Math 538 lecture 21, 27/3/2024

Recently: $K/\mathbb{Q}$ #field, $n = [K:\mathbb{Q}]$.
Then $\mathcal{O}_K \hookrightarrow K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R}$ is a lattice, of covolume $2^{-s}\sqrt{|d_K|}$ $\quad d_K = D_{K/\mathbb{Q}}$.

$\Rightarrow$ If $X \subset K_\infty$ is symmetric, convex, cpt, of volume $\geq 2^{n-s}\sqrt{|d_K|}$ then $\exists\, \alpha \in \mathcal{O}_K \cap X$, $\alpha \neq 0$
↑ Minkowski's thm

Application: $\leq$ finitely many K of deg n with $d_K \leq t$. Pf: choose X carefully, then the α created above has $K = \mathbb{Q}(\alpha)$.

Today: further discriminant bounds, class group, units

Theorem: $|d_K|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^n$

Pf: let $X_t = \{(x_v) \in K_\infty \mid \sum_{v|\infty} \|x_v\| \leq t\}$

Ex: $\mathrm{Vol}(X_t) = 2^r (2\pi)^s \frac{t^n}{n!}$.

Choose t s.t. $t^n = n!\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$ then
$\mathrm{vol}(X_t) = 2^{n-s}\sqrt{|d_K|}$.

Let $\alpha \in X_t \cap O_k$ be nonzero. Then

$$1 \le |N_{\mathbb{Q}}^K(\alpha)| = \prod_{v|\infty} \|\alpha\|_v \le \left(\frac{1}{n}\sum_{v|\infty}\|\alpha_v\|\right)^n \le \frac{1}{n^n} \cdot t^n$$

$$= \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_k|} \,. \quad \blacksquare$$

Cor: (Hermite) There are finitely many extensions of $\mathbb{Q}$ of discr $\le X$.

Pf: By stirling $n! \ll \sqrt{n}\,\frac{n^n}{e^n}$

so $|d_k|^{1/2} \gg \frac{1}{\sqrt{n}}\left(\frac{e\pi}{4}\right)^n \xrightarrow[n\to\infty]{} \infty$ since $\frac{e\pi}{4} > 1$

So if $|d_k| \le X$ then $[k:\mathbb{Q}] \ll_X 1$, then apply thm from last time

Cor: (Minkowski) $\mathbb{Q}$ has no unramified extensions

Pf: More precisely $n! \le \sqrt{2\pi n}\,\frac{n^n}{e^n}\,e^{1/12n}$

$\Rightarrow |d_k| \ge \frac{1}{2\pi n}\left(\frac{\pi e}{4}\right)^{2n} e^{-1/6n}$ grows exponentially

with n. Check small values to verify if $n \geq 1$, $|d_k| > 1$, so some prime divides d_k.

eg. at $n = 2$, $|d_k|^{1/2} > \frac{\pi}{2}$.

Finiteness of the class group

Fix # field K, deg n, discr d_k.
$\mathcal{O}_k$ = ring of integers. $Cl(K)$ = class group
= {fractional ideals} / {principal ideals}

Thm: Let $C_n = \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s$. Then every ideal class has a representative of norm at most

$$C_n^{-1} |d_k|^{1/2}$$

Pf: Let $\alpha \triangleleft \mathcal{O}_k$. Recall $N\alpha = [\mathcal{O}_k : \alpha]$, so image of α in K_∞ is a lattice of covol

$$N\alpha \cdot |d_k|^{1/2} 2^{-s}.$$

As in discr bound thm, choose t s.t.

$$t^n = n!\left(\frac{4}{\pi}\right)^s N\mathfrak{a}\,|d_k|^{1/2}$$

Then $\exists\ 0 \neq \alpha \in \chi_t \cap \mathfrak{a}$. For this α:

$$(N_{\mathbb{Q}}^K \alpha) \leq \frac{t^n}{n^n} = C_n^{-1} \cdot N\mathfrak{a} \cdot |d_k|^{1/2}.$$

Then $N(\alpha\mathfrak{a}^{-1}) = \frac{N\alpha}{N\mathfrak{a}} \leq C_n^{-1}|d_k|^{1/2}$

since $(\alpha) \subset \mathfrak{a}$, $\alpha\mathfrak{a}^{-1} \subset \mathcal{O}_k$ so is an ideal

$\Rightarrow$ class of $\mathfrak{a}^{-1}$ contains a rep of norm $\leq C_n^{-1}|d_k|^{1/2}$.

But class of $\mathfrak{a}^{-1}$ is an arbitrary ideal class. ∎

Cor: $\#Cl(K) < \infty$.

Pf: $\mathcal{O}_K \cong \mathbb{Z}^n$ as an abelian gp, hence has at most finitely many subgps of index $\leq C_n^{-1}|d_k|^{1/2}$

Dirichlet's Unit Theorem

Fix # field K, restrict injection $\mathcal{O}_K \hookrightarrow K_\infty$ to the units, get map $\mathcal{O}_K^\times \to K_\infty^\times$.
Apply norm to get map

$$\mathcal{O}_K^\times \to \prod_{v \mid \infty} \mathbb{R}_{>0}^\times$$

maps $\varepsilon \mapsto (\|\varepsilon\|_v)_{v \mid \infty}$.

Aside: $\mathbb{R}_{>0}^\times$ is cocompact in $\mathbb{R}^\times$, $\mathbb{C}^\times$ (complements $\{\pm 1\}$, S^1 resp.)

compose with the logarithm $\mathbb{R}_{>0}^\times \xrightarrow{\sim} \mathbb{R}^+$, get map

$$\log : \mathcal{O}_K^\times \to \mathbb{R}^{r+s}$$

$$\varepsilon \mapsto (\log \|\varepsilon\|_v)_{v \mid}$$

Recall the pdt formula $\prod_{v \in |K|} \|\varepsilon\|_v = 1$

Note if v is finite, $\varepsilon \in \mathcal{O}_v^*$ so $\|\varepsilon\|_v = 1$.

$\Rightarrow \prod_{v \in |K|_\infty} \|\varepsilon\|_v = 1 \Leftrightarrow \sum_{v|\infty} \log \|\varepsilon\|_v = 0.$

$\Rightarrow$ image of log lies in the hyperplane $\sum_v y_v = 0$

<u>Lemma:</u> The image of $\mathcal{O}_K^\times$ in $\mathbb{R}^{r+s}$ is discrete.

<u>Pf:</u> Suppose $|\log \|\varepsilon\|_v| \leq 1$ for all v,

in which case $\|\varepsilon\|_v \leq e$ for all v.

By discreteness of $\mathcal{O}_K$ in K_∞, at most finitely many such ε.

(Equiv: if $X \subset \mathbb{R}^{r+s}$ is cpt, then

$$\{x \in K_\infty : \log|x| \in X\} = \prod_{v|\infty} (\text{sphere of } K_v) \times \exp(X)$$

so is cpt.)

<u>Cor:</u> Image of log is isom to $\mathbb{Z}^t$ for $0 \leq t \leq r+s-1$

Lemma (Kronecker) Let $\alpha \in \mathcal{O}_{\mathbb{Q}}$ be non-zero, has all its conjugates in the unit disc. Then α is a root of unity.

Pf: Ex

Cor: The kernel of log consists of the roots of unity in K, is finite

Pf: if $\log \alpha = 0$ then $\|\alpha\|_v = 1$ for all $v \mid \infty$

By Kronecker, α is a root of unity.

Conversely, if $\alpha^m = 1$, then $|\alpha| = 1$ for any absolute value on K.

If $\zeta_m \in K$, then $\mathbb{Q}(\zeta_m) \subset K$, so $n \geq \phi(m)$
$= [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$

But $\phi(m) \to \infty$ as $m \to \infty$, so only finitely many roots of unity in K.

$\Rightarrow$ Kernel of log = torsion of $\mathcal{O}_K^\times$.

$\Rightarrow \mathcal{O}_K^\times \cong \mu_m \times \mathbb{Z}^t$ where μ_m = roots of unity of order $\mid m$
$\cong C_m$ as a gp

Thm: (Dirichlet) $t = r+s-1$, $\log \mathcal{O}_K^\times$ is a lattice in the hyperplane.

(Better: $\mathcal{O}_K^\times$ is a lattice in $\{x \in \prod_{v|\infty}^{K_\infty^\times} K_v^\times \mid \prod_{v|\infty} \|x\|_v = 1\}$)

Examples: (1) $K = \mathbb{Q}$, $r=1$, $s=0$, $\mathbb{Z}^\times = \{\pm 1\}$

(2) $\mathbb{Q}(\sqrt{-d})$, $r=0$, $s=1$, $\mathcal{O}_K^\times$ = roots of unity.
CPS1: check which $\mathbb{Q}(\sqrt{-d})$ contain roots of unity other than ± 1.

(3) $K = \mathbb{Q}(\sqrt{2})$, $r=2$, $s=0$. $r+s-1 = 1$

$$\mathcal{O}_K^\times = \{\pm(1+\sqrt{2})^n\}_{n\in\mathbb{Z}}$$

coset of $\mathcal{O}_K^\times$ in hyperplane is $\log(1+\sqrt{2})$

(4) $K = \mathbb{Q}(\sqrt{d})$ unit $\leftrightarrow$ Pell's equation $N\epsilon = \pm 1$.

(5) $K = \mathbb{Q}(\sqrt[3]{2})$ $r=1$, $s=1$, $r+s-1=1$,

$$\mathcal{O}_K^\times = \{\pm(1-\sqrt[3]{2})^n\}_{n\in\mathbb{Z}}$$

Pf of unit thm

Lemma: For each $v_0 \mid \infty$ there is $\varepsilon \in \mathcal{O}_k^\times$ s.t. $|\varepsilon|_v < 1$ if $v \neq v_0$.

Pf: Let $M > 2^s |d_k|$. Identify $K_\infty \cong \mathbb{R}^n$ consider the rectangle

$$X_\delta = [-M\delta^{-(n-1)}, M\delta^{-(n-1)}] \times [-\delta, \delta]^{n-1}$$

↑ co-ord in V_0

$\mathrm{vol}(X_\delta) = 2^n \cdot M$, so for all $\delta > 0$, $X_\delta \cap \mathcal{O}_k \neq \{0\}$

If $\alpha \in \mathcal{O}_k \cap X_\delta$, $N\alpha$ bdd in terms of M

$\Rightarrow$ Elements α have finitely many norms

$\Rightarrow$ Ideals (α) have bdd norm
$\Rightarrow$ see finitely many such ideals
$\Rightarrow$ Have infinite sequence $\alpha_i \in X_{\delta_i} \cap \mathcal{O}_k \setminus \{0\}$ s.t. $\delta_i \to 0$ and (α_i) all equal. Then $\alpha_i \alpha_j^{-1}$ is a unit for all i, j. Fix j, let $i \to \infty$, $|\alpha_i \alpha_j^{-1}|_v \to 0$

if $v \neq v_0$, so for i large enough $\epsilon = \sigma_i \sigma_j^{-1}$ has $|\epsilon|_v < 1$ if $v \neq v_0$.

Lemma: Let $V = \left(\begin{smallmatrix}1\\ \vdots \\ 1\end{smallmatrix}\right)^{\perp} = \{\underline{v} \in \mathbb{R}^n \mid \sum_i v_i = 0\}$

Let $\{\underline{v}^i\}_{i=1}^{n-1} \subset V$ be such that $v_j^i < 0$ if $j \neq i$.

Then $\{\underline{v}^i\}_{i=1}^{n-1} \subset V$ are linearly indep.

Def: The regulator of K, denoted R_K, is the covolume of U_K^x in the hyperplane.

$$\Rightarrow \quad R_K = \left|\det\left(\log|u_i|_v\right)_{i,v}\right|$$

where v runs over infinite places, u_i run over basis of U_K^x/μ_m.

(omit one place).

$\#Cl(\mathbb{Q}(\sqrt{d})) \xrightarrow[d\to\infty]{} \infty$

Cohen-Lenstra Heuristics:

$Cl(\mathbb{Q}(\sqrt{d}))$ is a random abelian group

Ex: A = set of isom classes of finite abelian groups

$$Z = \sum_{A \in A} \frac{1}{\#Aut(A)} < \infty$$

Conj:
$$\frac{\#\{d < X \text{ squarefree} \mid Cl(\mathbb{Q}(\sqrt{d})) \cong A\}}{\#\{d < X \text{ squarefree}\}} \xrightarrow[X\to\infty]{} \frac{1/\#Aut(A)}{Z}$$