Lecture 14: Hilbert's Ramification Theory II

Last time: L/K normal, $\mathfrak{p}$ a prime of $\mathcal{O}_K$.

$G = \mathrm{Gal}(L/K)$, $\mathfrak{q}$ a prime of $\mathcal{O}_L$ above $\mathfrak{p}$.

decomp. group. $D = D(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$

inertial group. $E = \{\sigma \in D \mid \sigma \text{ acts trivially on } \mathcal{O}_L/\mathfrak{q}\}$

Picture: $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^e \cdots \mathfrak{q}_r^e$ where $f_i = f$

		ram index	inertial degree	degree
L	$\mathfrak{q}$			
		e	1	e
inertial field L_E	$\mathfrak{q}_E$			
		1	f	f
decomp. field L_D	$\mathfrak{q}_D$			
		1	1	r
K	$\mathfrak{p}$			

Last time

Consider the residue fields

$$\begin{array}{c} K(\mathfrak{q}) = \mathcal{O}_L/\mathfrak{q} \\ | \\ K(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p} \end{array}$$

Prop: This extension is normal, and $D \to \mathrm{Gal}(K(\mathfrak{q})/K(\mathfrak{p}))$ is surjective.

Proof: By last time, we know $K(\mathfrak{q}_D) \cong K(\mathfrak{p})$, and so we can reduce to the case where $L_D = K$, i.e. $G = D$.

Let $\bar{\theta} \in K(\mathfrak{q})$ be a primitive element, θ a lift to $\mathcal{O}_L$.
Let $\bar{g} \in K(\mathfrak{p})[X]$ be the min. poly of $\bar{\theta}$. [Want: factors into linear things in $K(\mathfrak{q})[X]$]
Consider the min poly $f \in \mathcal{O}_K[X]$ of θ. As L/K is normal, f factors into linear terms in $\mathcal{O}_L[X]$. Now $\bar{f}(\bar{\theta}) = 0$
$\Rightarrow \bar{g} \mid \bar{f} \Rightarrow \bar{g}$ in $K(\mathfrak{q})[X]$ divides $\prod$ (linear factors)
$\Rightarrow \bar{g}$ factors completely in $K(\mathfrak{q})[X] \Rightarrow K(\mathfrak{q})/K(\mathfrak{p})$ is normal.

Now suppose $\bar{\sigma} \in \mathrm{Gal}(K(\mathfrak{q})/K(\mathfrak{p}))$. We have $\bar{\sigma}(\bar{\theta}) = \bar{\theta}'$ where $\bar{\theta}'$ is another root of $\bar{g}$; $\bar{\theta}'$ has a lift $\theta' \in \mathcal{O}_L$ which is a root f. Then $\exists\, \sigma \in G$ s.t. $\sigma(\theta) = \theta'$ and so $\sigma \mapsto \bar{\sigma}$ under $G \to \mathrm{Gal}(K(\mathfrak{q})/K(\mathfrak{p}))$. ∎
Thus the map is surjective.

Thus

$$1 \to E \to D \to \mathrm{Gal}(K(\mathfrak{q})/K(\mathfrak{p})) \to 1$$

<u>Prop</u>: (i) L_E/L_D is normal with Galois group $\cong \mathrm{Gal}(K(\mathfrak{q})/K(\mathfrak{p}))$.
(ii) $|E| = [L : L_E] = e$ and $[D:E] = [L_E : L_D] = f$
(iii)

	ram index	inertial deg
$\mathfrak{q}$ over $\mathfrak{q}_E$ has	e	1
$\mathfrak{q}_E$ over $\mathfrak{q}_F$ has	1	f

<u>Proof</u>: (i) $E \trianglelefteq D$.

(ii) We know $[D:E] = \left| \mathrm{Gal}(K(\mathfrak{q})/K(\mathfrak{p})) \cong \mathbb{Z}/f\mathbb{Z} \right| = f$ by definition. Also

$$ef \underset{\substack{\uparrow \\ \text{last time}}}{=} |D| = [D:E]\,|E| \Rightarrow |E| = e.$$

(iii) <u>Claim</u>: $K(\mathfrak{q}_E) \cong K(\mathfrak{q})$, i.e. $f(\mathfrak{q} : \mathfrak{q}_E) = 1$.

If so, recall that $\mathfrak{q}_D$ is non-split in $\mathcal{O}_L$ (and hence $\mathcal{O}_{L_E}$) and then by the fund. ident:

$$e = [L:L_E] = e(\mathfrak{q}|\mathfrak{q}_E)\cdot f(\mathfrak{q}/\mathfrak{q}_E) \Longrightarrow e(\mathfrak{q}|\mathfrak{q}_E) = 1.$$

Multiplicativity now determines the data for $\mathfrak{q}_E/\mathfrak{q}_D$.

<u>Pf of Claim</u>: For L/L_E, we have

$$\text{Inertial group} = \text{decomp group} = \mathrm{Gal}(L/L_E) = E$$

By the last prop we have

$$1 = \text{decomp}/\text{interial} \cong \mathrm{Gal}(K(\mathfrak{q})/K(\mathfrak{q}_E))$$

and so $K(\mathfrak{q}) \cong K(\mathfrak{q}_E)$. ∎

Ex: $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{5})$, $K = \mathbb{Q}$ $\quad G = (\mathbb{Z}/2\mathbb{Z})^3$

$\mathfrak{p} = (5)$ which splits in $\mathbb{Q}(i)$ $\quad [L:K] = 8$

inert in $\mathbb{Q}(\sqrt{2})$ (2 not a square in $\mathbb{F}_5$)

ramified in $\mathbb{Q}(\sqrt{5})$

$\Rightarrow 5\mathcal{O}_L$ has at least 2 factors and $e \geq 2$.

By Fund identity, must have $e = f = 2$.

$$\begin{array}{c} L \\ | \\ L_E = \mathbb{Q}(i, \sqrt{2}) \\ | \\ L_D = \mathbb{Q}(i) \\ | \\ K = \mathbb{Q} \end{array}$$

Thus all these extensions have degree 2, and so $L_D = \mathbb{Q}(i)$ by

Thm: L_D = largest field between K and L where ram index = inertial deg = 1.

or just check all 7 poss degree 2 extensions of $\mathbb{Q}$. Then

$L_E = \mathbb{Q}(i, \sqrt{2})$ or $\underbrace{\mathbb{Q}(i, \sqrt{5}) \text{ or } \mathbb{Q}(i, \sqrt{10})}_{\text{not these as 5 ramifies}}$

In particular, $(2+i)$ and $(2-i)$ are primes of $\mathbb{Q}(i, \sqrt{2})$.