Lecture 12: Ramified Primes

Last time $K \subseteq L$, $\mathfrak{p}$ a prime of $\mathcal{O}_K$

$\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}$ where $\mathfrak{q}_i$ are primes of $\mathcal{O}_L$. $\mathcal{O}/\mathfrak{q}_i$

Fund. Identity: $\sum e_i f_i = [L:K]$ where $f_i = \deg$ of $\mathcal{O}/\mathfrak{p}$

Prop: L/K is normal. If $\mathfrak{q}, \mathfrak{q}'$ are primes in $\mathcal{O}_L$ above $\mathfrak{p} \subseteq \mathcal{O}_K$, then $\exists \sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\mathfrak{q}) = \mathfrak{q}'$.

Pf: Suppose not. By the Chinese Remainder Thm, there is $\alpha \in \mathcal{O}_L$ with $\alpha \in \mathfrak{q}'$ and $\alpha \notin$ any $\sigma(\mathfrak{q})$.
Now $N_{L/K}(\alpha) \in \mathfrak{q}' \cap \mathcal{O}_K = \mathfrak{p}$. However, each $\sigma^{-1}(\alpha)$ is not in $\mathfrak{q}$, and so $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}} \sigma^{-1}(\alpha) \notin \mathfrak{q}$ as $\mathfrak{q}$ is prime. As $\mathfrak{q} \supseteq \mathfrak{p}$, this is a contradiction. ∎

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

$\mathfrak{p}$ a prime in $\mathcal{O}_K$

Ramified: some $e_i > 1$.

totally split: $\mathfrak{p} = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ where $n = [L:K]$ all $f_i = 1$

inert: $\mathfrak{p}\mathcal{O}_L$ is prime.

Thm: K a number field. If $p \in \mathbb{Z}$ is ramified, then $p \mid \Delta_K$.

[Note: The converse is also true.]

$v \in \mathbb{Z}^n$ is primitive if $v \neq mv'$ for some $m > 1$.
[Equiv, the gcd (entries of $\vec{v}$) = 1]

Lemma: If v_1 is primitive, then $\exists v_i$ so that $v_1, v_2, \dots, v_n$ generate $\mathbb{Z}^n$.

Ex: $\vec{V}_1 = (2,3)$ take $\vec{V}_2 = (1,1)$ as $\begin{vmatrix} 2 & 1 \\ 3 & 1 \end{vmatrix} = -1$.
[In general c.f. classification of modules over a P.I.D.]

Pf of Thm: Suppose $p\mathcal{O}_K = \mathfrak{p}\mathfrak{a}$ where $\mathfrak{a} \subseteq$ every prime over p.

Fix $\alpha \in \mathfrak{a} \setminus p\mathcal{O}_K$. There is an int basis $\beta_1, \dots, \beta_n$ of $\mathcal{O}_K$ where $\alpha = m\beta_1$ with m in $\mathbb{Z}$ coprime to p. Let H be the subgroup of $(\mathcal{O}_K, +)$ gen by $\alpha, \beta_2, \dots, \beta_n$. Then

$$\operatorname{disc}(H) = [\mathcal{O}_K : H]^2 \Delta_K = m^2 \Delta_K$$

As $\gcd(m, p) = 1$, its enough to show $p \mid \operatorname{disc}(H)$

Now

$$\mathrm{disc}(H) = \left[\det\begin{pmatrix} \sigma_1(\alpha) & \sigma_2(\alpha) & \cdots & \sigma_n(\alpha) \\ \vdots & & & \vdots \end{pmatrix}\right]^2$$

Let L be an extension of K where $L/\mathbb{Q}$ is normal.

Let $\mathfrak{q} \subseteq \mathcal{O}_L$ be a prime above p.

<u>Claim</u> $\sigma_i(\alpha) \in \mathfrak{q}$ for all $i \iff \alpha \in \sigma_i^{-1}(\mathfrak{q})$

as $\sigma_i^{-1}(\mathfrak{q}) \supseteq \underbrace{\sigma_i^{-1}(\mathfrak{q}) \cap \mathcal{O}_K}_{\text{some prime above } p} \supseteq \mathfrak{a} \ni \alpha$.

Now by the claim, $\mathrm{disc}(H) \in \mathfrak{q} \cap \mathbb{Z} = (p)$

$\Rightarrow p \mid \Delta_K.$ ▨

<u>HW #4</u> (Wed Feb 25)

Marcus Ch 3: #14, 16, 17, 24, 33