3.3. Relative different & discriminant

Recall: L/K fin. ext. of #-fields

Then $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ ramified in $\mathcal{O}_L \iff \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is reduced

$\iff$ $k(\mathfrak{p})$-bil. pairing

$$\mathrm{Tr}: \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \times \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \to k(\mathfrak{p})$$

is non-deg.

$\iff$ $\mathfrak{p} \mid \Delta_L$

$\uparrow$ if $K = \mathbb{Q}$

Generalize last "$\iff$" to arbitrary K

Def: $\mathfrak{q} \subseteq \mathcal{O}_L$ max'l, $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$

$\Rightarrow N_{L/K}(\mathfrak{q}) := \mathfrak{p}^{f(\mathfrak{q}|\mathfrak{p})}$

(ideal) norm of $\mathfrak{q}$

If $0 \neq I \subseteq L$ fract.,

$I := \prod_{i=1}^{r} \mathfrak{q}_i^{a_i} \Rightarrow N_{L/K}(I)$

$:= \prod_{i=1}^{r} N_{L/K}(\mathfrak{q}_i)^{a_i}$

La: 1) $N_{L/K}(I \cdot J) = N_{L/K}(I) \cdot N_{L/K}(J)$

2) If $K = \mathbb{Q} \Rightarrow$

$N_{L/K}(I) = (N(I))$, where

$N(I) = \#(\mathcal{O}_L / I)$

3) If $I = J \cdot \mathcal{O}_L$ for $0 \neq J \subseteq \mathcal{O}_K$

$\Rightarrow N_{L/K}(I) = J^{[L:K]}$

4) M/L finite, $I \subseteq M$ fract.

$\Rightarrow N_{M/K}(I) = N_{L/K}(N_{M/L}(I))$

5) $I = (x)$, $x \in L \setminus \{0\}$

$\Rightarrow N_{L/K}((x)) = (N_{L/K}(x))$

Pf: 1) ✓

2) w.log $I = \mathfrak{q}$ max.

$\Rightarrow N(\mathfrak{q}) = \#(\mathcal{O}_L/\mathfrak{q}) = \#k(\mathfrak{q})$

$= p^{f(\mathfrak{q}|p)}$, $(p) = \mathfrak{q} \cap \mathbb{Z}$

3) Wenn $I = \mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$

$\Rightarrow N_{L/K}(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{g} (\mathfrak{p}^{f(\mathfrak{P}_i|\mathfrak{p})})^{e_i}$

$= \mathfrak{p}^{\sum_{i=1}^{g} f(\mathfrak{P}_i|\mathfrak{p}) \cdot e_i} = \mathfrak{p}^{[L:K]}$

↑ last time

4) ✓ $f(-|-)$ transitive

5) Exercise (Hint: Localize & use that a Dedekind ring with fin. many primes is a PID)

Def: $\delta_{L/K}^{-1} := \{x \in L \mid Tr_{L/K}(x \cdot \eta) \in \mathcal{O}_K \quad \forall \eta \in \mathcal{O}_M\} \supseteq \mathcal{O}_M$

inverse relative different

** $\delta_{L/K} := (\delta_{L/K}^{-1})^{-1}$

* $Disc_{L/K} := N_{L/K}(\delta_{L/K})$

Note: $\mathfrak{p} \subseteq \mathcal{O}_K$ ramifies in $\mathcal{O}_L$

$\Leftrightarrow \mathfrak{p} \mid Disc_{L/K}$

* If $K = \mathbb{Q}$, $Disc_{L/\mathbb{Q}} = (\Delta_{ML})$

La: $I \subseteq K$ fract.

$\Rightarrow I \cdot \mathcal{O}_L \cdot \delta_{L/K}^{-1} = \{x \in L \mid Tr_{L/K}(x) \in I\}$

Proof: $Tr_{L/K}(x) \in I$

$\Leftrightarrow Tr_{L/K}(x) \cdot I^{-1} \subseteq \mathcal{O}_K$

$\Leftrightarrow Tr_{L/K}(x \cdot I^{-1}) \subseteq \mathcal{O}_K$

$\Leftrightarrow x \cdot I^{-1} \cdot \mathcal{O}_L \subseteq \delta_{L/K}^{-1}$

$\Leftrightarrow x \in I \cdot \mathcal{O}_L \cdot \delta_{L/K}^{-1}$ ∎

Prop: M/L finite

$\Rightarrow \delta_{M/K} = \delta_{L/K} \cdot \mathcal{O}_M \cdot \delta_{M/L}$

$\Rightarrow Disc_{M/K} = Disc_{L/K}^{[M:L]} \cdot N_{L/K}(Disc_{M/L})$

Proof: $x \in \delta_{M/K}^{-1}$

$\Leftrightarrow \mathrm{Tr}_{M/K}(x \cdot y) \in \mathcal{O}_K \quad \forall y \in \mathcal{O}_M$

$\Leftrightarrow \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x \cdot y)) \in \mathcal{O}_K \quad \forall y \in \mathcal{O}_M$

$\Leftrightarrow \mathrm{Tr}_{M/L}(x \cdot y) \in \delta_{L/K}^{-1} \quad \forall y \in \mathcal{O}_M$

$\overset{\text{Prev. Le}}{\Leftrightarrow} x \cdot y \in \delta_{L/K}^{-1} \cdot \mathcal{O}_M \cdot \delta_{M/L}^{-1} \quad \forall y \in \mathcal{O}_M$

$\Leftrightarrow x \in \delta_{L/K}^{-1} \cdot \mathcal{O}_M \cdot \delta_{M/L}^{-1}$ □

"$\Rightarrow$" Let $z \in \mathcal{O}_L$. Stp:

$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x \cdot y) \cdot z) \in \mathcal{O}_K$

$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x \cdot y \cdot \underbrace{z}_{\in \mathcal{O}_M}))$

Prop: L_1, L_2 number fields,
$M = L_1 \cdot L_2$. Assume
$M \simeq L_1 \underset{\mathbb{Q}}{\otimes} L_2$ ($\Leftrightarrow L_1 \cap L_2 = \mathbb{Q}$)

Then:

1) $\delta_{L_2} \cdot \mathcal{O}_M \subseteq \delta_{M/L_1}$

2) Δ_M divides $\Delta_{L_1}^{[L_2:\mathbb{Q}]} \cdot \Delta_{L_2}^{[L_1:\mathbb{Q}]}$

3) If $\gcd(\Delta_{L_1}, \Delta_{L_2}) = 1$

$\Rightarrow |\Delta_M| = |\Delta_{L_1}|^{[L_2:\mathbb{Q}]} \cdot |\Delta_{L_2}|^{[L_1:\mathbb{Q}]}$

Proof: 1) $\langle \beta_1, \dots, \beta_m \rangle_{\mathbb{Z}} \subseteq \mathcal{O}_{L_2}$,

$x \in \delta_{M/L_1}^{-1}$

Write $x = \sum_{i=1}^{m} x_i \beta_i^\vee$, $x_i \in L_1$

$(\langle \beta_1^\vee, \dots, \beta_m^\vee \rangle_{L_1} = M)$

Know: $(\mathrm{Tr}_{L_2/\mathbb{Q}}(\beta_i \beta_j^\vee) = \delta_{ij})$

$\mathrm{Tr}_{M/L_1}(x \cdot \eta) \in \mathcal{O}_{L_1} \quad \forall \eta \in \mathcal{O}_M$

$(x \in \delta_{M/L_1}^{-1})$

In part., $\mathrm{Tr}_{M/L_1}(x \cdot \beta_i)$

$$= \sum_{j=1}^{m} x_j \underbrace{\mathrm{Tr}_{M/L_1}(\beta_j^\vee \beta_i)}_{= \mathrm{Tr}_{L_2/\mathbb{Q}}(\beta_j^\vee \beta_i)} = x_i \in \mathcal{O}_{L_1}$$

$\Rightarrow x \in \mathcal{O}_{L_1} \cdot \delta_{L_2}^{-1} \subseteq \mathcal{O}_M \cdot \delta_{L_2}^{-1}$

$(\delta_{L_2}^{-1} = \langle \beta_1^\vee, \dots, \beta_m^\vee \rangle_{\mathbb{Z}}$

2) (Δ_M) $\quad K = \mathbb{Q}$

$$= N_{L_1/\mathbb{Q}}(\mathrm{Disc}_{M/L_1}) \cdot \underbrace{\mathrm{Disc}_{L_1/\mathbb{Q}}^{[L_2:\mathbb{Q}]}}_{(\Delta_{L_1})^{[L_2:\mathbb{Q}]}}$$

& $\mathrm{Disc}_{M/L_1} \mid N_{M/L_1}(\delta_{L_2} \cdot \mathcal{O}_M)$

(by 1)

$$\Rightarrow N_{L_1/\mathbb{Q}}(\mathrm{Disc}_{M/L_1}) \mid N_{M/\mathbb{Q}}(\delta_{L_2} \cdot \mathcal{O}_M)$$

$$\| $$

$$N_{L_2/\mathbb{Q}}(\underbrace{N_{M/L_2}(\delta_{L_2} \cdot \mathcal{O}_M)}_{\delta_{L_2}^{[L_1:\mathbb{Q}]}})$$

$$= \mathrm{Disc}_{L_2/\mathbb{Q}}^{[L_1:\mathbb{Q}]}$$

$$= (\Delta_{L_2})^{[L_1:\mathbb{Q}]}$$

$= 1$

$$(\Delta_M) \mid (\Delta_{L_1})^{[L_2 : \mathbb{Q}]} \cdot (\Delta_{L_2})^{[L_1 : \mathbb{Q}]}$$

3) $\mathcal{O}_M = \mathcal{O}_{L_1} \cdot \mathcal{O}_{L_2} \simeq \mathcal{O}_{L_1} \otimes_{\mathbb{Z}} \mathcal{O}_{L_2}$

$\Rightarrow \delta_{M/L_1} = \delta_{L_2} \cdot \mathcal{O}_M$

$\Rightarrow$ argue as in 2)

$\mathcal{O}_{L_1} \xrightarrow{\mathrm{Tr}} \mathcal{O}_{L_1}^{\vee}$

$\wr \otimes_{\mathbb{Z}} \mathcal{O}_{L_2}$

$\mathcal{O}_M \xrightarrow{\mathrm{Tr}} \mathcal{O}_M^{\vee}$

$\square$

3.4. Decomposition of primes in Galois extensions

L/K finite, Galois ext. of #-fields

$\mathfrak{p} \subseteq \mathcal{O}_K$ max

$\Rightarrow \mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_g^{e_g}$, $\mathfrak{q}_i \subseteq \mathcal{O}_L$ prime

Recall

A $G := \mathrm{Gal}(L/K)$ acts transitively on $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_g\}$

$\Leftrightarrow e := e_1 = \ldots = e_g$,

$f := f(\mathfrak{q}_1/\mathfrak{p}) = \ldots = f(\mathfrak{q}_g/\mathfrak{p})$

$\#G = [L:K] = g \cdot e \cdot f$ (if $\mathfrak{q}_i$ pairw. distinct)

Def: $\mathfrak{q} \subseteq \mathcal{O}_L$ max., $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$

$\Rightarrow$ $D(\mathfrak{q}|\mathfrak{p}) := \mathrm{Stab}_G(\mathfrak{q})$

$= \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\} \subseteq G$

"decomposition group at $\mathfrak{q}$ relative to $\mathfrak{p}$"

La: $K \subseteq M \subseteq L$ subext, $H = \mathrm{Gal}(L/M)$, ($\sim M = L^H$)

$\mathfrak{q}_M = \mathfrak{q} \cap \mathcal{O}_M$

Then: $H \subseteq D(\mathfrak{q}|\mathfrak{p})$

iff $\mathfrak{q} \subseteq \mathcal{O}_L$ is the only prime above $\mathfrak{q}_M$

Pf: $\mathfrak{q} = \mathfrak{q}_1, \dots \mathfrak{q}_g \subseteq \mathcal{O}_L$

primes above $\mathfrak{p} \subseteq \mathcal{O}_K$

$\Rightarrow$ H-orbit of $\mathfrak{q}_1 = \mathfrak{q}$

L/M Galois $= \{$ primes above $\mathfrak{q}_M \}$ •

Note: $D(\mathfrak{q}|\mathfrak{p}) \supseteq k(\mathfrak{q}) = \mathcal{O}_L/\mathfrak{q}$

via $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$

$\rightsquigarrow$ can. hom.

$\varphi_{\mathfrak{q}} : D(\mathfrak{q}|\mathfrak{p}) \to Gal(k(\mathfrak{q})/k(\mathfrak{p}))$

$\{$ auto. Galois as $k(\mathfrak{p})$ finite (holds more gen. if $k(\mathfrak{q})/k(\mathfrak{p})$ is sep.)

Def: $I(\mathfrak{q}|\mathfrak{p}) := \ker(\varphi_{\mathfrak{q}})$

"inertia subgrp at $\mathfrak{q}$ relative to $\mathfrak{p}$"

Prop: 1) φ_q is surj, i.e.

$$1 \to I(q|p) \to D(q|p) \to Gal(k(q)/k(p)) \to 1$$

2) $\#D(q|p) = e \cdot f$,

$\#I(q|p) = e$

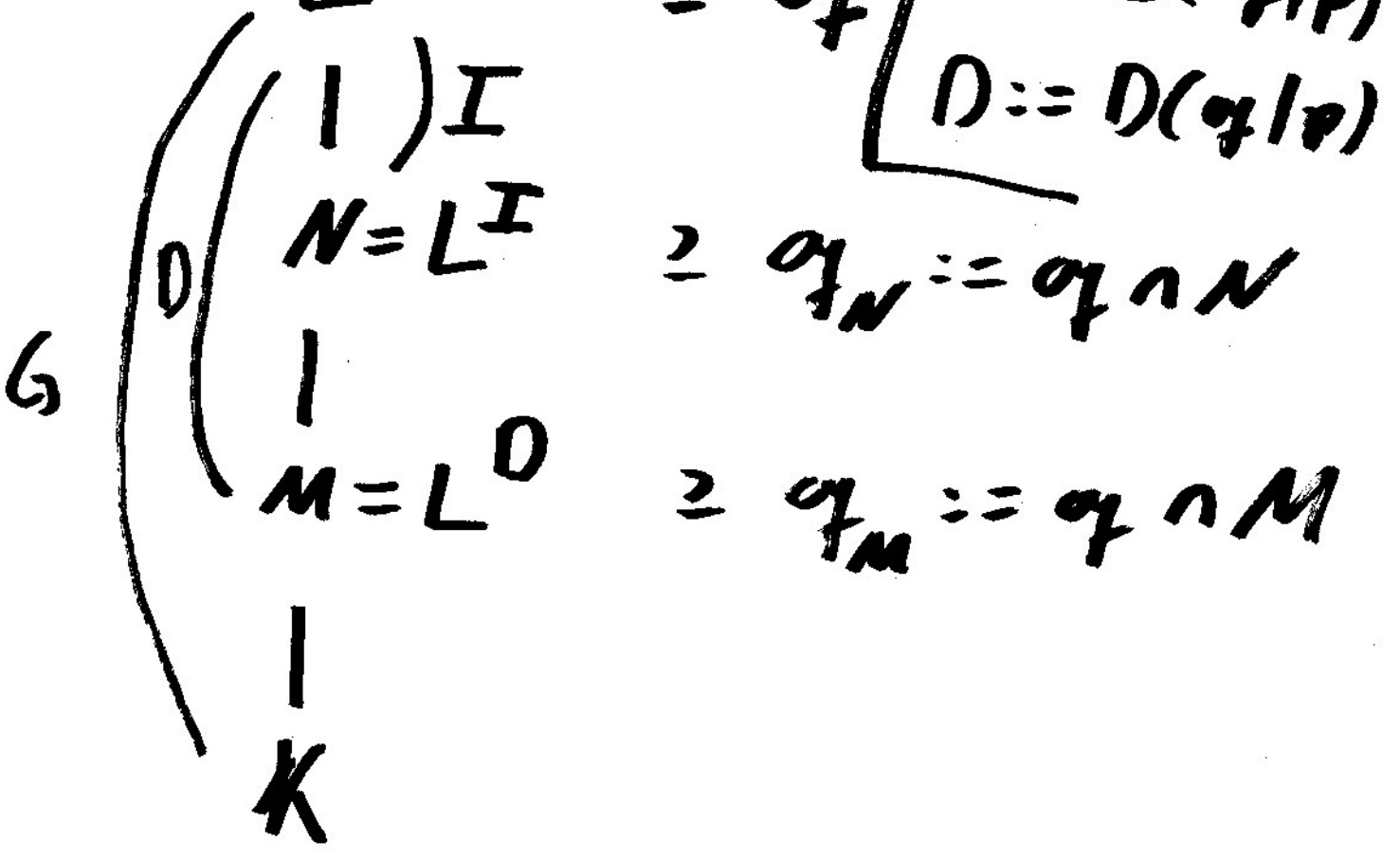
$(\Rightarrow I(q|p) = \{1\}$ for almost all q)

Pf: 2) $\#G = q^{ef} \Rightarrow \#D(q|p) = e \cdot f$

$\#Gal(k(q)/k(p)) = f$

$\overset{1)}{\Rightarrow} \#I(q|p) = e$

Set



Claim: $k(\mathfrak{q}) = k(\mathfrak{q}_N)$

$(\sim)$ $f(\mathfrak{q}|\mathfrak{q}_N) = 1, \#I = e(\mathfrak{q}|\mathfrak{q}_N)$
prev. La

Pf: Pick $\beta \in k(\mathfrak{q})$, $\alpha \in \mathcal{O}_L$
lift of β
Let $f \in \mathcal{O}_N[x]$ min. Poly of α

$\Rightarrow f \mid \prod_{\sigma \in I} (x - \sigma(\alpha))$

$\Rightarrow$ Min poly of β $(\in k(\sigma_N)[X]$
divides $\overline{f}$ = red. of f

$\Rightarrow$ Min poly of β divides
$\prod_{\sigma \in I} (X - \sigma(\alpha)) = (X-\beta)^{\#I}$

$\Rightarrow$ $\beta \in k(\sigma_N)$.

Now, $e(\sigma_f | \sigma_N) = \#I$
& $e(\sigma_f | \sigma_N) \mid e(\sigma_f | \sigma)$

$\Rightarrow$ Assume $\#I < e$

$\Rightarrow$ $\#D/I > f = \#Gal(k(\sigma_f)/k(\sigma))$

$\not\downarrow$ to $D/I \hookrightarrow Gal(k(\sigma_f)/k(\sigma))$ $\square$

$\#I = e \Rightarrow 2)$
$\Leftrightarrow 1)$

⚠ Recall: k finite field $\simeq \mathbb{F}_q$

k'/k finite, $k' \simeq \mathbb{F}_{q^f}$, $f = [k':k]$

$$\Rightarrow \mathrm{Gal}(k'/k) \underset{\wr}{\simeq} \mathbb{Z}/f \cdot \mathrm{Frob}_q$$

canonically

$$\mathrm{Frob}_q : k' \to k', \; x \mapsto x^q$$

Back to L/K finite, Galois ext.

$\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$

Assume $\mathfrak{p}$ unram. in $\mathcal{O}_L$ (i.e. $I(\mathfrak{q}\mid\mathfrak{p}) = 1$)

$$\Rightarrow D(\mathfrak{q}\mid\mathfrak{p}) \simeq \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$$

$$\psi \qquad\qquad \psi$$

$$\sigma_{\mathfrak{q}} \longleftarrow \mathrm{Frob}_q, \; q = \#k(\mathfrak{p})$$

$\wr$

⚠ Frobenius element at $\mathfrak{q}$

Notation: $\left(\frac{L/K}{\mathfrak{q}}\right) \in \mathrm{Gal}(L/K)$

Note: 1) $\tau \in \mathrm{Gal}(L/K)$

$\Rightarrow \sigma_{\tau(\mathfrak{q})} = \tau \sigma_{\mathfrak{q}} \# \tau^{-1}$

$\Rightarrow C_{\mathfrak{p}} := \{\sigma_{\mathfrak{q}} \mid \mathfrak{q} \text{ divides } \mathfrak{p}\mathcal{O}_L\}$

$\subseteq \mathrm{Gal}(L/K)$

is a conjugacy class

(the Frobenius class at $\mathfrak{p}$)

(ex. for $\mathfrak{p} \subset \mathcal{O}_K$ unramified in $\mathcal{O}_L$)

If $\mathrm{Gal}(L/K)$ abelian

$\Rightarrow C_{\mathfrak{p}} = \{\sigma_{\mathfrak{q}}\}$ $\forall \mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$

Write $\sigma_{\mathfrak{p}} := \sigma_{\mathfrak{q}} \in \mathrm{Gal}\left(\frac{L/K}{\mathfrak{p}}\right)$

for $\sigma_{\mathfrak{q}}$, $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$

2) $\sigma_{\mathfrak{q}}$ has order $f(\mathfrak{q}|\mathfrak{p})$ in $\mathrm{Gal}(L/K)$

In part. $\mathfrak{p}$ splits completely in $L \Leftrightarrow C_{\mathfrak{p}} = \{1\}$

Next: $L = \mathbb{Q}(\zeta_N) \supseteq K = \mathbb{Q}$

1) p unram. in $L \Leftrightarrow p \nmid N$

2) $p \nmid N \Rightarrow \sigma_{\mathfrak{p}} \equiv p$ in $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/N)^*$

$\Rightarrow$ p splits compl. in L iff $p \equiv 1 \ (N)$