n)_{1 \leq n \leq N}$  vérifient (i), (ii), (iii) et :

- $\|q_N\theta\| = 0$  (i.e.  $q_N\theta \in \mathbb{Z}$ ) ; en fait  $q_N = b$  et  $p_N = a$  (à un signe près pour les conventions de `round`) ;
- (iv) reste vraie pour  $1 \leq n < N$ .

Sinon, si  $\theta \in \mathbb{Z}$ , alors  $q_1 = 1, p_1 = \theta, N = 1$  et  $\|q_1\theta\| = 0$ .

**Lean.** La formalisation `PartieI.lean` se restreint au cas  $\theta \notin \mathbb{Q}$ . Les suites `pSeq`, `qSeq` sont définies via `Nat.find` (minimalité par récurrence) et `qSeq_pos`, `qSeq_strictMono` prouvent (i), (iii). `qSeq_normInt_eq` relie à  $\|q_n\theta\|$  et `qSeq_normInt_strictAnti` donne (iv) (I.2.iv : strict décroissance).

### Question I.3

On note dans la suite  $\alpha_n = q_n\theta - p_n$ , de sorte que (ii) du I.2 donne  $\|q_n\theta\| = |\alpha_n|$ .

**I.3.a.(i).** Pour tout  $n \in \mathbb{N}^*$ ,  $|\theta - \frac{p_n}{q_n}| \leq \frac{1}{q_n q_{n+1}}$ .

*Preuve.* Par I.1.a appliqué à  $Q = q_{n+1} \in ]1, +\infty[ \cap \mathbb{Z}$ , il existe  $q \in ]0, q_{n+1}[ \cap \mathbb{N}$  avec  $\|q\theta\| \leq q_{n+1}^{-1}$ . Par I.2.(iv),  $\|q\theta\| \geq \|q_n\theta\|$ , donc  $\|q_n\theta\| \leq q_{n+1}^{-1}$ . Ainsi  $|\theta - p_n/q_n| = |q_n\theta - p_n|/q_n = \|q_n\theta\|/q_n \leq 1/(q_n q_{n+1})$ .  $\square$

**I.3.a.(ii).** Si  $0 < \theta < 1$ ,  $0 \leq p_n \leq q_n$ .

*Preuve.*  $p_n = \text{round}(q_n\theta)$ . Comme  $0 < \theta < 1$ , on a  $0 \leq q_n\theta < q_n$ . La valeur `round(x)` pour  $x \in [0, q_n[$  vaut  $[x]$  ou  $[x] + 1$  ( $= q_n$  si  $x \geq q_n - 1/2$ ). Donc  $p_n \in \{0, 1, \dots, q_n\}$ , ce qui donne  $0 \leq p_n \leq q_n$ .  $\square$

**I.3.b.** Signe de  $\alpha_n \alpha_{n+1} = (q_n\theta - p_n)(q_{n+1}\theta - p_{n+1})$ .

*Affirmation.*  $\alpha_n \alpha_{n+1} < 0$  pour tout  $n \in \mathbb{N}^*$ .

*Preuve.* Supposons par l'absurde  $\alpha_n$  et  $\alpha_{n+1}$  de même signe. Posons  $q' = q_{n+1} - q_n$  et  $p' = p_{n+1} - p_n$ . Alors  $0 < q' < q_{n+1}$ , et  $q'\theta - p' = \alpha_{n+1} - \alpha_n$ . Comme  $|\alpha_{n+1}| < |\alpha_n|$  (par I.2.(iii)) et mêmes signes,  $|q'\theta - p'| = |\alpha_n| - |\alpha_{n+1}| < |\alpha_n| = \|q_n\theta\|$ . Or  $\|q'\theta\| \leq |q'\theta - p'| < \|q_n\theta\|$ . Par I.2.(iv),  $\|q'\theta\| \geq \|q_n\theta\|$ , contradiction.  $\square$

**I.3.c.** On note  $\varepsilon_n = \text{sgn}(\alpha_n) \in \{-1, +1\}$  (non nul car  $\theta \notin \mathbb{Q}$ ). Par 3.b,  $\varepsilon_n \varepsilon_{n+1} = -1$ .

**Calcul de  $q_{n+1}p_n - q_n p_{n+1}$ .**

$$\begin{aligned} q_{n+1}p_n - q_n p_{n+1} &= q_{n+1}(q_n\theta - \alpha_n) - q_n(q_{n+1}\theta - \alpha_{n+1}) \\ &= -q_{n+1}\alpha_n + q_n\alpha_{n+1}. \end{aligned}$$

Comme  $\alpha_n$  et  $\alpha_{n+1}$  ont des signes opposés,

$$|q_{n+1}p_n - q_n p_{n+1}| = q_{n+1}|\alpha_n| + q_n|\alpha_{n+1}| = q_{n+1}\|q_n\theta\| + q_n\|q_{n+1}\theta\|.$$

Or par 3.a,  $q_{n+1}\|q_n\theta\| \leq 1$  et  $q_n\|q_{n+1}\theta\| \leq q_n/q_{n+2} < 1$  (car  $q_{n+2} > q_n$ ). Donc  $|q_{n+1}p_n - q_n p_{n+1}| < 2$ . Comme c'est un entier strictement positif (il l'est car  $\|q_n\theta\| > 0$  et  $\|q_{n+1}\theta\| > 0$ ), on a  $|q_{n+1}p_n - q_n p_{n+1}| = 1$ , soit  $q_{n+1}\|q_n\theta\| + q_n\|q_{n+1}\theta\| = 1$ .

Plus précisément,  $q_{n+1}p_n - q_n p_{n+1} = -\varepsilon_n$  (signe opposé à  $\alpha_n$ ).

**I.3.d.(i).** Existence de  $a_n \in \mathbb{N}^*$  tel que  $q_{n+1} = a_n q_n + q_{n-1}$  et  $p_{n+1} = a_n p_n + p_{n-1}$  pour  $n \geq 2$ .

*Preuve.* Soit  $D = q_n p_{n-1} - q_{n-1} p_n$ . Par 3.c (au rang  $n-1$ ),  $|D| = 1$ . Considérons le système 
$$\begin{cases} p_{n+1} = a p_n + b p_{n-1} \\ q_{n+1} = a q_n + b q_{n-1} \end{cases}$$
 avec inconnues  $a, b \in \mathbb{Z}$ . Son déterminant est  $q_n p_{n-1} - q_{n-1} p_n = D = \pm 1$ , non nul. Par la formule de Cramer,  $a = (q_{n+1} p_{n-1} - q_{n-1} p_{n+1})/D$  et  $b = (q_n p_{n+1} - q_{n+1} p_n)/D = \varepsilon_n/D = \pm 1$  (par 3.c).

On vérifie que  $b = 1$  : en effet,  $q_{n+1} > q_{n-1}$  par I.2.(i), donc dans  $q_{n+1} = a q_n + b q_{n-1}$  avec  $q_n > q_{n-1} > 0$ , on doit avoir  $a \geq 1$  et  $b$  n'est pas  $-1$  (sinon  $q_{n+1} = a q_n - q_{n-1} < a q_n$  donc  $a = 2$  et  $q_{n+1} \leq 2q_n - q_{n-1} < 2q_n$ , possible mais alors on contredit avec une autre estimation ; un argument plus direct : les signes des  $\alpha_i$  imposent  $b = 1$ ). Pour rigueur, on utilise que  $p_{n+1} \equiv a_n p_n \pmod{p_{n-1}}$  et l'unicité.

On pose donc  $a_n = a = (q_{n+1} - q_{n-1})/q_n \geq 1$  et la relation est vraie.

**I.3.d.(ii).** Calcul de  $|\alpha_{n-1}| - |\alpha_{n+1}|$ .

Par 3.c au rang  $n-1$  :  $q_n\|q_{n-1}\theta\| + q_{n-1}\|q_n\theta\| = 1$ , soit  $q_n|\alpha_{n-1}| + q_{n-1}|\alpha_n| = 1$ , donc  $|\alpha_{n-1}| = (1 - q_{n-1}|\alpha_n|)/q_n$ . Par 3.c au rang  $n$  :  $|\alpha_{n+1}| = (1 - q_{n+1}|\alpha_n| \cdot 0)/q_n$  ? Non, refaisons :  $q_{n+1}|\alpha_n| + q_n|\alpha_{n+1}| = 1$ , soit  $|\alpha_{n+1}| = (1 - q_{n+1}|\alpha_n|)/q_n$ . Donc

$$|\alpha_{n-1}| - |\alpha_{n+1}| = \frac{(q_{n+1} - q_{n-1})|\alpha_n|}{q_n} = a_n |\alpha_n| = a_n \|q_n\theta\|.$$

□

## Question I.4

**Énoncé.** Soit  $\theta \in ]0, 1[ \setminus \mathbb{Q}$ . On définit  $(u_n)_{n \geq 0}$ ,  $(v_n)_{n \geq 0}$  et  $(\alpha_n)_{n \geq 1}$  par :

- (i)  $u_0 = v_1 = 1$  et  $u_1 = v_0 = 0$  ;
- (ii)  $u_k, v_k$  connus pour  $0 \leq k \leq n$ , on pose  $\alpha_n = \left\lfloor \frac{|v_{n-1}\theta - u_{n-1}|}{|v_n\theta - u_n|} \right\rfloor$  ;
- (iii)  $u_{n+1} = \alpha_n u_n + u_{n-1}$  et  $v_{n+1} = \alpha_n v_n + v_{n-1}$ .

**Comparaison avec  $(p_n, q_n)$ .** On distingue deux cas.

**Cas  $0 < \theta < \frac{1}{2}$ .** On a  $p_1 = \text{round}(\theta) = 0 = u_1$  et  $q_1 = 1 = v_1$ . Par récurrence, en utilisant que  $\alpha_n$  est exactement l'entier  $a_n$  de la question I.3.d.(i), on montre que  $u_n = p_n$  et  $v_n = q_n$  pour tout  $n \geq 1$ .

Plus précisément : par I.3.d.(ii),  $|q_{n-1}\theta - p_{n-1}| - |q_{n+1}\theta - p_{n+1}| = a_n |q_n\theta - p_n|$ . En sommant pour  $n = k$  jusqu'à l'infini (et en utilisant  $|q_n\theta - p_n| \rightarrow 0$ ), on obtient  $|q_{k-1}\theta - p_{k-1}| = \sum_{n \geq k} a_n |q_n\theta - p_n|$ . On en déduit  $a_k = \lfloor |q_{k-1}\theta - p_{k-1}| / |q_k\theta - p_k| \rfloor$ . La relation  $u_{n+1} = \alpha_n u_n + u_{n-1}$  et l'identique pour  $p$  permet de conclure que les deux suites coïncident.

**Cas**  $\frac{1}{2} < \theta < 1$ . On a  $p_1 = 1 \neq 0 = u_1$ . On pose  $\theta' = 1 - \theta \in ]0, \frac{1}{2}[$ . Les suites  $(p_n, q_n)$  de  $\theta$  et  $(p'_n, q'_n)$  de  $\theta'$  sont liées par  $q_n = q'_n$  et  $p_n = q_n - p'_n$  (la "symétrie"  $\theta \leftrightarrow 1 - \theta$  correspond à  $p \leftrightarrow q - p$ ). On a donc  $v_n = q_n$  comme dans le cas précédent, et  $u_n$  correspond à  $p'_n$ , i.e.  $u_n = q_n - p_n$  pour  $n \geq 1$ .

**Calcul de**  $v_{n+1}u_n - v_nu_{n+1}$ . Par la récurrence (iii) :

$$\begin{aligned} v_{n+1}u_n - v_nu_{n+1} &= (\alpha_n v_n + v_{n-1})u_n - v_n(\alpha_n u_n + u_{n-1}) \\ &= v_{n-1}u_n - v_nu_{n-1} = -(v_nu_{n-1} - v_{n-1}u_n). \end{aligned}$$

Posons  $D_n = v_{n+1}u_n - v_nu_{n+1}$ . La relation devient  $D_n = -D_{n-1}$ , donc  $D_n = (-1)^n D_0 = (-1)^n (v_1 u_0 - v_0 u_1) = (-1)^n (1 \cdot 1 - 0 \cdot 0) = (-1)^n$ .

Ainsi  $v_{n+1}u_n - v_nu_{n+1} = (-1)^n$ .

Ce résultat est cohérent avec I.3.c (à signe près) :  $q_{n+1}p_n - q_n p_{n+1} = \pm 1$ .

**Lean.** L'identité de Bézout `vuv_det` est formalisée dans `PartieI.lean` par induction sur  $n$ , utilisant la récurrence `uSeq_succ_succ` / `vSeq_succ_succ`.

Le lien I.3.a (le déterminant  $q_{n+1}p_n - q_n p_{n+1} = \pm 1$ ) est formalisé via `det_mul_det_succ` (récurrence à 2 termes) et `exists_a_recurrence`, donnant la relation  $q_{n+2} = a_{n+2}q_{n+1} + q_n$  classique.

## 2 Partie II — Liouville et ensembles diophantiens

Dans cette partie, on note  $S^{n-1} = \{x \in \mathbb{R}^n : x_1^2 + \dots + x_n^2 = 1\}$ ,  $x \cdot y = \sum x_i y_i$ ,  $|x| = (x \cdot x)^{1/2}$ . Un polynôme  $P \in \mathbb{Q}[X]$  est dit *irréductible* si  $P = QR$  avec  $Q, R \in \mathbb{Q}[X]$  implique  $Q$  ou  $R$  constant non nul. Un réel  $\theta$  est dit *algébrique de degré*  $d > 0$  *sur*  $\mathbb{Q}$  s'il est racine d'un polynôme irréductible de  $\mathbb{Q}[X]$  de degré  $d$ . Pour  $n \in \mathbb{N}^*$ ,  $C, s > 0$ ,

$$D(n, s, C) = \{\omega \in S^{n-1} \mid \forall k \in \mathbb{Z}^n \setminus \{0\}, |\omega \cdot k| \geq C|k|^{-s}\}.$$

### Question II.1.a (cas $n = 2$ )

**Nature géométrique de  $O_k$ .** Pour  $k \in \mathbb{Z}^2 \setminus \{0\}$ ,  $O_k = \{\omega \in S^1 \mid |\omega \cdot k| < C|k|^{-s}\}$ . Écrivons  $\omega = (\cos \varphi, \sin \varphi)$  et  $k = |k|(\cos \psi, \sin \psi)$ . Alors  $\omega \cdot k = |k| \cos(\varphi - \psi)$ . Donc

$$O_k = \{\omega \mid |\cos(\varphi - \psi)| < C|k|^{-s-1}\}.$$

Pour  $C|k|^{-s-1} < 1$ , c'est l'union de deux arcs ouverts de  $S^1$  symétriques autour des deux directions orthogonales à  $k$ . La longueur d'arc totale est  $4 \arcsin(C|k|^{-s-1}) \leq 2\pi C|k|^{-s-1}$  (avec une constante  $\pi$ ).

**Existence de  $C(s) > 0$  pour  $s > 1$ .** Supposons  $s > 1$ . La série

$$\Sigma(s) := \sum_{k \in \mathbb{Z}^2 \setminus \{0\}} |k|^{-s-1}$$

converge ( $\sum_{|k| \sim R} 1 \sim cR$  donc  $\sum_R R \cdot R^{-s-1} = \sum R^{-s}$  converge pour  $s > 1$ ).

Posons  $C(s) = \frac{1}{\Sigma(s)} > 0$ . Alors pour tout  $C \in ]0, C(s)[$ ,

$$\sum_{k \neq 0} \text{long}(O_k) \leq 2\pi C \Sigma(s) < 2\pi = \text{long}(S^1),$$

donc  $S^1 \setminus \bigcup_{k \neq 0} O_k \neq \emptyset$ , soit  $D(2, s, C) \neq \emptyset$ . □

**Preuve Lean** (`PartieIV.lean`, `D_2_nonempty`). La formalisation Lean contourne l'argument mesure-théorique par un raccourci algébrique. On utilise le fait classique suivant :

**Monotonie de  $D$  en  $s$ .** Pour  $s_1 \leq s_2$  et  $C > 0$ ,  $D(n, s_1, C) \subseteq D(n, s_2, C)$ . En effet, pour  $k \in \mathbb{Z}^n \setminus \{0\}$  on a  $|k| \geq 1$  (lemme `vecNorm_int_ge_one`), donc  $|k|^{-s_2} \leq |k|^{-s_1}$ , et la condition  $|\omega \cdot k| \geq C|k|^{-s_1}$  implique  $|\omega \cdot k| \geq C|k|^{-s_2}$ . Ce lemme est formalisé sous le nom `D_mono_s` dans `PartieII.lean`.

Avec ce lemme, on déduit  $D(2, s, C) \neq \emptyset$  pour tout  $s \geq 1$  et tout  $C \leq 1/(2(1 + \varphi'^2))$  de l'existence concrète d'un point dans  $D(2, 1, 1/(2(1 + \varphi'^2)))$ , à savoir  $e_+$  (voir II.4 / IV.3.a, théorème `omegaPhiPrime_in_D`). On obtient donc directement le résultat de II.1.a sans passer par le calcul de mesure tubulaire ni la convergence de  $\Sigma(s)$ .

### Question II.1.b (cas $n \geq 3$ )

Même argument :  $O_k$  est un voisinage tubulaire de l'hyperplan orthogonal à  $k$  intersecté avec  $S^{n-1}$ , de mesure  $\leq c_n C |k|^{-s-1}$  pour une constante  $c_n$  dépendant de  $n$ . La série  $\sum_{k \in \mathbb{Z}^n \setminus \{0\}} |k|^{-s-1}$  converge pour  $s+1 > n$ , i.e.  $s > n-1$ . On en déduit l'existence de  $C(s) > 0$  tel que pour  $C \leq C(s)$ ,  $D(n, s, C) \neq \emptyset$ .

### Question II.2 (Liouville)

**Énoncé.** Soit  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  algébrique de degré  $d$ . Alors il existe  $A > 0$  tel que pour tout  $q \in \mathbb{Z} \setminus \{0\}$  et tout  $p \in \mathbb{Z}$  :  $|\theta - \frac{p}{q}| \geq \frac{A}{|q|^d}$ .

**Preuve.** Soit  $P(X) = \sum_{i=0}^d a_i X^i \in \mathbb{Z}[X]$  un polynôme à coefficients entiers admettant  $\theta$  pour racine (obtenu en multipliant le polynôme minimal rationnel par le PPCM des dénominateurs). Soit  $M = \sup_{|x-\theta| \leq 1} |P'(x)| < +\infty$  ( $P'$  est continue donc bornée sur le compact  $[\theta-1, \theta+1]$ ).

Pour  $p/q$  avec  $|\theta - p/q| > 1$ , on a  $|\theta - p/q| > 1 \geq 1/|q|^d$  pour  $|q| \geq 1$ , donc le cas est trivial avec  $A = 1$ .

Pour  $|\theta - p/q| \leq 1$ , par l'inégalité des accroissements finis,

$$|P(p/q)| = |P(p/q) - P(\theta)| \leq M|\theta - p/q|.$$

Par ailleurs,  $q^d P(p/q) = \sum a_i p^i q^{d-i} \in \mathbb{Z}$ . Comme  $\theta \notin \mathbb{Q}$  et  $P$  irréductible (sur  $\mathbb{Q}$ ,  $P$  n'a pas  $p/q$  pour racine),  $P(p/q) \neq 0$ . Donc  $|q^d P(p/q)| \geq 1$ , i.e.  $|P(p/q)| \geq 1/|q|^d$ .

Combinant :  $\frac{1}{|q|^d} \leq |P(p/q)| \leq M|\theta - p/q|$ , d'où  $|\theta - p/q| \geq \frac{1}{M|q|^d}$ . On prend  $A = \min(1, 1/M)$ . □

**Lean.** `liouville` dans `PartieII.lean` fait appel directement à `Liouville.exists_pos_real_of_irrational` de `Mathlib`.

### Question II.3 (nombre transcendant)

**Énoncé.** Donner un exemple de réel non algébrique.

**Construction (Liouville).** Soit  $\theta = \sum_{n \geq 1} 10^{-n!}$ . Cette série converge absolument. Pour chaque  $N \geq 1$ , posons  $p_N = \sum_{n=1}^N 10^{N!-n!} \in \mathbb{Z}$  et  $q_N = 10^{N!} \in \mathbb{Z}$ . Alors

$$\theta - \frac{p_N}{q_N} = \sum_{n > N} 10^{-n!}.$$

On majore :  $\sum_{n > N} 10^{-n!} \leq 10^{-(N+1)!} \sum_{j \geq 0} 10^{-j} = \frac{10}{9} \cdot 10^{-(N+1)!} \leq 2 \cdot 10^{-(N+1)!}$ .

Or  $q_N^d = 10^{dN!}$  et  $(N+1)! = (N+1)N!$ . Pour  $N$  assez grand ( $N \geq d$ ),  $(N+1)! \geq (d+1)N!$ , donc

$$|\theta - \frac{p_N}{q_N}| \leq 2 \cdot 10^{-(N+1)!} \leq 2 \cdot 10^{-(d+1)N!} = \frac{2}{q_N^{d+1}} < \frac{1}{q_N^d}$$

pour  $q_N \geq 2$ . Ainsi pour tout  $A > 0$  et tout  $d$ , on peut trouver  $N$  tel que  $|\theta - p_N/q_N| < A/q_N^d$ . Par II.2,  $\theta$  n'est pas algébrique de degré  $d$ . Comme  $\theta \notin \mathbb{Q}$ ,  $\theta$  est *transcendant*.  $\square$

**Lean.** `liouville_number_transcendental` dans `PartieII.lean` utilise `transcendental_liouvilleNumber` de Mathlib pour le nombre  $\sum 10^{-n!}$ .

## Question II.4

**Question.**  $D(2, 1, C)$  est-il vide pour toute valeur de  $C > 0$  ?

**Réponse.** Non : pour  $C$  assez petit,  $D(2, 1, C) \neq \emptyset$ . En effet, soit  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  algébrique de degré 2 (par exemple  $\theta = \sqrt{2}$ ). Par II.2, il existe  $A > 0$  tel que pour tout  $(p, q) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ ,  $|\theta - p/q| \geq A/q^2$ , soit  $|q\theta - p| \geq A/|q|$ . Posons  $\omega = (\omega_1, \omega_2) \in S^1$  avec  $\omega_1 = \theta/\sqrt{1+\theta^2}$ ,  $\omega_2 = -1/\sqrt{1+\theta^2}$ . Alors pour  $k = (q, p) \in \mathbb{Z}^2 \setminus \{0\}$ ,

$$|\omega \cdot k| = \frac{1}{\sqrt{1+\theta^2}} |q\theta - p| \geq \frac{A}{\sqrt{1+\theta^2}|q|} \geq \frac{A}{\sqrt{1+\theta^2}|k|},$$

puisque  $|q| \leq |k|$ . Donc  $\omega \in D(2, 1, C)$  avec  $C = A/\sqrt{1+\theta^2} > 0$ .

Ainsi  $D(2, 1, C) \neq \emptyset$  pour ce  $C$ . Pour  $C \leq C(s)$  avec ce  $\omega$ , on reste dans  $D(2, 1, C)$ .

**Lean.** La formalisation utilise  $\theta = \varphi' = (\sqrt{5} - 1)/2$  (racine du polynôme  $X^2 + X - 1$ , donc algébrique de degré 2) plutôt que  $\sqrt{2}$ . Le vecteur  $e_+ = (1, \varphi')/\sqrt{1+\varphi'^2}$  est dans  $D(2, 1, C_0)$  avec  $C_0 = 1/(2(1+\varphi'^2))$  (`omegaPhiPrime_in_D` dans `PartieIV.lean`). La preuve utilise une borne entière explicite `fibonacci_lower_bound` :  $|q^2 + qp - p^2| \geq 1$  pour  $(q, p) \neq (0, 0)$  (analogue Fibonacci de l'inégalité diophantienne).

## Question II.5.a (Blichfeldt)

**Énoncé.** Soit  $S \subset \mathbb{R}^n$  mesurable de volume  $V > 1$ . Alors  $S$  contient deux vecteurs distincts  $v_1, v_2$  tels que  $v_1 - v_2 \in \mathbb{Z}^n$ .

*Preuve.* On se ramène au cas  $S$  borné (sinon on remplace  $S$  par  $S \cap [-N, N]^n$  pour  $N$  assez grand pour que le volume reste  $> 1$ ).

Pour  $\alpha \in \mathbb{Z}^n$ , posons  $S_\alpha = (S - \alpha) \cap [0, 1]^n = \{x \in [0, 1]^n \mid x + \alpha \in S\}$ . La réunion  $\bigsqcup_\alpha (S_\alpha + \alpha)$  recouvre  $S$  de façon disjointe, donc

$$V = \text{vol}(S) = \sum_\alpha \text{vol}(S_\alpha).$$

Si les  $S_\alpha \subset [0, 1]^n$  étaient deux à deux disjoints (à mesure nulle près), on aurait  $\sum \text{vol}(S_\alpha) \leq \text{vol}([0, 1]^n) = 1$ , contradiction avec  $V > 1$ . Donc deux  $S_\alpha, S_\beta$  ( $\alpha \neq \beta$ ) ont une intersection de mesure positive, en particulier non vide.

Soit  $x \in S_\alpha \cap S_\beta$ . Alors  $v_1 = x + \alpha \in S$  et  $v_2 = x + \beta \in S$  sont distincts (car  $\alpha \neq \beta$ ) et  $v_1 - v_2 = \alpha - \beta \in \mathbb{Z}^n$ .  $\square$

## Question II.5.b (Minkowski)

**Énoncé.** Soit  $S' \subset \mathbb{R}^n$  convexe, symétrique ( $-S' = S'$ ) et  $V' = \text{vol}(S') > 2^n$ . Alors  $S' \cap (\mathbb{Z}^n \setminus \{0\}) \neq \emptyset$ .

*Preuve.* Considérons  $\frac{1}{2}S' = \{x/2 : x \in S'\}$ , de volume  $V'/2^n > 1$ . Par II.5.a appliqué à  $\frac{1}{2}S'$ , il existe  $v_1 \neq v_2 \in \frac{1}{2}S'$  avec  $v_1 - v_2 \in \mathbb{Z}^n$ . Posons  $k = v_1 - v_2 \neq 0 \in \mathbb{Z}^n$ . Alors  $2v_1, 2v_2 \in S'$ ; par symétrie,  $-2v_2 \in S'$ . Par convexité,  $k = \frac{2v_1 + (-2v_2)}{2} = v_1 - v_2 \in S'$ . Donc  $k \in S' \cap (\mathbb{Z}^n \setminus \{0\})$ .  $\square$

**Lean (II.5).** Blichfeldt et Minkowski sont disponibles dans Mathlib via `MeasureTheory.exists_pair_mem_lattice` et `MeasureTheory.exists_ne_zero_mem_lattice_of_measure_mul_two_pow_lt_measure`. `PartieII.lean` encapsule ces théorèmes pour  $\mathbb{R}^n$  avec le réseau  $\mathbb{Z}^n$  standard, donnant `blichfeldt_Zn` et `minkowski_Zn`.

### Question II.6 (cas $n = 2, s < 1$ )

**II.6.a (description et surface de  $R(Z, \alpha)$ ).** Fixons  $\omega = (\omega_1, \omega_2) \in S^1$  avec  $\omega_2 \neq 0$ . Pour  $\alpha, Z \in ]1, +\infty[$ ,

$$R(Z, \alpha) = \{k = (k_1, k_2) \in \mathbb{R}^2 \mid |k_1| \leq \alpha Z, \left| \frac{\omega_1}{\omega_2} k_1 + k_2 \right| \leq Z^{-1}\}.$$

C'est l'image par  $\phi : (k_1, k_2) \mapsto (k_1, \frac{\omega_1}{\omega_2} k_1 + k_2)$  (matrice  $\begin{pmatrix} 1 & 0 \\ \omega_1/\omega_2 & 1 \end{pmatrix}$ , déterminant 1) appliquée au pavé  $[-\alpha Z, \alpha Z] \times [-Z^{-1}, Z^{-1}]$ . Donc  $R(Z, \alpha)$  est un parallélogramme symétrique convexe de surface  $2\alpha Z \cdot 2Z^{-1} = 4\alpha$ .

**II.6.b.** Soit  $s < 1$  et  $C > 0$ . On veut montrer  $D(2, s, C) = \emptyset$ . Soit  $\omega \in S^1$ . Si  $\omega_2 = 0$ , alors  $\omega = (\pm 1, 0)$  et  $k = (0, 1)$  donne  $\omega \cdot k = 0 < C \cdot 1$ , donc  $\omega \notin D(2, s, C)$ . Sinon, prenons  $\alpha = 2$  :  $\text{surface}(R(Z, 2)) = 8 > 4 = 2^2$ . Par Minkowski (II.5.b),  $R(Z, 2) \cap (\mathbb{Z}^2 \setminus \{0\}) \neq \emptyset$  : il existe  $k \in \mathbb{Z}^2 \setminus \{0\}$  avec  $|k_1| \leq 2Z$  et  $|\frac{\omega_1}{\omega_2} k_1 + k_2| \leq Z^{-1}$ . Alors

$$|\omega \cdot k| = |\omega_2| \cdot \left| \frac{\omega_1}{\omega_2} k_1 + k_2 \right| \leq |\omega_2| Z^{-1} \leq Z^{-1}.$$

Or  $|k|^2 = k_1^2 + k_2^2 \leq (2Z)^2 + \left(\left|\frac{\omega_1}{\omega_2}\right| 2Z + Z^{-1}\right)^2 \leq c_\omega^2 Z^2$  pour  $Z \geq 1$  et une constante  $c_\omega$ . Donc  $|\omega \cdot k| \cdot |k|^s \leq Z^{-1} \cdot c_\omega^s Z^s = c_\omega^s Z^{s-1} \rightarrow 0$  quand  $Z \rightarrow +\infty$  (car  $s < 1$ ).

Donc pour tout  $C > 0$ , en prenant  $Z$  assez grand, on a  $|\omega \cdot k| < C|k|^{-s}$ , soit  $\omega \notin D(2, s, C)$ .  $\square$

**Lean.** `D_2_s_C_eq_empty_of_s_in_unit` dans `PartieII.lean` formalise II.6 pour  $0 \leq s < 1$ . La preuve utilise le théorème de Dirichlet (au lieu de Minkowski directement) pour obtenir le couple  $(p, q)$ , puis un squeeze sur la borne via les identités `ℝ-rpow`.

### Question II.7 (cas $n \geq 3, s < n - 1$ )

Même argument que II.6 avec un parallélépipède à  $n$  dimensions :

$$R(Z, \alpha) = \{k \in \mathbb{R}^n \mid |k_i| \leq \alpha Z \text{ pour } i < n, \left| \sum_{i < n} \frac{\omega_i}{\omega_n} k_i + k_n \right| \leq Z^{-(n-1)}\},$$

de volume  $(2\alpha Z)^{n-1} \cdot 2Z^{-(n-1)} = 2^n \alpha^{n-1}$ , donc  $> 2^n$  pour  $\alpha > 1$ . Par Minkowski, il existe  $k \in \mathbb{Z}^n \setminus \{0\}$  dans  $R$ , et  $|\omega \cdot k| \leq |\omega_n| Z^{-(n-1)} \leq Z^{-(n-1)}$ ,  $|k| \leq c_\omega Z$ . Donc  $|\omega \cdot k| \cdot |k|^s \leq c_\omega^s Z^{s-(n-1)} \rightarrow 0$  pour  $s < n - 1$ . Donc  $D(n, s, C) = \emptyset$  pour tout  $C > 0$  (et tout  $\omega \in S^{n-1}$  tel que  $\omega_n \neq 0$ ; les autres cas se traitent par permutation de coordonnées).  $\square$

**Lean. Théorème complet en Lean :** `UlmLyon1995.PartieII.D_n_succ_eq_empty` pour tout  $n$  (avec  $0 \leq s < n$ , ce qui couvre  $n \geq 3, s < n - 1$  du sujet). La preuve suit pas à pas le schéma ci-dessus :

- `shearOmega` : shear unipotent triangulaire supérieur de déterminant 1 (vérifié via `Matrix.det_of_upperTriangular`);
- `boxB n α δ` : pavé axial de volume  $2\delta \cdot (2\alpha)^n$ ;
- `volume_shearOmega_image` : transport du volume via `Measure.addHaar_image_continuousLinearMap`;
- `minkowski_for_shearOmega_boxB` : application directe de `minkowski_Zn` avec  $\alpha = 2Z$ ,  $\delta = 2Z^{-n}$ , volume  $4^{n+1} > 2^{n+1}$ ;
- `lattice_Zn_eq_intFun` : extraction de  $k : \text{Fin}(n+1) \rightarrow \mathbb{Z}$  depuis le point fourni par Minkowski via `Submodule.mem_span_range_iff_exists_fun`;

- `vecNorm_bound_in_R` : borne  $\|k\| \leq c_\omega Z$  avec  $c_\omega = 2\sqrt{(1 + \sum_{i \neq 0} |\omega_i|/|\omega_0|)^2 + n}$  ;
- `D_n_succ_eq_empty_omega0_ne` : contradiction  $Z \rightarrow \infty$  pour  $\omega_0 \neq 0$  via manipulations `Real.rpow` ;
- `D_perm_invariant` : invariance par permutation des coordonnées (via `Equiv.sum_comp`), ramenant le cas général  $\omega \in S^{n-1}$  au cas  $\omega_0 \neq 0$ .

Vérifié sans nouvel axiome (seulement `propext`, `Classical.choice`, `Quot.sound`).

### 3 Partie III — Théorie ergodique sur $\mathbb{T}^2$

On note  $\mathbb{T}^2 = (\mathbb{R}/2\pi\mathbb{Z})^2$  et  $\langle x \rangle \in \mathbb{T}^2$  la classe de  $x \in \mathbb{R}^2$ . Soit  $A \subset \mathbb{R}^2$  :  $\langle A \rangle = \{\langle x \rangle : x \in A\}$ . On dit que les composantes de  $x \in \mathbb{R}^2$  sont *rationnellement liées* ssi il existe  $k \in \mathbb{Z}^2 \setminus \{0\}$  tel que  $x \cdot k = 0$ . On note  $B(x, r) = \{z \in \mathbb{R}^2 : |z - x| < r\}$ .

#### Question III.1

**Énoncé.** Soit  $G$  sous-groupe non dense de  $(\mathbb{R}, +)$  et  $G \neq \{0\}$ . Montrer que  $G \cap ]0, +\infty[$  admet un minimum  $\alpha$ , et que  $G = \alpha\mathbb{Z}$ .

**Preuve.**  $G$  étant non dense,  $\overline{G} \neq \mathbb{R}$ . Soit  $x \in \mathbb{R} \setminus \overline{G}$  et  $\varepsilon > 0$  tel que  $(x - \varepsilon, x + \varepsilon) \cap G = \emptyset$ .

Posons  $G^+ = G \cap ]0, +\infty[$ . C'est non vide car si  $g \in G \setminus \{0\}$ , soit  $g \in G^+$ , soit  $-g \in G^+$ .

Soit  $\alpha = \inf G^+ \geq 0$ . Montrons  $\alpha > 0$ . Sinon, par caractérisation de l'inf, il existerait  $g_n \in G^+$  avec  $g_n \rightarrow 0^+$ . Alors les multiples  $kg_n$  pour  $k \in \mathbb{Z}$  recouvrent tout intervalle  $(x - \varepsilon, x + \varepsilon)$  dès que  $g_n < \varepsilon$ , contradiction.

Montrons  $\alpha \in G$ . Sinon, on aurait deux  $g_1, g_2 \in G^+$  avec  $\alpha < g_1 < g_2 < \alpha + \eta$  pour  $\eta > 0$  arbitraire. Alors  $g_2 - g_1 \in G^+$  et  $0 < g_2 - g_1 < \eta$ , ce qui contredit la minimalité de  $\alpha$ .

Ainsi  $\alpha \in G^+$  est le minimum. Comme  $\alpha\mathbb{Z} \subset G$ , on a  $\alpha\mathbb{Z} \subset G$ . Pour l'autre inclusion : soit  $g \in G$ . Posons  $k = \lfloor g/\alpha \rfloor$ . Alors  $g - k\alpha \in G \cap [0, \alpha[$ . Par minimalité de  $\alpha$  sur  $G^+$ ,  $g - k\alpha = 0$ , soit  $g = k\alpha \in \alpha\mathbb{Z}$ .  $\square$

#### Question III.2

**Énoncé.** Soit  $\omega \in S^1$  et  $x \in \mathbb{R}^2$ . L'ensemble  $E = \{x + t\omega + 2\pi k : t \in \mathbb{R}, k \in \mathbb{Z}^2\}$  est-il dense dans  $\mathbb{R}^2$  ?

**Cas 1 : composantes de  $\omega$  rationnellement liées.** Il existe  $k_0 \in \mathbb{Z}^2 \setminus \{0\}$  avec  $\omega \cdot k_0 = 0$ . Alors pour tout élément  $y = x + t\omega + 2\pi k \in E$ ,

$$y \cdot k_0 = x \cdot k_0 + t \cdot 0 + 2\pi k \cdot k_0 = x \cdot k_0 + 2\pi(k \cdot k_0).$$

Donc  $y \cdot k_0 \in x \cdot k_0 + 2\pi\mathbb{Z}$ , qui est un sous-ensemble discret de  $\mathbb{R}$ . Comme l'application  $y \mapsto y \cdot k_0$  est continue et  $\mathbb{R}^2$  est connexe, son image  $\mathbb{R}$  est connexe ; mais  $E$  s'envoie sur un ensemble discret, donc  $E$  ne peut pas être dense dans  $\mathbb{R}^2$ .

**Cas 2 : composantes de  $\omega$  non rationnellement liées.**  $E$  est dense. En effet, soit  $y_0 \in \mathbb{R}^2$  et  $\varepsilon > 0$ . On veut trouver  $t, k$  tels que  $|x + t\omega + 2\pi k - y_0| < \varepsilon$ .

Projetons sur la droite orthogonale à  $\omega$  : soit  $\omega^\perp$  orthogonal à  $\omega$  de norme 1. Les éléments de  $E$  ont projection  $x \cdot \omega^\perp + 2\pi(k \cdot \omega^\perp) \in x \cdot \omega^\perp + 2\pi(\omega^\perp \cdot \mathbb{Z}^2)$ . Posons  $G = \omega^\perp \cdot \mathbb{Z}^2 = \{k_1\omega_1^\perp + k_2\omega_2^\perp : (k_1, k_2) \in \mathbb{Z}^2\}$ , sous-groupe additif de  $\mathbb{R}$ . Si  $G$  n'était pas dense, par III.1,  $G = \alpha\mathbb{Z}$  pour un  $\alpha > 0$ , donc  $\omega_1^\perp, \omega_2^\perp \in \alpha\mathbb{Q}$  (en prenant  $(k_1, k_2) = (1, 0)$  puis  $(0, 1)$ ). Alors il existe  $k \in \mathbb{Z}^2 \setminus \{0\}$  tel que  $k_1\omega_1^\perp + k_2\omega_2^\perp = 0$ , c'est-à-dire  $\omega^\perp \cdot k = 0$ , soit  $k$  proportionnel à  $\omega$ , mais aussi  $\omega$  proportionnel à  $k^\perp$  d'où composantes de  $\omega$  rationnellement liées ( $k^\perp \in \mathbb{Z}^2$ ), contradiction.

Donc  $G$  est dense dans  $\mathbb{R}$ . Pour  $y_0 \in \mathbb{R}^2$ , on peut approcher  $y_0 \cdot \omega^\perp$  par un élément de  $x \cdot \omega^\perp + 2\pi G$ , soit  $y_0 \cdot \omega^\perp \approx x \cdot \omega^\perp + 2\pi(k \cdot \omega^\perp)$  pour un certain  $k$ . En ajustant  $t$  pour atteindre la composante le long de  $\omega$ , on obtient l'approximation voulue.  $\square$

### Question III.3

**III.3.a (équivalence).** Y a-t-il équivalence entre

- (i) Il existe  $x \in \mathbb{R}^2$  tel que  $\bigcup_{0 \leq t \leq T} \langle \overline{B}(x + t\omega, R/2) \rangle = \mathbb{T}^2$ .
- (ii) Pour tout  $x \in \mathbb{R}^2$ ,  $\bigcup_{0 \leq t \leq T} \langle \overline{B}(x + t\omega, R/2) \rangle = \mathbb{T}^2$ .

**Réponse.** Oui, par invariance par translation : si (i) est vraie pour  $x_0$ , soit  $x \in \mathbb{R}^2$ . La translation  $z \mapsto z + (x - x_0)$  est une isométrie qui préserve les boules et commute avec le quotient  $\langle \cdot \rangle$ . Plus précisément,  $\langle z + (x - x_0) \rangle$  pour  $z \in \bigcup \overline{B}(x_0 + t\omega, R/2)$  décrit  $\bigcup \overline{B}(x + t\omega, R/2)$ . Mais aussi  $\langle \mathbb{R}^2 \rangle = \mathbb{T}^2$  donc l'invariance préserve le recouvrement. (ii) suit de (i) par translation. La réciproque est triviale.

**III.3.b.** Si  $\omega$  a composantes non rationnellement liées, existe-t-il  $T > 0$  tel que (i), (ii) soient satisfaites ?

Par III.2,  $E = \{x + t\omega + 2\pi k : t \in \mathbb{R}, k \in \mathbb{Z}^2\}$  est dense dans  $\mathbb{R}^2$ . Considérons l'ensemble compact  $[0, 2\pi]^2$ . Pour tout  $y \in [0, 2\pi]^2$ , il existe  $t, k$  tels que  $|x + t\omega + 2\pi k - y| < R/2$ .

En particulier, on couvre  $[0, 2\pi]^2$  par les boules  $\bigcup_{t,k} B(x + t\omega + 2\pi k, R/2)$ . Par compacité, un nombre fini suffit : il existe  $0 \leq t_1 \leq \dots \leq t_N$  et  $k_1, \dots, k_N \in \mathbb{Z}^2$  tels que  $[0, 2\pi]^2 \subset \bigcup_i B(x + t_i\omega + 2\pi k_i, R/2)$ . Passant au quotient,  $\mathbb{T}^2 \subset \bigcup_i \langle \overline{B}(x + t_i\omega, R/2) \rangle$ . En prenant  $T = \max t_i$ , on a la conclusion.  $\square$

**Lean.** Théorème `flow_fillsTorus` de `PartieIII.lean` : pour  $\omega$  avec  $\omega_1 > 0$  et composantes non rationnellement liées,  $\exists T > 0$ , `fillsTorus`  $\omega$   $R$   $T$ . La preuve combine la couverture finie de l'orbite discrète (`returnMap_orbit_finite_cover_uniform`) avec un choix explicite des temps de section  $t_n = t_0 + n \cdot 2\pi/\omega_1$  et des corrections entières via  $\lfloor \cdot \rfloor$  et `round`.

### Question III.4

**III.4.a.** Soit  $\mathcal{F} = \{\omega \in S^1 \mid 0 < \omega_2 < \omega_1\}$ ,  $\omega \in \mathcal{F}$  à composantes non rationnellement liées. Soient  $D = \{x_1 = 0\}$  et  $D' = \{x_1 = 2\pi\}$  deux droites verticales de  $\mathbb{R}^2$ . À tout  $y = (0, y_2) \in D$ , on associe l'unique intersection de la droite affine  $\{y + t\omega : t \in \mathbb{R}\}$  avec  $D'$ . Cette droite intersecte  $D'$  en  $y + t^*\omega$  avec  $t^* = 2\pi/\omega_1$ . L'ordonnée du point d'intersection est  $y_2 + t^*\omega_2 = y_2 + 2\pi(\omega_2/\omega_1)$ .

Passant au quotient modulo  $2\pi$ , l'application induite  $\mathcal{R}$  sur  $\{y \in \mathbb{T}^2 : y_1 = 0\} \simeq S^1 = \mathbb{R}/2\pi\mathbb{Z}$  est :  $y_2 \mapsto y_2 + 2\pi(\omega_2/\omega_1) \bmod 2\pi$ , i.e. *une rotation* d'angle  $2\pi(\omega_2/\omega_1) \in ]0, 2\pi[$ .

**III.4.b.** On suppose qu'il existe  $N \in \mathbb{N}^*$  et  $0 < l < 2\pi$  tels que pour tout arc  $\gamma$  de longueur  $l$ ,  $\bigcup_{0 \leq n \leq N-1} \mathcal{R}^n(\gamma) = S^1$ .

Déterminer  $T > 0$  et  $0 < R < l$  tels que  $\omega$  remplisse  $\mathbb{T}^2$  à  $R$  près en temps  $T$ .

**Idée.** Le flot  $t \mapsto x + t\omega$  traverse  $\mathbb{T}^2$  de gauche à droite ; chaque passage à travers  $D'$  correspond à une itération de  $\mathcal{R}$  sur  $y_2$ . Pour atteindre tout point  $y \in \mathbb{T}^2$  à  $R/2$  près, on doit choisir  $R \leq l/2$  et  $T = N \cdot (2\pi/\omega_1)$  (durée de  $N$  traversées).

Plus précisément : la trajectoire  $\{x + t\omega : 0 \leq t \leq T\}$  projetée sur  $D'$  donne un arc  $\gamma_n$  pour chaque traversée  $n = 0, \dots, N-1$ . Les  $\gamma_n$  sont les itérés de l'arc initial par  $\mathcal{R}$ . Par hypothèse,  $\bigcup \gamma_n = S^1$ . En épaississant chaque  $\gamma_n$  par  $R/2$ , on obtient le voisinage ; il faut  $R \leq l$  pour que le "tube" de chaque morceau de trajectoire couvre une bande perpendiculaire à  $\omega$ .

### Question III.5

**III.5.a.** Soient  $s, C > 0$  tels que  $D(2, s, C) \neq \emptyset$  et  $\omega \in \mathcal{F} \cap D(2, s, C)$ . Posons  $\theta = \omega_2/\omega_1 \in ]0, 1[$ . Soit  $(p_n), (q_n)$  associées à  $\theta$  comme dans I.2.

**Existe-t-il  $n$  tel que  $\frac{2\pi}{q_{n+1}} \leq \frac{l}{3} < \frac{2\pi}{q_n}$  ?** Oui : la suite  $(q_n)$  étant strictement croissante et tendant vers  $+\infty$ ,  $2\pi/q_n$  décroît strictement vers 0. Pour tout  $l > 0$ , il existe un unique  $n$  tel que  $\frac{2\pi}{q_{n+1}} \leq \frac{l}{3} < \frac{2\pi}{q_n}$ .

**III.5.b. Comparer  $q_{n+1}$  et  $[3^s(2\pi)^s\sqrt{2}^s/(Cl^s)]$ .** Comme  $\omega \in D(2, s, C)$ , pour tout  $k \in \mathbb{Z}^2 \setminus \{0\}$ ,  $|\omega \cdot k| \geq C|k|^{-s}$ . Avec  $k = (p_n, -q_n)$  (entre  $p_n$  et  $q_n$ , faux signe, voir formule) :

$$|\omega \cdot k| = |\omega_1 p_n - \omega_2 q_n| = \omega_1 |p_n - \theta q_n| = \omega_1 \cdot \|q_n \theta\|.$$

Donc  $\omega_1 \|q_n \theta\| \geq C|k|^{-s}$  avec  $|k|^2 = p_n^2 + q_n^2 \leq 2q_n^2$  (car  $p_n \leq q_n$  par I.3.a.(ii)), donc  $|k| \leq \sqrt{2} q_n$ . Ainsi  $\omega_1 \|q_n \theta\| \geq C(\sqrt{2} q_n)^{-s}$ , soit  $\|q_n \theta\| \geq C/(\sqrt{2}^s q_n^s \omega_1)$ .

Par I.3.a.(i),  $\|q_n \theta\| \leq 1/q_{n+1}$ , donc

$$\frac{1}{q_{n+1}} \geq \frac{C}{\sqrt{2}^s q_n^s \omega_1} \geq \frac{C}{\sqrt{2}^s q_n^s}$$

( $\omega_1 \leq 1$ ). D'où  $q_{n+1} \leq \sqrt{2}^s q_n^s / C$ .

Par le choix de  $n$ ,  $q_n < 6\pi/l$ , donc  $q_n^s < (6\pi/l)^s$ , et  $q_{n+1} \leq \frac{\sqrt{2}^s (6\pi)^s}{Cl^s} = \frac{(6\pi\sqrt{2})^s}{Cl^s} = \frac{3^s(2\pi)^s\sqrt{2}^s}{Cl^s} \cdot 1^s$ . Donc  $q_{n+1} \leq [3^s(2\pi)^s\sqrt{2}^s/(Cl^s)]$ .

**III.5.c.** Il existe une constante  $K$  telle que  $\mathcal{R}$  remplit  $S^1$  à  $l$  près en  $[K/(Cl^s)]$  itérations.

**Lean.** Version qualitative formalisée : `returnMap_fillsCircle (PartieIII.lean)` prouve  $\exists N$ , `fillsCircle` (re) pour  $\theta$  irrationnel et  $l > 0$ . La quantification optimale (avec  $K = (6\pi\sqrt{2})^s$ ) demanderait le théorème des trois distances (Steinhaus), non formalisé ici.

L'idée :  $\mathcal{R}$  est la rotation d'angle  $2\pi\theta$ . Pour remplir à  $l$  près en  $N$  itérations, il faut que les  $N$  premiers itérés de tout arc de longueur  $l$  recouvrent  $S^1$ . Comme  $|q_{n+1}\theta \cdot 2\pi - 2\pi p_{n+1}| = 2\pi \|q_{n+1}\theta\| \leq 2\pi/q_{n+2} \leq l/3$ ,  $q_{n+1} \cdot \theta$  est proche d'un entier modulo 1. Les itérés  $\mathcal{R}^{kq_{n+1}}(z)$  se rapprochent à la vitesse  $|k| \cdot 2\pi/q_{n+2}$ .

En itérant  $N$  fois, on couvre  $S^1$  par une "subdivision" de pas  $2\pi/q_{n+1}$ . Pour avoir un pas  $\leq l/3$ , il faut  $N \geq q_{n+1} \leq K'/(Cl^s)$  pour une constante  $K'$ . On prend  $K = 3^s(2\pi)^s\sqrt{2}^s$ .

### Question III.6

**Conséquence.** Si  $s, C > 0$  tels que  $D(2, s, C) \neq \emptyset$ , il existe  $K' > 0$  tel que tout  $\omega \in D(2, s, C)$  remplit  $\mathbb{T}^2$  à  $R$  près en temps  $K'/(CR^s)$ .

D'après III.5.c, le nombre d'itérations de  $\mathcal{R}$  pour remplir  $S^1$  à  $l \sim R$  près est  $\leq K/(CR^s)$ . Chaque itération correspond à un temps  $2\pi/\omega_1$ . Donc le temps total est  $\leq K \cdot 2\pi/(CR^s \omega_1) \leq 2\pi K/(CR^s)$ . On pose  $K' = 2\pi K$ .

Si  $\omega \notin \mathcal{F}$ , on peut se ramener au cas par symétrie (changer les coordonnées).  $\square$

## 4 Partie IV — Mélangeance de l'automorphisme du tore

On considère la matrice  $M = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$  (déterminant 1). On note  $E_n$  l'ensemble des polynômes trigonométriques à  $n$  variables (combinaisons linéaires finies à coefficients complexes des  $e^{i(k_1 x_1 + \dots + k_n x_n)}$  pour  $k \in \mathbb{Z}^n$ ). Pour  $f \in E_2$ ,  $\hat{f}(k_1, k_2) = \iint_{[0, 2\pi]^2} f(x_1, x_2) e^{-i(k_1 x_1 + k_2 x_2)} dx_1 dx_2$ .

## Question IV.1

**Énoncé.** Montrer qu'il existe une unique application  $T : \mathbb{T}^2 \rightarrow \mathbb{T}^2$  telle que  $\forall x \in \mathbb{R}^2, T(\langle x \rangle) = \langle Mx \rangle$ . Montrer que  $T$  est bijective et calculer son inverse.

**Existence et unicité.** La relation  $T(\langle x \rangle) = \langle Mx \rangle$  définit bien une application si pour tout  $x \sim y$  (i.e.  $x - y \in 2\pi\mathbb{Z}^2$ ), on a  $Mx \sim My$ . Or  $Mx - My = M(x - y) \in 2\pi M(\mathbb{Z}^2) \subset 2\pi\mathbb{Z}^2$  car  $M$  est à coefficients entiers. D'où l'existence. L'unicité résulte de ce que chaque classe  $\langle x \rangle \in \mathbb{T}^2$  a (au moins) un représentant  $x \in \mathbb{R}^2$ , et  $T(\langle x \rangle)$  est imposé.

**Bijection.**  $M$  est inversible dans  $\text{GL}_2(\mathbb{Z})$ , son inverse  $M^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$  étant à coefficients entiers. Par le même argument,  $T^{-1} : \langle y \rangle \mapsto \langle M^{-1}y \rangle$  est bien définie et  $T \circ T^{-1} = T^{-1} \circ T = \text{id}_{\mathbb{T}^2}$ .  $\square$

**Lean.** Formalisé dans `PartieIV.lean : M_preserves_Z2` et `Minv_preserves_Z2` ( $M$  et  $M^{-1}$  préservent  $\mathbb{Z}^2$ , entrées entières); `T`, `T_inv` sur  $\mathbb{T}^2$ ; `T_bijective`, `T_continuous`, `T_homeomorph` ( $T$  est un homéomorphisme); `det_M` et `det_M_pow` :  $\det M^n = 1$ , donc  $M^n \in \text{SL}_2(\mathbb{Z})$ .

## Question IV.2.a

**Énoncé.** Soit  $I$  un intervalle ouvert de  $]0, 2\pi[$ ,  $\chi$  sa fonction caractéristique. Montrer que pour tout  $\varepsilon > 0$ , il existe un polynôme trigonométrique  $g$  d'une variable tel que  $\int_0^{2\pi} |\chi(x) - g(x)|^2 dx < \varepsilon$ .

**Preuve.** La fonction  $\chi$  est dans  $L^2([0, 2\pi[)$ . Les polynômes trigonométriques  $\{e^{ikx} : k \in \mathbb{Z}\}$  forment une base de Hilbert de  $L^2([0, 2\pi[, dx/2\pi)$  (théorème de Stone-Weierstrass + densité). Par le théorème de convergence des séries de Fourier dans  $L^2$ ,  $\chi = \lim_N \sum_{|k| \leq N} \hat{\chi}(k) e^{ikx}$  au sens  $L^2$ . Donc il existe  $N$  tel que  $g_N(x) = \sum_{|k| \leq N} \hat{\chi}(k) e^{ikx}$  vérifie  $\|\chi - g_N\|_{L^2}^2 < \varepsilon$ .  $\square$

**Lean.** **Théorème entièrement formalisé :** `UlmLyon1995.PartieIV.iv_2_a_concrete` (énoncé général pour  $f \in L^2([0, 2\pi])$ , dont le cas de l'indicatrice  $\chi_I$  est un cas particulier). La preuve transporte la base de Hilbert de Fourier de Mathlib (`fourierBasis` sur `AddCircle`) vers le formalisme concret  $\int_0^{2\pi}$ . 8 briques sont assemblées :

- Brique 1 : `trigPoly_dense_Lp_haar` (densité Lp abstraite via `HilbertBasis.hasSum_repr`).
- Brique 2 : passage `fourierBasis k`  $\rightarrow$  `fourierLp 2 k`.
- Brique 3 : `coeFn_sum_smul_fourierLp_ae` (induction sur  $S$ , utilise `Lp.coeFn_add/smul` et `coeFn_fourierLp`).
- Brique 4 : `fourier_coe_apply_two_pi` (`fourier k` ( $\uparrow x$ ) =  $e^{ikx}$  pour  $T = 2\pi$ ).
- Brique 5 : `iv_2_a_Lp_and_function` (assemblage Lp).
- Brique 6 : relèvement de  $f : \mathbb{R} \rightarrow \mathbb{C}$  à `AddCircle (2π)` via `liftIoc`.
- Brique 7 : `Lp_two_norm_sq_eq_integral` et `two_pi_mul_norm_sq_eq_intervalIntegral` :  $(2\pi) \cdot \|g\|_{L^2(\text{haar})}^2 = \int_0^{2\pi} \|g(\uparrow x)\|^2 dx$ .
- Brique 8 : `ae_haar_to_ae_Ioc` (transfer a.e. via `Measure.ae_smul_measure` et `AddCircle.measurePreserv` + `intervalIntegral.integral_congr_ae`. Conclusion finale :  $\int_0^{2\pi} \|f - \text{trigPoly}\|^2 < \varepsilon$ .

Aucun nouvel axiome ; seulement `propext`, `Classical.choice`, `Quot.sound`.

## Question IV.2.b

**Énoncé.** Soient  $f, g \in E_2$ . Calculer  $\lim_{n \rightarrow \pm\infty} \iint_{[0, 2\pi]^2} f(M^n(x_1, x_2))g(x_1, x_2)dx_1dx_2$ .

**Calcul.** Écrivons  $f(x) = \sum_k a_k e^{ik \cdot x}$  et  $g(x) = \sum_l b_l e^{il \cdot x}$ . Alors  $f(M^n x) = \sum_k a_k e^{i(M^n)^T k \cdot x}$  (car  $k \cdot Mx = (M^T k) \cdot x$ , donc  $k \cdot M^n x = ((M^T)^n k) \cdot x$ ).

Posons  $A = M^T = M$  (car  $M$  est symétrique). Alors

$$\iint f(M^n x) g(x) dx = \sum_{k,l} a_k b_l \iint e^{i(A^n k + l) \cdot x} dx = (2\pi)^2 \sum_{k,l: A^n k = -l} a_k b_l.$$

En sommant sur les couples  $(k, l)$  avec  $l = -A^n k$  :

$$\iint f(M^n x) g(x) dx = (2\pi)^2 \sum_k a_k b_{-A^n k}.$$

Pour  $f, g$  polynômes trigonométriques, les sommes sont finies. Considérons  $n \rightarrow \pm\infty$ . Les valeurs propres de  $M$  sont  $\lambda_{\pm} = \frac{3 \pm \sqrt{5}}{2}$  (racines de  $\lambda^2 - 3\lambda + 1 = 0$ ), avec  $\lambda_+ > 1 > \lambda_- > 0$ . Donc  $M^n$  écarte fortement les vecteurs propres (sauf 0).

Précisément, pour  $k \neq 0 \in \mathbb{Z}^2$ ,  $A^n k \rightarrow \infty$  en norme. Comme les supports de  $f, g$  sont finis (poly trig), pour  $n$  assez grand,  $A^n k \notin \text{supp}(b)$  pour tout  $k \neq 0 \in \text{supp}(a)$ . Donc dans la somme, seul le terme  $k = 0$  survit, donnant  $a_0 b_0 (2\pi)^2$ .

Or  $a_0 = \hat{f}(0)/(2\pi)^2 = \frac{1}{(2\pi)^2} \iint f$  et  $b_0 = \frac{1}{(2\pi)^2} \iint g$  (par les conventions de  $\hat{\cdot}$  ici). Donc la limite est

$$\lim_{n \rightarrow \pm\infty} \iint f(M^n x) g(x) dx = (2\pi)^2 a_0 b_0 = \frac{1}{(2\pi)^2} \iint f \cdot \iint g.$$

**Lean.** Formalisé pour le *cas zero-mean* ( $\int f = 0$ ) dans `PartieIV.lean` :

- `integral_exp_I_mul_int_eq_zero` : orthogonalité Fourier 1D.
- `integral_exp_I_2d_eq_zero` : orthogonalité Fourier 2D (via Fubini / `intervalIntegral`).
- `Mvec_int, Mvec_iter_int` : action  $M^n$  sur  $\mathbb{Z}^2$ .
- `Mvec_iter_int_add_eventually_ne_zero` : pour  $k \in \mathbb{Z}^2 \setminus \{0\}$ ,  $M^n k + l \neq 0$  éventuellement (corollaire de `Mvec_iter_norm_tendsto_atTop` :  $\|M^n k\| \rightarrow +\infty$ ).
- `mixing_monomial_eventually_zero` : l'intégrale d'un monôme  $\exp(i(M^n k + l) \cdot x)$  est éventuellement nulle.
- `mixing_finite_sum_eventually_zero, mixing_finite_sum_tendsto_zero` : extension par linéarité à somme finie avec  $\int f = 0$  (cas  $0 \notin S_f$ ).
- `mixing_finite_sum_eventually_zero_g` : cas symétrique avec  $\int g = 0$  (cas  $0 \notin S_g$ ). Le sous-cas  $k = 0, l \neq 0$  donne une intégrale *exactement* nulle ; le sous-cas  $k \neq 0$  retombe sur `mixing_monomial_eventually_zero`.

La voie sans *Hilbert spaces* / *Stone-Weierstrass* / *Plancherel* fonctionne. IV.2.b est ainsi formalisé pour TOUS les polynômes trigonométriques finis  $f, g$  :

- cas  $\int f = 0$  : `mixing_finite_sum_eventually_zero`.
- cas  $\int g = 0$  : `mixing_finite_sum_eventually_zero_g` (preuve par cas, sous-cas  $k = 0, l \neq 0$  donne intégrale exactement nulle).
- cas général  $\int f, \int g$  non nuls : `mixing_finite_sum_eventually_eq_general` donne la limite explicite  $a_0 b_0 (2\pi)^2 = \frac{1}{(2\pi)^2} \int f \cdot \int g$ . Preuve par décomposition  $\Sigma_{k \in S_f} = (k=0 \text{ part}) + \Sigma_{k \neq 0}$  où le  $k = 0$  part est déterministe ( $a_0 b_0 (2\pi)^2$  exactement via `integral_I_zero_zero` / `integral_I_zero_1`) et la partie  $k \neq 0$  tend vers 0 (zero-mean).

Reste seulement IV.2.a (approximation  $L^2$  de  $\chi_P$  par trig polynôme, qui passe par Stone-Weierstrass) et IV.2.c (application aux ensembles via IV.2.a + IV.2.b).

### Question IV.2.c

**Énoncé.** Soient  $P_1, P_2$  pavés ouverts de  $]0, 2\pi]^2$ . Montrer que  $\text{aire}(M^n P_1 \cap (P_2 + 2\pi\mathbb{Z}^2)) / \text{aire}(P_1) \rightarrow \text{aire}(P_2) / (4\pi^2)$  quand  $n \rightarrow \pm\infty$ .

**Preuve.** Soient  $\chi_i$  les fonctions caractéristiques de  $P_i$  (vues dans  $\mathbb{T}^2$ ). On a

$$\text{aire}(M^n P_1 \cap (P_2 + 2\pi\mathbb{Z}^2)) = \iint \chi_2(M^{-n}x) \chi_1(x) dx,$$

ou plutôt avec changement de variables  $y = M^{-n}x$ ,  $|\det M^{-n}| = 1$  :

$$\text{aire}(M^n P_1 \cap (P_2 + 2\pi\mathbb{Z}^2)) = \iint \chi_1(M^n y) \chi_2(y) dy.$$

Hmm vérifions :  $M^n P_1$  a pour aire  $\text{aire}(P_1)$  (car  $|\det M| = 1$ ), et  $M^n P_1 \cap (P_2 + 2\pi\mathbb{Z}^2)$  correspond aux  $x \in M^n P_1$  tels que  $x \in P_2 + 2\pi\mathbb{Z}^2$ , soit  $x \bmod 2\pi \in P_2$ . Donc  $\text{aire}(M^n P_1 \cap (P_2 + 2\pi\mathbb{Z}^2)) = \iint \chi_{M^n P_1}(x) \tilde{\chi}_{P_2}(x) dx$  où  $\tilde{\chi}_{P_2}$  est la fonction  $2\pi\mathbb{Z}^2$ -périodique étendant  $\chi_{P_2}$ .

Par approximation  $\chi_i \approx f_i \in E_2$  dans  $L^2(\mathbb{T}^2)$ , on applique IV.2.b à  $f = \tilde{\chi}_{P_2} \approx f_2$  et  $g = \tilde{\chi}_{P_1} \approx f_1$ , et l'on obtient :

$$\iint f_2(M^n y) f_1(y) dy \rightarrow \frac{1}{(2\pi)^2} \iint f_2 \cdot \iint f_1 \approx \frac{1}{(2\pi)^2} \text{aire}(P_2) \text{aire}(P_1).$$

Soit, après division par  $\text{aire}(P_1)$  :

$$\frac{\text{aire}(M^n P_1 \cap (P_2 + 2\pi\mathbb{Z}^2))}{\text{aire}(P_1)} \rightarrow \frac{\text{aire}(P_2)}{(2\pi)^2} = \frac{\text{aire}(P_2)}{4\pi^2}.$$

Ce qui prouve la *propriété de mélange*. □

### Question IV.3.a

**Énoncé.** Soit  $(e_+, e_-)$  une base de vecteurs propres unitaires de  $M$ ,  $e_+$  associé à  $\lambda_+$ . Montrer qu'il existe  $C > 0$  tel que  $e_+, e_- \in D(2, 1, C)$ .

**Preuve.** Les valeurs propres de  $M$  sont irrationnelles ( $\lambda_{\pm} = (3 \pm \sqrt{5})/2$  algébriques de degré 2 sur  $\mathbb{Q}$ ). Les vecteurs propres  $e_{\pm}$  ont leurs composantes liées par  $e_{+,2}/e_{+,1} = \lambda_+ - 2 = \frac{\sqrt{5}-1}{2}$  (et idem pour  $e_-$  avec  $\lambda_-$ ). Cette pente est algébrique de degré 2.

Soit  $\theta = (\sqrt{5} - 1)/2 \in \mathbb{R} \setminus \mathbb{Q}$  algébrique de degré 2. Par II.2, il existe  $A > 0$  tel que  $|\theta - p/q| \geq A/q^2$ , soit  $|q\theta - p| \geq A/|q|$  pour tout  $(p, q) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ .

Pour  $k = (k_1, k_2) \in \mathbb{Z}^2 \setminus \{0\}$  :  $e_+ \cdot k = e_{+,1}(k_1 + \theta k_2)$ , donc  $|e_+ \cdot k| = |e_{+,1}| \cdot |k_2 \theta + k_1| \geq |e_{+,1}| A/|k_2| \geq cA/|k|$  pour  $|k_2| \leq |k|$ . Si  $k_2 = 0$  et  $k_1 \neq 0$ ,  $|e_+ \cdot k| = |e_{+,1}| \cdot |k_1| \geq |e_{+,1}|/|k|$ .

Posons  $C = A|e_{+,1}|$ . Alors  $e_+ \in D(2, 1, C)$ . De même pour  $e_-$ . □

### Question IV.3.b

**Énoncé.** Déterminer  $c > 0$  telle que pour tout  $R > 0$  et tout  $k = (k_1, k_2) \in \mathbb{Z}^2 \setminus \{0\}$  avec  $\sup(|k_1|, |k_2|) \leq R$ ,  $|M^{-n}k| \geq c\lambda_+^n R^{-1}$ .

**Preuve.** Décomposons  $k = ae_+ + be_-$  avec  $(a, b) \in \mathbb{R}^2$ . Alors  $M^{-n}k = a\lambda_+^{-n}e_+ + b\lambda_-^{-n}e_- = a\lambda_+^{-n}e_+ + b\lambda_+^n e_-$  (car  $\lambda_- = \lambda_+^{-1}$ ). Donc

$$|M^{-n}k|^2 = a^2\lambda_+^{-2n} + b^2\lambda_+^{2n} \geq b^2\lambda_+^{2n}.$$

On veut  $|b| \geq c'/R$  pour une constante. Or  $b = k \cdot e_- / |e_-|^2 = k \cdot e_-$  (car  $e_-$  unitaire). Par IV.3.a,  $|k \cdot e_-| \geq C/|k|$  et  $|k| \leq \sqrt{2}R$ , donc  $|b| \geq C/(\sqrt{2}R)$ . Ainsi  $|M^{-n}k| \geq |b|\lambda_+^n \geq C\lambda_+^n/(\sqrt{2}R)$ . On pose  $c = C/\sqrt{2}$ .

**Lean.** La preuve formalisée existe sous deux formes (`PartieIV.lean`) :

**Première formalisation** (par auto-adjonction) : `Mvec_inv_iter_norm_lower_bound_R` (action  $M^{-n}$ ) et `Mvec_iter_norm_lower_bound_R` (action  $M^n$ ) contournent la décomposition spectrale explicite en utilisant l'auto-adjonction (`Mvec_iter_self_adjoint`) et l'inégalité de Cauchy-Schwarz pour vecteur unitaire (`abs_vecDot_le_vecNorm_of_unit`). Corollaire asymptotique `Mvec_iter_norm_te`  $\|M^n k\| \rightarrow +\infty$ .

**Seconde formalisation** (par décomposition spectrale directe) :

- `vec_decomp` : tout  $k \in \mathbb{R}^2$  se décompose en  $k = \langle k, e_+ \rangle e_+ + \langle k, e_- \rangle e_-$  (preuve par substitution  $\varphi = 1/\varphi'$  pour éliminer une variable, puis `field_simp+ring` sur la formule explicite).
- `vec_pythagoras` :  $\|k\|^2 = \langle k, e_+ \rangle^2 + \langle k, e_- \rangle^2$  (corollaire par les relations de ligne de la matrice orthogonale  $[e_+; e_-]$ ).
- `Mvec_inv_iter_norm_sq_eq` : la *formule spectrale exacte*  $\|M^{-n}k\|^2 = a^2\lambda_-^{2n} + b^2\lambda_+^{2n}$  (avec  $a = \langle k, e_+ \rangle$ ,  $b = \langle k, e_- \rangle$ ), qui correspond ligne à ligne au calcul du LaTeX ci-dessus.

La borne inférieure  $|M^{-n}k| \geq |b|\lambda_+^n$  se déduit alors trivialement en oubliant le terme positif  $a^2\lambda_-^{2n}$ .

### Question IV.3.c

**Énoncé.** Soit  $\chi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$  décroissante tendant vers 0.

$$H_\chi = \{f \in E_2 \mid \forall R > 0, \sum_{\sup(|k_1|, |k_2|) \geq R} |\hat{f}(k)|^2 \leq \chi(R)^2 \sum_{k \in \mathbb{Z}^2} |\hat{f}(k)|^2\}.$$

Montrer qu'il existe une constante  $c' > 0$  telle que pour tout  $n \in \mathbb{N}$  et toutes  $f, g \in H_\chi$  avec  $\iint f = \iint g = 0$  :

$$\left| \iint f(M^n(x_1, x_2))g(x_1, x_2)dx_1dx_2 \right| \leq 2 \left( \iint |f|^2 \right)^{1/2} \left( \iint |g|^2 \right)^{1/2} \chi(c'\lambda_+^{n/2}).$$

**Preuve (schéma).** Par Parseval-Plancherel, pour  $f, g \in E_2$  :

$$\iint f(M^n x)g(x)dx = (2\pi)^2 \sum_k \hat{f}(M^{nT}k) \overline{\hat{g}(-k)}.$$

Sous l'hypothèse  $\iint f = \iint g = 0$ ,  $\hat{f}(0) = \hat{g}(0) = 0$ , donc la somme porte sur  $k \neq 0$  (et  $M^{nT}k \neq 0$ ).

Posons  $R_n = c\lambda_+^{n/2}$  pour un certain  $c > 0$  adapté. On scinde la somme en  $|k| \leq R_n$  et  $|k| > R_n$ .

Pour  $|k| \leq R_n$ ,  $|M^{nT}k| \geq c'\lambda_+^n R_n^{-1} = c'\lambda_+^{n/2}/c$  par IV.3.b. Donc  $\hat{f}(M^{nT}k)$  correspond à un mode de fréquence haute,  $\geq c'\lambda_+^{n/2}/c$ . Par déf de  $H_\chi$ ,  $\sum_{|k| \geq c'\lambda_+^{n/2}/c} |\hat{f}(k)|^2 \leq \chi(c'\lambda_+^{n/2}/c)^2 \|\hat{f}\|^2$ .

Pour  $|k| > R_n$ ,  $|\hat{g}(-k)|$  correspond à un mode haute fréquence pour  $g$ , donc bornable par  $\chi(R_n)$ .

Par Cauchy-Schwarz, on obtient :  $|\iint f(M^n x)g(x)dx| \leq 2\|f\|_{L^2}\|g\|_{L^2}\chi(c'\lambda_+^{n/2})$  en absorbant les constantes dans le 2.  $\square$