4. Trace and norm

$K \subset L$ finite field ext., $x \in L$

Mult. by x gives an endomorph

$M_x \in End_K(L)$ $\quad M_x(y) = xy$

If $y_1, \dots, y_n$ – basis of L/K,

then $M_x y_i = \sum_{j=1}^{n} m_{ij} y_j$, $m_{ij} \in K$

(m_{ij}) = matrix of M_x

Def $\quad Tr_{L/K}(x) = tr(M_x) \in K$

$N_{L/K}(x) = \det(M_x) \in K$

Notation: if L and K are clear, just write $Tr(x)$, $N(x)$

Properties of Tr and N

Prop. 4.1 1) $\forall x_1, x_2 \in L$, $a \in K$

$Tr(x_1 + x_2) = Tr(x_1) + Tr(x_2)$

$Tr(a x_1) = a \cdot Tr(x_1)$

$N(x_1 x_2) = N(x_1) \cdot N(x_2)$

2) $a \in K \Rightarrow Tr(a) = [L:K] \cdot a$

$N(a) = a^{[L:K]}$

Proof 1) $M_{x_1+x_2}(y) = (x_1+x_2)y = x_1y + x_2y$

$\Rightarrow M_{x_1+x_2} = M_{x_1} + M_{x_2}$

$\operatorname{tr} M_{x_1+x_2} = \operatorname{tr} M_{x_1} + \operatorname{tr} M_{x_2}$

$M_{ax_1} = a \cdot M_{x_1} \Rightarrow \operatorname{tr} M_{ax_1} = a \cdot \operatorname{tr} M_{x_1}$

$M_{x_1x_2} = M_{x_1} \cdot M_{x_2} \Rightarrow \det M_{x_1x_2} = \det M_{x_1} \cdot \det M_{x_2}$

2) $M_a = a \cdot Id$, $\operatorname{tr} M_a = [L:K] \cdot a$

$\det M_a = a^{[L:K]}$ □

Prop. 4.2 $x \in L$, $f \in K[X]$ min. poly. of x. Write $f = X^d + a_1X^{d-1} + \dots + a_d$, $a_i \in K$. Then

$$Tr_{L/K}(x) = -[L:K(x)] \cdot a_1$$

$$N_{L/K}(x) = \left((-1)^d a_d\right)^{[L:K(x)]}$$

where $K(x)$ – subfield. gen. by x.

Proof $1, x, \dots, x^{d-1}$ – basis of $K(x)/K$

In terms of this basis:

$$1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad x = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad \dots \quad x^{d-1} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

M_x given by the matrix $A = \begin{pmatrix} 0 & 0 & \dots & -a_d \\ 1 & 0 & \dots & -a_{d-1} \\ & 1 & \ddots & \vdots \\ & & \ddots & \vdots \\ 0 & 0 & \dots & 1 \; -a_1 \end{pmatrix}$

$x^d = -a_d - a_{d-1}x - \dots - a_1x^{d-1}$

$\operatorname{tr} A = -a_1$; $\det A = (-1)^d a_d$

L is as $K(x)$-v.sp. $\underbrace{K(x) \oplus \dots \oplus K(x)}_{[L:K(x)] \text{ times}}$ | $K \subset K(x) \subset L$

M_x preserves the summands

$\Rightarrow M_x$ has block-matrix form $\begin{pmatrix} A & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & A \end{pmatrix}$ $[L:K(x)]$ blocks

$\Rightarrow \operatorname{tr} M_x = [L:K(x)] \cdot \operatorname{tr} A$;

$\det M_x = (\det A)^{[L:K(x)]}$ □

Prop. 4.3 $K \subset L$ separable extension, finite.

Let F = alg. closed field containing K;

$S = \{\sigma : L \hookrightarrow F \text{ field emb } / K\}$. Then

$$\operatorname{Tr}_{L/K}(x) = \sum_{\sigma \in S} \sigma(x); \quad N_{L/K}(x) = \prod_{\sigma \in S} \sigma(x)$$

Proof take f as in Prop. 4.2.

Separability $\Rightarrow f$ has d distinct roots in F

$x_1, \dots, x_d \in F$ $\quad f = \prod_{i=1}^{d} (X - x_i)$ in $F[X]$

$$a_1 = -\sum_{i=1}^{n} x_i \qquad a_d = (-1)^d \prod_{i=1}^{d} x_i$$

$$\Rightarrow \operatorname{Tr}_{L/K}(x) = [L:K(x)] \cdot \sum_{i=1}^{d} x_i$$

$$N_{L/K}(x) = \left(\prod_{i=1}^{d} x_i\right)^{[L:K(x)]}$$

$\forall \sigma \in S \quad \sigma(x) = x_i$ for some $i \in \{1 \dots d\}$

An emb. σ is determined by the choice of x_i, which gives an embedding $K(x) \hookrightarrow F$, and an extension of this emb. to L. There are $[L : K(x)]$ ways to produce such extension for arbitrary choice of x_i.

$\Rightarrow$ for any $i = 1 \dots d$ $\sigma(x) = x_i$ exactly for $[L : K(x)]$ embeddings $\sigma \in S$

$$\sum_{\sigma \in S} \sigma(x) = [L : K(x)] \sum_{i=1}^{d} x_i$$

$$\prod_{\sigma \in S} \sigma(x) = \left(\prod_{i=1}^{d} x_i \right)^{[L : K(x)]}$$

□

Prop. 4.4 Let $K \subset L \subset H$ be a tower of finite field ext., $x \in H$

$$Tr_{L/K}\left(Tr_{H/L}(x)\right) = Tr_{H/K}(x)$$

$$N_{L/K}\left(N_{H/L}(x)\right) = N_{H/K}(x).$$

Proof left as an exercise.

$K \subset L$ finite field ext.

Def The trace form $L \times L \longrightarrow K$ is given by $(x,y) \mapsto Tr_{L/K}(xy)$

Note: the trace form is symmetric $Tr(xy) = Tr(yx)$, and bilinear: $\forall x_1, x_2 \in L$, $a \in K$

$$Tr((x_1+x_2)y) = Tr(x_1y) + Tr(x_2y)$$

$$Tr(ax,y) = a \cdot Tr(x,y)$$

(this is Prop 4.1)

Thm 4.5 Assume $K \subset L$ finite, separable. Then the trace form is non-degenerate (i.e. $\forall x \in L^\times \; \exists y \in L : Tr(xy) \neq 0$)

Proof The case $\mathrm{char}\, K = 0$ is easy: for $x \in L^\times$ take $y = x^{-1}$, then

$$Tr(xy) = Tr(1) = [L:K] \neq 0.$$

In general: let $y_1, \dots, y_n$ be a basis of L/K. The trace form is represented by a matrix $A = (a_{ij})$

$$a_{ij} = Tr(y_i \cdot y_j) \in K.$$

Need to prove: $\det A \neq 0$

Let $\sigma_1, \dots, \sigma_n$ be all emb. $L \hookrightarrow \bar{K}$ $/K$ (exactly n of them by Prop 3.1)

Define the matrix $B = (b_{ij})$

$$b_{ij} = \sigma_j(y_i) \in \bar{K}$$

Compute $B \cdot B^t = (c_{ij})$

$$c_{ij} = \sum_{k=1}^{n} b_{ik} b_{jk} = \sum_{k=1}^{n} \sigma_k(y_i) \cdot \sigma_k(y_j)$$

$$= \sum_{k=1}^{n} \sigma_k(y_i y_j) \overset{\text{Prop 4.3}}{=} \mathrm{Tr}(y_i y_j) = a_{ij}$$

$\Rightarrow A = B \cdot B^t \Rightarrow \det A = (\det B)^2$

Enough to show that $\det B \neq 0$.

Assume the contrary: $\exists \alpha_1, \dots, \alpha_n \in \bar{K}$, s.t. not all α_i are zero and

$$\forall i \quad 0 = \sum_{j=1}^{n} \alpha_j b_{ij} = \sum_{j=1}^{n} \alpha_j \sigma_j(y_i)$$

Recall that y_i form a basis of L/K

$\Rightarrow$ can rewrite the last equality:

$$\sum_{j=1}^{n} \alpha_j \sigma_j = 0 \quad \text{as a map} \quad L \longrightarrow \bar{K}$$

Lemma (Artin) Let G be a group, $\sigma_1, \dots, \sigma_n : G \to F^\times$ n distinct group homomorphisms, where F is some field. Then σ_i are linearly indep over F, i.e $\sum_{j=1}^{n} \alpha_j \sigma_j = 0$ as a map $G \to F$, then $\alpha_j = 0$ $j = 1 \dots n$

Without proof

Apply Artin's lemma to $\sigma_j : L^\times \to \bar{K}^\times$

$\Rightarrow$ get a contradiction.

$\Rightarrow \det B \neq 0.$ □

Examples 1) $\mathbb{Q} \subset \mathbb{Q}(i) = \frac{\mathbb{Q}[x]}{(x^2+1)}$

$\sigma_1, \sigma_2 : \mathbb{Q}(i) \hookrightarrow \mathbb{C}$ $\quad \sigma_1(a+ib) = a+ib$

$\sigma_2(a+ib) = a-ib$

$Tr(a+ib) = \sigma_1 + \sigma_2 = 2a$

$N(a+ib) = \sigma_1 \cdot \sigma_2 = a^2 + b^2$

The trace form: choose a basis

$y_1 = 1, \; y_2 = i;$ $\quad A = (a_{ij})$

$a_{ij} = Tr(y_i y_j)$

$$A = \begin{pmatrix} Tr(y_1^2) & Tr(y_1 y_2) \\ Tr(y_2 y_1) & Tr(y_2^2) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$$

$\operatorname{sign} A = ($number of positive eigenvalues, number of negative eigenvalues$)$

$= (1, 1)$

2) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) = \dfrac{\mathbb{Q}[x]}{(x^2-2)}$

$\sigma_1, \sigma_2 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C}$

$\sigma_1(a + \sqrt{2}\, b) = a + \sqrt{2}\, b$

$\sigma_2(a + \sqrt{2}\, b) = a - \sqrt{2}\, b$

$Tr(a + \sqrt{2}b) = 2a; \quad N(a + \sqrt{2}\, b) = a^2 - 2b^2$

$1, \sqrt{2}$ – basis of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

the trace form:

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} \qquad \operatorname{sign}(2, 0)$$