Math 538, Lecture 18, 15/3/2024

Last time: Discriminants

$\mathrm{Hom}_K(L, \bar{K}) = \{\mu_j\}_{j=1}^{n}$ $\quad n = [L:K]$

$\Omega \subset L$ K-basis

$$\Rightarrow a_{ij} = \mu_j(\omega_i)$$

$$D_{L/K}(\Omega) \overset{\text{def}}{=} (\det A)^2 = \det(AA^t) \in K^\times$$

$$(AA^t)_{ij} = \mathrm{Tr}_K^L(\omega_i \omega_j).$$

$L = K(\alpha)$, $\Omega = \{\alpha^i\}_{i=0}^{n-1}$ $\Rightarrow D_{L/K}(\Omega) = \prod_{i<j} (\alpha_i - \alpha_j)^2$

Galois conj $\{\alpha_i\}_{i=1}^{n}$ $\quad = \mathrm{discr}(f)$.

$\mathfrak{a} \subset L$ $\quad \mathcal{O}_K$-submodule, $\quad D_{L/K}(\mathfrak{a}) = \left(\{ D_{L/K}(\Omega) \mid \underset{K\text{-basis}}{\Omega \subset \mathfrak{a}} \} \right)$

$$D_{L/K} = D_{L/K}(\mathcal{O}_L) \subset \mathcal{O}_K.$$

Prop: (local-to-global) L/K # fields, $v \in |K|_f$.
Then closure of $D_{L/K}$ in $\mathcal{O}_v$ is $\prod_{w|v} D_{L_w/K_v}$.

Pf: Saw $\overline{D_{L/K}} \supset \prod_{w|v} D_{L_w/K_v}$.

(idea: look at K_v-alg $L \otimes_K K_v \cong \bigoplus_{w|v} L_w$.)

approximate K_v-bases $\bigcup_w \mathcal{O}_w$ by basis $\mathcal{A} \subset L$.

For converse, let $\mathcal{A} \subset \mathcal{O}_L$ be a K-basis.

Its image in $\bigoplus_{w|v} L_w$ is a K_v-basis

Fact: Let K_v be complete wrt discrete valuation, V K_v-vsp (f.d.), $\mathcal{A}, \mathcal{A}' \subset V$ K_v-bases. Then there is $g \in GL_n(\mathcal{O}_{K_v})$ changes basis from $\{w_j'\} = \mathcal{A}'$ to

$$\sum_i g_{ij} w_j' = \varpi_v^{d_i} w_i.$$

$\varpi_v \in \mathcal{O}_{K_v}$ is a uniformizer.

---

replacing $\mathcal{A}$ with $g \cdot \mathcal{A}$ changes $D_{\mathcal{A}}(\mathcal{A})$ by element of $\mathcal{O}_{K_v}^\times$, can ensure $g\mathcal{A}$ lies in $\bigcup_w \mathcal{O}_{L_w}$.

Pf of fact: Gaussian elimination, choose pivot of max'l absolute value

Thm: $D_{L/K} = N^L_K \mathcal{D}_{L/K}$. (discr = norm of diff)

Pf: Since both discr & diff localize enough to show when L/K complete wrt discrete valuation

Now $\mathcal{O}_K$ is a PID so $\mathcal{O}_L = \bigoplus_{i=1}^n \mathcal{O}_K w_i$
for some K-basis $\{w_i\}$.

$\Rightarrow D_{L/K} = D_{L/K}(\Omega)$ $\Rightarrow \mathcal{C}_{L/K} = \bigoplus_{i=1}^n \mathcal{O}_K w_i^*$

let A, A^* be the matrices assoc to Ω, Ω^*.

$$(A \cdot {}^tA^*)_{ij} = Tr^L_K(w_i w_j^*) = (w_i, w_j^*) = \delta_{ij}$$

$\Rightarrow A \cdot {}^tA^* = Id$, so $D_{L/K}(\Omega) \cdot D_{L/K}(\Omega^*) = 1$

On the other hand, $\mathcal{C}_{L/K} = \beta^{-1}\mathcal{O}_L$ for some $\beta \in \mathcal{O}_L$

$\Rightarrow$

$$D_{L/K}(\Omega^*) = D_{L/K}(\mathcal{C}_{L/K}) = (N^L_K \beta)^{-2} \cdot D_{L/K}$$

$$1 = D_{L/K} \cdot D_{L/K}(\Omega^*) = (N^L_K \mathcal{D}_{L/K})^{-2} \cdot D_{L/K}^2$$

$\beta \mathcal{O}_L$
different

$\Rightarrow D_{L/K} = N^L_K \mathcal{D}_{L/K}$ ∎

Cor: (discr in towers) If $M/L/K$ # fields

$$D_{M/K} = D_{L/K}^{[M:L]} \cdot N_K^L D_{M/L}$$

Pf: for differents, $\mathcal{D}_{M/K} = \mathcal{D}_{L/K} \cdot \mathcal{D}_{M/L}$.

Digression: $\Delta(f)$

Let $f(x) = \prod_i (x - \alpha_i)$ be a polynomial

Then $\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$ is a symmetric poly

in roots, hence a poly in coeff $\{a_i\}_{i=0}^{n-1}$ of f.

Also, Δ is homogeneous of deg $n(n-1)$ in roots

$\Rightarrow$ each monomial of $\Delta = \Delta(a_0, \ldots, a_{n-1})$ must be

of deg $n(n-1)$, where $\deg a_i = n - i$.

Prop: (1) Let $f(x) = x^n + b$. $\Delta(f) = (-1)^{\frac{n(n-1)}{2}} n^n b^{n-1}$.

(2) $f(x) = x^n + ax + b$.

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}}\left[n^n b^{n-1} + (-1)^{n-1}(n-1)^{(n-1)} a^n\right].$$

Pf: HW, note b^{n-1}, a^n only monomials in a, b of deg $n(n-1)$, so $\Delta(f) = C_1(n) b^{n-1} + C_2(n) a^n$.

Example: $D(x^3 + ax + b) = -\left[4a^3 + 27b^2\right]$

$$\propto \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2.$$

Example: $\mathbb{Q}(\zeta_n)$

Let ζ_n be a primitive root of unity of deg n, ($\zeta_n^n = 1$, $\zeta_n^d \neq 1$ if $d < n$) Then $\mathbb{Q}(\zeta_n)$ = splitting field of $x^n - 1$, thus Galois.

Get injection $Gal(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$

by $\sigma \mapsto a$

s.t. $\sigma(\zeta_n) = \zeta_n^a$.

hom: if $\sigma(\zeta_n) = \zeta_n^a$, $\tau(\zeta_n) = \zeta_n^b$

then $(\sigma\tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^b) = \sigma(\zeta_n)^b = \zeta_n^{ab}$.

$\Rightarrow$ $Gal(\mathbb{Q}(\zeta_n):\mathbb{Q})$ is abelian, $[\mathbb{Q}(\zeta_n):\mathbb{Q}] \mid \phi(n)$

Def: The n'th Cyclotomic polynomial is

$$\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a) \in \mathbb{Z}[x]$$

clearly $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$.

Key point: Φ_n irred. $\Rightarrow$ equality, $Gal(\mathbb{Q}(\zeta_n):\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Step 1: $n = p^r$, p prime

$K = \mathbb{Q}(\zeta_n)$

Prop: $[K:\mathbb{Q}] = p^{r-1}(p-1) = \phi(p^r)$; $K/\mathbb{Q}$ is only ramified at p (and ∞), where it is totally ramified and $\pi = 1 - \zeta_{p^r}$ is a prime element

Pf: $\Phi_{p^r}(X) = \dfrac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = \Phi_p(X^{p^{r-1}}) = \sum_{j=0}^{p-1} X^{jp^{r-1}}$.

$\pi = \zeta_{p^r} - 1$ is a root of $\Phi_{p^r}(Y+1)$

which is Eisenstein at p:

mod p, $\Phi_{p^r}(X) \equiv \dfrac{(X-1)^{p^r}}{(X-1)^{p^{r-1}}} = (X-1)^{p^r - p^{r-1}}$.

$\Phi_{p^r}(Y+1) \equiv Y^{p^r - p^{r-1}} \pmod p$

$\Phi_{p^r}(1) = \sum_{j=0}^{p-1} 1 = p$ not 0 mod p^2.

Also ζ_n is a root of $x^n - 1$, ~~its~~ derivative nx^{n-1}, so $p \mid \Delta(x^n - 1)$ iff $p \mid n$, so only $p \mid n$ may ramify in $\mathbb{Q}(\zeta_n)$

<u>Alternative:</u> $\dfrac{1-\zeta_{p^r}^k}{1-\zeta_{p^r}} = \sum_{j=0}^{k-1} \zeta_{p^r}^j \in \mathbb{Z}[\zeta_n]$.

for any invertible a, b mod p^r, write $b = ac$ for $c < p^r$ then

$$\frac{1-\zeta_{p^r}^b}{1-\zeta_{p^r}^a} = \sum_{j=0}^{c-1} \zeta_{p^r}^{ja}$$

$\Rightarrow \dfrac{1-\zeta_{p^r}^b}{1-\zeta_{p^r}^a} \in \mathbb{Z}[\zeta_{p^r}]^\times$ ("cyclotomic units")

$\Rightarrow 1-\zeta_{p^r}^a$ all associate

$\Rightarrow \pi^{\phi(p^r)} \sim \prod'_{a(p^r)} (1 - \zeta_{p^r}^a) = \Phi_{p^r}(1) = p$

$\Rightarrow$ If $\mathfrak{P}$ prime of K contains π, $e(\mathfrak{P} : p) \geq \phi(p^r)$
but $[K : \mathbb{Q}] \leq \phi(p^r)$ $\Rightarrow$ get $e(\mathfrak{P} : p) = [K : \mathbb{Q}] = \phi(p^r)$

π prime
(unique prime ideal containing (π) because sum of ramification indices is at most degree) ∎

<u>Lemma</u>; $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$.

<u>Pf</u>; let $\mathcal{O} = \mathbb{Z}[\zeta_{p^r}] \subset \mathcal{O}_K$

Now $\mathcal{O}_K / \pi \mathcal{O}_K \simeq \mathbb{Z}/p\mathbb{Z}$ (extension totally ramified, or by hand) $\Rightarrow \mathcal{O}_K = \mathbb{Z} + \pi \mathcal{O}_K$.
$= \mathcal{O} + \pi \mathcal{O}_K$

recursively $\mathcal{O}_K = \mathcal{O} + \pi^l \mathcal{O}_K$ for all l

(if true, also $\pi^l \mathcal{O}_K = \pi^l \mathcal{O} + \pi^{l+1} \mathcal{O}_K$).

<u>Approach 1</u>; $D_{K/\mathbb{Q}}(\mathcal{O}) = \Delta(\Phi_{p^r}) =$ power of p
(divide $\Delta(x^{p^r} - 1)$)

so $[\mathcal{O}_K : \mathcal{O}]$ is a power of p

so index will remain same in π-adic completion

But closures have $\overline{\mathcal{O}_K} = \overline{\mathcal{O}} + \pi^\ell \overline{\mathcal{O}_K}$
can take $\ell \to \infty$ get $\overline{\mathcal{O}_K} = \overline{\mathcal{O}}$ so $\mathcal{O} = \mathcal{O}_K$

Approach: $\pi^{\phi(p^r) - \ell} \sim p^\ell$ in $\mathcal{O}$
Then
$$\mathcal{O}_K = \mathcal{O} + p^\ell \mathcal{O}_K$$

But since $[\mathcal{O}_K : \mathcal{O}]$ = power of p

$\Rightarrow$ $p^\ell \mathcal{O}_K \subset \mathcal{O}$ for ℓ large

$\Rightarrow$ $\mathcal{O}_K \subset \mathcal{O}$. ∎

Cors $D_{K/\mathbb{Q}} = \mathrm{discr}(\Phi_{p^r}) = \pm p^{p^{r-1}(rp-r-1)}$

(HW)

Step 2: $K = \mathbb{Q}(\zeta_n)$, $n = \prod_{i=1}^{s} p_i^{r_i}$.

Recaps $(X^n - 1)' = nX^{n-1}$, different $\mathcal{D}_{K/\mathbb{Q}} \mid n$

so only p_i may ramify. Also $K \supset \mathbb{Q}(\zeta_{p_i^{r_i}})$
so all p_i do ramify.

let $K_j = \mathbb{Q}(\{\zeta_{p_i^{r_i}}\}_{i=1}^{j})$ so $K_0 = \mathbb{Q}$.

$K_s = K$ since $\prod_{i=1}^{s} \zeta_{p_i^{r_i}}$ is primitive of order $\prod_i p_i^{r_i}$.

For each i, p_i is unram in K_{i-1}:

if p unram in K_1/F, K_2/F

it's unram in K_1K_2/F ! $K_2 = F(\alpha)$

then $K_1K_2 = K_1(\alpha)$.

so ramification index at p of K_i/K_{i-1} is at most $\phi(p_i^{r_i})$. But this is $=$ index $K_i/\mathbb{Q}$
$\geq$ index $(\mathbb{Q}(\zeta_{p_i^{r_i}}) : \mathbb{Q}) = \phi(p_i^{r_i})$

$\Rightarrow [K_i : K_{i-1}] \geq \phi(p_i^{r_i})$

so $\Phi_{p_i^{r_i}}$ is still irred in K_{i-1}.

$\Rightarrow [K_i : K_{i-1}] = \phi(p_i^{r_i})$

$\Rightarrow [K_s : K_0] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \prod_i \phi(p_i^{r_i}) = \phi(n)$.

$\Rightarrow \Phi_n$ is irred in $\mathbb{Z}[x]$

(in $\mathbb{Z}[\zeta_m][x]$ if $(m,n)=1$)

Thm: $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$