Lecture 22: Class groups are finite / M.L.P.T.

Last time:

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

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

[s = # of pairs of comp. embed; dep on M.L.P.T.]

Thm: The class group $Cl_K = J_K / P_K$ (fractional ideals / principle ideals) is finite.

Pf: As there are finitely many primes of $\mathcal{O}_K$ above each nat'l prime, there a finitely many ideals of $\mathcal{O}_K$ with bounded norm. Thus, it suffices to show

Claim: Every elt in Cl_K can be rep by an integral ideal $\mathfrak{a}'$ with $N(\mathfrak{a}') \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|} = M$

Given $c \in Cl_K$, pick an int ideal $\mathfrak{a}$ with $[\mathfrak{a}] = c$.

[Idea: $N(\mathfrak{a})$ might be very large, e.g. if $\mathfrak{a} = (\delta)\mathfrak{a}'$ and $N(\delta)$ is large. So need to modify $\mathfrak{a}$...]

Let $\mathfrak{b} \subseteq \mathcal{O}_K$ be an ideal with $[\mathfrak{a}][\mathfrak{b}] = 1$

(i.e. pick $\gamma \in \mathcal{O}_K$ with $\gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$ and set $\mathfrak{b} = \gamma\mathfrak{a}^{-1}$)

If $\beta \in \mathfrak{b}$, then $[\mathfrak{a}] = [\mathfrak{b}^{-1}] = [\beta \mathfrak{b}^{-1}]$ and $\beta \mathfrak{b}^{-1} \subseteq \mathcal{O}_K$.

By this, can choose β so that $N_{K/\mathbb{Q}}(\beta) \leq M N(\mathfrak{b})$.

Let $\mathfrak{a}' = \beta \mathfrak{b}^{-1}$. Then $N(\mathfrak{a}') = N_{K/\mathbb{Q}}(\beta) N(\mathfrak{b})^{-1} \leq M$ as desired. ▨

Minkowski Lattice Point Theorem

Γ a complete lattice in a Euclidean vector space V of dim n. If $X \subseteq V$ is a centrally symmetric convex set with $\mathrm{Vol}(X) > 2^n \mathrm{Vol}(\Gamma)$, then X contains a non-zero element of Γ.

Pf: First we argue that it suffices to show

Claim: $\exists\, \gamma_1 \neq \gamma_2$ in Γ with $\left(\gamma_1 + \frac{1}{2}X\right) \cap \left(\gamma_2 + \frac{1}{2}X\right) \neq \emptyset$.

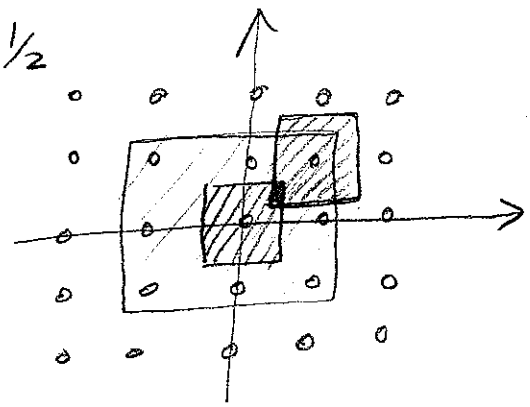
for if these sets intersect, say at

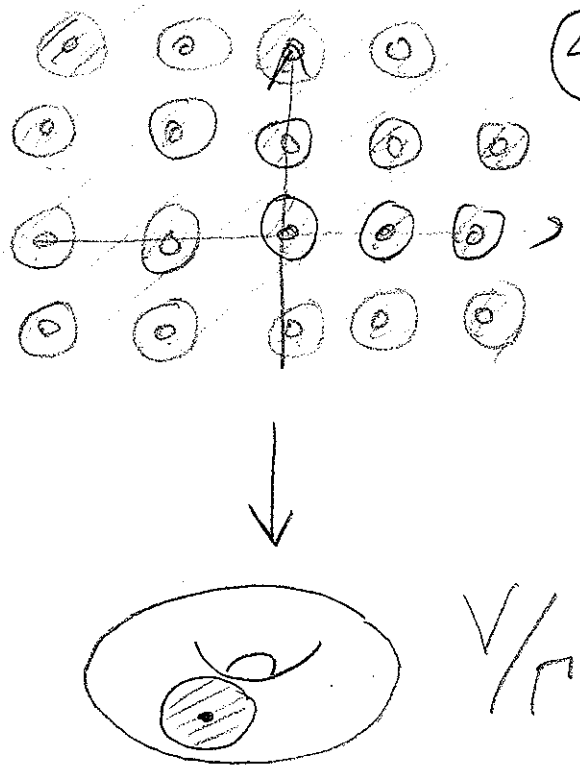
$p = \gamma_1 + \frac{1}{2}x_1 = \gamma_2 + \frac{1}{2}x_2$ where $x_i \in X$,

then $\gamma_1 - \gamma_2 = \frac{1}{2}x_1 - \frac{1}{2}x_2$ is in $\Gamma \cap X$.

trans $\frac{1}{2}X$ by γ_1

scale by $1/2$





V/Γ

Pf of Claim: Suppose not. Then $\frac{1}{2}X \to V/\Gamma$ is not injective. (if $y_1, y_2 \in \frac{1}{2}X$ map to the same pt, then $\gamma = y_1 - y_2 \in \Gamma$ and $\frac{1}{2}X \cap (\gamma + \frac{1}{2}X)$))

Thus $\underset{\|}{\mathrm{Vol}(\frac{1}{2}X)} \leq \mathrm{Vol}(V/\Gamma) = \mathrm{Vol}(\Gamma)$

$2^{-n}\mathrm{Vol}(X)$ a contradiction. ▨

On HW, you'll show that one can replace M in the first thm by $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}$

Cor: If $K = \mathbb{Q}(\sqrt{5})$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is a P.I.D. ($\Rightarrow$ it's a U.F.D.)

Pf: $cl_K = 1$ since every elt can be rep'd by an ideal with norm $\leq \frac{2!}{4}\sqrt{5} = \frac{\sqrt{5}}{2} \simeq 1.12\ldots$