Math 538, Lecture 20, 22/3/2024

Last time: Lattices
(discrete co-compact subgroups $\Lambda < V$
V = real vsp f.d.)

Call $\underline{v} \in \mathbb{Z}^d$ primitive if gcd(entries) = 1
$\Leftrightarrow$ if $\underline{v} = \alpha \underline{u}$ for $\underline{u} \in \mathbb{Z}^d$ then $\alpha = \pm 1$.
(makes sense in any free $\mathbb{Z}$-module)
Ex: $\underline{v}$ is primitive iff $\exists \{\underline{v}_i\}_{i=1}^d \subset \mathbb{Z}^d$ free basis with $\underline{v}_1 = \underline{v}$
(a subgp H is primitive if $(\mathrm{span}_{\mathbb{Q}} H) \cap \mathbb{Z}^d = H$
if $\{v_i\}_{i=1}^r$ $\mathbb{Z}$-span a primitive subgp can extend to $\{v_i\}_{i=1}^{d}$)

Saw: $\Lambda < \mathbb{R}^n$ is (1) discrete iff $\Lambda = \mathrm{Span}_{\mathbb{Z}} \{\underline{v}_i\}_{i=1}^r$ s.t. $\{\underline{v}_i\}_{i=1}^r$ are indep/$\mathbb{R}$.
(2) cocompact iff cofinite iff $r = n$

In that case $\mathcal{F} = \{ \sum_{i=1}^n a_i \underline{v}_i \mid a_i \in [0,1] \}$
(or $a_i \in [-\frac{1}{2}, \frac{1}{2}]$)
surjects on $\mathbb{R}^n/\Lambda$, injects up to a set of measure 0.

Claim: $\#(\Lambda \cap B(R)) \sim \frac{\mathrm{vol}(B(R))}{\mathrm{vol}(\mathcal{F})}$ as $R \to \infty$

Cor: $\mathrm{vol}(\mathcal{F})^{-1} = \lim_{R\to\infty} \frac{\#(\Lambda \cap B(R))}{\mathrm{vol}(B(R))}$ is indep of $\mathcal{F}$

$\quad\quad \mathrm{vol}(\mathbb{R}^n/\Lambda)$

Pf: let $\mathcal{F}$ be a bounded fundamental domain, say $\mathrm{diam}(\mathcal{F}) \leq B(D)$

consider $\bigcup_{\lambda \in \Lambda \cap B(R)} (\lambda + \mathcal{F}) \subseteq B(R+D)$

Conversely, let $x \in B(R-D)$. Then $\exists \lambda \in \Lambda$ st. $x - \lambda \in \mathcal{F}$.

$\Rightarrow |\lambda| \leq |x| + D \leq R$ so $\lambda \in \Lambda \cap B(R)$

Thus $B(R-D) \subseteq \bigcup_{\lambda \in \Lambda \cap B(R)} (\lambda + \mathcal{F}) \subseteq B(R+D)$

Take volume. If $\mathrm{vol}(\partial \mathcal{F}) = 0$ then
$$\mathrm{vol}\Big(\bigcup_{\lambda \in \Lambda \cap B(R)} (\lambda + \mathcal{F})\Big) = \#(\Lambda \cap B(R)) \cdot \mathrm{vol}(\mathcal{F})$$

$$\Rightarrow \frac{\mathrm{vol}(B(R-D))}{\mathrm{vol}(B(R))} \leq \frac{\#(\Lambda \cap B(R))}{\mathrm{vol}(B(R))} \cdot \mathrm{vol}(\mathcal{F}) \leq \frac{\mathrm{vol}(B(R+D))}{\mathrm{vol}(B(R))}$$

But $vol(B(R)) = c_n \cdot R^n$

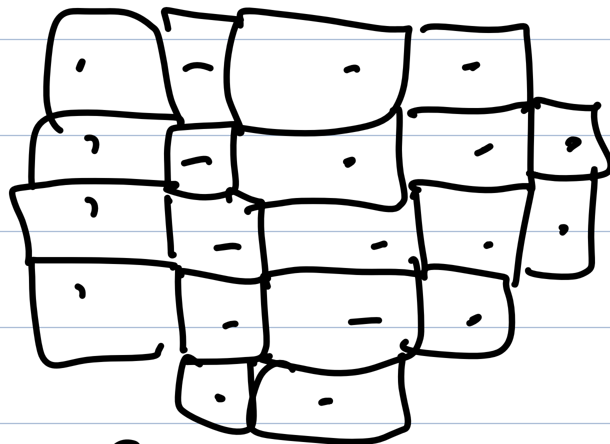
and

$$\frac{(R \pm O)^n}{R^n} = 1 + O\left(\frac{1}{R}\right) \xrightarrow[R\to\infty]{} 1$$

$\blacksquare$

Today: Examples, produce lattice points, Apply to # fields

($\mathbb{Z}^n \subset \mathbb{R}^n$



$\{$squares contained in disc$\} \subset$ disc $\subset \{$squares that meet disc$\}$

difference are squares that meet circle. their number is prop. to length of circle.

Thm: (Minkowski) Let $\Lambda \subset \mathbb{R}^n$ be a lattice, let $\mathfrak{X} \subset \mathbb{R}^n$ be convex, bounded, symmetric about origin ($\underline{x} \in \mathfrak{X}$ iff $-\underline{x} \in \mathfrak{X}$).

Suppose $vol(\mathfrak{X}) \geq 2^n vol(\mathbb{R}^n/\Lambda)$. (in case of equality also $\mathfrak{X}$ is closed)

Then $\exists\, \lambda \in (\Lambda \cap \mathfrak{X}) \setminus \{0\}$.

Taking $\Lambda = \mathbb{Z}^n$, $\mathfrak{X} = (-1,1)^n$ shows 2^n is best possible.

Pf: Suppose $\mathrm{vol}(\mathfrak{X}) > 2^n \mathrm{covol}(\Lambda)$, assume $\mathfrak{X} \cap \Lambda = \{0\}$

$\Rightarrow$ translates of $\frac{1}{2}\mathfrak{X}$ by Λ are disjoint.

(if $\underline{x} \neq \underline{y} \in \mathfrak{X}$, $\lambda \in \Lambda$ s.t. $\frac{1}{2}\underline{y} = \frac{1}{2}\underline{x} + \lambda$ then $-\underline{x} \in \mathfrak{X}$ so $\lambda = \frac{1}{2}((-\underline{x}) + (\underline{y})) \in \mathfrak{X}$, $\lambda \neq \underline{0}$ since $\underline{x} \neq \underline{y}$.)

But then $\mathrm{vol}\left(\bigcup_{\lambda \in B(R) \cap \Lambda} (\frac{1}{2}\mathfrak{X} + \lambda)\right)$

$$= \#(B(R) \cap \Lambda) \cdot \mathrm{vol}(\tfrac{1}{2}\mathfrak{X}) \leq \mathrm{vol}(B(R+D))$$

$\frac{1}{2}\mathfrak{X} \subseteq B(D)$

$$\Rightarrow \mathrm{vol}(\tfrac{1}{2}\mathfrak{X}) \leq \frac{\mathrm{vol}(B(R+D))}{\#(B(R) \cap \Lambda)} \xrightarrow[R\to\infty]{} \mathrm{vol}(\mathbb{R}^n/\Lambda) \Rightarrow \Leftarrow$$

Suppose $\mathrm{vol}(\frac{1}{2}\overline{\mathfrak{X}}) = \mathrm{vol}(\mathbb{R}^n/\Lambda)$

Then for any $1 > \varepsilon > 0$, have $\underline{0} \neq \lambda_\varepsilon \in (1+\varepsilon)\mathfrak{X} \cap \Lambda$

Since Λ is discrete, $2\mathfrak{X}$ bdd, $\Lambda \cap 2\mathfrak{X}$ finite, so λ_ε constant from some point on

Then $\lambda = \lambda_\varepsilon \in \bigcap_{\varepsilon>0} (1+\varepsilon)\,\Sigma = \Sigma$ if Σ closed & cpt. ∎

$(\Leftarrow \exists \varepsilon > 0$ st. $N_\varepsilon(\Sigma) \cap \Lambda = \Sigma \cap \Lambda)$

Examples of lattices:

$\mathbb{Z}^n \subset \mathbb{R}^n$, $\mathbb{Z}[i] \subset \mathbb{C}$

$\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ not a lattice: $1, \sqrt{2}$ linearly dep

in fact, $\mathbb{Z}[\sqrt{2}]$ is dense!

But $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}^2$ is a lattice with embedding

$\mathbb{Z}[x]/(x^2-2) \to \mathbb{R}^2$

$a+bx \mapsto (a+b\sqrt{2},\ a-b\sqrt{2})$

(indeed $(1,0)$, $(\sqrt{2}, -\sqrt{2})$ indep / $\mathbb{R}$)

$\mathbb{Z}[\sqrt[3]{2}] \subset \mathbb{R}$ also dense

$= \{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a,b,c \in \mathbb{Z} \}$

But

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto$$

$$\mapsto \left(a + b\sqrt[3]{2} + c\sqrt[3]{4},\ a + b\sqrt[3]{2}\,\omega + c\sqrt[3]{4}\,\omega^2\right) \in \mathbb{R} \times \mathbb{C}$$

$\left(\omega = \frac{-1+\sqrt{-3}}{2}\right)$ is discrete: $(1,1)$, $(\sqrt[3]{2}, \sqrt[3]{2}\,\omega)$, $(\sqrt[3]{4}, \sqrt[3]{4}\,\omega^2)$

$\mathbb{R}$-indep in $\mathbb{R} \times \mathbb{C}$.

---

§2. Discrimant bounds

Lemma: For a #field K, the image of $\mathcal{O}_K$ in $K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R}$ is a lattice, of covolume

$$2^{-s}\sqrt{|d_K|}.$$

d_K: abs discr $= D_{K/\mathbb{Q}}$, s = # of complex places of K

Pf: Let $T \subset \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ be a set of representatives for ∞ places of K (orbit reps for complex conj)

Write $T = T_{\mathbb{R}} \sqcup T_{\mathbb{C}}$

Let $\iota: K \to K_\infty = \prod_{\tau \in T} K_\tau$ be the diagonal map

ι induces isom $K \otimes_{\mathbb{Q}} \mathbb{Q}_\infty \to K_\infty$

$\Rightarrow \iota$ maps $\mathbb{Q}$-bases of K to $\mathbb{R}$-bases of K_∞

Now $\mathcal{O}_K$ is $\mathbb{Z}$-span of $\mathbb{Q}$-basis of K,
so $\iota(\mathcal{O}_K) = \mathbb{Z}$-span of $\mathbb{R}$-basis of K_∞.

[Alternative: Let $B = \prod_{\tau \in T} B_\tau \subset K_\infty$ be a pdt of balls of rad R.

Suppose $\iota(\alpha) \in B \Rightarrow$ all Galois conjugates of α have magnitude $\leq R$
$\Rightarrow$ Coeff of poly $\prod_{\mu \in \mathrm{Hom}(K,\mathbb{C})} (x - \mu(\alpha))$ are bounded

But $\mathbb{Z} \subset \mathbb{R}$ discrete $\Rightarrow$ finitely many such poly
$\Rightarrow$ finitely many such α]

On K_∞ define inner pdt by

$$\langle (x_\tau), (y_\tau) \rangle = \sum_\tau x_\tau \bar{y}_\tau$$

Then if $w_i, w_j \in \mathcal{O}_K$, $\langle \iota(w_i), \iota(w_j) \rangle = \sum_\tau \tau(w_i) \bar{\tau}(w_j)$

Also set $(w, w') = \sum_{\nu \in \mathrm{Hom}(K,\mathbb{C})} \nu(w)\,\bar{\nu}(w')$

$\det\left((w_i, w_j)_{ij}\right) = |d_K|^2$. ∎

Thm: Fix a field K. There are finitely many extensions of K of degree n with any particular discriminant.

Pf: Enough to count extensions of $\mathbb{Q}$ of degree n, discr $\leq d$, enough to count $L/\mathbb{Q}$ s.t. $i \in L$.

$\mathrm{discr}(L(i)/\mathbb{Q})$ is bdd in terms of $\mathrm{discr}(L/\mathbb{Q})$

So counting totally complex L. Fix $v_0 \in |L|_\infty$

Let $X = \left\{ (x_v)_v \in L_\infty \;\middle|\; \begin{array}{l} |\mathrm{Im}\, x_{v_0}| \leq C\sqrt{d} \\ |\mathrm{Re}\, x_{v_0}| < 1 \end{array}, \; \begin{array}{l} \forall v \neq v_0 \\ |x_v| < 1 \end{array} \right\}$

Clearly X is convex, symmetric about 0 has volume $C'\sqrt{d}$ for some C' depending on C, n.

Can choose C s.t. $C' > 2^n \cdot 2^{-n/2} \cdot \sqrt{|d_L|}$
$= 2^n \cdot \mathrm{vol}(L_\infty / \mathcal{O}_L)$.

$\Rightarrow \exists \alpha \in \mathcal{O}_L \cap X, \; \alpha \neq 0$

$N^L_{\mathbb{Q}} \alpha \geq 1 \Rightarrow |\alpha|_{v_0} > 1 \Rightarrow |\operatorname{Im} \alpha_{v_0}| \neq 0$

$\Rightarrow$ all Galois cojugates of α are distincts

$\Rightarrow \alpha$ has deg $n / \mathbb{Q}$

$\Rightarrow L = \mathbb{Q}(\alpha)$.

But coeff of min poly of α are bdd in terms of $d, n \Rightarrow$ at most finitely many such α.