Lecture 14

Proposition 11.8: Suppose L/K a (finite) Galois and $\mathfrak{P}|\mathfrak{p}$ prime ideal of $\mathcal{O}_L$.

Then

(i) $L_\mathfrak{P}/K_\mathfrak{p}$ is Galois.

(ii) There is a natural map

$$\mathrm{res}: \mathrm{Gal}(L_\mathfrak{P}/L_\mathfrak{p}) \to \mathrm{Gal}(L/K)$$

which is injective and has image $G_\mathfrak{P}$.

Proof: (i) L/K Galois $\Rightarrow$ L is splitting field of a separable polynomial $f(X) \in K[X]$.

$\Rightarrow L_\mathfrak{P}$ is the splitting field of $f(X) \in K_\mathfrak{p}[X]$

$\Rightarrow L_\mathfrak{P}/K_\mathfrak{p}$ is Galois.

(ii) Let $\sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$, then $\sigma(L) = L$ since L/K is normal, hence we have a map

$$\mathrm{res}: \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$$

Since L is dense in $L_\mathfrak{P}$, res is injective.

By Lemma 8.2

$$|\sigma(x)|_\mathfrak{P} = |x|_\mathfrak{P} \quad \forall \sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}), \ x \in L_\mathfrak{P}.$$

$\Rightarrow \sigma(\mathfrak{P}) = \mathfrak{P} \quad \forall \sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$

$\Rightarrow \mathrm{res}(\sigma) \in G_{\mathfrak{p}} \ \forall \sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

To show surjectivity it suffices to show that

$$[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef = |G_{\mathfrak{P}}|.$$

We have $|G_{\mathfrak{P}}| = ef$.

$[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef$: Apply corollary 13.6 to $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ noting that e and f don't change when we take completions. □

V Ramification theory

$p = \rho_1 \rho_2$ in $\mathbb{Z}[i]$ iff $p = x^2 + y^2$

§ Different and discriminant

$\mathcal{O}_K$ Dedekind domain. $K = \mathrm{Frac}(\mathcal{O}_K)$.

L/K finite seperable ext. deg. n

$\mathcal{O}_L$ integral closure of $\mathcal{O}_K$ in L.

Notation: Let $x_1, \dots, x_n \in L$.

Set $\Delta(x_1, \dots, x_n) = \det\left(\mathrm{Tr}_{L/K}(x_i x_j)\right) \in K$.

$= \det(\sigma_i(x_j))^2$

$\sigma_i : L \to K^{sep}$ distinct embeddings

Note: $\beta \in L$, $\Delta(\beta x_1, \dots, \beta x_n) = N_{L/K}(\beta)^2 \Delta(x_1, \dots, x_n)$

~ change of bases matrix $[\mathrm{mult}(\beta)]_{x_1, \dots, x_n}$

Lemma 13.1: Let k be a perfect field. R a k-algebra which is finite dim. as a k vector space. The Trace form $(\ ,\ ) : R \times R \to k$, $(x, y) = \mathrm{Tr}_{R/k}(xy)$ $:= \mathrm{Tr}_k(\mathrm{mult}(xy))$ is non-degenerate iff $R \cong k_1 \times \dots \times k_n$, where

k_i/k finite (hence separable) extensions of k.

Proof: Ex sheet 3 $\square$

Theorem 12.2: Assume $k = \mathcal{O}_K/p$ finite. Let $p \subseteq \mathcal{O}_K$ prime ideal.

(i) If p ramifies in L, then for every $x_1, \dots, x_n \in \mathcal{O}_L$, we have $p \mid \Delta(x_1, \dots, x_n)$

(ii) If p is unramified in L, then there exists $x_1, \dots, x_n \in \mathcal{O}_L$ s.t. $p \nmid \Delta(x_1, \dots, x_n)$

Proof (i) Let $p\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$, $0 \neq P_i \subseteq \mathcal{O}_L$ distinct prime ideals, $e_i > 0$. CRT implies

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

4 If p ramifies in $L \Rightarrow \mathcal{O}_L/p\mathcal{O}_L$ has nilpotents

$\Rightarrow$ Trace form degenerate

$\Rightarrow \Delta(\bar{x}_1, \dots, \bar{x}_n) = 0 \quad \forall \bar{x}_i \in \mathcal{O}_L / p\mathcal{O}_L$

$\Rightarrow \Delta(x_1, \dots, x_n) \equiv 0 \bmod p$ any $x_1 \dots x_n \in \mathcal{O}_L$

$$\begin{tikzcd} \mathcal{O}_L \arrow[r] \arrow[d, "\mathrm{Tr}_{L/K}"] & \mathcal{O}_L/p = R \arrow[d, "\mathrm{Tr}_{R/k}"] \\ \mathcal{O}_K \arrow[r] & \mathcal{O}_K/p \end{tikzcd}$$

commutes.

(ii) p unramified $\Rightarrow \mathcal{O}_L/p$ product of fin. ext. of k

$\overset{\text{Lemma 13.1}}{\Rightarrow}$ trace form non-degenerate.

$\Rightarrow$ For $\bar{x}_1, \dots, \bar{x}_n$ basis of $\mathcal{O}_L/p\mathcal{O}_L$ as k v.s.,

$\Delta(\bar{x}_1, \dots, \bar{x}_n) \neq 0$.

$\Rightarrow \exists x_1, \dots, x_n \in \mathcal{O}_L$ s.t. $\Delta(x_1, \dots, x_n) \not\equiv 0 \bmod p$.

Definition 12.3: The discriminant is the ideal $d_{O_L/O_K} \subseteq O_K$ generated by $\Delta(x_1, \dots, x_n)$ for all choices of $x_1, \dots, x_n \in O_L$.

Remark: Write $d_{L/K}$ if O_L, O_K understood.

Corollary 12.4: p ramifies in $L \Rightarrow p \mid d_{L/K}$

In particular, only finitely many primes ramify in L. $\square$

Definition 12.5: The inverse different is

$$\mathcal{D}^{-1}_{O_L/O_K} = \{y \in L : \mathrm{Tr}_{L/K}(xy) \in O_K \ \forall x \in O_L\}$$

an O_L submodule of L containing O_L.

Write $\mathcal{D}^{-1}_{L/K}$ if O_L, O_K understood.

Lemma 12.6: $\mathcal{D}^{-1}_{L/K}$ is a fractional ideal in L.
(i.e. contained in $\frac{1}{d} O_L$, some $d \in L$)

Proof: Let $x_1, \dots, x_n \in O_L$ basis for L/K. Set

$d := \Delta(x_1, \dots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j))$ $(\neq 0)$ separable

For $x \in \mathcal{D}^{-1}_{L/K}$, $x = \sum_{i=1}^{n} \lambda_i x_i$. $\lambda_i \in K$.

Then $\sum_{i=1}^{n} \lambda_i \mathrm{Tr}_{L/K}(x_i x_j) = \mathrm{Tr}_{L/K}(x x_j) \in O_K$.

Multiply by adjugate matrix of $a_{ij} = \mathrm{Tr}_{L/K}(x_i x_j)$

$\Rightarrow \lambda_i = \frac{1}{d} O_K \Rightarrow x \in \frac{1}{d} O_L$

Thus $\mathcal{D}^{-1}_{L/K} \subseteq \frac{1}{d} O_K \Rightarrow \mathcal{D}^{-1}_{L/K}$ fractional ideal.

$Tr(x) \in \mathcal{O}_K \ \forall x \in \mathcal{O}_L \Rightarrow \mathcal{O}_L \subseteq \mathcal{D}_{LK}^{-1}$ $\square$

Fact: All fractional ideals I in a Dedekind domain are invertible - $\exists J$ s.t. $JI = \mathcal{O}_K$.

6 The inverse $\underset{\subseteq \mathcal{O}_L}{\mathcal{D}_{L/K}}$ of $\mathcal{D}_{L/K}^{-1}$ is the ~~different~~ ~~ideal~~.

I_L, I_K groups of fractional ideals

Prop. 9.7 $\Rightarrow I_K \cong \bigoplus_{\mathfrak{p} \text{ prime in } \mathcal{O}_K} \mathbb{Z}$, $I_L \cong \bigoplus_{\mathfrak{P} \text{ prime in } \mathcal{O}_L} \mathbb{Z}$

Define $N_{L/K}: I_L \to I_K$ group hom.

Determined by $\mathfrak{P} \mapsto \mathfrak{p}^f$, where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$,

$f = f(\mathfrak{P}/\mathfrak{p})$ residue class degree.

Theorem 12.7: $N_{L/K}(\mathcal{D}_{L/K}) = d_{L/K}$.

Proof: First assume $\mathcal{O}_K, \mathcal{O}_L$ a PID.

· Let $x_1, \dots, x_n$ be an $\mathcal{O}_K$-basis for $\mathcal{O}_L$ and $y_1, \dots, y_n$ be dual basis w.r.t. Trace form

Let $\sigma_1, \dots, \sigma_n : L \to \overline{K}$ distinct embeddings (separable.

$$\sum_{i=1}^{n} \sigma_i(x_j)\sigma_i(y_k) = \mathrm{Tr}_{L/K}(x_j y_k) = \delta_{jk}.$$

But $\Delta(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$.

Thus $\Delta(x_1, \dots, x_n)\,\Delta(y_1, \dots, y_n) = 1$.

Write $\mathcal{D}_{L/K}^{-1} = \beta \mathcal{O}_L$, some $\beta \in L$. Then

$$\begin{aligned} d_{L/K}^{-1} &= (\Delta(x_1, \dots, x_n))^{-1} \\ &= (\Delta(y_1, \dots, y_n)) \\ &= (\Delta(\beta x_1, \dots, \beta x_n)) \quad \text{as } y_i, \beta x_i \text{ are } \mathcal{O}_K\text{ basis for } \mathcal{D}_{L/K}^{-1} \\ &= N_{L/K}(\beta)^2 \Delta(x_1, \dots, x_n) \end{aligned}$$

Thus $d_{L/K}^{-1} = N_{L/K}(\mathcal{D}_{L/K}^{-1})^2 d_{L/K}$

so $N_{L/K}(\mathcal{D}_{L/K}) = d_{L/K}$.

In general, localize at $S = \mathcal{O}_K \setminus \mathfrak{p}$, and use

$S^{-1}\mathcal{D}_{L/K} = \mathcal{D}_{S^{-1}\mathcal{O}_L / S^{-1}\mathcal{O}_K}$ $\quad S^{-1} d_{L/K} = d_{S^{-1}\mathcal{O}_L / S^{-1}\mathcal{O}_K}$. omit details

Lecture 15

$\mathfrak{P}$ prime of $\mathcal{O}_L$, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Can define $D_{L_\mathfrak{P}/K_\mathfrak{p}}$ using $\mathcal{O}_{K_\mathfrak{p}}, \mathcal{O}_{L_\mathfrak{P}}$.

We identify $D_{L_\mathfrak{P}/K_\mathfrak{p}}$ with a power of $\mathfrak{P}$

Theorem 12.7: $D_{L/K} = \prod_{\mathfrak{P}} D_{L_\mathfrak{P}/K_\mathfrak{p}}$.

Proof: Let $x \in L$, $\mathfrak{p} \subseteq \mathcal{O}_K$ prime.

Then $Tr_{L/K}(x) = \sum_{\mathfrak{P}|\mathfrak{p}} Tr_{L_\mathfrak{P}/K_\mathfrak{p}}(x)$ $^{(*)}$ [Cordley 10.1(

Write $D_{L_\mathfrak{P}/K_\mathfrak{p}} = \mathfrak{P}^{\delta(\mathfrak{P}/\mathfrak{p})}$, $\delta(\mathfrak{P}/\mathfrak{p}) \geq 0$.

Suppose $x \in L$ with $v_\mathfrak{P}(x) \geq -\delta(\mathfrak{P}/\mathfrak{p})$.

(i.e. x is in all local differents)

Then $Tr_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ $\forall y \in \mathcal{O}_L$ and $\forall \mathfrak{P}$.

Then $(*) \Rightarrow Tr_{L/K}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ $\forall y \in \mathcal{O}_L$, $\forall \mathfrak{p}$.

$\Rightarrow Tr_{L/K}(xy) \in \mathcal{O}_K$ $\forall y \in \mathcal{O}_L$

$\Rightarrow x \in D_{L/K}^{-1}$.

$\Rightarrow \prod_\mathfrak{P} D^{-1}_{L_\mathfrak{P}/K_\mathfrak{p}} \subseteq D^{-1}_{L/K}$, and hence $\prod_\mathfrak{P} D_{L_\mathfrak{P}/K_\mathfrak{p}} \mid D_{L/K}$.

8 For reverse inclusion, fix $\mathfrak{P}$ prime of L, and set $r = v_\mathfrak{P}(D_{L/K})$. Let $x \in \mathfrak{P}^{-r} \setminus \mathfrak{P}^{-(r+1)}$.

Then $v_\mathfrak{P}(x) = -r$ and $v_{\mathfrak{P}'}(x) \geq 0$ $\forall \mathfrak{P}' \neq \mathfrak{P}$.

By $(*)$, $\underset{}{Tr_{L_\mathfrak{P}/K_\mathfrak{p}}(xy)} = \underbrace{Tr_{L/K}(xy)}_{\mathcal{O}_K} - \underbrace{\sum_{\substack{\mathfrak{P}'|\mathfrak{p} \\ \mathfrak{P}' \neq \mathfrak{P}}} Tr_{L_{\mathfrak{P}'}/K_\mathfrak{p}}(xy)}_{A}$ $\forall y \in \mathcal{O}_L$

Hence $Tr_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}} \quad \forall y \in \mathcal{O}_L$

$\Rightarrow Tr_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}} \quad \forall y \in \mathcal{O}_\mathfrak{P}$ by continuity

$\Rightarrow x \in \mathcal{D}^{-1}_{L_\mathfrak{P}/K_\mathfrak{p}} \Rightarrow -r = v_\mathfrak{P}(x) \geq -\delta(\mathfrak{P}/\mathfrak{p})$

$\Rightarrow v_\mathfrak{P}(\mathcal{D}_{L/K}) = r \leq \delta(\mathfrak{P}/\mathfrak{p})$

$\Rightarrow \mathcal{D}_{L/K} \mid \prod_{\mathfrak{P}} \mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}}$.

Corollary 12.8: $d_{L/K} = \prod_{\mathfrak{P}|\mathfrak{p}} d_{L_\mathfrak{P}/K_\mathfrak{p}}$.

Proof: Apply $N_{L/K}$ to $\mathcal{D}_{L/K} = \prod_{\mathfrak{P}} \mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}}$. □

Corollary 12.9: $e(\mathfrak{P}/\mathfrak{p}) > 1$ iff $\mathfrak{P} \mid \mathcal{D}_{L/K}$.

Proof: $\mathfrak{P} \mid \mathcal{D}_{L/K}$ iff $\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}}$. Since $e(\mathfrak{P}/\mathfrak{p}) = e_{L_\mathfrak{P}/K_\mathfrak{p}}$ suffices to consider case L/K extension of complete discretely valued fields.

$N_{L/K}(m_L) = m_K^{f_{L/K}}$ and hence

$m_L \mid \mathcal{D}_{L/K} \Leftrightarrow m_K \mid d_{L/K} \Leftrightarrow e_{L/K} > 1$