Lecture 11: More on primes in extensions.

Last time: $K \subseteq L$ number fields. $\mathfrak{p}$ a prime in $\mathcal{O}_K$.

$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}$ $\quad e_i$ = ramification index $\quad \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$

f_i = inertial degree = deg of $\mathcal{O}_K/\mathfrak{p}$ | $\mathcal{O}_K/\mathfrak{p}$

Fundamental Identity: $\sum e_i f_i = [L:K] = n$.

Proved when $K = \mathbb{Q}$; in general, follows from

Lemma: $N(\mathfrak{p}\mathcal{O}_L) = N(\mathfrak{p})^n$ where $n = [L:K]$.

Clear if $\mathfrak{p} = (\alpha)$ as $N(\mathfrak{p}\mathcal{O}_L) = N_{L/\mathbb{Q}}(\alpha)$

$= N_{K/\mathbb{Q}}(N_{L/K}(\alpha)) = N_{K/\mathbb{Q}}(\alpha^n) = N_{K/\mathbb{Q}}(\alpha)^n = N(\mathfrak{p})^n$.

Proof: Let $k = \mathcal{O}_K/\mathfrak{p}$ and $R = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$.

E.T.S. that $\dim_k R = n$. Suppose $\omega_1, \omega_2, \ldots, \omega_m$ in $\mathcal{O}_L$ give a basis $\bar{\omega}_1, \ldots, \bar{\omega}_m$ in R.

Claim: $\{\omega_i\}$ are K-linearly indep $\Rightarrow \dim_k R \leq n$.

If not, $\exists\, a_i \in \mathcal{O}_K$ such that $\sum a_i \omega_i = 0$ with not all $a_i = 0$. Then $\sum \bar{a}_i \bar{\omega}_i = 0 \Rightarrow \bar{a}_i = 0 \ \forall i \Rightarrow$ $a_i \in \mathfrak{p}$. [idea: divide through by $\gcd(a_i)$]

Let $\alpha = (a_1, \dots, a_n) \subseteq \mathcal{O}_K$. Pick $a \in \alpha^{-1}$ which is not in $\alpha^{-1}\beta$; this exists as if $\alpha^{-1} \subseteq \alpha^{-1}\beta$, then mult by α we have $\mathcal{O}_K \subseteq \beta$, which is silly. Now $aa_i \in \mathcal{O}_K$ but not all in β as $\alpha^{-1}\beta = \{k \in K \mid k\alpha \subseteq \beta\}$ ← check. Then $\sum (aa_i) w_i = 0 \Rightarrow \sum \overline{(aa_i)}\, \overline{w_i} = 0$, a contradiction as some $\overline{aa_i} \neq 0$.

To show that $\dim_k R = n$, let p in $\mathbb{Z}$ be prime below β, and suppose $p\mathcal{O}_K = \prod \beta_i^{e(\beta_i|p)}$ (say $\beta_1 = \beta$) and $\beta_i \mathcal{O}_L = \prod \sigma_{i,j}^{e(\sigma_{i,j}|\beta_i)}$

Then

$$p\mathcal{O}_L = \prod \sigma_{i,j}^{e(\sigma_{i,j}|\beta_i)\, e(\beta_i|p)}$$

where the $\sigma_{i,j}$ are distinct primes of $\mathcal{O}_L$.

and also

$$f(\sigma_{i,j}|p) = f(\sigma_{i,j}|\beta_i)\, f(\beta_i|p)$$

$\mathcal{O}_L/\sigma_{i,j}$
|
$\mathcal{O}_K/\beta_i$
|
$\mathbb{Z}/p\mathbb{Z}$

Then by the case we know ($K = \mathbb{Q}$),

$$[L:\mathbb{Q}] = \sum_{i,j} e(\sigma_{i,j}|\beta_i)\, e(\beta_i|p)\, f(\sigma_{i,j}|\beta_i)\, f(\beta_i|p)$$

$$= \sum_i e(\beta_i|p)\, f(\beta_i|p) \dim_{k_i} R_i$$

$$\leq \sum_i e(\beta_i|p) f(\beta_i|p)\, n = [K:\mathbb{Q}]\, n = [L:\mathbb{Q}]$$

$\blacksquare$

$\Rightarrow \dim_{k_i} R_i = n$ for all i.

Suppose L/K is normal. $\mathrm{Gal}(L/K)$ acts on the prime ideals of $\mathcal{O}_L$, permuting those lieing over the same prime of $\mathcal{O}_K$. Moreover,

Prop: $\mathfrak{P}, \mathfrak{P}'$ primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$ in $\mathcal{O}_K$.
$\exists\, \sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\mathfrak{P}) = \mathfrak{P}'$.

Pf: Suppose not. By the Chinese Remainder Thm, there is a $\alpha \in \mathcal{O}_L$ such that $\alpha \in \mathfrak{P}'$ and $\alpha \notin \sigma(\mathfrak{P})$ for all $\sigma \in \mathrm{Gal}(L/K)$. Now $N_{L/K}(\alpha) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$.
But $\sigma^{-1}(\alpha) \notin \mathfrak{P}$ $\forall \sigma$, which implies
$N_{L/K}(\alpha) = \prod \sigma^{-1}(\alpha) \notin \mathfrak{P}$ as $\mathfrak{P}$ is prime.
As $\mathfrak{P} \supseteq \mathfrak{p}$, this is a contradiction $\blacksquare$

Cor: When L/K is normal, e and f depend only on $\mathfrak{p}$.