More geometry of lattices

$L \subset V$ — fin. dim. $\mathbb{R}$-vector space w/ positive definite inner product

a lattice is a discrete, cocompact subgroup of V.

forces $\Rightarrow \operatorname{rank} L \leq \dim_{\mathbb{R}} V$

Recap: the Minkowski space of a number field

$r_1 + 2r_2 = [K:\mathbb{Q}]$

$K = \#$ field. Signature (r_1, r_2) $= (r, s)$

to a first approximation, $K_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

$\mathcal{O}_K \hookrightarrow K \hookrightarrow K_{\mathbb{R}}$

correct normalization: inner product on $K_{\mathbb{R}}$ restricts to the trace pairing on K

e.g. $K = \mathbb{Q}(i)$, this means we take $\langle \ , \ \rangle_{K_{\mathbb{R}}} = 2\langle \ , \ \rangle_{\mathbb{C}}$

$K_{\mathbb{R}} \subseteq K_{\mathbb{C}} = \prod_{T} \mathbb{C}$ $\circlearrowleft F$ $\quad K_{\mathbb{R}} = (K_{\mathbb{C}})^F$

$K \hookrightarrow K_{\mathbb{R}}$

Recap: the lattice associated to an ideal

$\mathcal{O}_K \subset K \hookrightarrow K_{\mathbb{R}}$ gives a lattice of covolume $\sqrt{|\operatorname{Disc} \mathcal{O}_K|}$

similarly, for any fractional ideal I of K, $I \hookrightarrow K_{\mathbb{R}}$ is a lattice of covolume $\sqrt{|\operatorname{Disc} \mathcal{O}_K|} \cdot [\mathcal{O}_K : I]$

generalized index

$$= \frac{[\mathcal{O}_K : I \cap \mathcal{O}_K]}{[I : I \cap \mathcal{O}_K]}$$

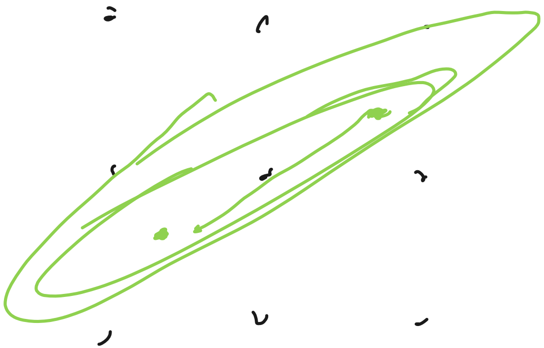
Minkowski's lattice point theorem

Theorem Let $L \subset V$ be a lattice $(\dim V = n)$

Let X be a convex, centrally symmetric (measurable) subset of V such that $\mathrm{vol}(X) > 2^n \mathrm{covol}(L)$

$x \in X \iff -x \in X$

Then X contains a nonzero element of L.



$\mathrm{covol} = 1.$

Proof of Minkowski's theorem

The map

$\frac{1}{2}X \hookrightarrow V \longrightarrow V/L$

cannot be injective.

$\frac{1}{2}X = \{\frac{1}{2}x : x \in X\}$

$\mathrm{vol}(\frac{1}{2}X) > \mathrm{covol}(L)$

$\Rightarrow \exists\ x_1, x_2 \in X,\ \alpha_1, \alpha_2 \in L$ such that $x_1 \neq x_2$, $\alpha_1 \neq \alpha_2$

$$\frac{1}{2}x_1 + \alpha_1 = \frac{1}{2}x_2 + \alpha_2$$

$$\underset{\in L}{\alpha = \alpha_1 - \alpha_2} = \underset{\in X}{\frac{1}{2}x_2 - \frac{1}{2}x_1} = \underbrace{\frac{1}{2}(x_2 + (-x_1))}_{\in X \text{ by convexity}}$$

$-x_1 \in X$ by central symmetry.

Aside: detecting minimal polynomials

Aside: the shortest vector problem

SVP: given a lattice L of fixed covolume, find the shortest nonzero element of L

Application: find minimal polynomials of algebraic numbers from complex approximation (factoring integer polynomials)

Lenstra-Lenstra-Lovasz (L^3) (LLL) (lattice basis reduction)

An application of Minkowski's theorem

<u>Theorem</u> K = # field, $I \subset \mathcal{O}_K$ integral ideal

Choose $c_\tau > 0$ for $\tau \in \mathrm{Hom}(K, \mathbb{C})$ s.t. $c_\tau = c_{\bar\tau}$

and $\prod c_\tau > A\,[\mathcal{O}_K : I]$ $\quad A = \left(\frac{2}{\pi}\right)^{r_2} \cdot \sqrt{|\mathrm{disc}(K)|}$

Then $\exists\, \alpha \in I$ nonzero such that $|\tau(\alpha)| < c_\tau$ $\forall \tau$.

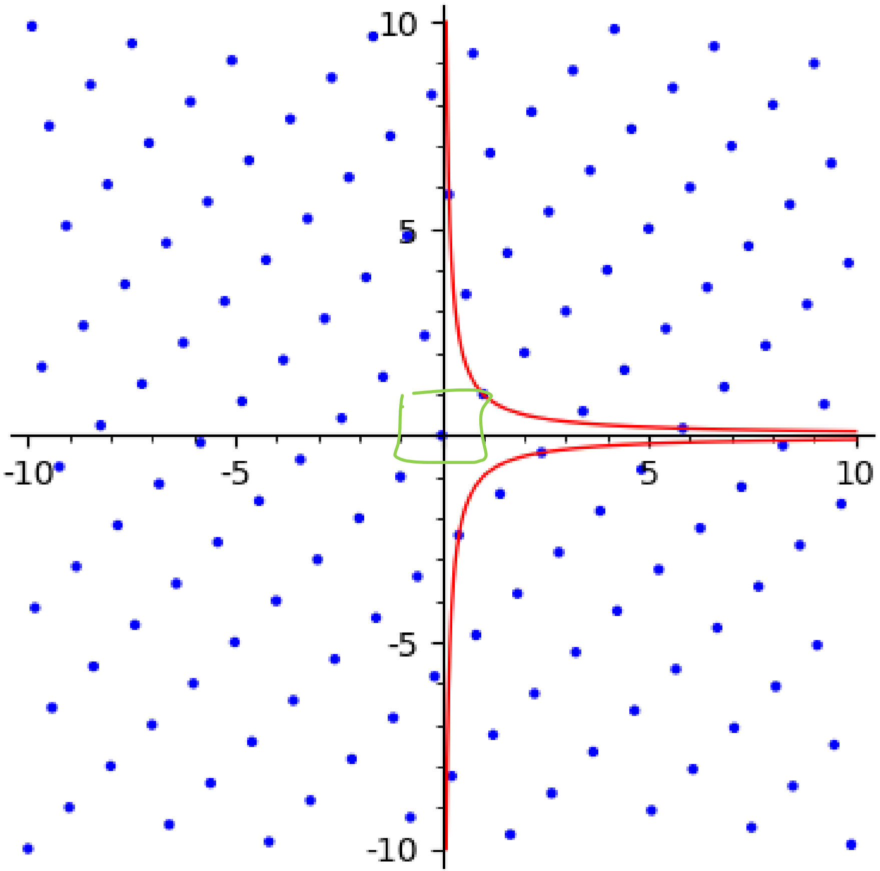
<u>Pf</u> Apply Minkowski to the set

$X = \{(z_\tau) \in K_{\mathbb{R}} : |z_\tau| < c_\tau \ \forall \tau\}$.

$$\mathrm{Vol}(X) = \left(2\right)^{r_1}\left(2\pi\right)^{r_2} \prod c_\tau$$

$$= 2^n \cdot \left(\frac{\pi}{2}\right)^{r_2}$$

A visualization $\mathbb{Z}[\sqrt{2}]$



Application to ideal classes

or fractional

For K a # field and I ~~$\subseteq \mathcal{O}_K$~~ an ~~integral~~ ideal,

Define the (absolute) norm $\boxed{\mathrm{Norm}(I) = [\mathcal{O}_K : I]}$

- $\mathrm{Norm}(I_1 I_2) = \mathrm{Norm}(I_1)\,\mathrm{Norm}(I_2)$ ← chinese remainder thm

$\mathrm{Norm}((\alpha)) = |\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|$ $\quad \alpha \in K^\times$

Lemma: For any ideal I of $\mathcal{O}_K$,

$\exists\ \alpha \in I$ s.t.

$$|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^{s_2} \sqrt{|d_K|}\ \mathrm{Norm}(I)$$

Fact Theorem Cl_K is finite.