Lecture 10: Primes and Extensions.

Notation: $K \subseteq L$ are number fields, $n = [L:K]$.

Prop: $\mathfrak{p}$ a prime (ideal) of $\mathcal{O}_K$, $\mathfrak{q}$ a prime of $\mathcal{O}_L$.

T.F.A.E. ① $\mathfrak{q} \supseteq \mathfrak{p}\mathcal{O}_L$
② $\mathfrak{q} \supseteq \mathfrak{p}$
③ $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$

} "$\mathfrak{q}$ lies over $\mathfrak{p}$, $\mathfrak{p}$ lies under $\mathfrak{q}$."

Pf: ①⟺② since $\mathfrak{q}$ is an ideal. ③⇒② is obvious.

②⇒③ Let $r = \mathfrak{q} \cap \mathcal{O}_K$ a prime ideal $\mathcal{O}_K$ (its proper as $1 \in r \Rightarrow 1 \in \mathfrak{q}$). Now $r \supseteq \mathfrak{p}$ so by maximality of prime ideals we have $r = \mathfrak{p}$. ▨

Prop: ① Every prime $\mathfrak{q}$ of $\mathcal{O}_L$ lies over a unique prime $\mathfrak{p}$ of $\mathcal{O}_K$. ② Every prime $\mathfrak{p}$ in $\mathcal{O}_K$ lies under at least one prime $\mathfrak{q}$ of $\mathcal{O}_L$.

Pf: ① Let $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_L$, which is prime and nonzero as it contains $N_{L/K}(\alpha)$ for any $\alpha \in \mathfrak{q}$.

[$N_{L/K}(\alpha) = \alpha \cdot \beta$ where $\beta \in \mathcal{O}_L$]

② Take $\mathfrak{q}$ to be any prime dividing $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. The last assertion is because if not we have

$\mathfrak{p}^{-1}\mathcal{O}_L = \mathfrak{p}^{-1}\mathfrak{p}\mathcal{O}_L = \mathcal{O}_K\mathcal{O}_L = \mathcal{O}_L$, which is silly as $\mathfrak{p}^{-1} \subseteq \mathfrak{p}^{-1}\mathcal{O}_L$ and $\mathfrak{p}^{-1} \supsetneq \mathcal{O}_K$ and so contains a non alg. integer. ▨

In general, if $\mathfrak{p} \subseteq \mathcal{O}_K$ is prime then $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}$. The e_i are called the ramification indices. [typically $e_i = 1$]

As $\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$, we have an extension of finite fields; its degree f_i is the inertial degree of $\mathfrak{q}_i$ wrt to $\mathfrak{p}$.

$\mathcal{O}_L/\mathfrak{q}_i$ | $\mathcal{O}_K/\mathfrak{p}$

Ex: $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$

(a) $2\mathcal{O}_L = \mathfrak{q}^2$ where $\mathfrak{q} = (1+i)\mathcal{O}_L$

now $|\mathcal{O}_L/\mathfrak{q}| = N(\mathfrak{q}) = N_{L/K}(1+i) = 2$

and $|\mathcal{O}_K/(2)| = 2$ so here $e=2, f=1$.

(b) $3\mathcal{O}_L$ is prime. $|\mathcal{O}_L/3| = N(3\mathcal{O}_L) = N_{L/K}(3) = 9 = 3^2$

and $|\mathcal{O}_K/3| = 3$ so $\begin{matrix}\mathbb{F}_9 \\ | \\ \mathbb{F}_3\end{matrix} \Rightarrow e=1, f=2$

(c) $5\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2$ where $\mathfrak{q}_1 = (2+i)$, $\mathfrak{q}_2 = (2-i)$

Here $e_1 = e_2 = 1$, $f_1 = f_2 = 1$.

Ex: $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[6]{2})$ $17\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$

$f = 1, 1, 2, 2$

$2\mathcal{O}_L = (\sqrt[6]{2})^6$ $e = 6, f = 1$

$31\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_6$

$f = 1, 1, \ldots 1$

$13\mathcal{O}_L =$ prime; $f = 6$

Fundamental identity: L/K as above. If $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ with $\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}$ and $\mathfrak{q}_i$ has inertial degree f_i, then $\sum e_i f_i = [L:K]$

Pf when $K = \mathbb{Q}$: We have $\mathfrak{p} = (p)$. For each $\mathfrak{q}_i$,

$\mathcal{O}_L/\mathfrak{q}_i \cong \mathbb{F}_{p^{f_i}}$ and so $\mathcal{N}(\mathfrak{q}_i) = p^{f_i}$.

$\mathcal{O}_L/\mathfrak{q}_i$ | degree f_i | $\mathbb{Z}/p\mathbb{Z}$

Thus we have

$$\Rightarrow p^n = \mathcal{N}(\mathfrak{p}\mathcal{O}_L) = \prod \mathcal{N}(\mathfrak{q}_i)^{e_i} = \prod (p^{f_i})^{e_i} = p^{\sum e_i f_i}.$$

Thus $n = \sum e_i f_i$ ∎

In general, one just needs

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

We will prove this next time, and also show

Def: A prime $\mathfrak{p}$ in $\mathcal{O}_K$ is ramified if some $e_i > 1$.