More applications of lattices in number theory

Intro video for CoCalc: see course website
or Zulip (General Announcements/CoCalc)

Reminder: small elements of ideals

$K = \#$ field

Lemma For any nonzero ideal I of $\mathcal{O}_K$, there exists $\alpha \in I$ $\alpha \neq 0$ s.t.

$$|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}\, \mathrm{Norm}(I)$$

$d_K = \mathrm{disc}(\mathcal{O}_K)$

$r_1 = \#$ real embeddings

$r_2 = \#$ pairs of complex embeddings

by application of Minkowski's lattice point theorem

Small ideals in ideal classes

Lemma: every class in $Cl_K = J_K / P_K$ contains an integral ideal of norm $\le \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}$ (not optimal)

Pf Pick ~~any~~ integral ideal I in the inverse of this class.

Apply previous lemma to find $\alpha \in I$, $\alpha \neq 0$ s.t. $\mathrm{Norm}(\alpha) \le \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\,\mathrm{Norm}(I)$

$$\Rightarrow \mathrm{Norm}(\underbrace{\alpha I^{-1}}_{\subseteq \mathcal{O}_K}) \le \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}$$

in class of I^{-1}

There are only finitely many ideals of a given norm

Lemma For any positive integer N, $\exists$ finitely many ideals of $\mathcal{O}_K$ of norm N.

Pf $\text{Norm}(I) = [\mathcal{O}_K : I]$

in fact, only finitely many subgroups of $\mathcal{O}_K$ of index N, because they all contain $N\mathcal{O}_K$

$N\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$ $\qquad\qquad$ $\mathcal{O}_K / N\mathcal{O}_K \cong (\mathbb{Z}/N\mathbb{Z})^{[K:\mathbb{Q}]}$

Finiteness of the class group

<u>Theorem</u> Cl_K is a <u>finite</u> abelian group

<u>Pf</u> By previous slides

- each class contains an integral ideal of norm $\leq$ ✱
- these ideals come from a finite set.

A multiplicative version of Minkowski theory

$$K \longrightarrow K_{\mathbb{R}} \longrightarrow K_{\mathbb{C}} = \prod_{\tau} \mathbb{C}$$

$$K_{\mathbb{R}}^{*} \hookrightarrow K_{\mathbb{C}}^{*} = \prod_{\tau} \mathbb{C}^{*}$$

$$= K_{\mathbb{R}} \cap K_{\mathbb{C}}^{*}$$

$$K_{\mathbb{R}}^{*} \xrightarrow{\log} \mathbb{R}^{r_1+r_2}$$

$$= (\mathbb{R}^{*})^{r_1} \times (\mathbb{C}^{*})^{r_2} \quad \nearrow (\log |x_{\tau_1}|, 2\log |x_{\tau_2}|, \dots)$$

$$K^{*} \longrightarrow K_{\mathbb{R}}^{*} \xrightarrow{\log} \mathbb{R}^{r_1+r_2}$$

The norm functional

interested in units α of $\mathcal{O}_K$. These have the property that $|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| = 1$

$$= \prod_{\tau} |\tau(\alpha)| \Rightarrow \underbrace{\sum_{\tau} \log|\tau(\alpha)| = 0}$$

i.e. image of $\mathcal{O}_K^\times$ under

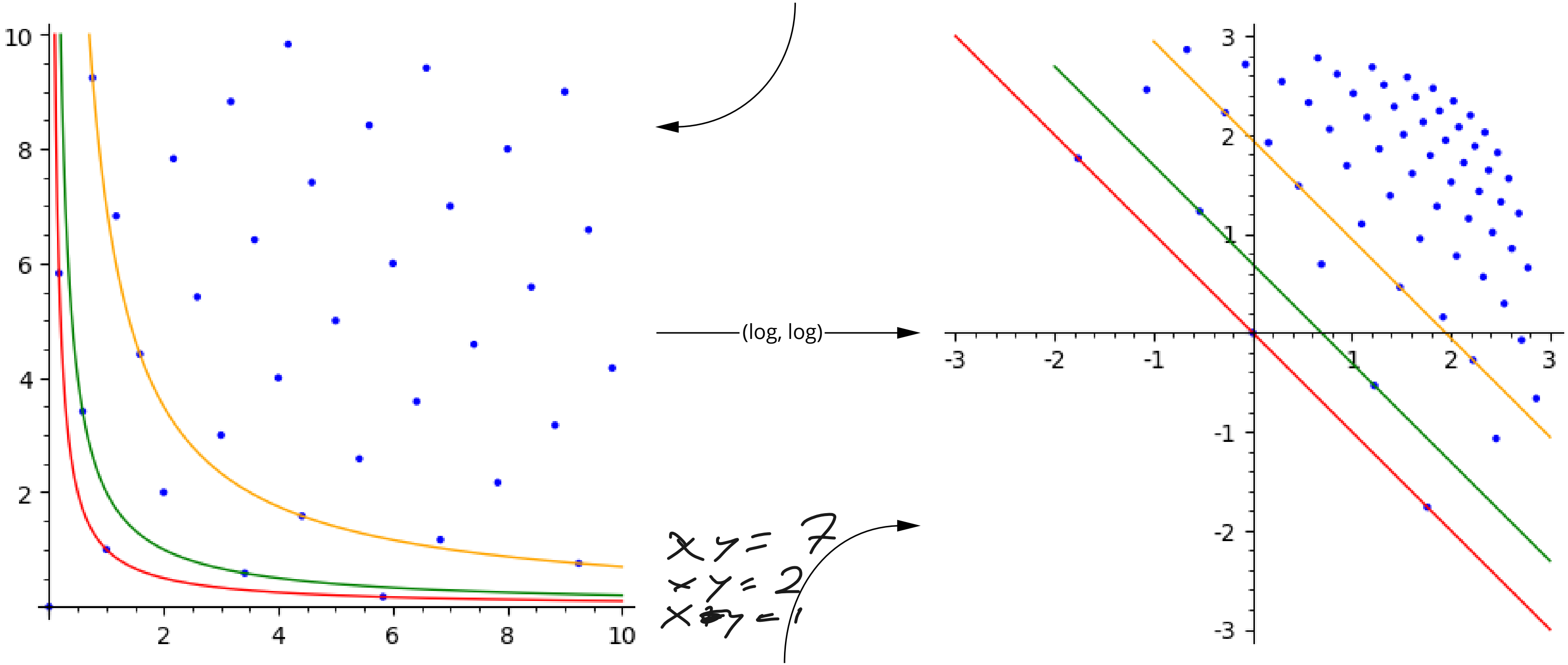
$K^\times \longrightarrow K_{\mathbb{R}}^\times \xrightarrow{\log} \underline{\mathbb{R}^{r_1+r_2}}$ lands in a hyperplane

(trace-zero hyperplane).

$$\underline{H} = \Big\{ 0 = \sum_{\tau \text{ real}} x_\tau + \sum_{\substack{\tau \text{ complex,} \\ \text{one per pair}}} 2x_\tau \Big\}$$

Visualization

```
l = [(a+b*sqrt(2.0), a-b*sqrt(2.0)) for a in range(-10,10) for b in range(-10,10)]
l = [(x,y) for x,y in l if 0 <= x and x <= 10 and 0 <= y and y <= 10]
list_plot(l, aspect_ratio=1) + plot(1/x,(x,0.1,10), color="red") + plot(2/x, (x,0.2,10), color="green") +
plot(7/x, (x,0.7,10), color="orange")
```




```
l = [(log(a+b*sqrt(2.0)), log(a-b*sqrt(2.0))) for a in range(-10,10) for b in range(-10,10) if (a+b*sqrt(2.0) > 0 and a-b*sqrt(2.0) > 0)]
l = [(x,y) for x,y in l if -10 <= x and x <= 10 and -10 <= y and y <= 10]
list_plot(l, aspect_ratio=1) + plot(-x, (-3, 3), color="red") + plot(log(2.0)-x, (-2, 3), color="green") + plot(log(7.0)-x, (-1, 3), color="orange")
```

The kernel of the logarithm map

Let $\mu(K)$ be the group of roots of unity in K.

This is a finite subgroup of $\mathcal{O}_K^*$

(if ζ is a primitive n-th root of unity,

$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) \to \infty$ as $n \to \infty$)

Lemma $\mu(K) =$ kernel of $\log : \mathcal{O}_K^* \to H$

Pf HW 1. (element of kernel is a root of monic poly $P(x) \in \mathbb{Z}[x]$ whose roots in $\mathbb{C}$ lie in unit disc.)

A lattice in the unit hyperplane

Theorem Image of $\mathcal{O}_K^\times$ in H is a lattice

$\Rightarrow \mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r_1 + r_2 - 1$

(Dirichlet unit theorem)

discrete

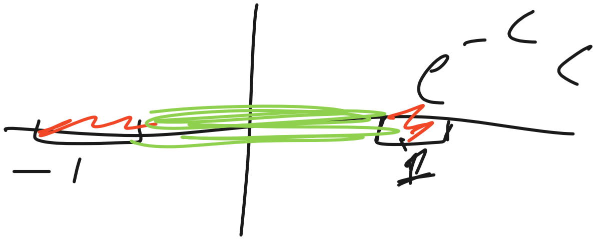
+ cocompact

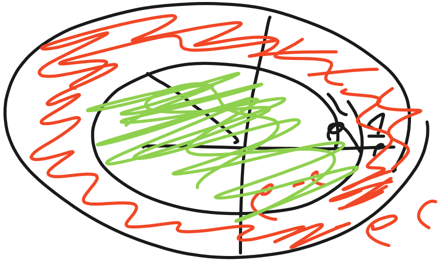
Discreteness

Lemma: For any $c > 0$, only finitely many units $\alpha \in \mathcal{O}_K^\times$ s.t. $-c < \log|\tau(\alpha)| < c$ $\forall$ embeddings τ of K.

$$\Updownarrow$$

$$e^{-c} < |\tau(\alpha)| < e^{c}$$





Much more is true!

Cocompactness (if time permits)

Interesting part!

Use ~~non units~~ to find units

integers of small norm.