# Lecture 25 (3.2.)

## 8.7 (Un)ramified primes

Here is an important corollary of Thm 8.42.

**Thm 8.45**

Let $d := d(1, \theta, \dots, \theta^{n-1})$ be the discriminant of the basis $1, \theta, \dots, \theta^{n-1}$ of $L$. Then all $P \in \operatorname{Spec} R$ which are coprime to $d$ and to $\mathfrak{F}$ are unramified in $S$. In particular, only finitely many $P$ are ramified in $S$.

**Proof:**

Recall from Cor 5.12 that $d = \pm \operatorname{Res}(p, p')$. Let $\bar{p} := p \bmod P$. Then $\bar{d} = \overline{\operatorname{Res}(p, p')} = \operatorname{Res}(\bar{p}, \bar{p}')$. Since $d \notin P$, $\bar{d} \neq 0$, so $\operatorname{Res}(\bar{p}, \bar{p}') \neq 0$. By Lemma 5.9 this means that $\bar{p}, \bar{p}'$ have no common root, so the factorization of $\bar{p}$ is $\bar{p} = \bar{p}_1 \cdots \bar{p}_r$, all $\bar{p}_i$ coprime. Since $P$ is coprime to $\mathfrak{F}$, Thm 8.42 implies that $e_i = 1$ $\forall i$. Moreover, $\bar{p}, \bar{p}'$ no common root means that $\bar{p}$ is separable. If $Q_i$ is a prime over $P$, the extension $R/P \subset S/Q_i$ is generated by $\theta \bmod Q_i$. The minimal polynomial of $\theta \bmod Q_i$ divides $\bar{p}$, hence it is separable, hence $R/P \subset S/Q_i$ is separable. In total: $P$ unramified. $\square$

**Remark 8.46**

One can show that the ramified $P$ are precisely the divisors of the <u>discriminant ideal</u>

$$d_{S/R} := \text{ideal of } S \text{ generated by all } K\text{-bases of } L \text{ contained in } S.$$

## 8.8 Galois theory of primes

As before: $R$ Dedekind domain with fraction field $K$. Assume now that $K \subseteq L$ is a finite <u>Galois</u> extension. Let $S = R^{\mathrm{int}, L}$, $G := \operatorname{Gal}_K(L)$.

<u>Note</u>: if $a \in S$, then also $\sigma(a) \in S$ $\forall \sigma \in G \Rightarrow G$ acts on $S$. This is an action by ring automorphisms, so if $Q \subseteq S$ is a prime ideal, so is $\sigma(Q)$.

If $Q$ lies above $P$, then so does $\sigma(Q)$ since

$$\sigma(Q) \cap R = \sigma(Q) \cap \sigma(R) = \sigma(Q \cap R) = \sigma(P) = P \quad (\sigma \text{ fixes } K)$$

Def 8.47

The prime ideals $\sigma(Q)$, $\sigma \in G$, are called the conjugates of $Q$.

Lemma 8.48

$G$ acts transitively on the primes of $S$ lying above a prime $P$ of $R$, i.e. they are all conjugates of each other.

Proof:

Let $Q, Q'$ be two primes above $P$. Suppose that $\sigma Q' \neq Q$ $\forall \sigma \in G$. Chinese Remainder Theorem:

$$S / Q' \cdot \prod_{\sigma \in G} \sigma(Q) \simeq S/Q' \times \prod_{\sigma \in G} S/\sigma(Q).$$

Hence, there is $x \in S$ such that

$$x \equiv 0 \mod Q' \quad \text{and} \quad x \equiv 1 \mod \sigma(Q) \ \forall \sigma \in G.$$

We have

$$N_{L|K}(x) = \prod_{\sigma \in G} \sigma(x) = x \cdot \prod_{\substack{\sigma \in G \\ \sigma \neq 1}} \sigma(x)$$

Hence, since $x \in Q'$ and $x$ integral over $R$, $N_{L|K}(x) \in Q' \cap R = P$.

On the other hand, $x \notin \sigma(Q)$ $\forall \sigma \in G \Rightarrow \sigma(x) \notin Q$ $\forall \sigma \in G \Rightarrow \prod_{\sigma \in G} \sigma(x) \notin Q \cap R = P$ ↯

$\square$

Def 8.49

Let $Q$ be a prime of $S$. The decomposition group of $Q$ (over $R$) is

$$G_Q := \{ \sigma \in G \mid \sigma P = P \}$$

Lemma 8.50

Let $P \in \operatorname{Spec} R$.

a) The ramification indices $e_i$ and inertia degrees $f_i$ of the primes $Q_i$ above $P$ are independent of $i$.

b) The factorization of $P$ in $S$ is of the form

$$PS = \left(\prod_{\sigma \in G/G_Q} \sigma Q\right)^e,$$

where $Q$ is an arbitrary prime over $P$.

Proof:

Let $Q_1, \dots, Q_r$ be the primes above $P$. Set $Q := Q_1$. By Lemma 8.48 we can find for each $i$ a $\sigma_i \in G$ with $Q_i = \sigma_i Q$. Since $\sigma_i$ is a ring isomorphism $S \longrightarrow S$, it follows that $S/Q \simeq S/\sigma_i Q$, hence

$$f_i := [S/Q_i : R/P] = [S/Q : R/P] =: f \quad \forall i$$

Moreover, since $\sigma_i(PS) = PS$ $\forall i$, we have

$$Q^b \mid PS \Leftrightarrow \sigma_i(Q^b) \mid PS \Leftrightarrow (\sigma_i Q)^b \mid PS,$$

hence $e_i = e_1 =: e$ $\forall i$. The claim in b) is now clear.

$\square$

Def 8.51

The fixed field

$$L^{G_Q} = \{x \in L \mid \sigma x = x \ \forall \sigma \in G_Q\}$$

is called the decomposition field of $Q$ (over $R$).

Lemma 8.52

$S^{G_Q}$ is the integral closure of $R$ in $L^{G_Q}$ and this is a Dedekind domain.

Proof:

Follows from $S = R^{\mathrm{int}, L}$ and from the general Lemma 8.31.

$\square$

Prop 8.53

Fix $Q \in \operatorname{Spec} S$ over $P \in \operatorname{Spec} R$. Then $Q^{G_Q} = Q \cap S^{G_Q} \in \operatorname{Spec} S^{G_Q}$.

a) $Q^{G_Q}$ is non-split in $S^{G_Q} \subset S$, i.e. $Q$ is the only prime above $Q^{G_Q}$.

b) The ramification indices and inertia degrees of $Q$ over $P$ are those of $Q$ over $Q^{G_Q}$

c) The ramification indices and inertia degrees of $Q^{G_Q}$ over $P$ are equal to 1 (i.e. $P$ totally split in $R \subset S^{G_Q}$)

$$\begin{tikzcd}
Q \arrow[d, dash, "e,f \text{ happens here}"'] & S \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash] \\
Q^{G_Q} \arrow[d, dash, "\text{splitting happens here}"'] & S^{G_Q} \arrow[r, dash] \arrow[d, dash] & L^{G_Q} \arrow[d, dash] \\
P & R \arrow[r, dash] & K
\end{tikzcd}$$

Proof:

a) Note that $\mathrm{Gal}_{L^{G_Q}}(L) = G_Q$. Hence, by Lemma 8.50, the primes over $Q^{G_Q}$ are $\sigma Q$ for $\sigma \in G_Q$. Hence, they are all equal to $Q$.

b+c) By Lemma 8.50, the fundamental equation (see Thm 8.37) reads

$$n = efr,$$

where

$n = \dim_K L = |G|$

$e =$ ram index of $Q$ over $P$

$f =$ inert deg of $Q$ over $P$

$r = \#$ of primes in $S$ over $P = [G : G_Q]$.

Hence,

$$|G| = n = efr = ef \cdot [G : G_Q].$$

$$\Rightarrow [L : L^{G_Q}] = |G_Q| = ef$$

Let $e'$ resp $e''$ be the ram index of $Q$ in $S^{G_Q} \subset S$ resp of $Q^{G_Q}$ in $R \subset S^{G_Q}$. Then $PS^{G_Q} = (Q^{G_Q})^{e''} \cdot$ powers of other primes.

Since $Q$ is the only prime over $Q^{G_Q}$ by a), it follows that $Q^{G_Q}S = Q^{e'}$.

Hence, $PS = Q^{e'e''} \cdot$ powers of other primes

$\Rightarrow e = e'e''$.

If $f'$ resp $f''$ denotes the inert deg of $Q$ in $S^{G_Q} \subset S$ resp of $Q^{G_Q}$ in $R \subset S^{G_Q}$, then clearly

$$f = [S/Q : R/P] = [S/Q : S^{G_Q}/Q^{G_Q}] \cdot [S^{G_Q}/Q^{G_Q} : R/P] = f'f''.$$

The fundamental equation for the decomposition of $Q^{G_Q}$ in $S^{G_Q} \subset S$ is $[L : L^{G_Q}] = e'f'$. Hence, $ef = e'f' \Rightarrow e = e'$, $f = f'$, $e'' = 1 = f''$.

$\square$