Exercise sheet – Geometry of Numbers
Tel Aviv University, Fall 2020

Notation. Unless specified otherwise, $\langle u, v\rangle$ is the standard inner product of $u, v \in \mathbb{R}^n$, $\| \cdot \|$ is the corresponding ℓ_2 norm on $\mathbb{R}^n$ and $B(x, r)$ is the open ball around x of radius r, with respect to this norm. The Lebesgue measure on $\mathbb{R}^n$ is denoted by Vol. For a set $F \subset \mathbb{R}^n$,

$$\mathrm{conv}(F) = \left\{ \sum_{x \in F_0} a_x x : F_0 \subset F \text{ is finite}, \, a_x \geqslant 0, \sum_{x \in F_0} a_x = 1 \right\}.$$

A set $K \subset \mathbb{R}^n$ is called *convex* if $K = \mathrm{conv}(K)$, and is called a *convex body* if it is compact, convex, and has nonempty interior. For two sets $A, B \subset \mathbb{R}^n$ we define $A + B \stackrel{\text{def}}{=} \{a + b : a \in A, b \in B\}$ and $-A \stackrel{\text{def}}{=} \{-a : a \in A\}$. A convex set K is *centrally symmetric* if $K = -K$. The *dual* L^* of L is defined by

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

A *grid* is a set of the form $x + L$ where $x \in \mathbb{R}^n$ and $L \subset \mathbb{R}^n$ is a lattice. The *covolume* of the grid $x+L$ is $\mathrm{covol}(L)$. Let $\mathcal{X}_n$ denote the collection of lattices of covolume 1 in $\mathbb{R}^n$, and let $\mathcal{Y}_n$ denote the collection of grids of covolume 1 in $\mathbb{R}^n$. The $\mathrm{SL}_n(\mathbb{R})$-invariant probability measure on $\mathcal{X}_n$ is denoted by $m_{\mathcal{X}_n}$.

1. Let $L \subset \mathbb{R}^n$ and let V be its Voronoi cell. Prove that V is a polytope, that is there is a finite $F_0 \subset \mathbb{R}^n$ such that $V = \mathrm{conv}(F_0)$. Prove that V is centrally symmetric. A *face* of $\mathrm{conv}(F_0)$ is a subset of the form $\mathrm{conv}(F_1)$ where $F_1 \subset F_0$ and $\mathrm{conv}(F_1)$ contains no interior points of $\mathrm{conv}(F_0)$. The *dimension* of a face V' is $\dim \mathrm{span}_{\mathbb{R}}(V' - V')$. Prove that for each $n-1$-dimensional face V' of V there is $x_0 \in V'$ such that $V' - x_0$ is centrally symmetric. Prove that the maximal number of parallel $n-2$ faces of V is either 4 or 6, and show by example that these bounds are achieved.

2. Let $L = \mathbb{Z}^n$ and let $p \in \mathbb{N}$. What is the number of sublattices $L' \subset L$ such that $[L : L'] = p$? For p a prime, write down an algorithm for exhibiting all of them. That is, for each such L', find a matrix A such that $L' = A\mathbb{Z}^n$.

3. Let $L \subset \mathbb{R}^n$ be a lattice and let $S \subset \mathbb{R}^n$ be a bounded convex set with nonempty interior. For $r > 0$, define $r \cdot S = \{rs : s \in S\}$. Prove that

$$\lim_{r \to \infty} \frac{\#\left(L \cap r \cdot S\right)}{r^n} = \frac{\mathrm{Vol}(S)}{\mathrm{covol}(L)}.$$

Show that in fact

$$\#(L \cap r \cdot S) = cr^n + O(r^{n-1}), \quad \text{for } c = \frac{\mathrm{Vol}(S)}{\mathrm{covol}(L)}.$$

4. Let $L \subset \mathbb{R}^n$ be a lattice and for $i = 1, \dots, n$, let

$$\lambda_i \overset{\text{def}}{=} \inf\{r > 0 : L \cap B(0,r) \text{ contains } i \text{ linearly independent vectors}\}$$

be its Minkowski successive minima. Also let

$$\bar{\lambda}_i \overset{\text{def}}{=} \inf\{r > 0 : L \cap B(0,r) \text{ contains a primitive } i\text{-tuple of vectors}\}.$$

(a) Choose a basis of $\mathbb{R}^n$ successively as follows. Let v_1 be a shortest nonzero vector in L, and given $v_1, \dots, v_r$ for some $r < n$, let v_{r+1} be a shortest vector in

$$A_r \overset{\text{def}}{=} \{v \in L : v_1, \dots, v_r, v \text{ are linearly independent}\}.$$

Prove that for all i, $\|v_i\| = \lambda_i$.

(b) Choose $\bar{v}_1, \dots, \bar{v}_n$ successively by the algorithm described in (a), replacing A_r with

$$\bar{A}_r \overset{\text{def}}{=} \{v \in L : \bar{v}_1, \dots, \bar{v}_r, v \text{ is a primitive } (r+1)\text{-tuple}\}.$$

Give an example of a lattice for which $\|\bar{v}_n\| > \bar{\lambda}_n$.

(c) In (b), for a given n, what is the maximal possible number of indices i for which $\|\bar{v}_i\| \neq \bar{\lambda}_i$?

5. Let $L \subset \mathbb{R}^n$ be a lattice and let K be a convex body. Prove that:

(i) If $\dim \operatorname{span}_{\mathbb{R}}(K \cap L) = n$ then

$$\#(K \cap L) \leqslant n! \, \frac{\mathrm{Vol}(K)}{\mathrm{covol}(L)} + n.$$

(ii) If K is centrally symmetric then

$$\#(K \cap L) \geqslant 2 \left\lfloor \frac{\mathrm{Vol}(K)}{2^n \, \mathrm{covol}(L)} \right\rfloor + 1.$$

6. Let $\|\cdot\|$ be a norm on $\mathbb{R}^n$, and let $\lambda_i(L)$ denote the successive minima of a lattice L with respect to the norm. Prove that for any lattice $L \subset \mathbb{R}^n$,

$$\frac{2^n}{n!} \frac{\mathrm{covol}(L)}{\mathrm{Vol}(B(0,1))} \leqslant \prod_{i=1}^{n} \lambda_i(L).$$

7. Given a lattice $L \subset \mathbb{R}^n$ let $\kappa_i(L) \overset{\text{def}}{=} \|v_i\|$, where $v_1, \dots, v_n$ are a basis of L obtained by the Korkine Zolotarev reduction procedure (recall that in case of ties the Korkine-Zolotarev basis is not uniquely defined, and thus $\kappa_i(L)$ depends on the particular choice of the basis $v_1, \ldots, v_n$). Let

$$\alpha_i(L) \stackrel{\mathrm{def}}{=} \inf\{\mathrm{covol}(L_0) : L_0 \subset L \text{ an additive subgroup, } \dim \mathrm{span}_{\mathbb{R}}(L_0) = i\},$$

and let $\lambda_i(L)$ denote the Minkowski successive minima. Say that functions $A(L), B(L)$ on the collection of lattices in $\mathbb{R}^n$ satisfy $A \asymp B$ if there is a constant C (depending on n) such that for all L,

$$C^{-1}A(L) \leqslant B(L) \leqslant CA(L).$$

Prove that $\kappa_i(L) \asymp \lambda_i(L)$ and $\alpha_i(L) \asymp \lambda_1(L) \cdots \lambda_i(L)$.

8. Let $L \subset \mathbb{R}^n$ be a lattice and let $m \in \mathbb{N}$. Suppose $A \subset \mathbb{R}^n$ is a Borel set with $\mathrm{Vol}(A) > m\,\mathrm{covol}(L)$. Prove that there are $x_0, x_1, \ldots, x_m \in A$, distinct elements such that $x_i - x_j \in L$ for every i, j.

9. Let $G_n = \bigoplus_{p=0}^n \mathbb{R}^n_p$ denote the Grassmann algebra. Prove or disprove:

- there is $u \in G_n \smallsetminus \{0\}$ such that $u \wedge u \neq 0$.
- there are $u, v \in G_n$ such that $\|u \wedge v\| > \|u\|\,\|v\|$.

10. Let L be a lattice and let $\{0\} = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_k \subsetneq L_{k+1} = L$ be its Harder-Narasimhan filtration. L is called *stable* if $k = 0$. For each i let $V_i \stackrel{\mathrm{def}}{=} \mathrm{span}(L_i)^{\perp}$ and let $\pi_i : \mathbb{R}^n \to V_i$ be the orthogonal projection. The points $\{(\mathrm{rank}(L_i), \log \mathrm{covol}(L_i)) : i = 0, \ldots, k+1\}$ are the *profile* of L. Prove that:

- $\pi_i(L_j)$ is discrete for each i. Below we will consider it as a lattice in $V' \stackrel{\mathrm{def}}{=} \mathrm{span}(\pi_i(L_j))$, and compute its Harder-Narasimhan filtration and profile using the restriction of the Euclidean inner product to V'.
- For each i, the Harder-Narasimhan filtration of $\pi_i(L)$ is $\{0\} = \pi_i(L_i) \subsetneq \pi_i(L_{i+1}) \subsetneq \cdots \subsetneq \pi_i(L_k) \subsetneq \pi_i(L)$.
- $\pi_i(L_{i+1})$ is stable for each i.
- If $\mathrm{covol}(L) = 1$ then the profile of L^* is the image of the profile of L under the reflection $\mathbb{R}^2 \to \mathbb{R}^2$, $(x, y) \mapsto (n - x, y)$. For a fixed value of $c = \mathrm{covol}(L) \neq 1$, find a map $\varphi_c : \mathbb{R}^2 \to \mathbb{R}^2$ with the same property.

11. Let $\mathbf{Cl}(\mathbb{R}^n)$ denote the space of closed subsets of $\mathbb{R}^n$, equipped with the Chabauty-Fell metric D.

- Show that for $Y, Y_1, Y_2, \ldots \in \mathbf{Cl}(\mathbb{R}^n)$, we have $Y_j \to Y$ if and only if for every $y \in Y$ there is a sequence $y_j \in Y_j$ with $y_j \to y$, and whenever, for a subsequence $i_j \to \infty$, for any $y_{i_j} \in Y_{i_j}$ such that $y_\infty \stackrel{\mathrm{def}}{=} \lim_j y_{i_j}$ exists, we have $y_\infty \in Y$.

- Prove that $\mathbf{Cl}(\mathbb{R}^n)$ is compact.
- Show that if $L_j \to L$ are lattices, and $\mathbf{Vor}(L)$ is the Voronoi cell of L, considered as an element of $\mathbf{Cl}(\mathbb{R}^n)$, then $\mathbf{Vor}(L_j) \to \mathbf{Vor}(L)$.
- Show that if $L_j \to_j L$ then $\alpha_i(L_j) \to_j \alpha_i(L)$ and $\lambda_i(L_j) \to \lambda_i(L)$ for $i = 1, \ldots, n$.
- Show that for any $L \in \mathcal{X}_n$ there is $r_0 > 0$ such that for any $r \in (0, r_0)$, the closed ball $\{L' \in \mathcal{X}_n : D(L, L') \leqslant r\}$ is compact.
- We think of $\mathcal{X}_n$ and $\mathcal{Y}_n$ as subsets of $\mathbf{Cl}(\mathbb{R}^n)$. What are their closures $\overline{\mathcal{X}_n}$ and $\overline{\mathcal{Y}_n}$?

12. For $n = 2, 3$, list all perfect lattices and all eutactic lattices in $\mathbb{R}^n$.

13. The *Gram matrix* of an n-tuple $v_1, \ldots, v_n$ in $\mathbb{R}^n$ is the symmetric matrix $\left(\langle v_i, v_j \rangle\right)_{i,j=1,\ldots,n}$. Suppose $L = \mathrm{span}_{\mathbb{Z}}(v_1, \ldots, v_n)$ and let A be the Gram matrix of $v_1, \ldots, v_n$. Prove that $\det(A) = \mathrm{covol}(L)^2$. Suppose L is perfect. Prove that there is $t \in \mathbb{R} \setminus \{0\}$ so that tA has rational coefficients. The *Hermite constant* is $\mu_n \overset{\mathrm{def}}{=} \sup\{\lambda_1(L)^2 : L \in \mathcal{X}_n\}$. Prove that $\mu_n^n \in \mathbb{Q}$.

14. Let $F \subset \mathbb{R}^n$ be a finite set, and let $\{\lambda_x : x \in F\}$ be real numbers. Show that the following conditions are equivalent:

- For any $A \in \mathrm{Sym}_n$, $\mathrm{tr}(A) = \sum_{x \in F} \lambda_x \varphi_x(A)$, where $\varphi_x(A) = \langle Ax, x \rangle$.
- $\mathrm{Id} = \sum_{x \in F} \lambda_x ||x||^2 P_x$, where P_x is the orthogonal projection onto $\mathrm{span}(x)$.
- For any $y, z \in \mathbb{R}^n$, we have $\langle y, z \rangle = \sum_{x \in F} \lambda_x \langle y, x \rangle \langle z, x \rangle$.

15. Show that if an lcsc (locally compact second countable) group G acts transitively on an lcsc space X, then there is at most one invariant Radon measure on X (up to scaling). That is, if μ_1, μ_2 are nonzero Radon measures on X and satisfy $g_* \mu_i = \mu_i$ for all $g \in G$ and $i = 1, 2$, then there is $c > 0$ such that $\mu_1 = c\mu_2$. Give an example of a transitive action of an lcsc group on an lcsc space with no invariant Radon measures.

16. A map $f : \mathbb{R}^n \to \mathbb{R}^n$ is called *affine* if $\forall x_1, x_2 \in \mathbb{R}^n$, $\forall s \in \mathbb{R}$, we have $f(sx_1 + (1-s)x_2) = sf(x_1) + (1-s)f(x_2)$. Let $\mathrm{ASL}_n(\mathbb{R})$ denote the group of orientation preserving volume preserving affine maps $\mathbb{R}^n \to \mathbb{R}^n$. Show that $f \in \mathrm{ASL}_n(\mathbb{R})$ can be written uniquely as

$f(x) = A_f x + y_f$, where $A_f \in \mathrm{SL}_n(\mathbb{R})$ and $y_f \in \mathbb{R}^n$. Show that the map

$$\varphi : \mathrm{ASL}_n(\mathbb{R}) \to \mathrm{SL}_{n+1}(\mathbb{R}), \quad \varphi(f) = \begin{pmatrix} A_f & y_f \\ 0 & 1 \end{pmatrix}$$

is an injective group homomorphism, and that

$$\varphi(f)\begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} f(x) \\ 1 \end{pmatrix}, \quad \forall x \in \mathbb{R}^n.$$

Show that $\mathrm{ASL}_n(\mathbb{Z}) = \varphi^{-1}(\mathrm{SL}_{n+1}(\mathbb{Z}))$ is a lattice in $\mathrm{ASL}_n(\mathbb{R})$ and that $\mathcal{Y}_n$ is isomorphic to $\mathrm{ASL}_n(\mathbb{R})/\,\mathrm{ASL}_n(\mathbb{Z})$. Show that the map $\mathcal{Y}_n \to \mathcal{X}_n$ which sends a grid L to the lattice $L - L$ is proper, and that the fiber over $L_0 \in \mathcal{Y}_n$ is naturally isomorphic to $\mathbb{R}^n/L_0$. Show that a sequence $(L_j) \subset \mathcal{Y}_n$ satisfies $L_j \to \infty$ if and only if $\mathrm{covrad}(L_j) \to \infty$, where

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

State and prove an analogue of the Siegel summation formula for the space $\mathcal{Y}_n$.

17. Let $n \geqslant 3$ and let $B \subset \mathbb{R}^n$ be a Borel set. Prove that

- If $\mathrm{Vol}(B) < \infty$ then $\#(L \cap B) < \infty$ for $m_{\mathcal{X}_n}$-a.e. $L \in \mathcal{X}_n$.
- If $\mathrm{Vol}(B) = \infty$ then $\#(L \cap B) = \infty$ for $m_{\mathcal{X}_n}$-a.e. $L \in \mathcal{X}_n$.

18. A lattice $L \subset \mathbb{R}^n$ is called *even unimodular* if $\mathrm{covol}(L) = 1$ and $\|v\|^2 \in 2\mathbb{Z}$ for any $v \in L$. Prove that if L is even unimodular, then L is self-dual, that is, $L = L^*$. Also prove that the lattice

$$E_8 \stackrel{\mathrm{def}}{=} \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_8 \end{pmatrix} \in \mathbb{R}^8 : \forall i, 2x_i \in \mathbb{Z},\ 2x_1 \equiv \cdots \equiv 2x_8 \mod 2, \text{ and } \sum x_i \in 2\mathbb{Z} \right\}$$

is even unimodular. Show that $\lambda_1(E_8) = \sqrt{2}$ and that E_8 contains 240 shortest nonzero vectors.

19. Let $f \in C_c(\mathcal{X}_n)$, let $M \in \mathbb{N}$, and define $F_1, F_2 \in C_c(\mathcal{X}_n)$ by

$$F_1(L) \stackrel{\mathrm{def}}{=} f(L^*), \quad F_2(L) \stackrel{\mathrm{def}}{=} \frac{1}{S_M} \sum_{[L:L_1]=M} f(M^{-1/n} L_1)$$

(the sum in the definition ranges over all sub-lattices of index M, and S_M is the number of such sub-lattices).

Prove that $\int_{\mathcal{X}_n} f\, dm_{\mathcal{X}_n} = \int_{\mathcal{X}_n} F_1\, dm_{\mathcal{X}_n} = \int_{\mathcal{X}_n} F_2\, dm_{\mathcal{X}_n}$.

20. Let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ denote the standard basis of $\mathbb{R}^n$, let $f \in C_c(\mathbb{R}^n)$ and let $\hat{f} : \mathcal{X}_n \to \mathbb{R}$ be the function $\hat{f}(L) = \sum_{x \in L \smallsetminus \{0\}} f(x)$. For $t > 0$

and $\mathbf{a} = (a_1, \dots, a_{n-1}) \in [0,1)^{n-1}$, let

$$L_{t,\mathbf{a}} \stackrel{\text{def}}{=} \operatorname{span}_{\mathbb{Z}} \left(e^t \mathbf{e}_1, \dots, e^t \mathbf{e}_{n-1}, \sum_{i=1}^{n-1} e^t a_i \mathbf{e}_i + e^{-(n-1)t} \mathbf{e}_n \right).$$

Prove that

$$\lim_{t \to \infty} \int_{[0,1)^{n-1}} \hat{f}(L_{t,\mathbf{a}}) \, d\mathrm{Vol}(\mathbf{a}) = \int_{\mathcal{X}_n} \hat{f} \, dm_{\mathcal{X}_n}.$$

21. For $L \in \mathcal{X}_n$, define the *covering density* of L by

$$\Theta(L) \stackrel{\text{def}}{=} \inf\{\mathrm{Vol}(B) : L + B = \mathbb{R}^n,\ B \text{ is a Euclidean ball}\}.$$

What is $\int_{\mathcal{X}_n} \Theta(L) \, dm_{\mathcal{X}_n}(L)$?