Exercise Sheet, Geometry of numbers and lattices, Fall 2024

Notations and assumptions. Unless stated otherwise, all measures on a topological space are regular Borel Radon measures. 'lcsc' stands for locally compact second countable Hausdorff. A *topological group* G is a group endowed with a topology for which the operations $G \times G \to G, (g_1, g_2) \mapsto g_1 g_2$ and $G \to G, g \mapsto g^{-1}$ are both continuous.

1. Let $L \subset \mathbb{R}^n$. Prove that the following are equivalent.

- L is a lattice.
- L is a discrete additive subgroup and contains n vectors which are linearly independent over $\mathbb{R}$.
- L is a discrete additive subgroup and there is a compact $K \subset \mathbb{R}^n$ such that $\mathbb{R}^n = L + K$.
- L is a discrete additive subgroup and there is a nonzero finite measure on the quotient group $\mathbf{T} = \mathbb{R}^n/L$ which is *invariant under group translations*, i.e., satisfies $\mu(x + A) = \mu(A)$ for any Borel $A \subset \mathbf{T}$ and any $x \in \mathbf{T}$. Here $+$ denotes the group operation on $\mathbf{T}$.

2. Suppose $n \geq 2$, $L \subset \mathbb{R}^n$ is a lattice and $H \subset \mathbb{R}^n$ is a discrete subgroup. Prove:

- If $H \subset L$ and $[L : H] < \infty$ then H is a lattice, and $\mathrm{covol}(H) = [L : H] \cdot \mathrm{covol}(L)$.
- If $L \subset H$ then H is a lattice and $[H : L] < \infty$.
- Let p be a prime. What is the number $N_{p,n}$ of different groups H containing L as a subgroup of index p, and what is the number $N'_{p,n}$ of different groups H contained in L as a subgroup of index p? If $L = g\mathbb{Z}^n$ for $g \in \mathrm{GL}_n(\mathbb{R})$, write all these groups in the form $H = gM_i\mathbb{Z}^n$ and $H = gM'_j\mathbb{Z}^n$, for matrices M_i, M'_j, where i ranges over $1, \ldots, N_{p,n}$ and j ranges over $1, \ldots, N'_{p,n}$.

3. An lcsc topological group G is called *unimodular* there is a measure on G which is both left-invariant and right-invariant.

- Prove that if there is a discrete subgroup $\Gamma \subset G$ such that there is a finite G-invariant measure on G/Γ, then G is unimodular.
- Let $\mathrm{Aff}(\mathbb{R})$ denote the group of invertible affine transformations on the real line, i.e., maps of the form

  $$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = ax + b, \qquad \text{where } a \in \mathbb{R} \smallsetminus \{0\},\ b \in \mathbb{R}.$$

  Show that $\mathrm{Aff}(\mathbb{R})$ is isomorphic to the group

  $$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R} \smallsetminus \{0\}, b \in \mathbb{R} \right\},$$

with matrix multiplication.

- Show that there is no measure on $\mathrm{Aff}(\mathbb{R})$ which is both left-invariant and right-invariant.
- Show that $\mathrm{Aff}(\mathbb{R})$ acts transitively on $\mathbb{R}$ but there is no $\mathrm{Aff}(\mathbb{R})$-invariant Radon measure on $\mathbb{R}$.

4. Suppose $L \subset \mathbb{R}^3$ is a lattice, and $v_1, v_2, v_3 \in L$ are chosen by the 'greedy algorithm'. Namely, for $i = 1, 2, 3$, v_i is the shortest (w.r.t. the Euclidean norm) vector in $L \smallsetminus \mathrm{span}_{\mathbb{R}}(v_j : j < i)$. Prove that $L = \mathrm{span}_{\mathbb{Z}}(v_1, v_2, v_3)$.

5. Let $\| \cdot \|$ be a norm on $\mathbb{R}^n$, let $L \subset \mathbb{R}^n$ be a lattice, let $B(0,1)$ be the unit ball in $\mathbb{R}^n$ with respect to $\| \cdot |$, and let $\lambda_i(L)$ denote the Minkowski successive minima with respect to $\| \cdot \|$. Prove that

$$\frac{2^n}{n!} \frac{1}{\mathrm{Vol}(B(0,1))} \leq \frac{\lambda_1(L) \cdots \lambda_n(L)}{\mathrm{covol}(L)}$$

(this is one of the two inequalities in Minkowski's second theorem).

6. Let $L \subset \mathbb{R}^n$ be a lattice. Define the following quantities:

- $\alpha_i(L)$ is the minimal volume of a fundamental domain of $\mathrm{span}_{\mathbb{R}}(L')/L'$, where $L' \subset L$ is an additive subgroup of rank i.
- $\beta_1(L)$ is the Euclidean length of the shortest nonzero vector vector in L, and supposing $\beta_1(L) = \|v_1\|, \ldots, \beta_k(L) = \|v_k\|$ have been chosen, with $v_1, \ldots, v_k$ a primitive k-tuple in L, v_{k+1} is the shortest vector for which $v_1, \ldots, v_{k+1}$ is a primitive $k+1$-tuple in L, and $\beta_{k+1}(L) = \|v_{k+1}\|$ (with some tie-breaking rule).
- $\kappa_i(L) = \|u_i\|$ where $u_1, \ldots, u_n$ is the basis of L obtained by the Korkine-Zolotarev reduction scheme (with some tie-breaking rule).

If A and B are quantities depending on an index i and a lattice $L \subset \mathbb{R}^n$, write $A \asymp B$ if there is a constant C, independent of i and L but depending on n, such that $\frac{A}{C} \leq B \leq CA$. Prove that

$$\beta_i(L) \asymp \kappa_i(L) \asymp \lambda_i(L) \qquad \text{and} \qquad \alpha_i(L) \asymp \lambda_1(L) \cdots \lambda_i(L).$$

7. Let $L \subset \mathbb{R}^n$ be a lattice and let $x_1, \ldots, x_{2^n-1}$ be the non-identity elements in the quotient group $\frac{1}{2}L/L$. Let $V = \mathrm{Vor}(L)$ be the Voronoi cell of L. Prove that each x_i has a representative in the boundary ∂V, and no x_i has a representative in the interior V°. Prove that V has at most $2(2^n - 1)$ boundary faces, and that this bound is sharp. Prove that the map

$$\mathrm{Cl}(\mathbb{R}^d) \to \mathrm{Cl}(\mathbb{R}^d), \quad L \mapsto \mathrm{Vor}(L)$$

is continuous with respect the Chabauty-Fell metric.

8. Prove that if $G_1, G_2, \ldots$ is a sequence of closed subgroups of $\mathbb{R}^n$ and $G_i \to X_\infty$, with respect to the Chabauty-Fell metric on $\mathrm{Cl}(\mathbb{R}^n)$, then X_∞ is also a closed subgroup.

9. Prove that the topology on $\mathscr{X}_n$ obtained by restricting the Chabauty-Fell metric from $\mathrm{Cl}(\mathbb{R}^n)$, coincides with the quotient topology on $\mathscr{X}_n = \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$, where the topology on $\mathrm{SL}_n(\mathbb{R})$ is the one induced from its inclusion in the matrices $M_n(\mathbb{R})$ with their usual topology as a space isomorphic to $\mathbb{R}^{n^2}$.

10. In this exercise and the next one, lengths of vectors are defined using the Euclidean norm. A lattice $L \subset \mathbb{R}^n$ is called *well-rounded* if its shortest nonzero vectors span $\mathbb{R}^n$. Let $\mathcal{O} \stackrel{\mathrm{def}}{=} \mathrm{SO}_n(\mathbb{R})$ and let $\mathcal{S}_n = \mathcal{O}\backslash \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$ denote the space of *shapes of lattices*. An element of $\mathcal{S}_n$ is an orbit of a lattice in $\mathscr{X}_n$ under $\mathcal{O}$. We denote the orbit $\mathcal{O}L$ by $[L]$. We define

$$d : \mathcal{S}_n \times \mathcal{S}_n \to [0,\infty), \ \ d\left([L_1],[L_2]\right) \stackrel{\mathrm{def}}{=} \inf\left\{d_{CF}(O_1L_1, O_2L_2) : O_1, O_2 \in \mathcal{O}\right\},$$

where d_{CF} denotes the Chabauty-Fell metric.

(1) Show that d is a metric, the inf in the definition is actually a minimum, and can be written as

$$d\left([L_1],[L_2]\right) = \min\left\{d_{CF}(L_1, OL_2) : O \in \mathcal{O}\right\}.$$

(2) Show that the functions $[L] \mapsto \lambda_i(L)$ are well-defined on $\mathcal{S}_n$, and the set $\mathcal{WR}_n \stackrel{\mathrm{def}}{=} \{[L] \in \mathcal{S}_n : L \text{ is well-rounded}\}$ is well-defined.

(3) Show that $\mathcal{WR}_n$ is compact in $\mathcal{S}_n$.

(4) Define a map

$$\mathcal{S}_n \to \mathcal{S}_n, \qquad [L] \mapsto [L']$$

as follows. Given $[L] \in \mathcal{S}_n$, let $v_1, \ldots, v_n$ be vectors in L realizing the successive minima (that is $\lambda_i(L) = \|v_i\|$ for $i = 1, \ldots, n$). Let $\tilde{v}_1, \ldots, \tilde{v}_n$ be the orthogonal basis obtained by the Gram-Schmidt procedure and let $\bar{T} : \mathbb{R}^n \to \mathbb{R}^n$ be the linear transformation which sends $\tilde{v}_i$ to $\frac{1}{\lambda_i(L)}\tilde{v}_i$ for $i = 1, \ldots, n$. Finally let $L' \stackrel{\mathrm{def}}{=} c\bar{T}(L)$, where c is the unique positive constant for which $\mathrm{covol}(L') = 1$. Show that this map is well-defined (independent of the choice of the representative L and of the vectors $v_1, \ldots, v_n$) and continuous.

(5) Show that $\mathcal{WR}_n$ is the set of fixed points for T.

(6) Prove or disprove: $\lambda_1([L]) \le \lambda_1([L'])$.

(7) Prove or disprove: if $L_1, L_2 \in \mathscr{X}_n$ are not well-rounded and $d([L_1],[L_2]) \in (0,1)$, then $d([L_1'],[L_2']) < d([L_1],[L_2])$.

11. Define the *covering radius* of L to be

$$\mathrm{covrad}(L) \stackrel{\mathrm{def}}{=} \inf\{r > 0 : L + B(0,r) = \mathbb{R}^n\},$$

where balls are taken with respect to the Euclidean norm.

- Show that for all n, $\mathbb{Z}^n$ is well-rounded and satisfies
$$\mathrm{covol}(\mathbb{Z}^n) = 1, \quad \mathrm{covrad}(\mathbb{Z}^n) = \frac{\sqrt{n}}{2}.$$
- Show that for $n = 2, 3$, if L is well-rounded and satisfies $\mathrm{covol}(L) = 1$ then
$$\mathrm{covrad}(L) \le \frac{\sqrt{n}}{2}, \tag{0.1}$$
and this bound is sharp.
- For $i = 1, 2$ let $L_i \subset \mathbb{R}^{n_i}$ be a well-rounded lattice with $\mathrm{covol}(L_i) = 1$. Let $n = n_1 + n_2$ and let $\mathbf{0}_k$ denote the zero vector in $\mathbb{R}^k$. For $I = 1, 2$, we consider L_i as a discrete subgroup of $\mathbb{R}^n$ via the natural isomorphisms
$$\mathbb{R}^{n_1} \cong \mathbb{R}^{n_1} \oplus \{\mathbf{0}_{n_2}\} \quad \text{and} \quad \mathbb{R}^{n_2} \cong \{\mathbf{0}_{n_1}\} \oplus \mathbb{R}^{n_2}.$$
Show that there is a unique choice of positive α_1, α_2 such that the lattice
$$\alpha_1 L_1 \oplus \alpha_2 L_2 \stackrel{\mathrm{def}}{=} \{\alpha_1 \ell_1 + \alpha_2 \ell_2 : \ell_1 \in L_1, \ell_2 \in L_2\}$$
has covolume one and is well-rounded. Give a formula for $\mathrm{covrad}(\alpha_1 L_1 \oplus \alpha_2 L_2)$ in terms of α_i and $\mathrm{covrad}(L_i)$.
- Show that for all n sufficiently large there is a lattice $L \subset \mathbb{R}^n$ of the form $\alpha_1 L_1 \oplus \alpha_2 L_2$ as above, which does not satisfy the bound (0.1).

12. Show that for every $n \in \mathbb{N}$, every $\varepsilon > 0$ and every $c > 1$, there is $C > 0$ so that the following holds. Let $L \in K_\varepsilon$, where K_ε is the subset of $\mathscr{X}_n$ consisting of lattices whose shortest nonzero vector has length at least ε (with respect to the Euclidean norm). Let μ be a Radon measure on $\mathbb{R}^n$ which is invariant under translation by any element of L, and such that its restriction to a fundamental domain for L is a probability measure. Let B be a centrally symmetric convex set such that there is $r \ge 1$ for which $B_r \subset B \subset B_{cr}$, where B_ρ is the Euclidean ball around the origin of radius ρ. Then

$$|\mu(B) - \mathrm{Vol}(B)| < C\mathrm{Vol}(B)^{1-\frac{1}{n}}.$$

Give examples showing that in this statement, the dependence of C on ε and c cannot be avoided.

Deduce that for any lattice $L \subset \mathbb{R}_n$ and any $K \subset \mathbb{R}^n$ for which (K, L) is a packing,

$$\frac{\mathrm{Vol}(K)}{\mathrm{covol}(L)} = \lim_{\rho \to \infty} \frac{\mathrm{Vol}\left(B_\rho \cap \bigcup_{\ell \in L}(K + \ell)\right)}{\mathrm{Vol}(B_\rho)}.$$

13. Prove that for any $L \in \mathscr{X}_n$, any $x \in \mathbb{R}^n$, and any $B \subset \mathbb{R}^n$ such that B is bounded, $\mathrm{Vol}(B) > 0$ and $\mathrm{Vol}(\partial B) = 0$, we have

$$\lim_{t \to \infty} \frac{|(L + x) \cap tB|}{\mathrm{Vol}(tB)} = 1.$$

Here tB is defined as in Question 12.

14. Let $\langle \cdot, \cdot \rangle$ denote the standard inner product, and let λ_i be the successive minima defined using the Euclidean norm. Given a lattice $L \subset \mathbb{R}^n$, let

$$L^* \stackrel{\mathrm{def}}{=} \{x \in \mathbb{R}^n : \forall u \in L, \langle x, u \rangle \in \mathbb{Z}\}$$

(the dual lattice). Show that $\mathrm{covol}(L) = 1/\mathrm{covol}(L^*)$. Deduce that $(L^*)^* = L$ and that the mapping $\Psi(L) = L^*$ restricts to a mapping $\Psi : \mathscr{X}_n \to \mathscr{X}_n$. Show that $\Psi_* m_{\mathscr{X}_n} = m_{\mathscr{X}_n}$. A lattice L is called *self-dual* if $L = L^*$. Show that for any orthogonal matrix $O \in \mathrm{SL}_n(\mathbb{R})$, the lattice $O\mathbb{Z}^n$ is self-dual. Show that if $L \in \mathscr{X}_n$ and $\langle x, x \rangle$ is an even integer for any $x \in L$, then L is self-dual. Show that for any $i \in \{1, \ldots, n\}$ and any $L \in \mathscr{X}_n$ we have

$$\lambda_i(L)\lambda_{n+1-i}(L^*) \geq 1.$$

15. Fix $n \geq 2$ an integer. Let ν and ν_j be Borel probability measures on $\mathscr{X}_n$ and let $\mathcal{A}$ be a collection of Borel functions. We say that ν_j *converges to* ν *with respect to test functions in* $\mathcal{A}$ if for any $f \in \mathcal{A}$, f is integrable w.r.t. ν_j for all j and w.r.t. ν, and

$$\int_{\mathscr{X}_n} f \, d\nu_j \longrightarrow_{j \to \infty} \int_{\mathscr{X}_n} f \, d\nu. \tag{0.2}$$

Fix a sequence p_j of primes, $p_j \to \infty$. For each prime p let

$$\mathscr{F}_{p,n} \stackrel{\mathrm{def}}{=} \{p^{1/n} \cdot L : L \subset \mathbb{R}^n \text{ is a lattice}, \mathbb{Z}^n \subset L, [L : \mathbb{Z}^n] = p\}.$$

Prove that the uniform measures defined by

$$\nu_{p_j} \stackrel{\mathrm{def}}{=} \frac{1}{F_{p,n_j}} \sum_{L \in \mathscr{F}_{p_j,n}} \delta_L, \qquad \text{where } F_{p,n_j} \stackrel{\mathrm{def}}{=} \# \mathscr{F}_{p_j,n}$$

satisfy:

(1) ν_j converges to $m_{\mathscr{X}_n}$ as $j \to \infty$ with respect to the collection

$$\{\hat{f} : f \in C_c(\mathbb{R}^n \smallsetminus \{0\})\}, \qquad \text{where } \hat{f}(L) = \sum_{x \in L \smallsetminus \{0\}} f(x).$$

(2) ν_j converges to $m_{\mathscr{X}_n}$ as $j \to \infty$ with respect to the collection $C_c(\mathscr{X}_n)$.

16. Let $L \in \mathscr{X}_n$ be a lattice, let $\|\cdot\|$ be the Euclidean norm on $\mathbb{R}^n$, let V be the Voronoi cell of L, let $\lambda_1(L)$ be the first successive minimum, let $\rho(x) \stackrel{\text{def}}{=} e^{-\pi\|x\|^2}$, and let $\mathrm{covrad}(L)$ be the covering radius of L.

$$\eta_1 \stackrel{\text{def}}{=} \int_V \|x\| \, d\mathrm{Vol}(x), \qquad \eta_2 \stackrel{\text{def}}{=} \int_V \|x\|^2 \, d\mathrm{Vol}(x), \qquad \eta_3 \stackrel{\text{def}}{=} \int_V \rho(x) \, d\mathrm{Vol}(x).$$

Show the following:

- $\lambda_1(L) = 2 \sup\{r > 0 : B(0,r) \subset V\}$.
- $\mathrm{covrad}(L) = \inf\{r > 0 : B(0,r) \supset V\}$.
- $\eta_1(L) \le \mathrm{covrad}(L) \le 2\eta_1(L) \le 2\sqrt{\eta_2(L)}$.
- $\eta_3 \sum_{x \in L} \rho(x) \le 1$.
- $\inf_{L \in \mathscr{X}_n} \frac{\eta_1(L)}{\mathrm{covrad}(L)} = \frac{1}{2}, \qquad \inf_{L \in \mathscr{X}_n} \frac{\eta_2(L)}{\mathrm{covrad}(L)^2} \in \left[\frac{1}{4}, \frac{1}{3}\right]$.

17. Let d, m be positive integers, let $n = d+m$ and let $\mathbb{R}^n = \mathbb{R}^d \oplus \mathbb{R}^m$ be the standard direct sum decomposition where the projections $\pi_1 : \mathbb{R}^n \to \mathbb{R}^d$, $\pi_2 : \mathbb{R}^n \to \mathbb{R}^m$ are given by

$$\pi_1(x) = (x_1, \ldots, x_d), \quad \pi_2(x) = (x_{d+1}, \ldots, x_n), \quad (x = (x_1, \ldots, x_n)).$$

Let $W \subset \mathbb{R}^m$ be a bounded open set and let $L \subset \mathbb{R}^n$ be a lattice. Suppose that

$$\pi_2(L) \text{ is dense in } \mathbb{R}^m \text{ and } \pi_1|_L \text{ is injective.} \tag{0.3}$$

Let $\Lambda = \Lambda(L, W) \stackrel{\text{def}}{=} \pi_1(L \cap \pi_2^{-1}(W))$ (such sets Λ are called *cut-and-project sets*). Show that

- There are $0 < r < R$ such that the balls $\{B(x,r) : x \in \Lambda\}$ are disjoint and the balls $\{B(x,R) : x \in \Lambda\}$ cover $\mathbb{R}^d$.
- The limiting density
$$D(\Lambda) = \lim_{T \to \infty} \frac{\#\Lambda \cap B(0,T)}{\mathrm{Vol}_d(B(0,T))}$$
exists and is equal to $\frac{\mathrm{Vol}_m(W)}{\mathrm{covol}(L)}$ (here Vol_k is Lebesgue measure on $\mathbb{R}^k$).
- For $m_{\mathscr{X}_n}$-a.e. L, (0.3) holds.

- For fixed W there is $\delta > 0$ such that for almost every choice of L (with respect to $m_{\mathscr{L}_n}$), we have an error estimate
$$|\#\Lambda \cap B(0,T) - D(\Lambda)\mathrm{Vol}_d(B(0,T))| = O\left(T^{d-\delta}\right).$$