IV. higher ramification and the Kronecker Weber Thm

IV.1 The different ideal

$L|K$ extension of number fields.

Def: The codifferent $C(\mathcal{O}_L|\mathcal{O}_K) = \{\beta \in L \mid T_{L|K}(\beta \mathcal{O}_L) \subseteq \mathcal{O}_K\}$.

Prop: $C(\mathcal{O}_L|\mathcal{O}_K)$ is a fractional ideal.

Proof: $\Delta := \Delta[\mathcal{O}_L|\mathcal{O}_K] \subseteq \mathcal{O}_K$. Take $\underbrace{\{e_1,\dots,e_n\}}_{B}$ K-basis of $\mathcal{O}_L$, $B \subseteq \mathcal{O}_L$ integral.

$\forall \beta \in C(\mathcal{O}_L|\mathcal{O}_K)$, $\beta = \sum_{j=1}^n a_j e_j$, $a_i \in K$. Since $T(\beta e_j) \subseteq \mathcal{O}_K \Rightarrow \Delta a_i \in \mathcal{O}_K$

Indeed:
$$\mathcal{O}_K^n \ni \begin{bmatrix} T(\beta e_1) \\ \vdots \\ T(\beta e_n) \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^n a_j T(e_1 e_j) \\ \vdots \\ \sum_{j=1}^n a_j (T e_n e_j) \end{bmatrix} = \underbrace{\begin{bmatrix} T(e_1 e_1) & \cdots & T(e_1 e_n) \\ \vdots & \ddots & \vdots \\ T(e_n e_1) & \cdots & T(e_n e_n) \end{bmatrix}}_{M} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \Rightarrow$$

$$\Delta M \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in \Delta \mathcal{O}_K \Rightarrow \Delta \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in M^t_{adj} \mathcal{O}_K \subseteq \mathcal{O}_K \Rightarrow a_i \in \Delta^{-1} \mathcal{O}_K \ \#.$$

$M^{-1} = \Delta^{-1} M^t_{adj}$

Obs: $L \xrightarrow[\sim]{\varphi} \mathrm{Hom}_K(L|K)$, $x \mapsto T_{L|K}(x\,*)$ $\Rightarrow$ $C(B|A) \xrightarrow[\sim]{\varphi} \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ #

(check!).

Def: The different of $\mathcal{O}_L|\mathcal{O}_K$ is $D_{\mathcal{O}_L|\mathcal{O}_K}$ or $D(L|K) = C(B|A)^{-1}$.

Prop: This is an integral ideal (check!) of $\mathcal{O}_L$.

Write $D(\mathcal{O}_L|\mathcal{O}_K) = \prod_{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)} \mathfrak{P}^{d(\mathfrak{P})}$ $\quad d(\mathfrak{P}) \geq 0$ and $d(\mathfrak{P}) = 0$ for all but

finitely many primes.

Def: $d(\mathfrak{P})$ = differential exponent of $\mathfrak{P}$ over $\mathcal{O}_K$.

Prop: $K \subseteq K' \subseteq L$ extension of number fields $\Rightarrow$
$$D(\mathcal{O}_L|\mathcal{O}_K) = D(\mathcal{O}_L|\mathcal{O}_{K'}) D(\mathcal{O}_{K'}|\mathcal{O}_K).$$

Check!

Thm: Let $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)$ non-zero and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ its contraction. $d(\mathfrak{P})$:= differential exponent of $\mathfrak{P}$ over $\mathcal{O}_K$, $e(\mathfrak{P}|\mathfrak{p})$ the ramification index. Then $d(\mathfrak{P}) \geq e(\mathfrak{P}|\mathfrak{p}) - 1$.

Proof: We can assume, using a localisation argument ($\to$ Commutative algebra!!), that $\mathcal{O}_K$ is local principal. Let π be a generator of $\mathfrak{p}$. Assume:

$$\mathfrak{p}\mathcal{O}_L = (\pi)\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \quad \text{and} \quad d_i := d(\mathfrak{P}_i).$$

Since $C(\mathcal{O}_L|\mathcal{O}_K) = \prod_{i=1}^{g} \mathfrak{P}_i^{-d_i}$, it's enough to prove that $\prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i} \subseteq C(\mathcal{O}_L|\mathcal{O}_K)$

$(\Rightarrow D(L|K) \subseteq \prod_{i=1}^{g} \mathfrak{P}_i^{e_i - 1} \Rightarrow d_i \geq e_i - 1.)$

Let $\beta \in \prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i} \Rightarrow \beta\pi \in \prod_{i=1}^{g} \mathfrak{P}_i \Rightarrow \beta\pi \in \mathfrak{P}_i \ \forall i \Rightarrow T_{L|K}(\beta\pi) \in \mathfrak{p}$

$\Rightarrow \pi T_{L|K}(\beta) \in \mathfrak{p} \Rightarrow \boxed{T_{L|K}(\beta) \in \mathcal{O}_K} \Rightarrow T_{L|K}(\beta\mathcal{O}_L) \subseteq \mathcal{O}_K$ since $\prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i}$ is a $\mathcal{O}_L$-submodule of L and $\mathcal{O}_L \subseteq \prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i} \Rightarrow \beta\mathcal{O}_L \subseteq \prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i}$

$\forall \gamma \in \mathcal{O}_L \Rightarrow \gamma\beta = \underbrace{\gamma\pi^{-1}}_{\subseteq \prod \mathfrak{P}_i^{-e_i}} \cdot \underbrace{\pi \cdot \beta}_{\in \prod_{i=1}^{g} \mathfrak{P}_i} \in \prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i} \Rightarrow T(\gamma\beta) \in \mathcal{O}_K$ #

$\gamma \in \prod_{i=1}^{g} \mathfrak{P}_i^{n_i}$, $n_i \geq 0$

$\pi^{-1} \in \prod_{i=1}^{g} \mathfrak{P}_i^{-e_i}$

In fact:

Prop: $d(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) - 1 \iff p := \mathrm{char}(\mathcal{O}_K/\mathfrak{p}) \nmid e(\mathfrak{P}|\mathfrak{p})$.

Cor: The prime ideals of $\mathcal{O}_L$ which ramify are precisely those which divide $D(\mathcal{O}_L|\mathcal{O}_K)$.

Prop: $\Delta(L|K) = N(D(L|K))$ $\leftarrow$ Relative norm of an ideal

(exercise).

IV.2 Higher ramification

$G_{-1}(\mathfrak{P}|\mathfrak{p}) := D(\mathfrak{P}|\mathfrak{p})$, $G_0(\mathfrak{P}|\mathfrak{p}) := I(\mathfrak{P}|\mathfrak{p})$ so that

$1 \to G_0 \to G_{-1} \to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \mid \mathcal{O}_K/\mathfrak{p}) \to 1.$

Def: $L^{G_{-1}}$ = decomposition field of $\mathfrak{P}|\mathfrak{p}$.

L^{G_0} = inertia field.

Notice: $K \subseteq L^{G_{-1}} \subseteq L^{G_0} \subseteq L$ s.t $L|L^{G_0}$, $L|L^{G_{-1}}$, $L^{G_0}|L^{G_{-1}}$ are Galois with Galois groups G_0, G_{-1}, Residual.

Obs: Notice that $G_{-1} \ntrianglelefteq G$ in general

Def: $G_K(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p}) \mid \forall \beta \in \mathcal{O}_L,\ \beta^\sigma - \beta \in \mathfrak{P}^{k+1}\}$ so that σ acts trivially on $\mathcal{O}_L/\mathfrak{P}^{k+1} \Rightarrow G_K \trianglelefteq G_{-1}$ called the k-th ramification group $(k \geq -1)$.

$\hookrightarrow$ since $G_K = \mathrm{Ker}[G_1 \to \mathrm{Aut}_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{P}^{k+1})]$

Clearly: $\dots \to G_1 \to G_0 \to G_{-1} \to 1.$

$\exists\, n_0$ s.t $\forall k \geq n_0$, $G_K = \{1\}$.

Prop: $\forall k \geq 1$, G_K/G_{K+1} is abelian.

Prop: a) G_0/G_1 is isomorphic to a subgroup of $(\mathcal{O}_L/\mathfrak{P})^*$. In particular it's cyclic of order prime with $\mathrm{char}(\mathcal{O}_K/\mathfrak{p})$.

b) $\forall k \geq 1$, G_K/G_{K+1} is isomorphic to a subgroup of the additive group $\mathcal{O}_L/\mathfrak{P}$. In particular they are p-groups.

Def: $\mathcal{O}_L|\mathcal{O}_K$ is tamely ramified at $\mathfrak{P}$ over $\mathfrak{p}$ if $e(\mathfrak{P}|\mathfrak{p})$ is not divisible by the residual charact. Otherwise is called wildly ramified.

Cor: The decomposition group is solvable.

Def: $G_0 / G_1 :=$ tame inertia group and it's the p-free part of $e(\mathfrak{P}|\mathfrak{p})$.

Prop: G_0/G_1 is cyclic, order $| \, q^f - 1$.

IV.3. The Frobenius morphism

$\mathfrak{P} \in \operatorname{Spec}(\mathcal{O}_L)$ over $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$. Assume $L|K$ is not ramified at $\mathfrak{P}$.

Supp $(\mathcal{O}_K / \mathfrak{p}) = \mathbb{F}_q$, $q = p^r$.

$\Rightarrow G_0 = \{1\}$ and $\underset{\underset{\langle F_\mathfrak{P} \rangle}{\shortparallel}}{G_{-1}} \simeq \operatorname{Gal}(\mathcal{O}_L/\mathfrak{P} \,|\, \mathcal{O}_K/\mathfrak{p}) = \langle \varphi_q \rangle$ order $f = f(\mathfrak{P}|\mathfrak{p})$.

$\langle F_\mathfrak{P} \rangle$ preimage of φ_q.

Notice: $\forall \beta \in \mathcal{O}_L$, $F_\mathfrak{P}(\beta) - \beta \in \mathfrak{P}$.

Def: $F_\mathfrak{P} \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ is called Frobenius automorphism, has order f and it's denoted $\left(\frac{L|K}{\mathfrak{P}}\right)$ or $(\mathfrak{P}, L|K)$.

Prop: Let $\mathfrak{P}' \in \operatorname{Spec}(\mathcal{O}_L)$ be other prime of L over $\mathfrak{p}$ and let $\sigma \in \operatorname{Gal}(L|K)$ s.t. $\sigma(\mathfrak{P}) = \mathfrak{P}' \Rightarrow \left(\frac{L|K}{\mathfrak{P}'}\right) = \left(\frac{L|K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L|K}{\mathfrak{P}}\right) \sigma^{-1}$ in $\operatorname{Gal}(L|K)$.

Hence, if $L|K$ is Galois and unramified at $\mathfrak{p}$ ($\Rightarrow$ at all $\mathfrak{P}'$), we speak of the Frobenius element $\left(\frac{L|K}{\mathfrak{p}}\right)$ as the conjugacy class $\sigma\left(\frac{L|K}{\mathfrak{P}}\right)\sigma^{-1} \mid \sigma \in \operatorname{Gal}(L|K)$. (if it's abelian $= \left(\frac{L|K}{\mathfrak{P}}\right) \forall \mathfrak{P}$).

Cor: $L|K$ unramified at $\mathfrak{p}$. Then $\mathfrak{p}$ is totally split $\Leftrightarrow \forall \mathfrak{P}|\mathfrak{p}$, $\left(\frac{L|K}{\mathfrak{P}}\right) = Id$.