Reminder: Take L/K finite separable of degree n.

Proposition 6.7.1: The subset

$$\mathfrak{d} := \{x \in L \mid \forall y \in B\colon \operatorname{Tr}_{L/K}(xy) \in A\}$$

is a fractional ideal of B which contains B.

Definition 6.7.2: The ideal $\operatorname{diff}_{B/A} := \mathfrak{d}^{-1} \subset B$ is called the *different of B over A*.

Theorem 6.7.6: For any prime $\mathfrak{q}$ of B above a prime $\mathfrak{p}$ of A we have $\mathfrak{q} \nmid \operatorname{diff}_{B/A}$ if and only if $\mathfrak{q}$ is unramified over $\mathfrak{p}$.

$(b_1, \ldots, b_n)$ basis of L over K

$\mathrm{disc}(b_1, \ldots, b_n)$

6.8 Relative discriminant

Definition 6.8.1 The *relative discriminant of B/A* is the ideal of A that is generated by the discriminants

$$\mathrm{disc}(b_1, \ldots, b_n) \;=\; \det\big(\mathrm{Tr}_{L/K}(b_i b_j)\big)_{i,j=1,\ldots,n}$$

for all tuples $(b_1, \ldots, b_n)$ in B.

Proposition 6.8.2: We have $\mathrm{disc}_{B/A} = \mathrm{Nm}_{L/K}(\mathrm{diff}_{B/A})$.

Proof: Assume: A and B are PIDs.

Take basis $b_1, \ldots, b_n$ of B over A.

Write $\mathrm{diff}_{B/A} = dB$ for $d \in B \setminus \{0\}$.

Write each $d b_j = \sum_{k=1} x_{jk} b_k$ with $x_{jk} \in A$.

matrix $X := (x_{jk})_{jk}$ represents multiplication by d on B.

$\Rightarrow \det(X) = \mathrm{Nm}_{L/K}(d)$.

Let $c_1, \ldots, c_n$ be the dual basis of L over K w.r.t. the trace form.

$\Rightarrow d^{-1}B = \mathrm{diff}_{B/A}^{-1} = \vartheta$ has $c_1, \ldots, c_n$ as A-basis.

$\Rightarrow B$ has basis $dc_1, \ldots, dc_n$.

$$\mathrm{disc}(b_1, \ldots, b_n) \overset{\mathrm{def}}{=} \det(\mathrm{Tr}(b_i b_j))_{ij}$$

$$\in A^\times \cdot \det(\mathrm{Tr}(c_i d b_j))_{ij}$$

$$= A^\times \cdot \det\Big(\mathrm{Tr}\Big(c_i \sum_k x_{jk} b_k\Big)\Big)_{ij}$$

$$= A^\times \cdot \det\Big(\sum_k x_{jk} \cdot \underbrace{\mathrm{Tr}(c_i b_k)}_{\delta_{ik}}\Big)_{ij}$$

$$= A^\times \cdot \det(x_{ij})_{ij} = A^\times \cdot \mathrm{Nm}(d).$$

$$\Rightarrow \mathrm{disc}_{B/A} = A \cdot \mathrm{disc}(b_1, \ldots, b_n)$$

$$= A \cdot \mathrm{Nm}(d)$$

$$= \mathrm{Nm}(dB)$$

$$= \mathrm{Nm}(\mathrm{diff}_{B/A}).$$ qed

$$\begin{array}{ccccl} M & & C & \supset & \mathrm{diff}_{C/B} \\ | & & | & & \\ L & & B & \supset & \mathrm{diff}_{B/A} \\ | & & | & & \\ K & & A & & \end{array}$$

Proposition 6.8.3: We have $\mathrm{disc}_{C/A} = \mathrm{Nm}_{L/K}(\mathrm{disc}_{C/B}) \cdot \mathrm{disc}_{B/A}^{[M/L]}$.

Proof: $\mathrm{diff}_{C/A} = \mathrm{diff}_{C/B} \cdot \mathrm{diff}_{B/A} \cdot C$

$$\Rightarrow \mathrm{disc}_{C/A} = \mathrm{Nm}_{M/K}(\mathrm{diff}_{C/B} \cdot \mathrm{diff}_{B/A} \cdot C)$$
$$= \mathrm{Nm}_{L/K}(\underbrace{\mathrm{Nm}_{M/L}(\mathrm{diff}_{C/B})}) \cdot \mathrm{Nm}_{L/K}(\underbrace{\mathrm{Nm}_{M/L}(\mathrm{diff}_{B/A} \cdot C)})$$
$$= \mathrm{Nm}_{L/K}(\mathrm{disc}_{C/B}) \cdot \underbrace{\mathrm{Nm}_{L/K}(\mathrm{diff}_{B/A}^{[M/L]})}_{\mathrm{disc}_{B/A}^{[M/L]}}.$$

qed.

Theorem 6.8.4: (a) A prime $\mathfrak{p} \subset A$ is ramified in B if and only if $\mathfrak{p} | \mathrm{disc}_{B/A}$.

(b) At most finitely many primes of A are ramified in B.

Proof (a) $\mathfrak{p}$ ramified in $B \overset{6.7.6}{\Longleftrightarrow} \exists\, \mathfrak{q} \subset B$ above $\mathfrak{p}$ ramified over $\mathfrak{p}$

$\Longleftrightarrow \exists\, \mathfrak{q} \subset B \ \ldots$ with $\mathfrak{q} \,|\, \mathrm{diff}_{B/A}$.

$\mathrm{diff}_{B/A} = \prod_i \mathfrak{q}_i^{\nu_i}$ $\Rightarrow \mathrm{disc}_{B/A} = \prod_i \mathrm{Nm}_{L/K}(\mathfrak{q}_i)^{\nu_i} = \prod_i \mathfrak{p}_i^{\overbrace{f_{\mathfrak{q}_i|\mathfrak{p}_i} \cdot \nu_i}^{>0}}$

$\nu_i > 0$; $\mathfrak{q}_i | \mathfrak{p}_i$

$\Longleftrightarrow \mathfrak{p} \,|\, \mathrm{disc}_{B/A}$.

qed.

(b) ✓

Theorem 6.8.5: For any number field $K \neq \mathbb{Q}$ there exists a rational prime which is ramified in $\mathcal{O}_K$.

Proof: $K \neq \mathbb{Q} \Longrightarrow \mathrm{disc}_{\mathcal{O}_K/\mathbb{Z}} = \langle d_K \rangle \neq \langle 1 \rangle$ qed.

Example 6.8.6: Consider distinct primes $p_1 \equiv \ldots \equiv p_r \equiv 1 \bmod (4)$ with $r \geqslant 1$. Then the extension $\underbrace{\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})}_{L}/\underbrace{\mathbb{Q}(\sqrt{p_1 \cdots p_r})}_{K}$ is everywhere unramified.

$d := p_1 \cdots p_r \equiv 1 \ (4)$

$\langle p_i, \sqrt{d} \rangle =: \mathfrak{p}_i$ not principal.
$\Rightarrow \mathfrak{p}_i^2 = p_i \cdot \mathcal{O}_K$

$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \Rightarrow d_K = d$ odd.

$$L \overset{2^{r-1}}{\Big|} K \overset{2}{\Big|} \mathbb{Q}, \qquad [L:\mathbb{Q}] = 2^r$$

p ramified $\Leftrightarrow p = p_i$ for some i.

p ramified $\Leftrightarrow p = p_i$ for some i.

$d_{\mathbb{Q}(\sqrt{p_i})} = p_i$ coprime.

The fields $\mathbb{Q}(\sqrt{p_i})$ are linearly disjoint over $\mathbb{Q}$.

$\Rightarrow L = \bigotimes_{i=1}^{r} \mathbb{Q}(\sqrt{p_i})$

$\Rightarrow \mathcal{O}_L = \bigotimes_{i=1}^{r} \mathbb{Z}\left[\frac{1+\sqrt{p_i}}{2}\right]$

$d_L = p_1^N \cdots p_r^N$ for some $N > 0$.

$\mathrm{Gal}(L/\mathbb{Q}) =: \Gamma \cong C_2^r > \mathrm{Gal}(L/K)$

$\forall\, \mathfrak{q} \subset \mathcal{O}_L$ max. ideal:
inertia group of $\mathfrak{q}$ in Γ is
$$\left\{ \begin{array}{ll} \mathfrak{q} \mid p_i \text{ for some } i: \Rightarrow & \prod_{j=1}^{r} \left\{ \begin{array}{ll} C_2 & \text{if } j = i \\ 1 & \text{if } j \neq i \end{array} \right\} \\ \text{otherwise}: \Rightarrow & 1 \end{array} \right\} =: I_{\mathfrak{q}}$$

$\Rightarrow$ inertia group of $\mathfrak{q}$ in $\mathrm{Gal}(L/K)$ is $I_{\mathfrak{q}} \cap \mathrm{Gal}(L/K) = 1$. $\Rightarrow \mathfrak{q}$ unramified over K.