Math 538, lecture 19, 20/3/2024

Last time: $K = \mathbb{Q}(\zeta_n)$

Saw: $\Phi_n = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a)$ is irred,

$[K:\mathbb{Q}] = \phi(n)$, $\quad x^n - 1 = \prod_{d|n} \Phi_d(x)$ in $\mathbb{Z}[x]$.

Key tool: ramification.

Thm: $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

Pf: Proof by induction on number of prime divisors of n

Say $n = p^r m$, $(p, m) = 1$, write $M = \mathbb{Q}(\zeta_m)$
so $K = M(\zeta_{p^r})$

By induction, $\mathcal{O}_M = \mathbb{Z}[\zeta_m]$ Want: $\mathcal{O}_K = \mathcal{O}_M[\zeta_{p^r}]$.

Know p unram in $M/\mathbb{Q}$, say $p\mathcal{O}_M = \prod_j P_j$.

$\Phi_{p^r}(Y+1) \in \mathbb{Z}[Y]$ is p-Eisenstein

$\Rightarrow$ also $\mathfrak{p}_j$ - Eisenstein for all j.
(const coeff only has 1 p so only one $\mathfrak{p}_j$)
$\Rightarrow \Phi_{p^r}$ irred in $\mathcal{O}_M$.

Thus K/M is totally ramified over each $\mathfrak{p}_j$.
get single prime $\mathfrak{P}_j$ of K over each $\mathfrak{p}_j$

Recall $\pi = 1 - \zeta_{p^r}$. $\pi \mid p$ so (π) is a pdt of the $\mathfrak{P}_j$.

But $(\pi)^e = (p)$

where $e = \phi(p^r) = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = [K:M]$

<u>Recall:</u> $(p) = \prod_j \mathfrak{p}_j = \prod_j \mathfrak{P}_j^e = (\prod_j \mathfrak{P}_j)^e$

So $(\pi) = \prod_j \mathfrak{P}_j$, hence

$$\mathcal{O}_K / \pi \mathcal{O}_K \overset{\text{CRT}}{\cong} \prod_j \mathcal{O}_K / \mathfrak{P}_j \underset{\text{total ramification}}{\cong} \prod_j \mathcal{O}_M / \mathfrak{p}_j$$

$\overset{\text{CRT}}{\cong} \mathcal{O}_M / (p)$

Now repeat argument from before. $\blacksquare$

(set: $\mathcal{O}_K = \mathbb{Z}[\zeta_n] \to \mathcal{O}_K$)

Prop: $|D_K| = \left(\prod_{p^r \| n} p^{\frac{rp-r-1}{p-1}}\right)^{\phi(n)} = \dfrac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}$

$D_K = D_{K/\mathbb{Q}}$.

Pf: HW

Lemma: (Brill) Let K be any # field. Then the sign of D_K is $(-1)^s$, $s = $ # of complex places.

Pf: Fix integral basis $\{w_i\}_{i=1}^n$ of $\mathcal{O}_K$, $n = [K:\mathbb{Q}]$. $a_{ij} = \sigma_j(w_i)$, $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_j\}_j$

Then $\bar{A}$ is obtained from A by permuting the $\{\sigma_j\}$, specifically by swapping each pair of equivalent embeddings.
This premutation is a product of s 2-cycles so has det $(-1)^s$

$$\Rightarrow \overline{\det(A)} = \det(\bar{A}) = (-1)^s \cdot \det(A)$$

$$\Rightarrow \underbrace{|\det(A)|^2}_{|D_K|} = (-1)^s \cdot (\det(A))^2 = (-1)^s \cdot D_K$$

∎

Example: An everywhere unramified extension

Lemma: K field, $f \in K[x]$, $\Delta = \Delta(f)$.
Then any splitting field for f contains $\sqrt{\Delta}$.

Pf: $\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2 \qquad (f = \prod_i (x - \alpha_i))$

so $\sqrt{\Delta} = \prod_{i<j} (\alpha_i - \alpha_j) \in K(\{\alpha_i\})$

Lemma: Let $f \in \mathbb{Z}[x]$ be monic, L = splitting field of f. Suppose that $\Delta = \Delta(f) \in \mathbb{Z}$ is squarefree, set $K = \mathbb{Q}(\sqrt{\Delta})$.
Then L/K is everywhere unramified

Pf: D_K is divisible by all $p \mid \Delta$
$\Rightarrow D_L$ " " " " "

But $D_L \mid \Delta \Rightarrow |D_L| = |D_K| = |\Delta|$

so $D_{L/K} = (1)$

warning: to be fixed next time

Chapter 4: "Geometry of Numbers"

Minkowski: study $\mathcal{O}_K$ via embedding

$$\mathcal{O}_K \hookrightarrow K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R}$$

---

§1 Lattices in $\mathbb{R}^n$

Remark: more natural to work in a real vsp V.

Lemma: A subgp $\Lambda \subset \mathbb{R}^n$ is discrete iff $\Lambda = \bigoplus_i \mathbb{Z} v_i$, $\{v_i\}_i \subset \mathbb{R}^n$ lin. indep

Pf: Since $GL_n(\mathbb{R})$ acts transitively on indep subsets of size k, acts by homeos, so enough to prove discreteness for $\Lambda = \bigoplus_{i=1}^{k} \mathbb{Z} e_i$ $\{e_i\}$ std basis
But this $\Lambda \cong \mathbb{Z}^n$.

Converse: Let $\Lambda \subseteq \mathbb{R}^n$ be discrete.
let v_1 be the shortest vector in $\Lambda \setminus \{0\}$.

observe: $\mathbb{R}\underline{v}_1 \cap \Lambda = \mathbb{Z}\underline{v}_1$: if $\alpha \underline{v}_1 \in \Lambda$
also $\{\alpha\}\underline{v}_1 = \alpha\underline{v}_1 - [\alpha]\underline{v}_1 \in \Lambda$ so $\{\alpha\} = 0$.

Say we have chosen $\{\underline{v}_1, .., \underline{v}_r\}$ indep / $\mathbb{R}$,

s.t. $\Lambda \cap \underbrace{\mathrm{Span}_{\mathbb{R}}\{\underline{v}_i\}_{i=1}^{r}}_{V_r} = \mathrm{Span}_{\mathbb{Z}}\{\underline{v}_i\}_{i=1}^{r}$.

Suppose $\Lambda \nsubseteq V_r$. Then let $\underline{v}_{r+1} \in \Lambda \setminus V_r$ be such that its $\perp$ component is shortest.

Observation: $V_r / \Lambda \cap V_r$ is cpt:
Pf: $\{\sum_{i=1}^{r} a_i \underline{v}_i : \underline{a} \in [-\frac{1}{2}, \frac{1}{2}]^r\}$ surjects
or $[0,1]^r$

say $u_j \in \Lambda \setminus V_r$ have $u_j = u_j^\perp + u_j^{\parallel}$, $u_j^{\parallel} \in V_r$, $u_j^\perp \perp V_r$
have $u_j^\perp \to \inf\{\|u^\perp\| : u \in \Lambda \setminus V_r\}$
Modulo $\Lambda \cap V_r$ may assume $u_j^{\parallel} \in$ cpt set.
Also $\|u_j^\perp\|$ bdd so $\{u_j\} \subset \Lambda \cap$ cpt = finite.
Set $V_{r+1} = V_r \oplus \mathbb{R}\underline{v}_{r+1}$.

let $\underline{v} \in \Lambda \cap V_{r+1}$. want: $\underline{v} \in (\Lambda \cap V_r) \oplus \mathbb{Z}\underline{v}_{r+1}$

Write $\underline{v} = \underline{v}^{\perp} + \underline{v}^{\parallel}$, note: $\underline{v}^{\perp} \in \mathbb{R}\, \underline{v}_{r+1}^{\perp}$

say $\underline{v}^{\perp} = \alpha\, \underline{v}_{r+1}^{\perp}$, then $\Lambda \ni (\underline{v} - [\alpha]\underline{v}_{r+1})^{\perp} = \{\alpha\}\, \underline{v}_{r+1}^{\perp}$

must be 0. So $\underline{v} - [\alpha]\,\underline{v}_{r+1} \in V_r \cap \Lambda$ ∎

__Cor:__ If $\Lambda \subset V$ is discrete, $\operatorname{span}_{\mathbb{R}} \Lambda / \Lambda$ is cpt.

$$\cong (\mathbb{R}/\mathbb{Z})^d = \mathbb{R}^d/\mathbb{Z}^d, \quad d = \operatorname{rk}\Lambda$$

$\Rightarrow$ __Lemma:__ Λ is $\mathbb{Z}$-span of basis of V iff V/Λ is cpt.

($V/\Lambda = (\operatorname{span}_{\mathbb{R}} \Lambda / \Lambda) \oplus (\operatorname{span}_{\mathbb{R}} \Lambda)^{\perp}$)

(also iff V/Λ has finite volume)

__Def:__ A subgp $\Lambda \subset \mathbb{R}^n$ is a lattice if it's the $\mathbb{Z}$-span of a basis, equiv if it's discrete and cocompact, equiv. if it's discrete and $\operatorname{vol}(\mathbb{R}^n/\Lambda) < \infty$.

($SL_n(\mathbb{Z})$ is discrete in $SL_n(\mathbb{R})$, has finite covolume, <u>not</u> co compact).

<u>Notation</u>; $\mathcal{F} = \{ \sum_{i=1}^{n} a_i \underline{v}_i \mid |a_i| \leq \frac{1}{2} \} \subset \mathbb{R}^n$
(Call this a fundamental domain for Λ)

<u>Note</u>; $\bigcup_{\underline{\lambda} \in \Lambda} (\mathcal{F} + \underline{\lambda}) = \mathbb{R}^n$

<u>Def</u>; The covolume of Λ is the volume of $\mathcal{F}$.

$$= |\det(\underline{v}_1 \cdots \underline{v}_i \cdots \underline{v}_n)| = \sqrt{\det((\langle \underline{v}_i, \underline{v}_j \rangle)_{ij})}$$

<u>Prop</u>; $\# \{ \lambda \in \Lambda \cap B(0,R) \} \sim \dfrac{\mathrm{vol}(B(R))}{\mathrm{vol}(\mathcal{F})}$.

<u>Cor</u>; $\mathrm{vol}(\mathcal{F})$ indep of choice of $\mathcal{F}$.

---

volume: wrt Lebesgue measure on $\mathbb{R}^d$.

($\exists$ unique (up to scaling) $\mathbb{R}^d$-inv't measure on $\mathbb{R}^d$)

fix inner pdt set volume of unit cube to 1