Lecture 13

$\mathcal{O}_K$ Dedekind domain. L/K finite, separable.

Corollary 10.10: For $x \in L$, $N_{L/K}(x) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(x)$.

Proof: Let $B_1, \dots, B_r$ be bases for $L_{\mathfrak{P}_1}, \dots, L_{\mathfrak{P}_r}$ as $K_\mathfrak{p}$-vector spaces. Then $B = \cup B_i$ is a basis for $L \otimes_K K_\mathfrak{p}$ over $K_\mathfrak{p}$.

Let $[\text{mult}(x)]_B$ (resp $[\text{mult}(x)]_{B_i}$) denote the matrix for $\text{mult}(x): L\otimes_K K_\mathfrak{p} \to L\otimes_K K_\mathfrak{p}$ (resp $L_{\mathfrak{P}_i} \to L_{\mathfrak{P}_i}$) w.r.t. the basis B (resp B_i). Then

$$[\text{mult}(x)]_B = \begin{pmatrix} [\text{mult}(x)]_{B_1} & & \\ & \ddots & \\ & & [\text{mult}(x)]_{B_r} \end{pmatrix}$$

$$\Rightarrow \underbrace{\operatorname{Det}([\text{mult}(x)]_B)}_{= N_{L/K}(x)} = \prod_{i=1}^{r} \underbrace{\operatorname{Det}([\text{mult}(x)]_{B_i})}_{= N_{L_{\mathfrak{P}_i}/K_\mathfrak{p}}(x)}$$

i.e. $N_{L/K}(x) = \prod_{i=1}^{r} N_{L_{\mathfrak{P}_i}/K_\mathfrak{p}}(x)$. $\square$

§ Decomposition groups

$0 \neq \mathfrak{p}$ prime ideal of $\mathcal{O}_K$

$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, $\mathfrak{P}_i$ distinct prime ideals in $\mathcal{O}_L$

Note: For any i, $\mathfrak{p} \subseteq \mathcal{O}_K \cap \mathfrak{P}_i \subsetneq \mathcal{O}_K$, hence $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}_i$

Definition 11.1: (i) e_i is the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$.

(ii) We say p ramifies in L if some $e_i > 1$.

E.g. $\mathcal{O}_K = \mathbb{C}[t]$, $\mathcal{O}_L = \mathbb{C}[T]$

$$\mathcal{O}_K \to \mathcal{O}_L \text{ sends } t \mapsto T^n$$

$t\mathcal{O}_L = T^n \mathcal{O}_L \Rightarrow$ ramification index of (T) over (t) is n. Corresponds geometrically to the degree n covering of Riemann surfaces

$$\mathbb{C} \to \mathbb{C}, \quad x \mapsto x^n$$

Ramified at 0 with ram. index n.

Definition 11.2: $f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/p]$ is the residue class degree of $\mathfrak{P}_i$ over p.

Theorem 13.3: $\sum_{i=1}^{r} e_i f_i = [L:K]$.

Proof: Let $S = \mathcal{O}_K \setminus p$. The following properties of localization are left as an exercise.

(1) $S^{-1}\mathcal{O}_L$ is the integral closure of $S^{-1}\mathcal{O}_K$ in L.

(2) $S^{-1}p\, S^{-1}\mathcal{O}_L \cong S^{-1}\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$

(3) $S^{-1}\mathcal{O}_L/S^{-1}\mathfrak{P}_i \cong \mathcal{O}_L/\mathfrak{P}_i$ and $S^{-1}\mathcal{O}_K/S^{-1}p \cong \mathcal{O}_K/p$

In particular, (2) + (3) imply e_i and f_i don't change when we replace $\mathcal{O}_K$ and $\mathcal{O}_L$ by $S^{-1}\mathcal{O}_K$ and $S^{-1}\mathcal{O}_L$. Thus we may assume that $\mathcal{O}_K$ is a DVR (and hence a PID)

By CRT we have

by CRT, we have

$$\mathcal{O}_L/p\mathcal{O}_L \cong \prod_{i=1}^{r} \mathcal{O}_L/\mathfrak{p}_i^{e_i}$$

We count dimensions of both sides as $k = \mathcal{O}_K/p$ vector spaces.

RHS: For each i, $\exists$ decreasing sequence of k-subspaces

$$0 \subseteq \mathfrak{p}_i^{e_i-1}/\mathfrak{p}_i^{e_i} \subseteq \dots \subseteq \mathfrak{p}_i/\mathfrak{p}_i^{e_i} \subseteq \mathcal{O}_L/\mathfrak{p}_i^{e_i}$$

Thus $\dim_k \mathcal{O}_L/\mathfrak{p}_i^{e_i} = \sum_{j=0}^{e_i-1} \dim_k\left(\mathfrak{p}_i^j/\mathfrak{p}_i^{j+1}\right)$

Note that $\mathfrak{p}_i^j/\mathfrak{p}_i^{j+1}$ is an $\mathcal{O}_L/\mathfrak{p}_i$ - module and $x \in \mathfrak{p}_i^j \setminus \mathfrak{p}_i^{j+1}$ is a generator (Eg. can prove this after localizing at $\mathfrak{p}_i$). Then $\dim_k \mathfrak{p}_i^j/\mathfrak{p}_i^{j+1} = f_i$ and we have

$$\dim_k \mathcal{O}_L/\mathfrak{p}_i^{e_i} = e_i f_i$$

and hence $\dim_k \prod_{i=1}^{r} \mathcal{O}_L/\mathfrak{p}_i^{e_i} = \sum_{i=1}^{r} e_i f_i$.

LHS: Structure theorem for modules over PID's $\Rightarrow$ $\mathcal{O}_L$ a free module over $\mathcal{O}_K$ of rank $n = [L:K]$

Thus $\mathcal{O}_L/p\mathcal{O}_L \cong (\mathcal{O}_K/p)^n$ as $\mathcal{O}_K$-modules and hence $\dim_k \mathcal{O}_L/p = n$. $\square$

Geometric analogue:

$X \to Y$ degree n cover of compact Riemann surjective. For $y \in Y$

$$n = \sum_{x \in f^{-1}(y)} e_x$$

e_x ram. index of x.

Now assume L/K is Galois. Then for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(P_i) \cap \mathcal{O}_K = p$ and hence $\sigma(P_i) \in \{P_1, \dots, P_r\}$, $\Rightarrow$ $\mathrm{Gal}(L/K)$ acts on $\{P_1, \dots, P_r\}$

Proposition 11.4: The action of $\mathrm{Gal}(L/K)$
5 on $\{P_1, \dots, P_r\}$ is transitive.

Proof: Suppose not, so that $\exists i \neq j$ s.t.

$$\sigma(P_i) \neq P_j \quad \forall \sigma \in \mathrm{Gal}(L/K)$$

By CRT, we may choose $x \in \mathcal{O}_L$ s.t.

$$x \equiv 0 \bmod P_i, \quad x \equiv 1 \bmod \sigma(P_j) \quad \forall \sigma \in \mathrm{Gal}(L/K)$$

Then $N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathcal{O}_K \cap P_i = p \subseteq P_j$

Since P_j is prime, $\exists \tau \in \mathrm{Gal}(L/K)$ s.t. $\tau(x) \in P_j$

$\Rightarrow x \in \tau^{-1}(P_j)$ i.e. $x \equiv 0 \bmod \tau^{-1}(P_j)$.

$\#$ $\square$

Corollary 11.5: Suppose L/K Galois. Then $e_1 = e_2 = \dots = e_r =: e$, $f_1 = \dots = f_r =: f$, we have $n = efr$.

Proof: For any $\sigma \in Gal(L/K)$ we have

(i) $p = \sigma(p) = \sigma(P_1)^{e_1} \cdots \sigma(P_r)^{e_r}$

$\Rightarrow e_1 = \dots = e_r$

(ii) $O_L/P_i = O_L/\sigma(P_i)$

$\Rightarrow f_1 = \dots = f_r$ $\square$

- If L/K extension of complete discretely valued fields with normalized valuations v_L, v_K, uniformizers π_L, π_K.

Ramification index is $e := e_{L/K} = v_L(\pi_K)$

$$(\text{i.e. } \pi_L^e O_L = \pi_K O_L)$$

Residue class degree $f := f_{L/K} = [k_L : k]$.

Corollary 11.6: Let L/K finite separable, Then $[L:K] = ef$ $\square$

Remark: Corollary holds without assumption L/K separable - same proof works.

O_K a Dedekind domain.

Definition 11.7: Let L/K be (finite) Galois. The decomposition group at a prime P of O_L is the subgroup of $Gal(L/K)$ defined by

$$G_P = \{\sigma \in Gal(L/K) \mid \sigma(P) = P\}$$

Proposition 11.4 $\Rightarrow$ for any P, P' dividing p,

G_P and $G_{P'}$ are conjugate and have size q.