Math 361 lecture for Wednesday, Week 10

Minkowski's theorem for lattices

Goal. Let K be a number field. Let $\mathcal{F}$ be the multiplicative group of nonzero fractional ideals. A fractional ideal is called *principal* if it is generated as an $\mathfrak{O}_K$-module by a single element. So a principal fractional ideal has the from $c^{-1}(\alpha)$ where $c \in K \setminus \{0\}$ and $\alpha \in \mathfrak{O}_K$. Let $\mathcal{P} \subseteq \mathcal{F}$ denote the subgroup of nonzero principal fractional ideals. The *class group* of K is the quotient group

$$\mathcal{H} = \mathcal{F}/\mathcal{P}.$$

The *class* number $h_K := h(\mathfrak{O}_K) := |\mathcal{H}|$, the order of the class group. We will see that $h_K = 1$ if and only if $\mathfrak{O}_K$ is a PID. In general, h_K is a measure of how far way $\mathfrak{O}_K$ is from being a PID. **Our goal** is to prove that the class number is finite.

Lattices in $\mathbb{R}^n$.

Definition 1. A subset $L \subset \mathbb{R}^n$ is a *rank m lattice in* $\mathbb{R}^n$ if $L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \dots, v_m\}$ for some set $\{v_1, \dots, v_m\}$ of linearly independent vectors in $\mathbb{R}^n$.

A subset of $\mathbb{R}^n$ is *discrete* if its intersection with each compact subset of $\mathbb{R}^n$ is finite. Equivalently, the subset has no accumulation points.

Theorem 2. An additive subgroup $L \subset \mathbb{R}^n$ is a lattice if and only if it is discrete.

Definition 3. A *fundamental domain* for a rank n lattice L in $\mathbb{R}^n$ is a set of the form

$$F = \left\{\textstyle\sum_{i=1}^n a_i v_i : 0 \leq a_i < 1 \text{ for } i = 1, \dots n\right\}.$$

where $L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \dots, v_n\}$.

Remark 4. With notation as in the above definition,

1. The volume of F is $\mathrm{vol}(F) = |\det(v_1, \dots, v_n)|$.
2. For each $x \in \mathbb{R}^n$, there exists a unique $\ell \in L$ such that $x \in \ell + F$.

Example 5.

1. $\mathbb{Z}$ is a lattice in $\mathbb{R}$. Let $S^1 = \{z \in \mathbb{C} : |z|\}$ be the unit circle in $\mathbb{R}^2$ centered at the origin. We have a homeomorphism

$$\begin{aligned} \mathbb{R}/\mathbb{Z} &\to S^1 \\ x &\to e^{2\pi i x}. \end{aligned}$$

   A fundamental domain is $[0, 1)$.

2. Consider the number field $K = \mathbb{Q}(\sqrt{2})$ with number ring $\mathbb{Z}[1, \sqrt{2}]$. The embeddings of K into $\mathbb{C}$ are $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $\sigma_2(a + \sqrt{2}) = a - b\sqrt{2}$. Consider the homomorphism

$$\begin{aligned} K &\to \mathbb{R}^2 \\ x &\mapsto (\sigma_1(x), \sigma_2(x)). \end{aligned}$$

Then the image of $\mathbb{Z}[\sqrt{2}]$ in $\mathbb{R}^2$ is a lattice with generators $(\sigma_1(1), \sigma_2(1)) = (1, 1)$ and $(\sigma_1(\sqrt{2}), \sigma_2(\sqrt{2})) = (\sqrt{2}, -\sqrt{2})$. The fundamental domain corresponding to these generators has volume

$$\left| \det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix} \right| = 2\sqrt{2}.$$

Exercises:

(a) Draw a picture of this lattice and the fundamental domain specified above.

(b) Can you find a different fundamental domain? What is its volume?

Definition 6. The n-torus is the topological space

$$T^n = \underbrace{S^1 \times \cdots \times S^1}_{n \text{ times}}$$

with the product topology.

Proposition 7. Let L be a rank m lattice in $\mathbb{R}^n$ with generators $v_1, \dots, v_m$. Complete $v_1, \dots, v_m$ to a basis $v_1, \dots, v_n$ for $\mathbb{R}^n$. Then there is a homeomorphism

$$\begin{aligned} \phi \colon \mathbb{R}^n/L &\to T^m \times \mathbb{R}^{n-m} \\ \sum_{i=1}^{n} a_i v_i &\mapsto \left(e^{2\pi i a_1}, \dots, e^{2\pi i a_m}, a_{m+1}, \dots, a_n\right). \end{aligned}$$

The mapping ϕ is a bijection when restricted to the fundamental domain F.

Proof. Exercise. □

Example 8. Consider the lattices $L = \mathrm{Span}_{\mathbb{Z}}\{(1, 0), (0, 1)\}$ and $L' = \mathrm{Span}_{\mathbb{Z}}\{(1, 0)\}$ in $\mathbb{R}^2$. We have that $\mathbb{R}^2/L$ is homeomorphic to a torus and $\mathbb{R}^2/L'$ is homeomorphic to a cylinder.

Definition 9. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and consider the mapping $\pi : \mathbb{R}^n \to \mathbb{R}^n/L \xrightarrow{\phi} T^n$, the quotient mapping followed by the isomorphism ϕ defined above. The *volume* of $Y \subseteq T^n$ is defined to be

$$\mathrm{vol}(Y) = \mathrm{vol}(\phi^{-1}(Y) \cap F)$$

where F is a fundamental domain for L.

Proposition 10. Let $X \subset \mathbb{R}^n$ be a bounded such that $\mathrm{vol}(X)$ exists. With notation as in the above definition, suppose that π restricted to X is injective. Then $\mathrm{vol}(X) = \mathrm{vol}(\pi(X))$.

Proof. See Theorem 6.7 and the accompanying Figure 6.6. □

Minkowski's theorem.

Definition 11. Let $X \subseteq \mathbb{R}^n$. Then X is *convex* if it contains the line segment joining each pair of points in X. In other words, if $x, y \in X$, then $\lambda x + (1-\lambda)y \in X$ for $\lambda \in [0,1]$.

Example 12. If $P = \{p_1, \ldots, p_k\} \subset \mathbb{R}^n$, the smallest convex set containing P is

$$\mathrm{conv}(P) = \left\{ \sum_{i=1}^{k} \lambda_i p_i : \lambda_i \geq 0 \text{ and } \sum_{i=1}^{k} \lambda_i = 1 \right\}.$$

This set is called the *convex hull* of P.

Definition 13. Let $X \subseteq \mathbb{R}^n$. Then X is *centrally symmetric about the origin* if $x \in X$ implies $-x \in X$ for all $x \in X$. We will use the abbreviation *symmetric* to mean centrally symmetric about the origin in the context of Minkowski's theorem.

Theorem 14 (Minkowski's theorem)**.** Let $L \subset \mathbb{R}^n$ be a rank n lattice, and let F be a fundamental domain for L. Let $X \subset \mathbb{R}^n$ be bounded, convex, and symmetric. Suppose that

$$\mathrm{vol}(X) > 2^n \,\mathrm{vol}(F).$$

Then X contains a nonzero lattice point.

Exercise 15. Consider Minkowski's theorem for the cases:

- $L = \mathbb{Z} \subset \mathbb{R}$, and
- $L = \mathrm{Span}_{\mathbb{Z}}\{(1,0),(0,1)\} \subset \mathbb{R}^2$.

Proof of Minkowski's theorem. Consider the lattice $2L$, whose fundamental domain has volume $2^n \,\mathrm{vol}(F)$. If $\mathrm{vol}(X) > 2^n \,\mathrm{vol}(F)$, then we have seen that $\pi \colon \mathbb{R}^n \to \mathbb{R}^n/(2L)$ is not injective when restricted to X. Thus, there exist distinct $x, y \in X$ such that $\pi(x) = \pi(y)$. So $x - y \in 2L$, and thus

$$\frac{1}{2}(x-y) \in L.$$

Since X is symmetric, $-y \in X$. Since X is convex, it follows that

$$\frac{1}{2}(x-y) = \frac{1}{2}x + \frac{1}{2}(-y) \in X.$$

Since $x \neq y$, we have $(x-y)/2$ is a nonzero lattice point in X. □