Lecture 19: Frobenius Automorphisms

HW#6: Due Friday Mar 20.
Marcus Ch 3: 17, 27 + others T.B.A.

L/K normal, $\mathfrak{p}$ in $\mathcal{O}_K$ unramified in $\mathcal{O}_L$.

$$\begin{array}{ll} L = L_E & \mathfrak{P} \\ \mid & \\ L_D & \mathfrak{P}_D \\ \mid & \\ K & \mathfrak{p} \end{array}$$

Recall: $D \longrightarrow \mathrm{Gal}\left(K(\mathfrak{P})/K(\mathfrak{p})\right)$ is surjective, where $K(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$ and $K(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_{L_D}/\mathfrak{P}_D$

As $E = 1$, we have

$$D \cong \underbrace{\mathrm{Gal}\left(K(\mathfrak{P})/K(\mathfrak{p})\right)}_{\text{normal}} = \text{cyclic group gen by the Frobenius auto } \bar{\phi}: K(\mathfrak{P}) \circlearrowleft \text{ where } \bar{\phi}(\alpha) = \alpha^{N(\mathfrak{p})}$$

The cor. elt $\phi \in D$, is the Frobenius automorphism associated to $\mathfrak{P}$. One has $\phi(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$ for all $\alpha \in \mathcal{O}_L$ [This relationship chars ϕ. When $\mathrm{Gal}(L/K)$ is abelian, ϕ depends only on $\mathfrak{p}$.]

Thm: K a number field. Suppose $p \mid \Delta_K$. Then p ramifies in $\mathcal{O}_K$.

Pf: ($\Leftarrow$) [Did on Feb 18.]

($\Longrightarrow$) *Easy case*: power of p in Δ_K is p^k with k odd.

Let L be the normal closure of K, and note $\sqrt{\Delta_K} \in \mathcal{O}_L$ as $\sqrt{\Delta_K} = \det(\sigma_i(\alpha_j))$ where $\{\alpha_j\}$ are an int basis for $\mathcal{O}_L$. Since k is odd, p ramifies in $\mathbb{Q}(\sqrt{\Delta_K})$ as $p = (p, \sqrt{d'})^2$. Suppose p is unramified in K,

$\uparrow$ Δ_K made squarefree

and hence in each Galois conj K_i of K.

For a prime $\mathfrak{P}$ of $\mathcal{O}_L$ over p, we thus have $K_i \subseteq L_{D(\mathfrak{P}|p)} \Longrightarrow L_D = L$, i.e. p is unramified in L, a contradiction. ▨

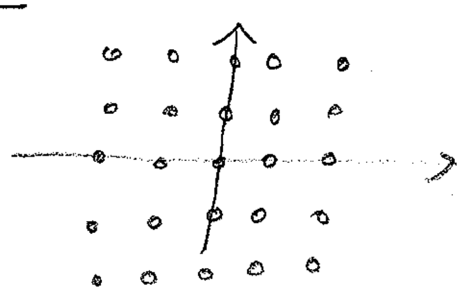
[For general case, see text.]

Both in Chapter 5 of text

Goals: Cl_K is finite and $\mathcal{O}_K^\times$ is finitely generated.

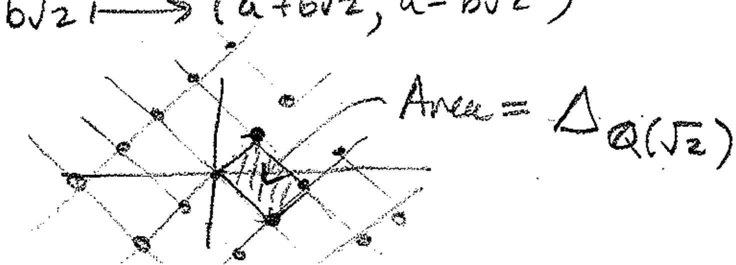
Tool: Minkowski theory aka "the geometry of numbers"

Ex: (a) $\mathbb{Z}[i]$



(b) $\mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{R}^2$

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



K a number field, $\tau_i : K \to \mathbb{C}$ embeddings

$j: K \longrightarrow K_{\mathbb{C}} := \mathbb{C}^n$ where $n = [K:\mathbb{Q}]$

$k \longmapsto (\tau_1(k), \dots, \tau_n(k))$

Define $Tr: K_{\mathbb{C}} \to \mathbb{C}$ by $Tr(\vec{x}) = \sum_{i=1}^{n} x_i$.

Thus $Tr_{K/\mathbb{Q}} = Tr \circ j$

$K_{\mathbb{C}}$ has a standard (hermitian) inner product

$\langle \vec{x}, \vec{y} \rangle = \sum_{i=1}^{n} x_i \overline{y_i}$ which is $\mathbb{C}$-linear in $\vec{x}$ with $\langle \vec{x}, \vec{y} \rangle = \overline{\langle \vec{y}, \vec{x} \rangle}$

Consider the generator F of $Gal(\mathbb{C}/\mathbb{R})$ where $F(z) = \overline{z}$, and denote $F \circ \tau$ by $\overline{\tau}$. Thinking of $K_{\mathbb{C}}$ as $\prod_{\tau} \mathbb{C}$, F acts on both the indices and the factors; we combine to define $F(z_\tau) = \overline{z}_{\overline{\tau}}$

<u>Ex</u>: $K = \mathbb{Q}(i)$

$\tau_1(a+bi) = a+bi$
$\tau_2(a+bi) = a-bi$

$K_{\mathbb{C}} = \underset{\tau_1}{\mathbb{C}} \oplus \underset{\tau_2}{\mathbb{C}}$

$F(z_1, z_2) = (\overline{z}_2, \overline{z}_1)$

<u>Point</u>: $F(j(k)) = j(k)$ [see above example.]

Let
$$K_{\mathbb{R}} = \{ \vec{x} \in K_{\mathbb{C}} \mid F\vec{x} = \vec{x} \} \supseteq j(K)$$

Let
$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}$$ be the real embeddings of K

and
$$\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s : K \to \mathbb{C}$$ be the complex (= non real) embeddings.

Here $n = r + 2s$.

Consider
$$K_{\mathbb{R}} \longrightarrow \mathbb{R}^{r+2s} = \mathbb{R}^r \oplus \mathbb{C}^s$$
$$k \longmapsto (\rho_1(k), \ldots, \rho_r(k), \sigma_1(k), \ldots, \sigma_s(k))$$
easy to see this is an isomorphism.

Notice $\langle F\vec{x}, F\vec{y} \rangle = F\langle \vec{x}, \vec{y} \rangle$ and hence $\langle , \rangle$ restricts to a pos. def inner product $K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$...

To be continued ....