Local theory / Global theory

$\mathbb{Q}_p$ $\mathbb{F}_p((t))$ $\mathbb{C}((t))$ / $\mathbb{Q}$, $\mathbb{F}_p(t)$, $\mathbb{C}(t)$

Local:

K field complete w.r.t. a discrete absolute value $|\cdot|$.

$\mathcal{O}_K = \{a \in K \mid |a| \le 1\}$ (is a complete DVR).

m_K maximal ideal in $\mathcal{O}_K$ $= \{a \in K \mid |a| < 1\}$

$k_K = \mathcal{O}_K / m_K$. Assume k is perfect.

Theorem If I fix a finite extension L/K

$k_L = \mathcal{O}_L / m_L$, then

$$\left\{ \begin{array}{c} K \subseteq M \subseteq L \\ M/K \text{ unramified} \end{array} \right\} \longleftrightarrow \left\{ k_K \subseteq k_M \subseteq k_L \right\}$$

(In particular there is a maximal unramified sub extension $K \subseteq L^{ur} \subseteq L$ corresponds to $k_K \subseteq k_L$).

L/L^{ur} totally ramified

L^{ur}/K unramified.

Def'n: If L/K is Galois, $G = \mathrm{Gal}(L/K)$

$G_i \trianglelefteq G : \{\sigma \in G \mid |\sigma(\alpha) - \alpha| < |\pi_L|^i \ \forall \alpha \in \mathcal{O}_L\}$

Ramification groups

(Here π_L generates the maximal ideal in $\mathcal{O}_L$).

$|\pi_L| = |\pi_K|^{1/e}$

Theorem: ① $\{e\} = \bigcap_{i \ge 0} G_i$.

G_0 is just $\sigma \mid \sigma(\alpha) \equiv \alpha \mod m_L$.

② $G/G_0 = \mathrm{Gal}(k_L/k_K)$.

(3) $G_0/G_1 \xhookrightarrow{\sigma \mapsto \sigma(\pi_L)/\pi_L} k_L^\times$

(4) $G_i/G_{i+1} \hookrightarrow k_L$ $\quad i \geq 1$

For $i \geq 1$
$G_i = \{\sigma \in G \mid |\sigma(\pi_L) - \pi_L| \leq |\pi_L|^i\}$

Corollary: If $\mathrm{Gal}(k_L/k_K)$ is solvable then so is $\mathrm{Gal}(L/K)$.

Example: If $K = \mathbb{Q}_p$, then $\mathrm{Gal}(L/\mathbb{Q}_p)$ is solvable.

Def'n:
- L/K is unramified if $e=1$
- L/K is tamely ramified if $\mathrm{char}\, k_K \nmid e$.

wildly ramified otherwise.

Corollary: If L/K is Galois, then
- L/K is unramified $\iff G_0 = \{e\}$.
- L/K is tamely ramified $\iff G_1 = \{e\}$.

$$\left(L^{G_0} = L^{ur} \qquad L^{G_1} = L^{tr} \right).$$

L^{tr}: maximal tamely ramified subextension

Global theory:

$K = \mathrm{Frac}\, \mathcal{O}_K \qquad \mathcal{O}_K$ is a DD

(assume $\mathcal{O}_K/p$ is perfect for any nonzero prime p).

E.g.

$K = \mathbb{Q}$ $\mathcal{O}_K = \mathbb{Z}$	$K = \mathbb{F}_q(t)$ $\mathcal{O}_K = \mathbb{F}_q[t]$	$K = \mathbb{C}(t)$ $\mathcal{O}_K = \mathbb{C}[t]$.

$K = \#$ field
$\mathcal{O}_K =$ ring of integers

Suppose L/K is Galois. $G = \mathrm{Gal}(L/K)$ ($\mathcal{O}_L$ integral closure of $\mathcal{O}_K$ in L).

If $\mathfrak{q} \in \mathcal{O}_L$ is a prime ideal.

Definition: The decomposition group $D(\mathfrak{q}) \leq G$, $D(\mathfrak{q}) = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$.

Lemma $D(\mathfrak{q}) \cong \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ $\quad \mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$.

$I(\mathfrak{q}) \leq D(\mathfrak{q})$ inertia group = preimage of $\mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})_0$

Theorem

$$\begin{tikzcd}
\mathfrak{q} & L \arrow[r, hook] \arrow[d, dash, "e"] & L_{\mathfrak{q}} \arrow[d, dash, "e"', "\text{ramified}"] & \\
& L^{I(\mathfrak{q})} \arrow[r, hook] \arrow[d, dash, "f"] & L_{\mathfrak{q}}^{I(\mathfrak{q})} \arrow[r, dashed, dash] \arrow[d, dash, "f"', "\text{unramified}"] & k_{\mathfrak{q}} \arrow[d, dash, "f"'] \\
& L^{D(\mathfrak{q})} \arrow[r, hook] \arrow[d, dash, "g"] & K_{\mathfrak{p}} \arrow[r, dashed, dash] & k_{\mathfrak{p}} \\
\mathfrak{p} & K \arrow[ur] & &
\end{tikzcd}$$

$\mathfrak{p} = \mathfrak{q}^e \mathfrak{q}_2^e \cdots \mathfrak{q}_g^e$

$[L:K] = efg.$

$f = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$

$\mathrm{Gal}(L/K)$ acts transitively on primes dividing $\mathfrak{p}$

If $\mathfrak{q}_1, \mathfrak{q}_2 \mid \mathfrak{p}$ then $D(\mathfrak{q}_1)$ & $D(\mathfrak{q}_2)$, $I(\mathfrak{q}_1)$ & $I(\mathfrak{q}_2)$ are conjugate.

$L_{\mathfrak{q}_1} \cong L_{\mathfrak{q}_2}$.

$k_{\mathfrak{q}_1} \cong k_{\mathfrak{q}_2}$.

One important consequence;

$L/\mathbb{Q}$ Then if p is unramified in L

$(p) = \mathfrak{q}_1 \cdots \mathfrak{q}_g$.

$D(\mathfrak{q}_i) \leq \mathrm{Gal}(L/\mathbb{Q})$.

$$\begin{aligned} &\;\; \wr\!\wr\!\wr \\ &\mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{q}_i) / \mathbb{F}_p\right) \\ &\;\; \| \\ &\mathrm{Gal}\left(\mathbb{F}_{p^f} / \mathbb{F}_p\right) \\ &\;\; \| \\ &\langle \mathrm{Frob} : x \mapsto x^p \rangle . \end{aligned}$$

$$\mathfrak{q}_i \longrightarrow \left(L/\mathbb{Q}, \mathfrak{q}_i\right) \in \mathrm{Gal}(L/\mathbb{Q})$$

Frobenius at $\mathfrak{q}_i$

These form a conjugacy class in $\mathrm{Gal}(L/\mathbb{Q})$ as i varies.

Frobenius conjugacy class attached to p.

Example: You proved quadratic reciprocity using Frobenius Galois elements in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.