$$\begin{array}{ccc} B & \subset & L \\ | & & | \\ A & \subset & K \end{array}$$

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

Definition 6.6.1: The *relative norm* of a fractional ideal $\mathfrak{b}$ of B is the A-submodule

$$\mathrm{Nm}_{L/K}(\mathfrak{b}) \;:=\; \big(\{\mathrm{Nm}_{L/K}(y) \mid y \in \mathfrak{b}\}\big) \;\subset\; K.$$

Proposition 6.6.2:

(a) This is a fractional ideal of A.

(b) If $\mathfrak{b} \subset B$ then $\mathrm{Nm}_{L/K}(\mathfrak{b}) \subset \mathfrak{b} \cap A$.

(c) For any $y \in L^\times$ we have $\mathrm{Nm}_{L/K}((y)) = (\mathrm{Nm}_{L/K}(y))$.

Lemma:

(a) For any $z \in L^\times$ we have $\boxed{\mathrm{Nm}_{L/K}(z\mathfrak{b}) = \mathrm{Nm}_{L/K}(z)\,\mathrm{Nm}_{L/K}(\mathfrak{b})}$.

(b) Suppose that $\mathfrak{b} \subset B$ and take $x \in \mathrm{Nm}_{L/K}(\mathfrak{b}) \smallsetminus \{0\}$ and $y \in \mathfrak{b}$ such that $\mathfrak{b} = (x, y)$. Then $\mathrm{Nm}_{L/K}(\mathfrak{b}) = (x, \mathrm{Nm}_{L/K}(y))$.

Proposition 6.6.3: For any two fractional ideals $\mathfrak{b}, \mathfrak{b}'$ of B we have

$$\mathrm{Nm}_{L/K}(\mathfrak{b}\mathfrak{b}') \;=\; \mathrm{Nm}_{L/K}(\mathfrak{b}) \cdot \mathrm{Nm}_{L/K}(\mathfrak{b}').$$

Proposition 6.6.4: For any fractional ideal $\mathfrak{c}$ of C we have

$$\mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\mathfrak{c})) = \mathrm{Nm}_{M/K}(\mathfrak{c}).$$

$$\begin{array}{ccc} C & \subset & M \\ | & & | \\ B & \subset & L \\ | & & | \\ A & \subset & K \end{array} \Bigg\} n$$

Exercise.

Proposition 6.6.5: For any fractional ideal $\mathfrak{a}$ of A we have $\mathrm{Nm}_{L/K}(\mathfrak{a}B) = \mathfrak{a}^n$.

Proof: Choose $x \in A$ with $x \cdot \mathfrak{a} \subset A \Rightarrow \mathrm{Nm}_{L/K}(\mathfrak{a}B) = \mathrm{Nm}_{L/K}(x^{-1} \cdot x\mathfrak{a}B)$

$= \mathrm{Nm}_{L/K}(x^{-1}) \cdot \underbrace{\mathrm{Nm}_{L/K}(x\mathfrak{a}B)}$

$\overset{?}{=} x^{-n} \cdot (x\mathfrak{a})^n = \mathfrak{a}^n$

May WLOG: $\mathfrak{a} \subset A$.

Choose $x \in \mathfrak{a} \setminus \{0\} \Rightarrow \begin{cases} x^n \in \mathfrak{a}^n \\ x^n \in \mathrm{Nm}_{L/K}(\mathfrak{a}) \end{cases}$

With $\mathfrak{a} = (x^n, y) \subset A \Rightarrow \mathrm{Nm}_{L/K}(\mathfrak{a}B) = (x^n, \mathrm{Nm}_{L/K}(y)) = (x^n, y^n)$

$\Rightarrow \mathfrak{a}B = (x^n, y) \subset B$

$\mathfrak{a}^n = (x^n, y)^n = (x^{n^2}, x^{n^2-n}y, \ldots, x^n y^{n-1}, y^n) = (x^n, y^n)$

$x^n \in \mathfrak{a}^n$

qed.

Proposition 6.6.6: For any prime $\mathfrak{q} \subset B$ above $\mathfrak{p} \subset A$ we have $\mathrm{Nm}_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{q}|\mathfrak{p}}}$. (Correction!)

$$\begin{array}{ccccc} L & \supset & B & \supset & \mathfrak{q} \\ | & & | & & | \\ K & \supset & A & \supset & \mathfrak{p} \end{array}$$

Proof: If L/K is galois with group Γ

$$\boxed{\begin{array}{l} e = e_{\mathfrak{q}|\mathfrak{p}}, \quad |\Gamma/\Gamma_{\mathfrak{q}}| = r \\ f = f_{\mathfrak{q}|\mathfrak{p}} \quad \Rightarrow n = ref \end{array}}$$

Then $\mathfrak{p}B = \prod_{[\sigma]\in\Gamma/\Gamma_{\mathfrak{q}}} \sigma\mathfrak{q}^{e}$

$$\Rightarrow \mathfrak{p}^{n} = \mathrm{Nm}_{L/K}(\mathfrak{p}B) = \prod_{[\sigma]\in\Gamma/\Gamma_{\mathfrak{q}}} \underbrace{\mathrm{Nm}_{L/K}(\sigma\mathfrak{q})}_{\text{independent of } \sigma}{}^{e} = \mathrm{Nm}_{L/K}(\mathfrak{q})^{re}$$

$$\mathfrak{p}^{n} = \mathfrak{p}^{ref}$$

General case: Let M be a galois closure of L/K;
$\cup$
C integral closure of A.
$\cup$
$\mathfrak{r}$ prime above $\mathfrak{q}$.

$$f_{\mathfrak{r}|\mathfrak{p}} = f_{\mathfrak{r}|\mathfrak{q}} \cdot f_{\mathfrak{q}|\mathfrak{p}}$$

$$\Rightarrow \quad \mathrm{Nm}_{M/K}(\mathfrak{r}) = \mathfrak{p}^{f_{\mathfrak{r}|\mathfrak{p}}}$$

$\Vert$ 6.6.4

$$\mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\mathfrak{r})) = \mathrm{Nm}_{L/K}(\mathfrak{q}^{f_{\mathfrak{r}|\mathfrak{q}}})$$

$$\Rightarrow \mathfrak{p}^{f_{\mathfrak{q}|\mathfrak{p}}} = \mathrm{Nm}_{L/K}(\mathfrak{q}).$$

qed.

6.7 Different

Recall from Proposition 1.7.1 that we have the non-degenerate symmetric K-bilinear form

$$L \times L \longrightarrow K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(xy).$$

Proposition 6.7.1: The subset

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

is a fractional ideal of B which contains B.

Proof: $\forall x \in B \ \forall y \in B: \ \mathrm{Tr}_{L/K}(x\underset{\in B}{y}) \in A \Rightarrow B \subset \mathfrak{d}$

$\mathrm{Tr}_{L/K}$ additive $\Rightarrow \mathfrak{d}$ subgroup. ; B-submodule: $\forall x \in \mathfrak{d} \ \forall b \in B: \forall y \in B:$ $\mathrm{Tr}_{L/K}((bx)y) = \mathrm{Tr}_{L/K}(x(by)) \in A$ $\Rightarrow bx \in \mathfrak{d}$.

Take a K-basis $b_1, \ldots, b_n \in B$ of L.

$\Rightarrow d := \mathrm{disc}(b_1, \ldots, b_n) \in A \setminus \{0\}$ and $c_1, \ldots, c_n \in L$ dual basis of $L \Rightarrow \mathrm{Tr}(b_i c_j) = \delta_{ij}$

$\Rightarrow \forall x_j \in K: \forall i: \ \mathrm{Tr}(b_i \sum x_j c_j) = x_i$. So $\sum x_j c_j \in \mathfrak{d} \Rightarrow x_i \in A$. So $\mathfrak{d} \subset A c_1 + \ldots + A c_n$. $\Rightarrow \mathfrak{d}$ fin. gen. qed.

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

nonzero ideal of B.

Proposition 6.7.3: Suppose that $B = A[\beta]$ and let $f \in A[X]$ be the minimal polynomial of β above K. Then $\mathrm{diff}_{B/A} = \left(\frac{df}{dX}(\beta)\right)$.

Proof: $B \cong A[X]/(f)$.

f separable $\Rightarrow \frac{df}{dX}$ coprime to f in $A[X]$

$\Rightarrow c := \frac{df}{dX}(\beta) \neq 0$.

Write $f(X) = \prod_{i=1}^{n} (X - \beta_i)$ in $L[X]$, with $\beta_1 = \beta$.

and $\frac{f(X)}{X-\beta} = \prod_{i=2}^{n} (X - \beta_i) = \sum_{i=0}^{n-1} b_i X^i$ with $b_i \in B$.

B has the basis $1, \beta, \dots, \beta^{n-1}$ over A.

Claim 1: The dual basis of L w.r.t. Tr is $\frac{b_0}{c}, \dots, \frac{b_{n-1}}{c}$

Proof of Claim 1: $\forall\, 0 \le r \le n-1$

$$\underbrace{\sum_{i=1}^{n} \frac{f(X)}{X-\beta_i} \cdot \frac{\beta_i^r}{\frac{df}{dX}(\beta_i)}}_{\text{polynomial of degree } \le n-1} = X^r$$

$\frac{df}{dX} = \sum_j \prod_{i \neq j} (X - \beta_i)$

$\frac{df}{dX}(\beta_j) = \prod_{i \neq j} (\beta_j - \beta_i)$

values at β_j are

$$\frac{df}{dX}(\beta_j) \cdot \frac{\beta_j^r}{\frac{df}{dX}(\beta_j)} = \beta_j^r.$$

Extend $\mathrm{Tr}_{L/K}$ to $L[X] \to K[X]$,
$\sum a_i X^i \mapsto \sum \mathrm{Tr}(a_i) X^i$

$$\Rightarrow \mathrm{Tr}\left(\frac{f(X)}{X-\beta} \cdot \frac{\beta^r}{\frac{df}{dX}(\beta)} \right) = X^r.$$

$$= \mathrm{Tr}\left(\sum b_i X^i \cdot \frac{\beta^r}{c} \right) = \sum_i \mathrm{Tr}\left(b_i \frac{\beta^r}{c}\right) \cdot X^i$$

$\Rightarrow \forall\, 0 \le i \le n-1$: $\mathrm{Tr}\left(\frac{b_i}{c} \cdot \beta^r\right) = \delta_{ir}$.

qed.

Proposition 6.7.4: In general $\mathrm{diff}_{B/A}$ is the ideal that is generated by $\frac{df}{dX}(\beta)$ for all $\beta \in B$ with minimal polynomial f over K.

Claim 1 $\Rightarrow \vartheta = A \cdot \frac{b_0}{c} \oplus \dots \oplus A \cdot \frac{b_{n-1}}{c}$. $\quad \Rightarrow \vartheta = \frac{B}{C}$

Claim 2: $B = A b_0 \oplus \dots \oplus A b_{n-1}$ $\quad \Rightarrow \mathrm{diff}_{B/A} = \vartheta^{-1} = (c)$.

Proof of Claim 2: Write $f(X) = \sum_{i=0}^{n} a_i X^i$ with $a_i \in A$, $a_n = 1$.

$$\Rightarrow (X-\beta)\cdot\left(\sum_{i=0}^{n-1} b_i X^i\right) = \sum_{i=0}^{n} a_i X^i$$

$$\Rightarrow \left.\begin{aligned} b_{n-1} &= a_n = 1 \\ b_{n-2} - \beta b_{n-1} &= a_{n-1} \\ &\vdots \\ b_0 - \beta b_1 &= a_1 \end{aligned}\right\} \Rightarrow \begin{aligned} &\forall\, 1 \le i \le n: \\ &b_{n-i} = \beta^{i-1} + a_{n-1}\beta^{i-2} + \dots + a_{n-i+1}. \end{aligned}$$

Since $1, \beta, \dots, \beta^{n-1}$ is a basis of B over A

$\rightarrow b_0, \dots, b_{n-1}$ ... ...

qed.

Proposition 6.7.5: We have $\mathrm{diff}_{C/A} = \mathrm{diff}_{C/B} \cdot \mathrm{diff}_{B/A}$.

Exercise.

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

$\mathfrak{p} = \mathfrak{q} \cap A$.

$\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i} \Longrightarrow B/\mathfrak{p}B \cong \bigtimes_{i=1}^{r} B/\mathfrak{q}_i^{e_i}$.

$\mathfrak{q} = \mathfrak{q}_1$

$\mathfrak{q}^{-1}\mathfrak{p}/\mathfrak{p}B = \mathfrak{q}^{e_1-1}/\mathfrak{q}^{e_1} \times \bigtimes_{i=2}^{r} \{0\}$

$\Rightarrow \mathfrak{q}^{-1}\mathfrak{p} = \mathfrak{q}_1^{e_1-1} \cdot \prod_{i>1} \mathfrak{q}_i^{e_i} \supsetneq \mathfrak{p}B$

Proof: $\mathfrak{q} \nmid \mathrm{diff}_{B/A}$

$\Longleftrightarrow \mathrm{diff}_{B/A} \not\subset \mathfrak{q}$

$\Longleftrightarrow \mathfrak{q}^{-1} \not\subset \mathcal{D}$

$\Longleftrightarrow \exists x \in \mathfrak{q}^{-1} \exists y \in B : \mathrm{Tr}(xy) \notin A$

$\Longleftrightarrow \mathrm{Tr}(\mathfrak{q}^{-1}) \not\subset A$.

K-linear

$\Longleftrightarrow \mathrm{Tr}(\mathfrak{q}^{-1}\mathfrak{p}) \not\subset \mathfrak{p}$

$\Longleftrightarrow \exists x \in \mathfrak{q}^{-1}\mathfrak{p} : \underset{\mathrm{Tr}(T_x)}{\underset{\shortparallel}{\mathrm{Tr}(x)}} \not\equiv 0 \mod \mathfrak{p}$.

Let $T_x : B \to B,\ y \mapsto xy$

and $\overline{T}_x : \underbrace{B/\mathfrak{p}B}_{} \to \underbrace{B/\mathfrak{p}B}_{},\ [y] \mapsto [xy]$.

$k(\mathfrak{p})$-vector space of dimension n.

Claim: $\mathrm{trace}(\overline{T}_x) = \mathrm{trace}(T_x) \mod \mathfrak{p}$.

Proof: $B \cong \bigoplus_{i=1}^{n} \mathfrak{a}_i$ with fractional ideals $\mathfrak{a}_i$ of A.

$\Rightarrow T_x = (\varphi_{ij})_{ij}$ with $\varphi_{ij} \in \mathrm{Hom}_A(\mathfrak{a}_j, \mathfrak{a}_i) \cong \mathfrak{a}_j^{-1} \cdot \mathfrak{a}_i$

$\varphi_{ii} \in \mathfrak{a}_i^{-1}\mathfrak{a}_i = A$.

$\Leftrightarrow \exists [x] \in \mathfrak{q}^{-1}\mathfrak{f}/\mathfrak{f} :$ trace$(\overline{T_x}) \neq 0$ in $k(\mathfrak{f})$

If $e_1 > 1$ then $(\mathfrak{q}^{-1}\mathfrak{f})^2 \subset \mathfrak{f} B$

$\Rightarrow \overline{T_x} \circ \overline{T_x} = 0$

$\Rightarrow$ trace$(\overline{T_x}) = 0$

If $e_1 = 1$ then $\mathfrak{q}^{-1}\mathfrak{f}/\mathfrak{f} = \underbrace{B/\mathfrak{q}}_{k(\mathfrak{q})} \times \bigtimes_{i=2}^{n} \{0\}$

$\Rightarrow$ trace$(\overline{T_x}) = $ Trace$_{k(\mathfrak{q})/k(\mathfrak{f})}(x \bmod \mathfrak{q})$

separable by assumption

$\Rightarrow$ Tr$_{k(\mathfrak{q})/k(\mathfrak{f})} \not\equiv 0$.

$\Leftrightarrow e_1 = 1$.

$\Rightarrow$ trace$(T_x) = \sum \varphi_{ii}$

$B/\mathfrak{f}B \cong \bigoplus_{i=1}^{n} \mathfrak{m}_i/\mathfrak{f}\mathfrak{m}_i$

$\overline{T_x} = (\overline{\varphi_{ij}})_{ij}$ for $\overline{\varphi_{ij}} \in \mathrm{Hom}_{k(\mathfrak{f})}(\mathfrak{m}_j/\mathfrak{f}\mathfrak{m}_j, \mathfrak{m}_i/\mathfrak{f}\mathfrak{m}_i)$

$\Rightarrow$ trace$(\overline{T_x}) = \sum$ trace$(\overline{\varphi_{ii}}) =$

$= \sum \varphi_{ii} \bmod \mathfrak{f}$

$=$ Trace$(T_x) \bmod \mathfrak{f}$. qed

qed.