Lecture 26 (5.2)

Let $Q \in \operatorname{Spec} S$ lie above $P \in \operatorname{Spec} R$. We have the residue field extension

$$k(P) := R/P \subset S/Q =: k(Q).$$

Every $\sigma \in G_Q$ induces an automorphism $\bar\sigma : k(Q) \to k(Q)$ fixing $k(P)$, hence $\bar\sigma \in \mathrm{Gal}_{k(P)}(k(Q))$.

Prop 8.54

recall: Galois = normal + separable

The extension $k(P) \subset k(Q)$ is normal and

$$G_Q \longrightarrow \mathrm{Gal}_{k(P)}(k(Q))$$

is a surjective group morphism.

Proof: By Prop 8.53, the inert deg of Q^{G_Q} over P is 1, i.e. $k(P) = k(Q^{G_Q})$. We can thus assume wlog that $L^{G_Q} = K$, i.e. $G_Q = G$. Let $\bar\Theta \in k(Q)$. We need to show that the minimal polynomial $p_{\bar\Theta}$ of $\bar\Theta$ over $k(P)$ splits into linear factors (normality). Let $\Theta \in S$ be a representative of $\bar\Theta$ and let p_Θ be the minimal polynomial of Θ over K. Note that $p_\Theta \in R[X]$ since Θ integral over S. Clearly, $\bar\Theta$ is a zero of $\overline{p_\Theta} \in k(P)[X]$, so $p_{\bar\Theta}$ divides $\overline{p_\Theta}$. Since $K \subset L$ is Galois, it is normal, hence p_Θ splits into linear factors. Hence, $p_{\bar\Theta}$ splits into linear factors as well $\Rightarrow k(P) \subset k(Q)$ is normal.

Let $k(P) \subset k^{sep}$ be the maximal separable subextension of $k(P) \subset k(Q)$. Then $\mathrm{Gal}_{k(P)}(k^{sep}) = \mathrm{Gal}_{k(P)}(k(Q))$ (fact from Galois theory).

Let $\bar\Theta$ be a primitive element for k^{sep} over $k(P)$ (exists by Thm 2.23)

Fix $\bar\sigma \in \mathrm{Gal}_{k(P)}(k(Q))$. Then $\bar\sigma\bar\Theta$ is a root of $p_{\bar\Theta}$, and thus of $\overline{p_\Theta}$. Hence, there is a root Θ' of p_Θ such that $\overline{\Theta'} = \bar\sigma\bar\Theta$. Now, Θ' is a conjugate of Θ, hence there is $\sigma \in \mathrm{Gal}_K(L)$ with $\Theta' = \sigma\Theta$

$\Rightarrow \overline{\sigma\Theta} = \bar\sigma\bar\Theta$. It follows that σ induces automorphism of $k(Q)$, so $\sigma \in G_Q$. Moreover, σ maps to $\bar\sigma$ under $G_Q \to \mathrm{Gal}_{k(P)}(k(Q))$. $\square$

Def 8,55

The kernel I_Q of $G_Q \longrightarrow Gal_{k(P)}(k(Q))$ is called the <u>inertia group</u> of Q over R. The fixed field L^{I_Q} is called <u>inertia field</u>.

Prop 8,56

a) The extension $L^{G_Q} \subset L^{I_Q}$ is normal and

$$Gal_{L^{G_Q}}(L^{I_Q}) \simeq Gal_{k(P)}(k(Q)), \quad Gal_{L^{I_Q}}(L) = I_Q.$$

b) If $k(P) \subset k(Q)$ is separable, the

$$|I_Q| = [L : L^{I_Q}] = e, \quad [G_Q : I_Q] = [L^{I_Q} : L^{G_Q}] = f$$

Moreover:

b1) The ramification index of Q in $S^{I_Q} \subset S$ is e, and the inertia index is 1

b2) The ramification index of Q^{I_Q} in $S^{G_Q} \subset S^{I_Q}$ is 1, and the inertia degree is 1.

$$\begin{tikzcd} L \arrow[d, dash, "e"'] \\ L^{I_Q} \arrow[d, dash, "f"'] \\ L^{G_Q} \arrow[d, dash, "r"'] \\ K \end{tikzcd}$$

Proof:

a) Since I_Q is a normal subgroup of G_Q (it is a kernel), the extension $K \subset L^{I_Q}$ is normal (by Galois theory). Then clearly also $L^{G_Q} \subset L^{I_Q}$ is normal. Hence (by Galois theory),

$$Gal_{L^{G_Q}}(L^{I_Q}) \simeq G_Q / I_Q \simeq Gal_{k(P)}(k(Q)).$$

Moreover, $\mathrm{Gal}_{L^{I_Q}}(L) = I_Q$ by Galois theory.

b) Since $k(P) \subset k(Q)$ is normal by Prop 8.54 and separable by assumption, it is Galois. Hence

$$f = [S/Q : R/P] = |\mathrm{Gal}_{k(P)}(k(Q))| = [G_Q : I_Q]$$

We have

$$|G| = [L:K] = e \cdot f \cdot [G:G_Q] = e\,[G_Q : I_Q][G:G_Q] = e\,[G:I_Q]$$

$\Rightarrow |I_Q| = e.$

b1+b2) Consider $L^{I_Q} \subset L$. By Prop 8.54 we have

$$\mathrm{Gal}_{L^{I_Q}}(L)_Q \twoheadrightarrow \mathrm{Gal}_{k(Q^{I_Q})}(k(Q))$$

By above, $\mathrm{Gal}_{L^{I_Q}}(L) = I_Q$. But this is the kernel of $G_Q \to \mathrm{Gal}_{k(P)}(k(Q))$. Hence, the above map sends everything to 1.

As it is surjective, we conclude $\mathrm{Gal}_{k(Q^{I_Q})}(k(Q)) = 1$

$\Rightarrow k(Q^{I_Q}) = k(Q)$.

$\Rightarrow$ inertia degree of Q in $S^{I_Q} \subset S$ is 1.

The claims now follow from the fundamental equation and Prop 8.53. $\square$

8.9 Ramification in quadratic extensions

Let $d \neq 0,1$ be square-free and let $L = \mathbb{Q}(\sqrt{d})$. Using Dedekind's Theorem 8.42 we can completely describe how prime numbers behave in $\mathcal{O}_L$.

Since $n = [L:\mathbb{Q}] = 2$, only three cases can occur by the fundamental equation:

a) p is (totally) split: $r=2, e=f=1$

b) p is inert: $r=1, e=1, f=2$

c) p is (totally) ramified: $r=1, e=2, f=1$

Let's see when which case happens. Let $\theta := \sqrt{d}$.
Recall from Exercise 2.4 that $\mathcal{O}_L = \mathbb{Z}[\alpha]$, where

$$\alpha = \begin{cases} \alpha & \text{if } d \equiv 2,3 \bmod 4 \\ \frac{1+\theta}{2} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

Hence,

$$d_{\mathcal{O}_L} = \begin{cases} 4d & \text{if } d \equiv 2,3 \bmod 4 \\ d & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

<u>Def 8.57</u>

The <u>Legendre symbol</u> for $a \in \mathbb{N}$ and an <u>odd</u> prime is

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if there is } x \text{ with } x^2 \equiv a \bmod p \text{ and } p \nmid a \\ -1 & \text{if there is no such } x \\ 0 & \text{if } p \nmid a \end{cases}$$

<u>Thm 8.57</u>

If p is <u>odd</u> then

$$p \text{ is } \begin{cases} \text{split} \\ \text{inert} \\ \text{ramified} \end{cases} \quad \text{iff} \quad \left(\frac{d}{p}\right) = \begin{cases} 1 \\ -1 \\ 0 \end{cases}$$

If p is <u>even</u> then

$$p \text{ is } \begin{cases} \text{ramified} \\ \text{inert} \\ \text{split} \end{cases} \quad \text{iff} \quad \begin{cases} d \equiv 2,3 \bmod 4 \\ d \equiv 5 \bmod 8 \\ d \equiv 1 \bmod 8 \end{cases}$$

<u>Proof:</u>

Let p be odd. Note that $[\mathcal{O}_L : d_{\mathbb{Z}[\theta]}] = \begin{cases} 1 & \text{if } d \equiv 2,3 \bmod 4 \\ 2 & \text{if } d \equiv 1 \bmod 4. \end{cases}$

Since p odd, we thus have $p \nmid [\mathcal{O}_L : \mathbb{Z}[\theta]]$ and we can apply Thm 8.42. The minimal poly of θ is $\mu = X^2 - d$ and the claim follows immediately.

Now let $p = 2$.

Suppose $d \equiv 2, 3 \bmod 4$. Then $[\mathcal{O}_L : \mathbb{Z}[\theta]] = 1$, so we can apply Thm 8.42. We have $d \equiv 0, 1 \bmod 2$, so

$$\mu \equiv X^2 \bmod 2 \quad \text{or} \quad \mu \equiv X^2 + 1 \ (\equiv (X+1)^2 \bmod 2)$$

Hence, 2 is ramified.

Suppose $d \equiv 1 \bmod 4$. Since $[\mathcal{O}_L : \mathbb{Z}[\theta]] = 2$, cannot apply Thm 8.42 with θ. Use α instead. The minimal polynomial of α is

$$\mu = X^2 - X + \frac{1-d}{4}.$$

If $d \equiv 1 \bmod 8$, this factors as $X^2 + X = X(X+1) \bmod 2$, so 2 is split. If $d \equiv 5 \bmod 8$ then $\mu \equiv X^2 + X + 1 \bmod 2$, which is irreducible, hence 2 is inert.

$\square$