Sous-groupes discrets de $\mathbb{R}^n$: réseaux

Plan

Remarques d'ordre général: il y a tellement à dire qu'il faut bien organiser votre plan. Par ailleurs on constate souvent que les candidats en savent très peu sur le sujet, dans ce cas mieux vaut peut être prendre l'autre choix...

- Commencez par un premier paragraphe de généralités dans un espace vectoriel dénué de toute structure:
  - Une partie Γ de V est un sous-réseau s'il existe une famille libre $\mathbf{e} = (e_1, \cdots, e_r)$ de V telle que $\Gamma = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$. On dit que $\mathbf{e}$ est une $\mathbb{Z}$-base de Γ et r est son rang. On dit que Γ est un réseau si $r = n$.
  - $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ n'est pas un sous-réseau de $\mathbb{R}$.
  - Soit Γ un réseau de V, $\mathbf{e}$ une $\mathbb{Z}$-base de Γ et $\mathbf{v}$ une base de V. Montrez que $\mathbf{v}$ est une $\mathbb{Z}$-base de Γ si et seulement si la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ appartient à $GL_n(\mathbb{Z})$ ou encore si et seulement s'il existe une matrice $A \in GL_n(\mathbb{Z})$ telle que
  $$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ \ddots \\ e_n \end{pmatrix}$$
  - théorème de la base adaptée: soient Γ un réseau de V et $\Lambda \subset \Gamma$ un sous-groupe alors Λ est un sous-réseau de V et il existe une $\mathbb{Z}$-base $(e_1, \cdots, e_n)$ de Γ, $1 \leq s \leq n$ et $a_1, \cdots, a_s \in \mathbb{Z}^\times$ vérifiant:
    - $(a_1 e_1, \cdots, a_s e_s)$ est une $\mathbb{Z}$-base de Λ,
    - pour $1 \leq i < s$, a_i divise a_{i+1}
  - Pour $K = \mathbb{Q}$, soient Γ, Λ des réseaux de V alors
    - il existe $d \in \mathbb{N}\backslash\{0\}$ tel que $d\Gamma \subset \Lambda$,
    - $\Gamma + \Lambda$ et $\Gamma \cap \Lambda$ sont des réseaux de V.
  - Pour $K = \mathbb{R}$, on munit V de sa topologie canonique alors tout sous-groupe discret (i.e. tel que pour tout compact $\mathcal{K}$ de V, $\mathcal{K} \cap \Gamma$ est fini) Γ de V en est un sous-réseau.
  - Soient $\epsilon > 0$ et $(\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n\backslash\mathbb{Q}^n$ alors il existe $p_1, \cdots, p_n \in \mathbb{Z}$ et $q \in \mathbb{N}$ non nul tels que pour tout $1 \leq i \leq n$, on ait $|\alpha_i - \frac{p_i}{q}| < \frac{\epsilon}{q}$.
    Indication: considérez le groupe Γ engendré par les vecteurs de la base canonique et le vecteur $(\alpha_1, \cdots, \alpha_n)$ et remarquez que Γ n'est pas un réseau et n'est donc pas discret.
  - classification des groupes abéliens de type fini.

- un deuxième paragraphe, on rajoute à V une structure euclidienne:
  - Pour Γ un réseau de $\mathbb{R}^n$ et $\mathbf{e} = (e_1, \cdots, e_n)$ une $\mathbb{Z}$-base de Γ, on pose
    - $P_{\mathbf{e},\Gamma} = \{\sum_{i=1}^n \lambda_i e_i;\ \lambda_1, \cdots, \lambda_n \in [0,1]\}$,
    - $D_{\mathbf{e},\Gamma} = \{\sum_{i=1}^n \lambda_i e_i;\ \lambda_1, \cdots, \lambda_n \in [0,1[\}$,

    On note $S_{\mathbf{e},\Gamma}$ (resp. $T_{\mathbf{e},\Gamma}$) la matrice de terme général $(e_i|e_j)$ (resp. $(\epsilon_i|e_j)$).
    (a) $\mu(P_{\mathbf{e},\Gamma}) = \sqrt{\det S_{\mathbf{e},\Gamma}}$ et $\mu(P_{\mathbf{e},\Gamma})$ ne dépend que de Γ et non de $\mathbf{e}$; on dit que c'est la mesure du réseau et on la note $\mu(\mathbb{R}^n/\Gamma)$.
    (b) Une partie $\mathcal{D}$ de $\mathbb{R}^n$ est un domaine fondamental de Γ, si $\mathcal{D}$ est μ-mesurable et si ses translatés par les vecteurs de Γ forment une partition de $\mathbb{R}^n$. Alors $D_{\mathbf{e},\Gamma}$ est un domaine fondamental et $\mu(\mathcal{D}) = \mu(\mathbb{R}^n/\Gamma)$ pour tout domaine fondamental $\mathcal{D}$ de Γ.
    (c) En utilisant le théorème de la base adaptée, si $\Lambda \subset \Gamma$ sont des réseaux alors Γ/Λ est fini et
    $$\mu(\mathbb{R}^n/\Lambda) = \mathrm{card}(\Gamma/\Lambda)\mu(\mathbb{R}^n/\Gamma)$$

– le théorème de Minkowski: soient Γ un réseau de $\mathbb{R}^n$ et A une partie μ-mesurable, convexe, symétrique par rapport à O et vérifiant $\mu(A) > 2^n\mu(\mathbb{R}^n/\Gamma)$, alors $A \cap \Gamma \neq \{O\}$. Ainsi si C est un convexe compact de $\mathbb{R}^n$, symétrique par rapport à O tel que $\mu(C) \geq 2^n\mu(\mathbb{R}^n/\Gamma)$ alors $C \cap \Gamma \neq \{O\}$. Et enfin en notant v_n le volume de la boule unité fermée de $\mathbb{R}^n$, alors il existe $\gamma \in \Gamma$ différent de O et de norme inférieure ou égale à deux fois la racine n-ième de $v_n^{-1}\mu(\mathbb{R}^n/\Gamma)$.

– théorème d'Hermite: Γ possède une base $e_1, \cdots, e_n$ telle que

$$N(e_1).\cdots.N(e_n) \leq (\frac{4}{3})^{n(n-1)/2} \det \Gamma$$

On rappelle que l'inégalité d'Hadamard donne que $\det \Gamma \leq N(e_1).\cdots.N(e_n)$. En déduire alors qu'il existe un vecteur non nul de Γ de norme inférieure ou égale à $(\frac{4}{3})^{n(n-1)/2} \det(\Gamma)^{1/n}$.

– minima successifs d'un réseau: $\lambda_1(\Gamma), \cdots, \lambda_n(\Gamma)$, où $\lambda_i(\Gamma)$ est le plus petit $\lambda \in \mathbb{R}_+^*$ tel qu'il existe i vecteurs libres de Γ de norme au plus λ. A partir de la dimension 5, il n'existe pas, en général, de base réalisant les minima successifs: par exemple

$$v_1 = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ v_2 = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ v_3 = \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \\ 0 \end{pmatrix},\ v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \\ 0 \end{pmatrix},\ v_5 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix},\ v_6 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \end{pmatrix}$$

alors $(v_1, v_2, v_3, v_4, v_5)$ est une base d'un réseau Γ, $v_6 = 2v_5 - v_4 - v_3 - v_2 - v_1 \in \Gamma$ et $(v_1, v_2, v_3, v_4, v_6)$ réalise les minima successifs sans être une base.

– Quelques problèmes algorithmiques:

  * étant donné une famille génératrice, trouver une base (OK en temps polynomial); soit A la matrice des vecteurs générateurs dans la base canonique, par opérations élémentaires sur les colonnes, il existe $U \in GL_n(\mathbb{Z})$ telle que $B = AU$ où B est sous une forme normale de Hermite, i.e. $B = (0\ C)$ où C est triangulaire supérieure, $c_{i,i} > 0$ et pour tout $j > i$, on a $0 \leq c_{i,j} < c_{i,i}$;
  * décider si un vecteur est un point du réseau (OK en temps polynomial: méthode du pivot);
  * trouver un vecteur de norme minimal: on conjecture que c'est NP-dur;
  * étant donné un point de l'espace, trouver un point du réseau le plus proche
  * étant donnée une base d'un réseau Γ, trouver une base la meilleure possible au sens suivants:
    · les vecteurs de base le plus courts possibles: réduction de Minkowski
    · la famille de vecteurs de base la plus orthogonale possible: réduction de Korkine et Zolotarev
    · réduction de Lenstra, Lenstra et Lovasz: étant donnée une base $(e_1, \cdots, e_n)$ on notera $(e_1^*, \cdots, e_n^*)$ la base obtenur par le procédé d'orthonormalisation de Gramm-Schmidt

$$e_i^* = e_i - \sum_{j=1}^{i-1} \mu_{i,j} e_j^*$$

où $\mu_{i,j} = \frac{<e_i|e_j^*>}{||b_j^*||^2}$. La base (e_i) est dite LLL-réduite si $|\mu_{i,j}| \leq 1/2$ et que

$$||e_i^* + \mu_{i,i-1}e_{i-1}^*||^2 \geq \frac{3}{4}||e_{i-1}^*||^2$$

On dispose alors d'un algorithme dit LLL qui permet de calculer une base LLL-réduite à partir d'une base quelconque: cependant si j'ai bien compris la complexité de cet algorithme est mal comprise.

En dimension 2 c'est très simple: on opère des translations successives

– en applications:

* si $p \equiv 1 \mod 4$, p premier, alors p est somme de deux carrés.
  Indication: (-1) étant un carré modulo p, soit $u \in \mathbb{Z}$ tel que $u^2+1 \equiv 0 \mod p$ et soit $\Gamma = \{(a,b) \in \mathbb{Z}^2 \ / \ a \equiv ub \mod p\}$. Soit $\psi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}/p\mathbb{Z}$ défini par $\psi(a,b) = \overline{a-ub}$. Montrez que Γ est un réseau de mesure p et utilisez le point (d) (iv) de l'exercice précédent.
* tout nombre premier p est somme de quatre carrés.
  Indication: montrez l'existence d'un couple $(u,v) \in \mathbb{Z}^2$ tel que $u^2+v^2+1 \equiv 0 \mod p$. On fixe un tel couple et soit $\Gamma = \{(a,b,c,d) \in \mathbb{Z}^4 \ / \ ua+vb \equiv c \mod p \text{ et } ub-va \equiv d \mod p\}$. Soit $\psi : \mathbb{Z}^4 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2$ défini par $\psi(a,b,c,d) = (\overline{c-ua-vb}, \overline{d+va-ub})$. Montrez que Γ est un réseau de $\mathbb{R}^4$ de mesure p^2 et utilisez le point (d) (iv) de l'exercice précédent.
* Le problème d'empilement régulier de sphères est de déterminer quelle est la proportion maximale de l'espace que peut occuper une famille de boules, mutuellement disjointes et de même rayon, centrées en les points d'un réseau. Etant donné un réseau Γ de volume $\mu(\Gamma)$ dont la norme minimale d'un vecteur non nul et $\lambda_1(\Gamma)$, la constant d'Hermite est $\gamma(\Gamma) := \frac{\lambda_1(\Gamma)^2}{\mu(\Gamma)^{2/n}}$. Il est aisé de constater que la densité maximale des boules centrées aux points du réseau est proportionnelle à $\gamma(\Gamma)$, le coefficient de proportionnalité étant $\frac{B_n}{2^n}$ où B_n est le volume de la boule unité.
  Hermite a montré que sur l'ensemble des réseaux de dimension n, $\gamma(\Gamma)$ est borné et atteint son maximum noté γ_n. Celui-ci n'est calculé que pour $n \leq 8$, en particulier $\gamma_2 = \frac{2}{\sqrt{3}}$ et correspond au réseau hexagonal. Le théorème de Minkowski donne $\gamma_n < n$).
  En ce qui concerne les empilements non nécessairement donnés par des réseaux, Rogers (1958), a donné un majorant de la densité: σ_n est le rapport du volume occupé par les sphères centrées en les sommets du simplexe Δ_n régulier d'arête 1, de rayon 1/2, à celui de Δ_n (à nouveau le calcul de σ_n est inextricable pour $n > 4$, le cas $n = 4$ étant déjà difficile). Pour $n = 2$ on vérifie immédiatement que ce maximum est atteint (réseau hexagonal, cf. ci-dessus). Pour $n = 3$ Kepler (1610) conjecture que la densité maximale est $\frac{\pi}{3\sqrt{2}}$, c'est à dire celle du réseau cubique à faces centrées: conjecture finalement prouvée en 1998 par Thomas Hales. Celui-ci est définie par $\Lambda = \{(x,y,z) \in \mathbb{Z}^3 \ / \ 2|x+y+z\}$ une base étant donnée par $(1,1,0)$, $(1,0,1)$ et $(0,1,1)$.
* le kissing number et les applications aux codes

- un troisième paragraphe sur les classes d'équivalences (en euclidien car sinon il n'y a pas grand chose d'intéressant à dire: $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$) et les applications:

  – deux réseaux Λ, Λ' sont dits équivalents s'il existe une similitude g telle que $g(\Lambda) = \Lambda'$. En dimension 2 tout réseau (w_1, w_2) est équivalent à un réseau de la forme $(1, \tau)$ où $\tau = w_1/w_2 \in \mathcal{H}/SL_2(\mathbb{Z})$ où $\mathcal{H}$ est le demi-plan de Poincaré: si (w_1', w_2') est une autre base, alors il existe $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tel que $w_1' = aw_1 + bw_2$ et $w_2' = cw_1 + dw_2$, alors $\tau' = w_1'/w_2' = A.\tau := \frac{a\tau+b}{c\tau+d}$.
  – le réseau dual, réseaux unimodulaires...
    * $L^* = \{v \in V \ / \ < v, \gamma > \in \mathbb{Z} > \in \mathbb{Z}\}$ est un réseau, sa matrice génératrice est ${}^tM^{-1}$.
    * Si Λ est un faisceau entier (i.e. la matrice de Gramm associée est à coefficients entiers) si et seulement si $\Lambda \subset \Lambda^*$. Le groupe quotient Λ^*/Λ est de cardinal $\det \Lambda$ et $\Lambda^* \subset \frac{1}{\det \Lambda}\Lambda$. Le réseau est dit autodual ou unimodulaire si $\det \Lambda = 1$ i.e. $\Lambda^* = \Lambda$.
    * si la diagonale de la matrice de Gramm est paire alors $< x, x > \in 2\mathbb{Z}$ pour tout x, le réseau est dit de type II, sinon il est dit de type I.
  – Étant donné un réseau de base $(a_1, \cdots, a_n)$; on l'envoie sur $\mathbb{Z}^n \subset \mathbb{R}^n$ muni de sa base canonique, par l'application linéaire $a_i \mapsto e_i$. On transforme du même coup le produit scalaire de l'espace euclidien en un forme quadratique de matrice $A = ((a_i|a_j))_{1 \leq i,j \leq n} = {}^tBB$. Réciproquement, toute forme quadratique définie positive A provient d'un réseau, défini à une transformation orthogonale près: on l'obtient en "redressant" l'ellipsoïde de la forme quadratique en une sphère. On a donc définit une correspondance bijective entre réseaux à isométries près (si on change la base orthonormée (e_i), O étant la matrice de passage, et si on change la base (a_i) par $(b_i) = P(a_i)$ avec $P \in GL_n(\mathbb{Z})$ alors $B' = OBP$ et $A' = {}^tPAP$) et classes de formes quadratiques définies positives.

Soit $q(x,y) = ax^2 + bxy + cy^2$ avec $a, b, c \in \mathbb{R}$, une forme quadratique définie, i.e. $\Delta = b^2 - 4ac < 0$. On dira que q est **réduite** si et seulement si

$$-a < b \leq a < c \text{ ou } 0 \leq b \leq a = c$$

Deux formes quadratique q, q' seront dites géométriquement équivalentes s'il existe $A \in SL_2(\mathbb{Z})$ telle que $Q' = {}^tAQA$.

- ∗ toute forme quadratique binaire définie est géométriquement équivalente à une forme réduite.
- ∗ Deux formes réduites sont géométriquement équivalentes si et seulement si elles sont égales.
- ∗ q sera dite entière si $a, b, c \in \mathbb{Z}$. Il n'y a qu'un nombre fini de classes d'équivalence géométrique de forme quadratique binaire définie entière de discriminant donné.
- ∗ Deux formes entières sont dites arithmétiquement équivalentes si elles représentent les mêmes nombres avec la même multiplicité. Montrez que les deux notions d'équivalence sont identiques.

– Soit E un réseau entier unimodulaire; on réduit modulo 2 de sorte que la forme quadratique est linéaire de sorte qu'il existe $\bar{u} \in \bar{\Gamma}$ tel que $< \bar{u}, \bar{x} >=< \bar{x}, \bar{x} >$. On remonte sur E de sorte qu'il existe $u \in E$ tel que $< u, x > \equiv < x, x > \mod 2$. Le nombre $< u, u >$ est alors défini modulo 8: on le note $\sigma(E)$.
- Dans le cas de la signature $(s,t) \neq (0,0)$, le réseau est de type I avec $\sigma(E) \equiv s - t \mod 8$.
- Dans le plan hyperbolique, on est de type II et $\sigma(E) = 0$.

– On note $S = \bigcup_n S_n$ la réunion de l'ensemble des réseaux unimodulaires de $\mathbb{R}^n$. On dit que $E, E' \in S$ sont stablement isomorphes s'il existe $F \in S$ tel que $E \oplus F \simeq E' \oplus F$ et soit $K_+(S)$ le quotient de S par cette relation puis $K(S)$ le groupe associé au monoide $K_+(S)$. On a alors les résultats suivants:

- ∗ $K(S)$ est un groupe abélien libre de base I_+, I_-;
- ∗ le rang r et $\tau = r - s$ définit un isomorphisme de $K(S)$ sur le sous-groupe de $\mathbb{Z}^2$ formé des éléments (a,b) tels que $a - b \equiv 0 \mod 2$;
- ∗ on a $\sigma(E) \equiv \tau(E) \mod 8$ et si E est de type II alors $\tau(E) \equiv 0 \mod 8$ ainsi que $r(E)$;
- ∗ dans le cas indéfini: E et E' sont isomorphes si et seulement si ils ont même rang, indice et type;
- ∗ dans le cas défini: pour tout n, S_n ne contient qu'un nombre fini de classes. Si on note C_n, l'ensemble de ces classes de type II et g_E le cardinal du groupe des automorphismes de $E \in C_n$, alors

$$M = \sum_{E \in C_n} \frac{1}{g_E} = 2^{1-8k} \frac{B_{2k}}{(4k)!} \prod_{j=1}^{4k-1} B_j$$

pour $n = 8k$ et où les B_k sont les nombres de Bernouilli

• des thèmes plus difficiles:

– groupe de paveurs: soit E un plan euclidien et P un compact connexe de E d'intérieur $\dot{P}$ non vide. Un groupe G sera dit un groupe de paveur de P si G est un sous-groupe du groupe des isométries directes $Is^+(E)$ de E vérifiant les deux propriétés suivantes:
(i) GP1: $\bigcup_{g \in G} g(P) = E$
(ii) GP2: $g(\dot{P}) \cap h(\dot{P}) \neq \emptyset \Rightarrow g(P) = h(P)$.
Soit $\Gamma := G \cap T(E)$. Soit alors $\vec{u}$ un vecteur de norme minimale (non nulle) tel qu'il existe une translation de Γ de vecteur $\vec{u}$ et soit $\vec{v} \notin \mathbb{R}\vec{u}$ de plus petite norme tel qu'il existe une translation de Γ de vecteur $\vec{v}$. Pour un point $e \in E$ quelconque on considère le parallélogramme $Q = \{e + t\vec{u} + s\vec{v} : \ t, s \in [0,1]\}$. En utilisant le fait que les $g(Q)$ pour $g \in \Gamma$, remplissent E, on a alors $\Gamma = \mathbb{Z}\vec{u} \oplus \mathbb{Z}\vec{v}$.

– anneaux d'entiers: considérons l'application

$$S : K \longrightarrow \mathbb{R}^s \times \mathbb{C}^t : x \mapsto (\sigma_i(x), i = 1, \cdots, s+t)$$

où $\sigma_1, \cdots, \sigma_s$ désigne les plongements complexes et $(\sigma_{s+1}, \bar{\sigma}_{s+1}, \cdots, \sigma_{s+t}, \bar{\sigma}_{s+t})$ désigne les plongements complexes. S est un homomorphisme de groupes injectifs appelé plongement canonique de K dans

$\mathbb{R}^s \times \mathbb{C}^t \simeq \mathbb{R}^n$. L'image de l'anneau des entiers $\mathcal{O}_K$ est alors un réseau de $\mathbb{R}^n$ de covolume $2^{-t}|D_K|^{1/2}$ où D_K est le discriminant de K, i.e. le déterminant de la matrice des $(\sigma_i(\omega_j)$ où $(\omega_1, \cdots, \omega_n)$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$. Ainsi pour tout idéal $\mathbf{a}$ de $\mathcal{O}_K$, $S(\mathbf{a})$ est donc un réseau de covolume $2^{-t}|D_K|^{1/2}N(\mathbf{a})$. Pour tout $c > 0$, la partie $B_c = \{(y_1, \cdots, y_s, z_{s+1}, \cdots, z_{s+t}),\ \sum_i |y_i| + 2\sum_j |z_j| \leq c\}$ est convexe symétrique par rapport à l'origine de volume $2^s(\frac{\pi}{2})^t\frac{c^n}{n!}$. Le théorème de Minskowski implique alors que si $c^n > (\frac{4}{\pi})^t n!|D_K|^{1/2}N(\mathbf{a})$, il existe un élément α non nul de $\mathbf{a}$ tel que $S(\alpha) \in B_c$. D'après l'inégalité des moyennes arithmétique et géométrique, un tel α vérifie

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_i |\sigma_i(\alpha)| \prod_j |\sigma_j(\alpha)|^2 \leq [\frac{1}{n}(\sum_i |\sigma_i(\alpha)| + 2\sum_j |\sigma_j(\alpha)|)]^n \leq \frac{c^n}{n^n}$$

Ainsi tout idéal entier non nul $\mathbf{a}$ contient un élément non nul de norme majorée en valeur absolue par $(\frac{4}{\pi})^t\frac{n!}{n^n}|D_K|^{1/2}N(\mathbf{a}) =: M_K N(\mathbf{a})$, où M_K est la constante de Minskowski. Ainsi si C est un élément du groupe de classe d'idéaux Cl_K, $\mathbf{a}$ un idéal entier représentant la classe inverse C^{-1} dans J_K (le groupe des idéaux fractionnaires) et α un élément non nul de $\mathbf{a}$ de norme $\leq M_K N(\mathbf{a})$. Alors l'idéal $\alpha\mathbf{a}^{-1}$ est entier et représente C dans J_K; sa norme qui vaut $|N_{K/\mathbb{Q}}(\alpha)|(N(\mathbf{a}))^{-1}$ est majorée par M_K. Ainsi on a montré que *tout élément de Cl_K admet parmi ses représentants dans J_K un idéal entier de norme inférieure ou égale à M_K.* On utilise ce résultat pour majorer le nombre de classe h_K: on calcule M_K et on regarde les idéaux de norme inférieur à M_K et on essaie de déterminer s'ils sont principaux ainsi que leurs relations.

Le groupe des unités de $\mathcal{O}_K$ est le produit direct du groupe fini μ_K formé des racines de l'unité dans K et d'un groupe libre de rang $s + t - 1$. En particulier pour K quadratique réel, il existe une unité u de $\mathcal{O}_K$ telle que $U_K = \{\pm 1\} \times u^{\mathbb{Z}}$. La détermination d'une telle unité, dite fondamentale, se ramène à la résolution des classiques équations de Pell-Fermat

– fonctions elliptiques: ce sont des fonctions méromorphes Γ-périodique. On considère la fonction $\mathfrak{P}$ de Weierstrass:

$$\mathfrak{P}_\Lambda(x) = x^{-2} + \sum_{\omega\in\Lambda-0} [(x-\omega)^{-2} - \omega^{-2}]$$

qui converge uniformément sur tout compact de $\mathbb{C}$ ne contenant pas les points du réseau Λ. En considérant $\mathfrak{P}'(x) = -2\sum_{x\in\Gamma}(x-\omega)^{-3}$, on obtient que $\mathfrak{P}$ est elliptique par rapport à Λ puis que l'ensemble des fonctions elliptiques par rapport à Λ est un corps sur $\mathbb{C}$ qui est engendré par $\mathfrak{P}$ et $\mathfrak{P}'$. (on est alors amené aux courbes elliptiques...)

– Les séries théta: ce sont des fonctions **entières** pour le réseau de périodes $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, où τ désigne un nombre complexe du demi-plan de Poincaré. Les propriétés de "périodicité" habituelles sont:

$$\begin{cases} \Theta(z+1) = \Theta(z) \\ \Theta(z+\tau) = F(z)\Theta(z) \end{cases}$$

où $F(z)$ est un facteur à déterminer vérifiant en particulier $F(z+1) = F(z)$. Le choix habituel de F est

$$F(z) = \frac{1}{ce^{2i\pi z}},\ c \in \mathbb{C}^\times$$

Puisque Θ est holomorphe de période 1, elle peut être développée en série de Fourier

$$\Theta(z) = \sum_{-\infty}^{+\infty} a_n e^{2i\pi nz}$$

où les a_n sont les coefficients de Fourier de Θ. la formule sommatoire de Poisson donne par prolongement analytique l'équation fonctionnelle

$$\theta(-\frac{1}{z}) = (-iz)^{1/2}\theta(z)$$

où $(-iz)^{1/2}$ est donné par la branche de la fonction sur $\mathcal{H}$ qui envoie iy sur $\sqrt{y}$. Cette relation jointe à la relation évidente $\theta(z+1) = \theta(z)$ donne une règle de transformation pour $f(\gamma z)$ pour tout $\gamma \in PSL_2(\mathbb{Z})$

agissant sur $\mathcal{H}$ par homographies. De même pour tout $k \geq 1$, $\theta(2z)^k$ satisfait à des formules de transformation analogues. Par ailleurs les égalités

$$\theta(2z)k = \sum_{n\geq 0} r_k(n)e^{nz}$$

où $r_k(n)$ désigne le nombre de représentations de n comme somme de k carrés d'entiers, justifient à elles seules, l'acharnement qu'ont subies ces séries. En particulier, on peut montrer les identités suivantes:

$$\begin{aligned} r_2(n) &= 4\sum_{d|n}\chi_4(d) \\ r_4(n) &= 8(3+(-1)^n)\sum_{d|n} d \\ r_6(n) &= 16\sum_{d|n} d^2\chi_4(\tfrac{n}{d}) - 4\sum_{d|n} d^2\chi_4(d) \end{aligned}$$

avec $\chi_4(n) = d_1(n) - d_3(n)$ où $d_1(m)$ (resp. $d_3(m)$) est le nombre de diviseur $d \equiv 1 \mod 4$ (resp. $d \equiv 3 \mod 4$) de n.

La théorie des formes modulaires permet d'expliquer la forme générale de ces formules, pourquoi il n'y a pas de formules élémentaires du même type pour k plus grand, et de donner une relation asymptotique sur $r_k(n) \sim n^{k-1}$ pour $k \geq 5$. En outre la série théta pour le réseau $\mathbb{Z}^n$ peut servir à prouver l'équation fonctionnelle de la fonction zéta de Riemann: pour $\mathrm{Re}(s) > 1$, $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. Soit aussi pour $\mathrm{Re}(s) > 0$, $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$ la fonction Γ usuelle. On pose

$$\Lambda(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$$

En écrivant $\Lambda(2s) = \int_0^\infty \left(\sum_{n=1}^{\infty} e^{-\pi n^2 t}\right) t^{s-1}dt$ on peut montrer que $\Lambda(s) + \frac{1}{s} + \frac{1}{s-1}$ peut-être prolongée holomorphiquement à tout le plan complexe et que l'on a l'équation fonctionnelle

$$\Lambda(s) = \Lambda(1-s)$$

– groupes de Coxeter, diagramme de Dynkin, groupes de Mathieu, le monstre...

Développements: on a l'embarras du choix

- théorème de la base adaptée d'un sous-réseau d'un réseau;
- caractérisation des sous-groupes discrets de $\mathbb{R}^n$ et approximations des irrationnels par des rationnels;
- théorème de Minkowski et application au théorème des 2 carrés et des 4 carrés;
- théorèmes de Hadamard et Hermite sur la comparaison entre le volume et la maille d'un réseau
- classe de similitudes de réseau, demi-plan de Poincaré et empilement de boules en dimension 2;
- réseaux unimodulaires de type II: $n \equiv 0 \mod 8$;
- quelques questions et réponses algorithmiques

Questions

- Montrez que le groupe des automorphismes orthogonaux d'un réseau est fini. Trouvez celui de $\mathbb{Z}^n$.
- Montrez que les notions d'équivalence arithmétique et géométrique sur les formes quadratiques entières sont identiques.
- Résolvez le problème des empilements de sphère (version réseau) en dimension 2.
- Soit $\Lambda = \{(x,y,z) \in \mathbb{Z}^3 \ / \ 2|x+y+z\}$, montrez que $(1,1,0)$, $(1,0,1)$ et $(0,1,1)$ définissent une base et donnez une base adaptée à l'inclusion $\Gamma \subset \mathbb{Z}^3$.

- Etant donné une famille génératrice, expliquez comment trouver une base.
- Expliquez comment décider si un vecteur est un point d'un réseau donné par une base.
- Montrez que les classes de similitude de réseau sont données par $\mathcal{H}/SL_2(\mathbb{Z})$.

Exercices corrigés

Exercice 1. *Montrez que les notions d'équivalence arithmétique et géométrique sur les formes quadratiques entières sont identiques.*

Preuve : On note $\sqrt{Q}$ la racine carrée symétrique positive de la matrice Q de la forme quadratique. L'ensemble des n représenté est alors $\Gamma = \sqrt{Q}\mathbb{Z}^2$. Si Q et Q' sont géométriquement équivalente alors $\Lambda' = g(\Lambda)$ pour $g \in SL_2(\mathbb{Z})$ et donc Q et Q' sont arithmétiquement équivalentes.

Réciproquement, $\Gamma := \sqrt{Q}\mathbb{Z}^2$ et $\Gamma' = \sqrt{Q'}\mathbb{Z}^2$ produisent les mêmes longueur avec les mêmes multiplicités. En particulier ils ont le même volume (regarder le nombre de points dans les disques centrés en l'origine). Soit alors un v, v' des vecteurs de norme minimale pour respectivement Γ et Γ', et soit une rotation g qui envoie v' sur v. Soit alors w, w' des vecteurs de respectivement $\Gamma, g(\Gamma')$ non colinéaire à v, de norme minimale: w et w' sont donc de même norme et le quotient du volume de Γ par celui de Γ' est égale à $\frac{\sin(\widehat{v,w})}{\sin(\widehat{v,w'})} = 1$. Ainsi soit $w' = w$ soit w' est l'image de w par la réflexion par rapport à la droite orthogonale à v, d'où le résultat.