14. Prime ideals in Galois ext.

Recall from last week: $K \subset L$ number fields.

$(0) \neq \mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$, $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$, $\mathfrak{p} \cdot \mathcal{O}_L = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$

where $\mathfrak{p}_i \in \operatorname{Spec}(\mathcal{O}_L)$, $\mathcal{O}_L/\mathfrak{p}_i = \mathbb{F}_{q^{f_i}}$ for some $f_i \geq 1$

Then $[L:K] = \sum_{i=1}^{k} e_i f_i$

We will now assume that L is Galois $/K$.

$G = \operatorname{Gal}(L/K)$ acts on $\mathcal{O}_L$ (i.e. $x \in \mathcal{O}_L$ and $g \in G$ $gx \in \mathcal{O}_L$, and $g|_{\mathcal{O}_K} = id$)

For $\mathfrak{q} \in \operatorname{Spec}(\mathcal{O}_L)$ $g \cdot \mathfrak{q} \in \operatorname{Spec}(\mathcal{O}_L)$

and $(g \cdot \mathfrak{q}) \cap \mathcal{O}_K = (g \cdot \mathfrak{q}) \cap (g \cdot \mathcal{O}_K) =$

$= g \cdot (\mathfrak{q} \cap \mathcal{O}_K) = \mathfrak{q} \cap \mathcal{O}_K$

So if we consider the decomposition

$$\mathfrak{p} \cdot \mathcal{O}_L = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i},$$

then $(g \cdot \mathfrak{p}_i) \cap \mathcal{O}_K = \mathfrak{p}_i \cap \mathcal{O}_K = \mathfrak{p}$, so G permutes the prime ideals $\mathfrak{p}_i$

Prop 14.1 G acts on the set

$$\mathcal{P} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$$

transitively (i.e. $\forall i,j \ \exists g \in G : g \cdot \mathfrak{p}_i = \mathfrak{p}_j$)

Proof Decompose $\mathcal{P}$ into G-orbits. We

need to prove tha $\exists$ only one orbit.
If not, then we can find a decompos.

$$\mathcal{P} = \mathcal{P}_1 \sqcup \mathcal{P}_2 \quad (\text{disj. union})$$

$\mathcal{P}_1 \neq \emptyset$, $\mathcal{P}_2 \neq \emptyset$, and G preserves $\mathcal{P}_1$ and $\mathcal{P}_2$. After renumbering:

$$\mathcal{P}_1 = \{p_1, \dots, p_m\}, \quad \mathcal{P}_2 = \{p_{m+1}, \dots, p_k\}$$

By CRT we can find $x \in \mathcal{O}_L$,
s.t. $x \in p_i$, $i = 1, \dots m$;

$x \notin p_i$, $i = m+1, \dots, k$.

Then $y = \prod_{g \in G} g \cdot x \in \mathcal{O}_L \cap K = \mathcal{O}_K$

$\forall g \in G$ $\forall$ $i = 1 \dots m$ $g^{-1} p_i = p_j$ for some $j = 1 \dots m$

then $x \in p_j \Rightarrow gx \in p_i$

hence $gx \in p_i$ for all $i = 1 \dots m$

Analogously $gx \notin p_i$ for $i = m+1, \dots, k$

$\Rightarrow$ same for y: $y \in p_i$, $i = 1 \dots m$

$y \notin p_i$, $i = m+1, \dots k$

But $y \in \mathcal{O}_K \Rightarrow y \in \mathcal{O}_K \cap p_1 = p$

$\Rightarrow y \in \mathcal{O}_K \cap p_k = p$ contradiction $\square$

In the decomposition

$$p \cdot \mathcal{O}_L = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$$

the left-hand side is G-invariant,

$\forall\, i_0, j_0 \ \exists\, g \in G \quad \mathfrak{p}_{i_0} = g \cdot \mathfrak{p}_{j_0}$

$$\Rightarrow p \cdot \mathcal{O}_L = \prod_{i=1}^{k} g \cdot \mathfrak{p}_i^{e_i} =$$

$$= \mathfrak{p}_{i_0}^{e_{j_0}} \cdot \prod_{i \neq j_0} g \cdot \mathfrak{p}_i^{e_i}$$

the decomp. is unique up to permut.

$\Rightarrow e_{i_0} = e_{j_0}$, so $e_1 = \ldots = e_k = e$

Analogously $\mathcal{O}_L / \mathfrak{p}_{j_0} \simeq \mathcal{O}_L / g \cdot \mathfrak{p}_{j_0} = \mathcal{O}_L / \mathfrak{p}_{i_0}$

$\Rightarrow f_{i_0} = f_{j_0}$, so $f_1 = \ldots = f_k = f$.

<u>Corollary</u> (Fund. identity for Galois ext.)

$$[L : K] = k \cdot e \cdot f, \quad \text{where}$$

$$p \cdot \mathcal{O}_L = \prod_{i=1}^{k} \mathfrak{p}_i^{e}, \text{ and } \mathcal{O}_L / \mathfrak{p}_i = \mathbb{F}_{q^f}$$

<u>Def</u> The stabilizer of $\mathfrak{p}_i$ denoted by

$$G_{\mathfrak{p}_i} = \{ g \in G \mid g \cdot \mathfrak{p}_i = \mathfrak{p}_i \}$$

is called decomposition group of $\mathfrak{p}_i$

Decomposition groups of $\mathfrak{p}_i$'s are conjugate: for any $\mathfrak{p}_j$ $\exists h \in G$:

$$\mathfrak{p}_j = h \cdot \mathfrak{p}_i$$

Then $G_{\mathfrak{p}_j} = \{ g \in G \mid \underbrace{g \cdot \mathfrak{p}_j = \mathfrak{p}_j}_{\Updownarrow} \} = h G_{\mathfrak{p}_i} h^{-1}$:

$$h^{-1} g h \mathfrak{p}_i = \mathfrak{p}_i \Longleftrightarrow g h \mathfrak{p}_i = h \mathfrak{p}_i$$

$$\Updownarrow$$

$$h^{-1} g h \in G_{\mathfrak{p}_i}$$

For $g \in G_{\mathfrak{p}_i}$ we have a map of rings $\mathcal{O}_L \xrightarrow{g} \mathcal{O}_L$ preserving $\mathfrak{p}_i$

$\Rightarrow$ this map descends to the quotient

$$\mathbb{F}_{q^f} = \mathcal{O}_L / \mathfrak{p}_i \xrightarrow{\bar{g}} \mathcal{O}_L / \mathfrak{p}_i = \mathbb{F}_{q^f}$$

$$\bar{g} \in \mathrm{Gal}(\mathbb{F}_{q^f} / \mathbb{F}_q)$$

$\Rightarrow$ we get a group homomorphism

$$\gamma : G_{\mathfrak{p}_i} \longrightarrow \mathrm{Gal}(\mathbb{F}_{q^f} / \mathbb{F}_q)$$

<u>Def</u> The subfield of L fixed by $G_{\mathfrak{p}_i}$ denoted $L_{\mathfrak{p}_i} = L^{G_{\mathfrak{p}_i}}$ is called the <u>decomposition field</u> of $\mathfrak{p}_i$

We have $K \subset L_{\mathfrak{p}_i} \subset L$

Galois with group $G_{\mathfrak{p}_i}$

Let $\mathfrak{q}_i = \mathcal{O}_{L_{\mathfrak{p}_i}} \cap \mathfrak{p}_i$.

Note: $\mathfrak{p}_i$ is the only prime ideal lying over $\mathfrak{q}_i$: since $G_{\mathfrak{p}_i}$ act transitively on ideals lying over $\mathfrak{q}_i$ (Prop. 14.1) for any $\mathfrak{p}_j$ with $\mathcal{O}_{L_{\mathfrak{p}_i}} \cap \mathfrak{p}_j = \mathfrak{q}_i$ we must have some $g \in G_{\mathfrak{p}_i}$: $\mathfrak{p}_j = g \cdot \mathfrak{p}_i = \mathfrak{p}_i$

So we get:

$$\mathfrak{q}_i \cdot \mathcal{O}_L = \mathfrak{p}_i^{e'} \text{ for some } e'$$

Let $\mathcal{O}_{L_{\mathfrak{p}_i}}/\mathfrak{q}_i = \mathbb{F}_{q^{f'}}$ for some f'

<u>Lemma 14.2</u> $e' = e$, $f' = 1$

<u>Proof</u>: We have: $|G_{\mathfrak{p}_i}| = \frac{|G|}{k} = \frac{[L:K]}{k} = e \cdot f$ by the fund. identity for L/K.

For $L/L_{\mathfrak{p}_i}$:

$$\begin{array}{l} [L : L_{\mathfrak{p}_i}] = |G_{\mathfrak{p}_i}| = ef \\ \quad \| \\ e' [\mathbb{F}_{q^f} : \mathbb{F}_{q^{f'}}] = e' \cdot \frac{f}{f'} \end{array}$$

$\Rightarrow e' = e \cdot f'$! But $e' \leq e$, because otherwise $\mathfrak{p}_i$ would enter the decomp. of $\mathfrak{p}$ with multiplicity $> e$, which is not true.

$\Rightarrow e' = e$, $f' = 1$ $\square$

<u>Prop. 14.3</u> The homomorphism γ is surjective

<u>Proof</u> Assume that γ is not surj., then its image is a proper subgroup of $Gal(\mathbb{F}_{q^f}/\mathbb{F}_q)$ with fixed subfield H, i.e. $\mathbb{F}_q \subsetneq H \subset \mathbb{F}_{q^f}$

$\forall \bar{x} \in H \quad x \in \mathcal{O}_L$, s.t.

$$\bar{x} \equiv x \pmod{\mathfrak{p}_i}$$

Consider the polynomial

$$T = \prod_{g \in G_{\mathfrak{p}_i}} (X - g \cdot x)$$

$$T \in \mathcal{O}_{L_{\mathfrak{p}_i}}[X]$$

If we reduce mod $\mathfrak{p}_i$, we get $\overline{T} = \prod_{g \in G_{\mathfrak{p}_i}} (X - \overline{gx})$

But $\overline{gx} = \gamma(g) \cdot \overline{x} = \overline{x}$ by assumption

$\Rightarrow \overline{T} = (X - \overline{x})^{|G_{\mathfrak{p}_i}|}$, but

$\overline{T} \in (\mathcal{O}_{L_{\mathfrak{p}_i}} / \mathfrak{q}_i)[X] = \mathbb{F}_q[X]$

(because of Lemma 14.2)

$\Rightarrow$ all Gal-conjugates of $\overline{x}$ are roots of $\overline{T}$, so $\overline{x}$ is fixed by $\mathrm{Gal}(\mathbb{F}_{q^f} / \mathbb{F}_q)$

$\Rightarrow \overline{x} \in \mathbb{F}_q \Rightarrow H = \mathbb{F}_q$ — contradiction

$\square$

We have a surjection:

$$\gamma : G_{\mathfrak{p}_i} \twoheadrightarrow \mathrm{Gal}(\mathbb{F}_{q^f} / \mathbb{F}_q)$$

__Def__ $\mathrm{Ker}(\gamma) = I_{\mathfrak{p}_i}$ is called __inertia group__. Its fixed field is called __inertia field.__

Assume now that p is unramified in L, i.e. $p \cdot \mathcal{O}_L = \prod_{i=1}^{k} \mathfrak{p}_i$

then $[L:K]=k\cdot f$, $e=1$

$|G_{p_i}|=f=|Gal(\mathbb{F}_{q^f}/\mathbb{F}_q)|$

$\Leftrightarrow$ γ is an isomorphism

We denote by F the generator of $Gal(\mathbb{F}_{q^f}/\mathbb{F}_q)$; $F(\bar{x})=\bar{x}^q$

<u>Def</u> We assume p is unramified in L, then $\gamma^{-1}(F)$ is denoted

$$\left(\frac{L/K}{p_i}\right)\in Gal(L/K)$$

and called <u>Frobenius element</u> of p_i

Note: for $g\in Gal(L/K)$ $G_{g\cdot p_i}=g\,G_{p_i}g^{-1}$

so $$\left(\frac{L/K}{gp_i}\right)=g\left(\frac{L/K}{p_i}\right)g^{-1}$$

In particular, if $Gal(L/K)$ is abelian, this element is the same for all p_i lying over p.

<u>Def</u> In the case $Gal(L/K)$ is abelian, this element is denoted $\left(\frac{L/K}{p}\right)\in Gal(L/K)$

and is called <u>Artin symbol</u>