Decomposition, ramification

Let $\mathcal{O}_K$ be a Dedekind dom. with field of fractions K, let $L|K$ be a nondeg. deg. n ext. and let $\mathcal{O}_L$ be the int closure of $\mathcal{O}_K$ in L.

<u>Def</u> A <u>prime</u> of L is a max. ideal $\mathfrak{P} \subseteq \mathcal{O}_L$.

<u>Rmk</u> If $L = L_1 \times \dots \times L_r$. The primes of L are the ideals of the form $\mathfrak{P} = \mathcal{O}_{L_1} \times \dots \times \mathcal{O}_{L_{i-1}} \times \mathfrak{q} \times \mathcal{O}_{L_{i+1}} \times \dots \times \mathcal{O}_{L_r}$, where $\mathfrak{q}$ is a prime of L_i.

"$\{\text{primes of } L\} = \bigsqcup_i \{\text{primes of } L_i\}$"

<u>Rmk</u> If $\mathfrak{P}$ is a prime in L, then $\mathfrak{p} = \mathfrak{P} \cap K$ is a prime of K.

<u>Def</u> Assume that $L|K$ is a nondeg. G-ext.
Let $\mathfrak{P}$ be a prime of L and $\mathfrak{p} = \mathfrak{P} \cap K$.
We define the

<u>decomposition group</u> $D(\mathfrak{P}|\mathfrak{p}) = \{ g \in G \mid g\mathfrak{P} = \mathfrak{P} \}$.

<u>inertia group</u> $I(\mathfrak{P}|\mathfrak{p}) = \{ g \in D(\mathfrak{P}|\mathfrak{p}) \mid gx \equiv x \bmod \mathfrak{P} \ \forall x \in \mathcal{O}_L \}$

<u>higher ramification group</u> $(s \geq 0)$
$$I_s(\mathfrak{P}|\mathfrak{p}) = \{ g \in D(\mathfrak{P}|\mathfrak{p}) \mid gx \equiv x \bmod \mathfrak{P}^{s+1} \ \forall x \in \mathcal{O}_L \}.$$

<u>Rmk</u> $G \supseteq D \supseteq I = I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$
and $I_s = 1$ for sufficiently large s.

Rmk G acts transitively on the set of primes $\mathfrak{P}$ above a fixed prime $\mathfrak{p}$ of K.

Rmk
$$D(g\mathfrak{P}|\mathfrak{p}) = g\, D(\mathfrak{P}|\mathfrak{p})\, g^{-1}$$
$$I_s(g\mathfrak{P}|\mathfrak{p}) = g\, I_s(\mathfrak{P}|\mathfrak{p})\, g^{-1}$$

Rmk If $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ is a finite field, then $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ is a Galois ext. with Galois group

D/I.

. ..

The discriminants of all subext. are determined by the higher ramification groups:

Thm Let K be a global or local field.
$$v_\mathfrak{p}(D_{L|K}) = \frac{|G|}{|I|} \cdot \sum_{s=0}^{\infty} (|I_s| - 1)$$

More ~~generally~~ generally, for any $H \subseteq G$,
$$v_\mathfrak{p}(D_{L^H|K}) = \sum_{s=0}^{\infty} \left(\frac{[G:H]}{[I:I_s]} - \frac{1}{|I|} \cdot \sum_{g \in I_s} \#\{r \in G/H : gr = r\} \right)$$

Tamely ramified extensions

<u>Def</u> $L|K$ is <u>tamely ramified</u> at $\mathfrak{P}$ if $I_1(\mathfrak{P}|\mathfrak{p}) = 1$.

$$I_1 = I_2 = \ldots$$

<u>Rmk</u> $L|K$ is tamely ramified if and only if (the residue field characteristic p of) $\mathfrak{P}$ doesn't divide $|I|$.

In particular, $L|K$ is tamely ramified whenever $p \nmid |G|$.

<u>Cor</u> If K is a local field with res. field char. $p \nmid |G|$, then every cont hom. $\Gamma_K \to G$ factors through

$$\Gamma_K^{tame} := Gal(K^{tame}|K).$$

max. tamely ramified ext.

$$\Gamma_K \twoheadrightarrow \Gamma_K^{tame} \to G$$

We get a bij.

$$\{\text{cont. hom. } \Gamma_K \to G\} \leftrightarrow \{\text{cont. } \Gamma_K^{tame} \to G\}.$$

<u>Thm</u> The max. tamely ramified field extension of a local field K with residue field $\mathbb{F}_q$ is

$$K^{tame} = \bigcup K(\zeta_m, \pi^{1/m}$$

Cor of Thm

If $L|K$ is tamely ramified at $\mathfrak{P}$ and $I(\mathfrak{P}|\mathfrak{q}) \leq G$ is generated $\tau \in G$, then

$$v_{\mathfrak{q}}(D_{L|K}) = |G| - \frac{1}{\mathrm{ord}(\tau)}$$

and for any $H \leq G$,

$$v_{\mathfrak{q}}(D_{L^H|K}) = [G:H] - \frac{1}{\mathrm{ord}(\tau)} \cdot \sum_{k=0}^{\mathrm{ord}(\tau)-1} \#\{r \in G/H : \tau^k r = r\}$$

$$= [G:H] - \#(\text{cycles of the permutation representing left mult. by } \tau \text{ on } G/H).$$

$$\boxed{\begin{array}{l} \Gamma_k = \mathrm{Gal}(K^{sep}|K) \\ \quad \big\downarrow \\ \Gamma_k^{tame} = \mathrm{Gal}(K^{tame}|K) \end{array}}$$

Thm The max. tamely ramified field ext. of a local field K with residue field $\mathbb{F}_q$ is

$$K^{tame} = \bigcup_{\substack{m \geq 1 \\ \gcd(m,q)=1}} K(\zeta_m, \pi_K^{1/m}) = \bigcup_{t \geq 0} K(\zeta_{q^t - 1}, \pi_K^{1/(q^t-1)}).$$

Its Galois group Γ_K^{tame} contains the following dense (finitely presented) subgroup:

$$\langle \varphi, \tau \mid \varphi \tau \varphi^{-1} = \tau^q \rangle,$$

where τ is given by $\tau(\zeta_m) = \zeta_m$, $\tau(\pi_K^{1/m}) = \zeta_m \pi_K^{1/m}$

and φ is given by $\varphi(\zeta_m) = \zeta_m^q$, $\varphi(\pi_K^{1/m}) = \pi_K^{1/m}$

(lift of Frobenius).

Also $\langle \tau \rangle \overset{\mathbb{Z}}{\cong}$ is a dense subgroup of $I(K^{tame}/K)$

and $\langle \varphi \rangle \cong \mathbb{Z}$ is a dense subgroup of Γ_K^{tame}/I.

$$\begin{array}{c} K^{tame} \\ | \, I \\ K^{nr} \\ | \\ K \end{array}$$

$\cong Gal(K^{nr}/K)$
$\cong Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$
$\cong \widehat{\mathbb{Z}}$

Any subgroup of $Gal(K^{tame}/K)$ of finite index is open.

Cor We obtain a bij.

$$\{\text{cont. hom. } \Gamma_k^{\text{tame}} \to G\} \longleftrightarrow \{(\bar\varphi, \bar\tau) \in G \times G \mid \bar\varphi \bar\tau \bar\varphi^{-1} = \bar\tau^q\}$$

$$f \longmapsto (f(\varphi), f(\tau))$$

If f corresponds to the (tamely ramified) G-extension $L|K$, then $I(L|K)$ is generated by $\bar\tau = f(\tau)$.

Lemma Let C be a conjugacy class in G. Then,

$$\frac{1}{|G|} \cdot \#\{\text{cont. } f : \Gamma_k^{\text{tame}} \to G : f(\tau) \in C\}$$

$$= \begin{cases} 1, & \text{if } C = C^q, \\ 0, & \text{if } C \neq C^q. \end{cases}$$

Pf $LHS = \frac{1}{|G|} \cdot \#\{(\bar\varphi, \bar\tau) \in G \times C \mid \bar\varphi \bar\tau \bar\varphi^{-1} = \bar\tau^q\}$.

Since $\bar\tau, \bar\varphi \bar\tau \bar\varphi^{-1} \in C$, the LHS is 0 if $C \neq C^q$.

If $C = C^q$, fix any of the $|C|$ elements $\bar\tau$ of C.

Since $\bar\tau^q \in C^q = C$, there exists some $\bar\varphi_0 \in G$ s.t. $\bar\varphi_0 \bar\tau \bar\varphi_0^{-1} = \bar\tau^q$.

We have $\bar{\varphi} \bar{\tau} \bar{\varphi}^{-1} = \bar{\tau} g = \bar{\varphi}_0 \bar{\tau} \bar{\varphi}_0^{-1}$ if and only if $\bar{\varphi}_0^{-1} \bar{\varphi}$ commutes with (= lies in the centralizer of) $\bar{\tau}$. By the orbit-stabilizer theorem (applied to the action of G on C by conjugation), the centralizer has size $\frac{|G|}{|C|}$.

$\Rightarrow \; |C| \cdot \frac{|G|}{|C|} = |G|$ such pairs $(\bar{\varphi}, \bar{\tau})$ in total.

$\square$

G-extensions of number fields (Malle's conjecture)

Let K be a number field and $G \neq 1$ be a nontrivial finite group. Consider a function $d : G \longrightarrow \mathbb{R}^{\geq 0} \cup \{\infty\}$ satisfying the following properties:

a) $d(hgh^{-1}) = d(g) \quad \forall g, h \in G$

(so d is a class function $\{\text{conj. classes}\} \to \mathbb{R}^{\geq 0} \cup \{\infty\}$)

b) $d(g^n) = d(g) \quad \forall g \in G, \ n \in (\mathbb{Z}/|G|\mathbb{Z})^\times$

c) $d(g) = 0$ if and only if $g = id \in G$.

For any ~~place~~ place v of K, consider a <u>local invariant</u>

$\mathrm{inv}_v : \{\text{nondeg. } G\text{-ext. of } K_v\} \longrightarrow \mathbb{R}^{>0} \cup \{\infty\}$

such that for all but finitely many nonarchimedean $v = \mathfrak{q}$ with residue field char. $p \nmid |G|$ and any G-ext. L of K_v, we

$\mathrm{inv}_v(L) = \mathrm{Nm}(\mathfrak{q})^{d(\overline{\tau})}$, where $\overline{\tau} \in G$ generates the inertia group $I(L|K_v)$ (or $\overline{\tau} = f(\tau)$, where $f : \Gamma_k^{\text{tame}} \to G$ corresponds to the G-ext. L of K_v).

<u>Rmk</u> This is well-def. according to a), b).