

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

Proposition 6.7.1: The subset

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

is a fractional ideal of B which contains B .

Definition 6.7.2: The ideal $\text{diff}_{B/A} := \mathfrak{d}^{-1} \subset B$ 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 $\mathfrak{q} \nmid \text{diff}_{B/A}$ if and only if \mathfrak{q} is unramified over \mathfrak{p} .

6.8 Relative discriminant

(b_1, \dots, b_n) basis of L over K
 $\text{disc}(b_1, \dots, b_n)$

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

$$\text{disc}(b_1, \dots, b_n) = \det(\text{Tr}_{L/K}(b_i b_j))_{i,j=1, \dots, n}$$

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

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

Proof: Assume: A and B are P.I.D.s.

Take basis b_1, \dots, b_n of B over A .

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

W.l.o.g. write $dB_j = \sum_{k=1}^n x_{jk} b_k$ with $x_{jk} \in A$.

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

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

Let c_1, \dots, c_n be the dual basis of L over K .

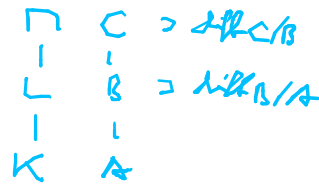
w.r.t. the trace form.

$\Rightarrow d^i B = \text{diff}_{B/A}^{-1} = \mathcal{I}$ has c_1, \dots, c_n as A -basis.

$\Rightarrow B$ has basis $d c_1, \dots, d c_n$.

$$\begin{aligned} \text{disc}(b_1, \dots, b_n) &= \det(\text{Tr}(b_i b_j))_{i,j} \\ &\in A^x \cdot \det(\text{Tr}(c_i d b_j))_{i,j} \\ &= A^x \cdot \det(\text{Tr}(c_i \sum_{k=1}^n x_{jk} b_k))_{i,j} \\ &= A^x \cdot \det(\sum_{k=1}^n x_{jk} \cdot \text{Tr}(c_i b_k))_{i,j} \\ &= A^x \cdot \det(X_{ij})_{i,j} = A^x \cdot \text{Nm}(d). \\ \Rightarrow \text{disc}_{B/A} &= A \cdot \text{disc}(b_1, \dots, b_n) \\ &= A \cdot \text{Nm}(d) \\ &= \text{Nm}(dB) \\ &= \text{Nm}(\text{diff}_{B/A}). \end{aligned}$$

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



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

$$\begin{aligned}
 \Rightarrow \text{disc}_{C/A} &= \text{Nm}_{M/K}(\text{diff}_{C/B} \cdot \text{diff}_{B/A} \cdot C) \\
 &= \text{Nm}_{L/K}(\text{Nm}_{M/L}(\text{diff}_{C/B})) \cdot \text{Nm}_{L/K}(\text{Nm}_{M/L}(\text{diff}_{B/A} \cdot C)) \\
 &= \text{Nm}_{L/K}(\text{disc}_{C/B}) \cdot \text{Nm}_{L/K}(\text{diff}_{B/A}^{[M/L]}) \\
 &= \text{Nm}_{L/K}(\text{disc}_{C/B}) \cdot \text{disc}_{B/A}^{[M/L]}
 \end{aligned}$$

qed.

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

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

Proof (a): \mathfrak{p} ramified in $B \Leftrightarrow \exists \mathfrak{q} \subset B$ s.t. $\mathfrak{p} \subset \mathfrak{q}$ ramified in \mathfrak{q}
 $\Leftrightarrow \exists \mathfrak{q} \subset B \dots$ with $\mathfrak{q} \mid \text{diff}_{B/A}$.

$$\text{diff}_{B/A} = \prod_{i: \nu_i > 0} \mathfrak{q}_i^{\nu_i} \Rightarrow \text{disc}_{B/A} = \prod_i \text{Nm}_{L/K}(\mathfrak{q}_i)^{\nu_i} = \prod_i \mathfrak{p}_i^{\sum \nu_i \cdot [L_i:K]}$$

$$\Leftrightarrow \mathfrak{p} \mid \text{disc}_{B/A}$$

(b) ✓

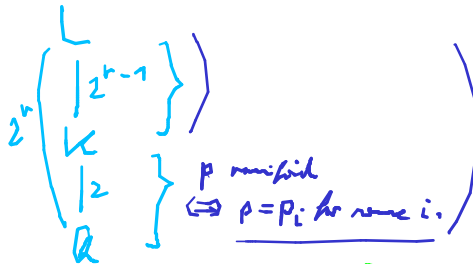
qed.

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

Example 6.8.6: Consider distinct primes $p_1 \equiv \dots \equiv p_r \equiv 1 \pmod{4}$ with $r \geq 1$. Then the extension $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r})/\mathbb{Q}(\sqrt{p_1 \cdots p_r})$ is everywhere unramified.

$d := p_1 \cdots p_r \equiv 1 \pmod{4}$



$(p_i, \sqrt{d}) = : \mathfrak{g}_i$ not prime.
 $\Rightarrow \mathfrak{g}_i^2 = p_i \cdot \mathcal{O}_K$

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

$d_{\mathbb{Q}(\sqrt{p_i})} = p_i$ 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 $N > 0$.

$\text{Gal}(L/\mathbb{Q}) = : \Gamma \cong \langle \mathbb{Z}_2^r \rangle > \text{Gal}(L/K)$

$\forall \mathfrak{q} \subset \mathcal{O}_L$ max. ideal:

which sup of \mathfrak{q} in Γ is $\left\{ \begin{array}{l} \mathfrak{q}_i \mid p_i \text{ for some } i \Rightarrow \prod_{j=1}^r \begin{cases} \mathbb{Z}_2 & \text{if } j=i \\ 1 & \text{if } j \neq i \end{cases} \\ \text{otherwise} : \Rightarrow 1 \end{array} \right\} = : I_{\mathfrak{q}}$

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