Blichfeldt's Lemma and Minkowski's Theorem

written by akrishna168 on Functor Network
original link: https://functor.network/user/1778/entry/798

In this post, I wanted to give a proof of Minkowski's Theorem on lattice points using a lemma of Blichfeldt. There's an intuitive probabilistic characterization of the lemma, but very few sources seem to rigorously establish the full proof, a gap which I attempted to fill in below. I wrote this as a note for Prof. Barry Mazur's algebraic number theory course in the spring of 2024; in a future post, I'll indicate the standard consequence of Minkowski's Theorem, which is finiteness of the class group of any algebraic number field.

Blichfeldt's Lemma. Let Λ be a full-rank lattice in $\mathbb{R}^n$ (a discrete, cocompact subgroup) with fundamental domain Π and B a bounded, measurable set such that

$$\mu(B) > \mu(\Pi)$$

Then there exist $x, y \in B$ such that $x - y \in \Lambda$.

Proof. We reduce to the case where $\Lambda = \mathbb{Z}^n$, applying a linear transformation as needed. Haar measure on $\mathbb{R}^n$ is just Lebesgue measure (which we denote here by vol), and is translation-invariant. Then $\text{vol}(\Pi) = 1$.

Write χ_B for the characteristic function of B. This function is Lebesgue-integrable because B is a measurable set. Let

$$\phi(x) = \sum_{m \in \mathbb{Z}^n} \chi_B(x + m).$$

Because B is bounded, it follows that ϕ is bounded, as there are finitely many nonzero terms for any given $m \in \mathbb{Z}^n$.

Now we integrate both sides of this expression over $\Pi = [0, 1]^n$. Thanks to our previous remark, we may freely switch integral and sum because the summation is a finite sum of nonnegative terms, so

$$\int_{[0,1]^n} \phi(x) \mathrm{d}x = \int_{[0,1]^n} \sum_{m \in \mathbb{Z}^n} \chi_B(x + m) \mathrm{d}x = \sum_{m \in \mathbb{Z}^n} \int_{[0,1]^n} \chi_B(x + m) \mathrm{d}x$$

$$= \sum_{m \in \mathbb{Z}^n} \int_{[0,1]^n + m} \chi_B(x) \mathrm{d}x = \int_{\mathbb{R}^n} \chi_B(x) \mathrm{d}x = \text{vol}(B) > 1$$

This implies that $\phi(x) \geq 2$ for some $x \in [0, 1]^n$, which gives the desired two points. $\square$

Minkowski's Theorem. Let $\Lambda \subseteq \mathbb{R}^n$ be a full-rank lattice with fundamental domain Π, and let $B \subset \mathbb{R}^n$ be convex, centrally symmetric, and measurable. If $\mathrm{vol}(B) > 2^n \cdot \mathrm{vol}(\Pi)$, then B contains some nonzero point of Λ.

Proof. Note that

$$\mathrm{vol}(B/2) = \frac{1}{2^n} \cdot \mathrm{vol}(B) > \mathrm{vol}(\Pi),$$

so by Blichfeldt's lemma, there exist distinct $x, y \in B/2$ such that $x - y \in \Lambda$. B and hence $B/2$ are both centrally symmetric, so $-2y \in B$. Because B is convex, $2x, -2y \in D$ implies that $(2x - 2y)/2 = x - y \in B$, so thus we have found our desired nonzero element in $B \cap \Lambda$. $\square$