Math 538, Lecture 16, 8/13/2024

Last time: L/K finite extension of (1) #fields, (2) fields complete wrt discrete valuation

For $\Lambda \subset L$, $\Lambda^* = \{x \in L \mid \forall y \in \Lambda : \mathrm{Tr}_K^L(xy) \in \mathcal{O}_K\}$

① If $\mathfrak{a} \subset L$ is a fractional ideal, so is $\mathfrak{a}^*$.

② Def: complementary module: $\mathfrak{C}_{L/K} = \mathcal{O}_L^* \supset \mathcal{O}_L$

③ Def: relative different $\mathcal{D}_{L/K} = \mathfrak{C}_{L/K}^{-1} \triangleleft \mathcal{O}_L$.

(saw: if $\mathfrak{a}$ is a fractional ideal, $\mathfrak{a}^* = \mathfrak{C}_{L/K} \cdot \mathfrak{a}^{-1}$)

Lemma: In tower $M/L/K$, $\mathcal{D}_{M/K} = \mathcal{D}_{L/K} \cdot \mathcal{D}_{M/L}$.

Today: Explicit calculation of $\mathcal{D}_{L/K}$
$\Rightarrow$ ramification

Prop: Suppose L/K separable, $L = K(\alpha)$, min poly of α is $f \in K[x]$. Define $b_i \in L$ by $\frac{f(x)}{x-\alpha} = \sum_{i=0}^{n-1} b_i x^i$. Then basis of L dual to $\{\alpha^i\}_{i=0}^{n-1}$ is $\left\{\frac{b_i}{f'(\alpha)}\right\}_{i=0}^{n-1}$. Furthermore, if $\alpha \in \mathcal{O}_L$ then $\mathcal{O}_K[\alpha]^* = \frac{1}{f'(\alpha)} \mathcal{O}_K[\alpha]$

Cor: Since $\mathcal{O}_K[\alpha] \subset \mathcal{O}_L$ if $\alpha \in \mathcal{O}_L$,
get $\mathcal{O}_L^* \subset \frac{1}{f'(\alpha)} \mathcal{O}_K[\alpha] \subset \frac{1}{f'(\alpha)} \mathcal{O}_L$

so $\mathcal{D}_{L/K} \supset f'(\alpha) \mathcal{O}_L$.

Pf of Prop: Let $g(x) = \frac{f(x)}{x-\alpha}$, let β be a root of f.

Then $g(\beta) = \begin{cases} f'(\beta) & \beta = \alpha \\ 0 & \beta \neq \alpha \end{cases}$

(write $f(x) = \prod_\beta (x-\beta)$ so $f'(x) = \sum_{f(\gamma)=0} \prod_{\beta \neq \gamma} (x-\beta)$)

Enumerate roots of f as $\{\alpha_i\}_{i=1}^n$, $\alpha_1 = \alpha$

Set
$$h(X) = \sum_{i=1}^n \frac{f(X)}{X-\alpha_i} \cdot \frac{\alpha_i^r}{f'(\alpha_i)}$$

Since $\frac{f(\alpha_j)}{\alpha_j - \alpha_i} = 0$ if $\alpha_j \neq \alpha_i$, $\frac{f(\alpha_j)}{\alpha_j - \alpha_j} = f'(\alpha_j)$

$$h(\alpha_j) = \alpha_j^r$$

so $h - X^r$ has n zeroes, degree $\leq n-1$ if $r \leq n-1$.

so $h = \delta^r$ if $r \le n-1$

But $h(\delta) = Tr^L_K \frac{f(\delta)}{x-\alpha} \cdot \frac{\alpha^r}{f'(\alpha)} = Tr^L_K \, g(\delta) \frac{\alpha^r}{f'(\alpha)}$

if take ith coeff get

$$\delta_{ir} = Tr^L_K \left(\frac{b_i}{f'(\alpha)} \alpha^r \right)$$

$\Rightarrow \left\{ \frac{b_i}{f'(\alpha)} \right\}_{i=0}^{n-1}$ is the dual basis. ✓

Now suppose $\alpha \in \mathcal{O}_L$, i.e. $f \in \mathcal{O}_K[x]$, $f = \sum_{i=0}^{n} a_i x^i$
with $a_i \in \mathcal{O}_L$, $a_n = 1$

Then

$$(x-\alpha) \sum_{i=0}^{n-1} b_i x^i = \sum_{j=0}^{n} a_j x^j$$

$\Leftrightarrow$ $b_i - \alpha b_{i+1} = a_{i+1}$ (set $b_{-1} = b_n = 0$)

i.e. $b_{n-1} = 1$, $b_i \in \mathcal{O}_K[\alpha]$.
[if $\{b_j\}_{j>i} \subset \mathcal{O}_K[\alpha]$, $b_i = a_{i+1} + \alpha b_{i+1} \in \mathcal{O}_K[\alpha]$].

$\Rightarrow \mathcal{O}_K[\alpha]^* = \bigoplus_i \mathcal{O}_K \frac{b_i}{f'(\alpha)} \subset \frac{1}{f'(\alpha)} \mathcal{O}_K[\alpha]$.

Conversely, suppose $\alpha^i \in \mathrm{Span}_{\mathcal{O}_k}\{b_j\}_{j \geq n-i-1}$

(e.g. $b_{n-1} = 1$ so $\alpha^0 \in \mathrm{Span}_{\mathcal{O}_k}\{b_{n-1}\}$)

Then $\alpha b_j = b_{j-1} - a_j b_{n-1}$

$$\alpha^i \in \mathrm{Span}\{b_j\}_{j \geq n-1-i}$$

so $\alpha^{i+1} \in \mathrm{Span}_{\mathcal{O}_k}\{\alpha b_j\}_{j \geq n-1-i}$

$$\subseteq \mathrm{Span}_{\mathcal{O}_k}\{b_{j-1}\}_{j \geq n-1-i} \cup \{b_{n-1}\} \quad \checkmark$$

$\mathcal{O}_k[\alpha] \subset \bigoplus_{i=0}^{n-1} \mathcal{O}_k \cdot b_i$, dualize. $\blacksquare$

Cor: $L = k(\alpha)$, $\alpha \in \mathcal{O}_L$, f min poly then

$$\mathfrak{D}_{L/k} \mid f'(\alpha)\mathcal{O}_L.$$

Ex: $\mathfrak{D}_{L/k} = \gcd\{f'(\alpha) : \begin{array}{l} L = k(\alpha) \\ f \text{ min poly} \end{array}\}$

Example: if L/K unram ext'n of complete fields with discrete valuation, then $\mathfrak{D}_{L/K} = (1)$

Pf: Let $\alpha \in \mathcal{O}_L$ s.t. $\lambda = \kappa(\bar{\alpha})$

$(\lambda = \mathcal{O}_L/\mathfrak{P}, \ \kappa = \mathcal{O}_K/\mathfrak{p}, \ \bar{\alpha} = \text{Image of } \alpha \text{ in } \lambda)$

f = min poly. Then $\bar{f} \in \kappa[x]$ is min poly of $\bar{\alpha}$: $\bar{f}(\bar{\alpha}) = 0$, $\deg f = \deg \bar{f} \geq [\lambda : \kappa] = [L : K]$.
So $\deg f = [L : K]$ and α generates L.
By def'n of "unramified" $\bar{f}'(\bar{\alpha}) \neq 0$

$$\bar{f}'(\bar{\alpha}) = \overline{f'(\alpha)}.$$

So $f'(\alpha) \in \mathcal{O}_L^\times$ so $f'(\alpha)\mathcal{O}_L = (1)$ ∎.

Next: show $D_{L/K} = \prod_{w \in |L|_f} D_{L_w/K_v}$ $\quad v = w|_K$.

Def: For $S \subset |L|_f$ finite, the S-integer are

$$\mathcal{O}_L^S = \{x \in L \mid \forall w \in |L|_f \setminus S : |x|_w \leq 1\}$$

Examples $\mathbb{Z}^{\{2\}} = \left\{\frac{m}{2^k} : \begin{array}{l} m \in \mathbb{Z}, 2 \nmid m \\ k \in \mathbb{Z} \end{array}\right\}$

$\mathbb{Z}^{\{2,3\}} = \left\{\frac{m}{2^k 3^l} : \begin{array}{l} m \in \mathbb{Z} \\ k, l \in \mathbb{Z} \end{array}\right\}$

lemma: $\mathcal{O}_L^S$ is dense in $L_S = \prod_{w \notin S} L_w$

(strong approximation)

[cf. L dense L_S ("weak approx")]

$\leftrightarrow$ $\forall (x_w)_{w \in S} \in \prod_w L_w$ $\forall \varepsilon$ $\exists x \in L$:

(1) $\forall w \in S$: $|x - x_w|_w < \varepsilon$

(2) $\forall w \notin S$ finite $|x|_w \leq 1$.

Pf in $\mathbb{Q}$: given $(x_p)_{p \in S}$ let k_p be st. $p^{k_p} x_p \in \mathbb{Z}_p$

define $\tilde{x}_p = \underbrace{(\prod_p p^{k_p})}_{Q} \cdot x_p$, $\tilde{x}_p \in \mathbb{Z}_p$ if $p \in S$

By CRT have $\tilde{x} \in \mathbb{Z}$ s.t. $\tilde{x} \equiv \tilde{x}_p \ (p^N)$ for each $p \in S$

Then $\overset{\text{if } p \in S}{|Q^{-1} \tilde{x} - x_p|_p} = |Q^{-1}|_p \cdot |\tilde{x} - \tilde{x}_p|_p$

$\leq p^{k_p} \cdot p^{-N}$;

if $p \notin S$ $|Q^{-1} \tilde{x}|_p \leq 1$: $\underset{p \nmid Q}{\tilde{x} \in \mathbb{Z}}$.

Prop: L/K # fields, $w \in |L|_f$, $v \in |K|_f$, $w|v$. Corresp ideal of L is $\mathfrak{P}$. Then exponent of $\mathfrak{P}$ in $\mathfrak{D}_{L/K}$ is the exponent of $\mathfrak{P}_w$ in $\mathfrak{D}_{L_w/K_v}$.

Pf: $\Leftrightarrow$ look at exponents for $\mathfrak{e}_{L/K}$, $\mathfrak{e}_{L_w/K_w}$.

Saw: exponents are same iff $\overline{\mathfrak{e}_{L/K}} = \mathfrak{e}_{L_w/K_v}$

top closure in L_w

$S = \{w' \text{ of } L \mid w|v\}$

If $x \in \mathfrak{e}_{L/K}$, $y \in \mathcal{O}_{L_w}$. By strong approx have $z \in \mathcal{O}_L^S$ s.t. z is w-close to y, z is is w'-close to 0 if $w'|v$, $w' \neq w$.

Want to understand $\mathrm{Tr}^{L_w}_{K_v} xy$

Know if $z \in L$, $\mathrm{Tr}^L_K(xz) = \mathrm{Tr}^{L_w}_{K_v}(xz)$

$$+ \sum_{\substack{w'|v \\ w' \neq w}} \mathrm{Tr}^{L_{w'}}_{K_v}(xz)$$

By choice of z, $z \in \mathcal{O}_L$, $\mathrm{Tr}^L_K(xz) \in \mathcal{O}_K \in \mathcal{O}_{K_v}$ ($x \in \mathfrak{e}_{L/K}$).

Get:

$$\mathrm{Tr}^{L_w}_{K_v}(xz) = \mathrm{Tr}^{L}_{K}(xz) - \sum_{\substack{w'|v \\ w'\neq w}} \mathrm{Tr}^{L_{w'}}_{K_v}(xz)$$

$$\overset{\cap}{\mathcal{O}_{K_v}} \qquad\qquad \overset{\cap}{\mathcal{O}_{K_v}}$$

since $|z|_{w'}$ small

st $|xz|_{w'} \le 1$

$$\Rightarrow \mathrm{Tr}^{L_w}_{K_v}(xy) = \mathrm{Tr}^{L_w}_{K_v}(xz) + \mathrm{Tr}^{L_w}_{K_v}(x(y-z))$$

can choose z st $x(y-z) \in \mathcal{O}_{L_w}$.

$$\Rightarrow \mathrm{Tr}^{L_w}_{K_v}(xy) \in \mathcal{O}_{K_v}.$$

<u>Conclude:</u> $\mathcal{C}_{L/K} \subset \mathcal{C}_{L_w/K_v} \Rightarrow \overline{\mathcal{C}_{L/K}} \subset \mathcal{C}_{L_w/K_v}$

<u>Conversely:</u> let $x \in \mathcal{C}_{L_w/K_v}$ let $z \in \mathcal{O}_L^S$ be st.

$|z-x|_w$, $|z|_{w'}$ small $(w' \neq w)$

wants $z \in \mathcal{C}_{L/K}$. let $y \in \mathcal{O}_L$, study $\mathrm{Tr}^L_K(zy)$

if $v' \neq v$ for all $w'|v'$, both z, y are w'-integral. so $\mathrm{Tr}^L_K(zy) = \sum_{w'|v'} \mathrm{Tr}^{L_{w'}}_{K_{v'}}(zy) \in \mathcal{O}_{K_{v'}}$

$\Rightarrow \mathrm{Tr}^{L}_{K}(zy)$ is v'-integral if $v' \neq v$.

At v, $\mathrm{Tr}^{L}_{K}(zy) = \mathrm{Tr}^{L_w}_{K_v}(zy) + \sum_{\substack{w'|v \\ w' \neq w}} \mathrm{Tr}^{L_{w'}}_{K_v}(zy)$

$= \underbrace{\mathrm{Tr}^{L_w}_{K_v}(xy)}_{\in\, \mathcal{O}_{K_v}} + \underbrace{\mathrm{Tr}^{L_w}_{K_v}((z-x)y)}_{\in\, \mathcal{O}_{K_v}} + \sum_{\substack{w'|v \\ w' \neq w}} \underbrace{\mathrm{Tr}^{L_{w'}}_{K_v}(zy)}_{\in\, \mathcal{O}_{K_v}}$

$x \in \mathfrak{C}_{L_w/K_v}$, $y \in \mathcal{O}_L \subseteq \mathcal{O}_{L_w}$

if $|z-x|_w \leq 1$

if $|z|_{w'} \leq 1$

$\Rightarrow \mathrm{Tr}^{L}_{K}(zy) \in \mathcal{O}_{K_v}$. $\Rightarrow \mathrm{Tr}^{L}_{K}(zy) \in \mathcal{O}_K$

$\Rightarrow z \in \mathfrak{C}_{L/K}$ so $\mathfrak{C}_{L/K}$ is dense in $\mathfrak{C}_{L_w/K_v}$. ∎

Summary: Know $D_{L/K} = \prod_{v \in |K|_f} \cdot \prod_{w|v} D_{L_w/K_v}$

if L/K unram at w, $D_{L_w/K_v} = (1)$

need converse: if $e(\mathfrak{P}_w : \mathfrak{p}_v) > 1$, $\mathfrak{P}_w \mid D_{L_w/K_v}$.

Prop: Let L_w/K_v be a finite extension of fields complete wrt discrete valuation. Let $e = e(L_w/K_v)$. Then $\mathfrak{P}_w^{e-1} \mid \mathcal{D}_{L_w/K_v}$:

(1) $e=1$ or ramification is tame $\Rightarrow$ equality
(2) ramification is wild: $\mathfrak{P}_w^{e} \mid \mathcal{D}_{L_w/K_v}$

$\Downarrow$

Thm: L/K finite extension of # fields $\mathfrak{P} \triangleleft \mathcal{O}_L$ above $\mathfrak{p} \triangleleft \mathcal{O}_K$. Then

$$v_{\mathfrak{P}}(\mathcal{D}_{L/K}) \geq e(\mathfrak{P} : \mathfrak{p}) - 1,$$

equality iff $p \nmid e(\mathfrak{P} : \mathfrak{p})$ (p = rational prime below $\mathfrak{p}, \mathfrak{P}$)

Cor: ① $\mathfrak{P} \mid \mathcal{D}_{L/K}$ iff $\mathfrak{P}$ ramified
② at most finitely many ramified primes