Lecture 21: Geometry of Numbers II.

Recall: K a number field; $n = [K:\mathbb{Q}]$

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

$$k \longmapsto (\tau(k))$$

Gen F of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts on $K_{\mathbb{C}}$; fixed pts denoted $K_{\mathbb{R}} \cong \mathbb{R}^r \oplus \mathbb{C}^s$ where r = # of real embed. s = # of pairs of comp. embed.

The hermitian form

$$\langle \vec{x}, \vec{y} \rangle = \sum_{\tau} x_\tau \bar{y}_\tau \quad \text{on } K_{\mathbb{C}}$$

becomes a pos def. bilinear form on $K_{\mathbb{R}}$, the canonical metric.

Thm: $j(\mathcal{O}_K)$ is a complete lattice in $K_{\mathbb{R}}$.

Moreover, $\mathrm{Vol}(j(\mathcal{O}_K)) = \mathrm{Vol}\left(K_{\mathbb{R}}/j(\mathcal{O}_K)\right) = \sqrt{|\Delta_K|}$

Proof: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for $\mathcal{O}_K$.

Let $\vec{v}_i = j(\alpha_i) = (\tau_1(\alpha_i), \tau_2(\alpha_i), \ldots, \tau_n(\alpha_i))$ in $K_{\mathbb{R}}$.

Consider the Gram matrix $G = (\langle \vec{v}_i, \vec{v}_j \rangle)$. Now

$\det G = \mathrm{Vol}(j(\mathcal{O}_K))^2$ because if $\mathcal{B}$ is an orthonormal

basis for $K_{\mathbb{R}}$, then if $V = \begin{pmatrix} — \vec{v}_1 — \\ — \vec{v}_2 — \\ \vdots \\ — \vec{v}_n — \end{pmatrix}$ ← in basis $\mathcal{B}$

we have $G = VV^t$ and so

$\det G = (\det V)^2$. Now if $A = \begin{pmatrix} — \vec{v}_1 — \\ \vdots \\ — \vec{v}_n — \end{pmatrix}$ ← usual basis for $K_{\mathbb{C}}$

we have $G = A\bar{A}^t$ and

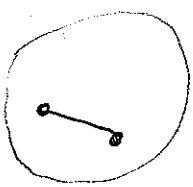
$(\det A)^2 = \Delta_K$. Thus $\mathrm{Vol}(j(\mathcal{O}_K))^2 = \det G = |\det A|^2 = |\Delta_K|$. ▨

[Query: Why didn't I just prove the first part of the thm?]

Cor: $\mathfrak{a} \subseteq \mathcal{O}_K$ an ideal. Then

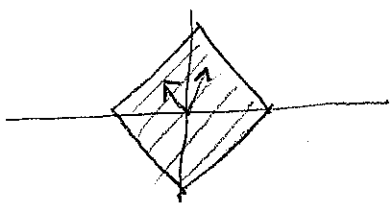
$$\mathrm{Vol}(j(\mathfrak{a})) = \mathcal{N}(\mathfrak{a})\sqrt{|\Delta_K|}$$

Minkowski's Lattice Point Theorem: Γ a complete lattice in a Euclidean vector space V of dim n. $X \subseteq V$ be a centrally symmetric convex subset. If $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma)$, then X contains some $\gamma \neq 0$ of Γ.

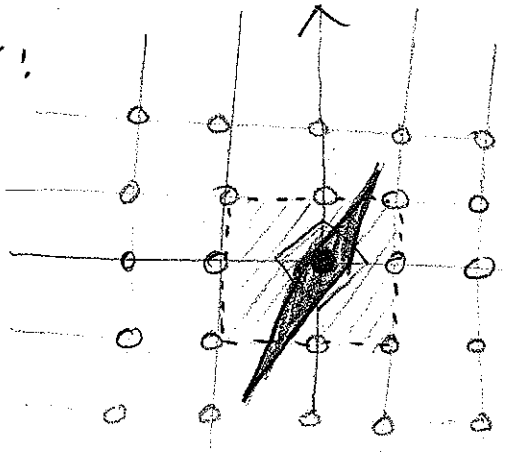
convex: 

$\vec{x}, \vec{y} \in X \Rightarrow$ line segment between them $\subseteq X$.

cent sym: $\vec{x} \in X \Rightarrow -\vec{x} \in X$



Ex:



We'll prove M.L.P.T next time, but first lets give an application.

Thm: $\mathfrak{a} \subseteq \mathcal{O}_K$ an ideal. Then $\exists\, a \neq 0$ in $\mathfrak{a}$ with

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}\, N(\mathfrak{a})$$

Pf: Let $c > 0$ be s.t. $c^n = A + \varepsilon$. Consider X in $K_{\mathbb{R}}$ given by $|z_\tau| \leq c$ for all τ. If $j(a) \in X$, then $|N(a)| = \prod_\tau |\tau(a)| \leq c^n = A + \varepsilon$. Now under $K_{\mathbb{R}} \cong \mathbb{R}^r \oplus \mathbb{C}^s$, we see $X = [-c,c]^r \times D_c^s$

So $\mathrm{Vol}_{can}(X) = (2c)^r \times \left(2\,\mathrm{Vol}_{Leb}(D_c)\right)^s = 2^{r+s} \pi^s c^{r+2s}$

$$= 2^n \sqrt{|\Delta_K|}\, N(\mathfrak{a}) + \varepsilon'$$

Thus by the M.L.P.T, $\exists\, a \in \mathfrak{a}$, $a \neq 0$ with $j(a) \in X$

$\Rightarrow N(a) \leq A + \varepsilon$. If we choose ε so that there are no ints in $(A, A+\varepsilon)$, this implies

$N(a) \leq A$ as desired. ▨

<u>Thm</u>: The class group $Cl_K = J_K / P_K$ ← principal ideals, ↖ fractional ideals
is finite.

<u>Pf</u>: There are only finitely many ideals of bounded norm, so E.T.S. every class $[\mathfrak{a}] \in Cl_K$ can be rep by $\mathfrak{a}' \subseteq \mathcal{O}_K$ with $N(\mathfrak{a}') \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|} = M$. ↖ int ideal.

Choose $\gamma \in \mathcal{O}_K$ s.t. $\mathfrak{b} = \gamma \mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. Now $\exists \alpha \neq 0$ in $\mathfrak{b}$ s.t. $|N_{K/\mathbb{Q}}(\alpha)| \leq M N(\mathfrak{b})$. Let $\mathfrak{a}' = \alpha \mathfrak{b}^{-1} = \alpha \gamma^{-1} \mathfrak{a} \subseteq \mathcal{O}_K$.
and note $N(\mathfrak{a}') = |N_{K/\mathbb{Q}}(\alpha)| N(\mathfrak{b})^{-1} \leq M$.
Since $[\mathfrak{a}'] = [\mathfrak{a}]$, we're done. ▨