

1. SOLUTIONS

- 1 (1) Bien que $G = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ soit un sous-groupe de \mathbb{R} , il n'est pas discret et n'est donc pas un réseau de \mathbb{R} . Pour le montrer, il "suffit" de trouver une suite de G qui tend vers 0. Une candidate est la suite de $(\sqrt{2} - 1)^n$, et il suffit donc de montrer que chacun de ses termes est dans G . Comme on a $(\sqrt{2} - 1)^n = \sum_{i=0}^n \binom{n}{i} \sqrt{2}^i (-1)^{n-i}$, il suffit de montrer que tous les $\sqrt{2}^i$ sont dans G . Si i est pair c'est immédiat, sinon $i = 2j + 1$ avec j entier et on peut écrire $\sqrt{2}^i = 2^j \sqrt{2} \in G$.
- (2) La pente de cette droite est irrationnelle, et elle ne contient donc aucun point dont les coordonnées sont entières. Autrement dit, $\mathbb{Z}^2 \cap V$ est le réseau trivial $\{0\}$, et le rang de l'intersection n'est pas celui "attendu" (on s'attendrait à 1). C'est un bon signal que la projection ne va pas être un réseau non plus. On calcule facilement une matrice $\mathbf{P} = \mathbf{v} \cdot (\mathbf{v}^t \mathbf{v})^{-1} \cdot \mathbf{v}^t$ pour la projection orthogonale π :

$$\mathbf{P} = \begin{bmatrix} 1 \\ \sqrt{2} \end{bmatrix} \cdot \|(1, \sqrt{2})\|^2 \cdot [1 \quad \sqrt{2}] = \frac{1}{3} \cdot \begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{2} & 2 \end{bmatrix}.$$

Ainsi, on a $3 \cdot \pi(x, y) = (x + \sqrt{2}y, \sqrt{2}x + 2y)$ pour tout $(x, y) \in \mathbb{R}^2$ et en particulier, on voit que $3 \cdot \pi(\mathbb{Z}^2) = (\mathbb{Z} + \sqrt{2}\mathbb{Z}) \cdot (1, \sqrt{2})$. D'après la question précédente, $(\mathbb{Z} + \sqrt{2}\mathbb{Z})$ est dense dans \mathbb{R} et donc $\pi(\mathbb{Z}^2)$, dense dans V , n'est pas un réseau.

- (3) C'est un exercice classique. Soit G un sous-groupe non trivial de \mathbb{R} . En particulier il est non-vide, et il existe donc au moins un élément strictement positif. Ceci nous permet de définir $\alpha = \inf G \cap \mathbb{R}_+^*$. Il y a alors deux cas de figure :
- **Cas $\alpha = 0$:** Dans ce cas G est dense. En effet, par la propriété de la borne inférieure et la définition de α , pour tout $\epsilon > 0$ on peut trouver $g \in G$ tel que $0 < g < \epsilon$. Soit $x \in \mathbb{R} \setminus G$ et notons $[a]$ le plus grand entier inférieur à un réel a , satisfaisant $[a] \leq a < [a] + 1$. Comme G est un groupe additif, on a $[x/g]g \in G$. On a de plus $0 \leq x - [x/g]g = g(x/g - [x/g]) < \epsilon$, ce qu'on voulait démontrer.
 - **Cas $\alpha > 0$:** On a directement que G est discret, puisque l'intervalle $(-\alpha/2, \alpha/2)$ ne contient que 0, donc par translation par les éléments de $g \in G$, les intervalles $(g - \alpha/2, g + \alpha/2)$ ne contiennent qu'un seul élément de G . Il faut montrer que $\alpha \in G$, puis que $G = \alpha\mathbb{Z}$. Deux utilisations de la propriété de la borne inférieure donnent $g, g' \in G$ tels que $\alpha \leq g < g' < 2\alpha$. Ceci entraîne que $0 < g' - g \leq \alpha$, et donc par définition de α que $\alpha = g' - g \in G$. Il est ensuite clair que $\alpha\mathbb{Z} \subset G$. Pour l'autre inclusion, notons que pour tout $g \in G$, on a $g - [g/\alpha]\alpha \in G$. Par définition, ceci implique $0 \leq \alpha(g/\alpha - [g/\alpha]) < \alpha$, ce qui n'est possible que si $g = [g/\alpha]\alpha$.

- 2 (1) Notons (b'_1, b'_2) la base obtenue après une itération de la boucle sur la base (b_1, b_2) . Alors matriciellement, on peut écrire

$$[b'_1, b'_2] = [b_1, b_2] \begin{bmatrix} -x & 1 \\ 1 & 0 \end{bmatrix},$$

donc la matrice de transformation a une déterminant -1 et des entrées entières.

- (2) Il s'agit d'observer que on note que $b'_1 - zb'_2 = b_2 - (x - z)b_1$, avec $x - z$ entier, et que par définition, b'_1 est la meilleure approximation entière de la projection orthogonale de b_2 sur $(\mathbb{R}b_1)^\perp$. Formellement, si on note $\tilde{x} = \frac{\langle b_1, b_2 \rangle}{\|b_1\|^2}$, on a $b'_1 = b_2 - xb_1 = \pi_{(\mathbb{R}b_1)^\perp}(b_2) - (x - \tilde{x})b_1$ d'une part ; d'autre part, $b'_1 - zb'_2 = \pi_{(\mathbb{R}b_1)^\perp}(b_2) - (x - \tilde{x} - z)b_1$, et le premier résultat vient par définition du plus proche entier.

Quand on sort de l'algorithme, les vecteurs sont échangés. En utilisant le résultat qu'on vient d'obtenir pour $z = \pm 1$, on obtient $\|b + b'\| \geq \|b'\|$ et $\|b - b'\| \geq \|b'\|$. On développe ensuite les carrés des normes pour obtenir le résultat.

- (3) Supposons qu'il existe $u \in \mathcal{L}$ tel que $\|u\| < \|b\|$, et écrivons $u = zb + z'b'$ avec $z, z' \in \mathbb{Z}$. On écrit alors $\|u\|^2 = z^2\|b\|^2 + 2zz'\langle b, b' \rangle + z'^2\|b'\|^2 < \|b\|^2$. D'après la question précédente, ceci implique que

$$(z^2 - 1 - |zz'|)\|b\|^2 + z'^2\|b'\|^2 < 0.$$

Avec les conditions de sortie de l'algorithme, on en déduit de plus que $z^2 + z'^2 - |zz'| - 1 < 0$. Les identités remarquables bien connus assurent que $z^2 + z'^2 \geq 2|zz'|$, et il est alors nécessaire que $|zz'| = 0$. Si $z = 0$ et $z' \neq 0$, il vient que $\|u\| = |z'|\|b'\| \geq \|b\|$; si $z \neq 0$ et $z' = 0$, il vient $\|u\| = |z|\|b\| \geq \|b\|$; dans les deux cas, ces choix contredisent l'hypothèse sur u , et donc $u = 0$.

Le raisonnement est similaire pour b' : supposons qu'il existe $u = zb + z'b'$ avec $z' \neq 0$ (sinon u est colinéaire à b), et tel que $\|u\| < \|b'\|$. On trouve alors

$$(z^2 - |zz'|)\|b\|^2 + (z'^2 - 1)\|b'\|^2 < 0,$$

avec $z'^2 - 1 \geq 0$. Toujours avec la condition de sortie de l'algorithme, on retrouve $z^2 + z'^2 - |zz'| - 1 < 0$, ce qui donne le résultat.

Preuve alternative et simultanée : Cette preuve utilise d'une autre manière les propriétés de la base obtenue. Soit $u = xb + yb'$ avec $x, y \in \mathbb{Z}$. Si $y = 0$, on a clairement $\|u\| \geq \|b\|$. Supposons donc que $y \neq 0$, et écrivons $x = qy + r$ avec $0 \leq |r| < |y|$ la division euclidienne de x par y . D'après la question précédente et la condition de sortie, on sait que $\|b' + qb\| \geq \|b'\| \geq \|b\|$. On peut alors écrire

$$\begin{aligned} \|u\| &= \|(y(b' + qb) + rb)\| \geq |y|\|b' + qb\| - |r|\|b\| \\ &= (|y| - |r|)\|b' + qb\| + |r|(\|b' + qb\| - \|b\|) \\ &\geq \|b' + qb\| \geq \|b'\| \geq \|b\|, \end{aligned}$$

où la première inégalité provient de l'inégalité triangulaire inverse combinée aux propriétés de la base, et la deuxième de la positivité du dernier terme. On obtient le résultat annoncé.

- (4) Supposons qu'on passe dans la boucle avec b_1, b_2 donnant $x = 0$; en particulier, on a $\|b_1\| \leq \|b_2\|$ avant ce passage. Comme $x = 0$, le passage dans la boucle ne fait qu'échanger b_1 et b_2 , et on vérifie maintenant la condition de sortie.
- (5) Si (b_1, b_2) donne $x = 1$, elle produit alors $(b'_1 = b_2 \pm b_1, b'_2 = b_1)$. Si on ne sort pas de la boucle, c'est qu'on a $\|b'_1\| < \|b'_2\|$, ou encore $\|b_1 \pm b_2\| < \|b_1\|$. Si on était déjà dans la boucle, ceci contredit la question (2), donc soit il s'agit de la première base considérée, soit on sort nécessairement de la boucle.
- (6) Si $|x| > 1$, en particulier on a $\frac{3}{2} \leq \frac{|\langle b_1, b_2 \rangle|}{\|b_1\|^2}$. On déroule ensuite les définitions et on se souvient que les Gram-Schmidt sont orthogonaux : $b_2 = \tilde{b}_2 + \frac{\langle b_1, b_2 \rangle}{\|b_1\|^2} b_1$, donc $\|b_2\|^2 \geq \|\tilde{b}_2\|^2 + \frac{9}{4}\|b_1\|^2$. De même, en posant \tilde{x} le nombre qui s'arrondit à x , on a $t = b_2 - xb_1 = \tilde{b}_2 - (x + \tilde{x})b_1$ et on sait que $|x - \tilde{x}| \leq 1/2$, ce qui donne l'inégalité pour t . On en déduit $\|b_2\|^2 \geq \|t\|^2 + 2\|b_1\|^2$, et le résultat provient de la condition de boucle pour la base (t, b_1) .

1. Merci à T. Espitau pour me l'avoir montrée, je la trouve bien plus élégante, quoique plus astucieuse.

- (7) D'après la question précédente, on a $(\|b_1\| \cdot \|b_2\|)^2 > 3(\|t\| \cdot \|b_1\|)^2$. Ainsi, si $(b_1^{(n)}, b_2^{(n)})$ est la base obtenue après n passage dans la boucle depuis (b_1, b_2) , on a

$$(\|b_1^{(n)}\| \cdot \|b_2^{(n)}\|)^2 < 3^{-n}(\|b_1\| \cdot \|b_2\|)^2.$$

L'algorithme manipule uniquement des bases du réseau ; par l'inégalité de Hadamard, on sait que pour tout n , on doit avoir $(\det \mathcal{L})^2 \leq (\|b_1^{(n)}\| \cdot \|b_2^{(n)}\|)^2$. On en tire que $n \leq 2 \log_3(\frac{\|b_1\| \|b_2\|}{\det \mathcal{L}})$. Comme \mathcal{L} est contenu dans \mathbb{Z}^m , son déterminant est un entier au moins égal à 1 : on est sur que l'algorithme fait un nombre d'itération au plus polynomial en la taille de son entrée. Pour aller un peu plus loin, on peut utiliser que $\|b_1\| \|\tilde{b}_2\| = \det \mathcal{L}$. Comme b_1, b_2 sont des vecteurs entiers et non colinéaires, on a nécessairement $\|\tilde{b}_2\| \geq 1$. En effet, par contraposée, on serait dans la situation où b_2 est un vecteur entier à distance strictement plus petite que 1 de $\mu_{21}b_1$, qui ne peut être que $\lfloor \mu_{21} \rfloor b_1$ ou $\lceil \mu_{21} \rceil b_1$. (Faire un dessin, rappel de cours, $\mu_{21} = \langle b_1, b_2 \rangle / \|b_2\|^2$). On obtient que $n \leq 2 \log_3(\|b_2\|) \leq 2 \log_3(\sqrt{m}B)$, si B est une borne sur les entrées de b_1 et b_2 . Ceci s'étend sans peine à $b_1, b_2 \in \mathbb{Q}^m$: il existe $d \in \mathbb{Z}$ tel que db_1, db_2 soient entiers (par exemple, prendre d comme le ppcm de tous les dénominateurs), donc on se ramène au cas entier.