Galois groups, splitting, and ramification

Action of Galois on primes

L/K = Galois extension of number fields

$G = \mathrm{Gal}(L/K)$. $\sigma \in L$

$\sigma \in G$ $\quad \sigma(\alpha) \in L$ $\quad$ if $\alpha \in K$, $\sigma(\alpha) = \alpha$

note: $\sigma : \mathcal{O}_L \longrightarrow \mathcal{O}_L$ $\quad P(\alpha) = 0 \Rightarrow P(\sigma(\alpha)) = 0$

for $\mathfrak{P} \subset \mathcal{O}_L$, a (prime) ideal $\quad \sigma(\mathfrak{P}) \subseteq \mathcal{O}_L$ is a (prime) ideal

$\sigma(\mathfrak{P})$ is (Galois) conjugate to $\mathfrak{P}$

Why is the action transitive?

Prop For any nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the primes of $\mathcal{O}_L$ above $\mathfrak{p}$ form a single Galois orbit.

Pf Let q_1, q_2 be primes of $\mathcal{O}_L$ above $\mathfrak{p}$, suppose not in the same orbit. By CRT, can find $\alpha \in \mathcal{O}_L$ s.t.

$$\alpha \equiv 0 \mod q_2$$
$$\alpha \equiv 1 \mod \sigma(q_1) \quad \forall \sigma \in G$$

$\mathrm{Norm}_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \in K \cap q_2 = \mathfrak{p}$. On the other hand,

$\alpha \notin \sigma^{-1}(q_1) \ \forall \sigma \in G$, so $\sigma(\alpha) \notin q_1 \ \forall \sigma \in G$. Since q_1 is prime,

$\mathrm{Norm}_{L/K}(\alpha) \notin q_1 \supseteq \mathfrak{p}$.

The decomposition group of a prime ideal

For $\mathfrak{q} \subseteq \mathcal{O}_L$ a prime above $\mathfrak{p} \subseteq \mathcal{O}_K$, the <u>decomposition group</u> of $\mathfrak{q}$ is $G_{\mathfrak{q}} = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}$ $\left(= \mathrm{Stab}_G(\mathfrak{q}) \right)$

If $\mathfrak{q}'$ is another one of these, then $\mathfrak{q}' = \tau(\mathfrak{q})$ for some $\tau \in G$

then $G_{\mathfrak{q}'} = \tau G_{\mathfrak{q}} \tau^{-1}$

Splitting and the decomposition group

$\mathfrak{p} \subset \mathcal{O}_K$ prime

$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ — $\Rightarrow$ since L/K Galois,

$e_1 = \cdots = e_r$

$f_1 = \cdots = f_r$

$\tau(\mathfrak{q}_1) = \mathfrak{q}_2$

$\tau : \mathcal{O}_L/\mathfrak{q}_1 \xrightarrow{\sim} \mathcal{O}_L/\mathfrak{q}_2$ as extensions of $\mathcal{O}_K/\mathfrak{p}$

and $\underbrace{r}_{\text{size of orbit}} = [G : \underbrace{G_{\mathfrak{q}_1}}_{\text{size of stabilizer}}]$

(is unramified)

in particular, $G_{\mathfrak{q}_1} = \{e\} \Longleftrightarrow \mathfrak{p}$ splits completely

$G_{\mathfrak{q}_1} = G \Longleftrightarrow r = 1$ $\quad e \cdot f = [L : K]$

(includes totally inert case but also some ramified cases)

A comment about the non-Galois case

say M/K an extension of number fields with Galois closure L/K.

$\mathfrak{p} \subset O_K$ prime. Let $\mathfrak{q} \subseteq O_L$ be a prime above $\mathfrak{p}$ then the prime ideals of M above $\mathfrak{p}$ are of the form

$\sigma(\mathfrak{q}) \cap M$.

$\sigma(\mathfrak{q}) \cap M$

$G = Gal(L/K) \supseteq H = Gal(L/M)$

$\uparrow$

$H\sigma G_\mathfrak{q}$

in bijection with $H \backslash G / G_\mathfrak{q}$

space of double cosets (pairwise disjoint) $H\sigma G_\mathfrak{q}$

$\sigma \in H\sigma_1 G_{\mathfrak{q}} \cap H\sigma_2 G_{\mathfrak{q}_2} \Rightarrow H\sigma_1 G_{\mathfrak{q}} = H\sigma G_{\mathfrak{q}} = H\sigma_2 G_{\mathfrak{q}_2}$

The decomposition field of a prime ideal

$\mathfrak{q} \subset \mathcal{O}_L$ prime above $\mathfrak{p} \subset \mathcal{O}_K$

$G_\mathfrak{q} \subset G = \mathrm{Gal}(L/K)$ $\quad Z_\mathfrak{q}$ = fixed field of $G_\mathfrak{q}$ in L

<u>decomposition field</u>

$$\begin{array}{cc} L & \mathfrak{q} \\ | & \\ Z_\mathfrak{q} & \mathfrak{q}_Z \\ | & \\ K & \mathfrak{p} \end{array}$$

~~rup~~ let $\mathfrak{q}_Z = \mathfrak{q} \cap Z_\mathfrak{q}$. Then:

- $\mathfrak{q}$ is <u>only</u> prime of L above $\mathfrak{q}_Z$
- $e(\mathfrak{q}/\mathfrak{q}_Z), f(\mathfrak{q}/\mathfrak{q}_Z) = e(\mathfrak{q}/\mathfrak{p}), f(\mathfrak{q}/\mathfrak{p})$
- $e(\mathfrak{q}_Z/\mathfrak{p}) =$ $\qquad f(\mathfrak{q}_Z/\mathfrak{p}) = \underline{1}$

follows from: $\underset{\mathfrak{q}}{L} / M / \underset{\mathfrak{p}}{K}$ in general, decomposition grp of $\mathfrak{q}$ relative to M is $G_\mathfrak{q} \cap \mathrm{Gal}(L/M)$.

An example: a biquadratic extension

$K = \mathbb{Q}$

$L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\alpha)/p(\alpha)$ (or $L = \mathbb{Q}(\zeta_8)$, $x^4 + 1$)

$G(L/K) = C_2 \times C_2$

Claim (prove soon): for $p \neq 2, 3$, $q \subset \mathcal{O}_L$ prime above p, G_q is cyclic

$\Rightarrow G_q \neq G$, so $r > 1$ always.

elementary version of this: $p(x)$ is reducible mod p for all $p \neq 2, 3$.

(in $\mathbb{F}_p$, one of $\left(\frac{2}{p}\right), \left(\frac{3}{p}\right), \left(\frac{6}{p}\right)$ must be $+1$.)

Action of the decomposition group on the residue field

$G_{\mathfrak{q}} \subset G$ acts on $\mathcal{O}_L/\mathfrak{q}$ $\quad \mathfrak{q} \subset \mathcal{O}_L$ above $\mathfrak{p} \subset \mathcal{O}_K$ primes

Prop $\quad G_{\mathfrak{q}} \longrightarrow \mathrm{Gal}\left(\mathcal{O}_L/\mathfrak{q} \,\middle/\, \mathcal{O}_K/\mathfrak{p} \right)$ is surjective

(and this is a Galois extension)

(Skip proof for now)

The inertia group of a prime ideal

$$G_{\mathfrak{q}} \twoheadrightarrow \mathrm{Gal}\left(\mathcal{O}_L/\mathfrak{q} \,/\, \mathcal{O}_K/\mathfrak{p}\right)$$

kernel is called the <u>inertia group</u> of $\mathfrak{q}$, called $I_{\mathfrak{q}}$

<u>Claim:</u> $e(\mathfrak{q}|\mathfrak{p}) = \# I_{\mathfrak{q}}$

$$f(\mathfrak{q}/\mathfrak{p}) = [G_{\mathfrak{q}} : I_{\mathfrak{q}}] = G_{\mathfrak{q}}/I_{\mathfrak{q}}$$

In particular, $\mathfrak{q}/\mathfrak{p}$ unramified $\Leftrightarrow I_{\mathfrak{q}} = \{e\}$.