4.4 Norm and trace

Def: L/K finite Galois

$G = Gal(L/K)$

The <u>norm of L/K</u> is the map

$$N_{L/K} : L \longrightarrow K$$
$$a \longmapsto \prod_{\sigma \in G} \sigma(a)$$

and the <u>trace of L/K</u> is the map

$$Tr_{L/K} : L \longrightarrow K.$$
$$a \longmapsto \sum_{\sigma \in G} \sigma(a)$$

Rem:
- Since for all $\tau \in G$,

$$\tau\Big(\prod_{\sigma \in G} \sigma(a)\Big) = \prod_{\sigma \in G} \tau\sigma(a) = \prod_{\sigma \in G} \sigma(a),$$

and

$$\tau\Big(\sum_{\sigma \in G} \sigma(a)\Big) = \sum_{\sigma \in G} \tau\sigma(a) = \sum_{\sigma \in G} \sigma(a),$$

$$N_{L/K}(a),\ Tr_{L/K}(a) \in L^G = K.$$

- For all $a, b \in L$,

$$N_{L/K}(ab) = N_{L/K}(a) \cdot N_{L/K}(b)$$

and

$$Tr_{L/K}(a+b) = Tr_{L/K}(a) + Tr_{L/K}(b).$$

- If $a \in K$, then $N_{L/K}(a) = a^n$ and $Tr_{L/K}(a) = na$ for $n = [L:K]$.

Lemma 1: $K \subset E \subset L$ s.t. L/K, L/E and E/K are Galois

Then $N_{L/K} = N_{E/K} \circ N_{L/E}$

and

$$Tr_{L/K} = Tr_{E/K} \circ Tr_{L/E}$$

$$\left.\begin{array}{c} L \\ \text{Galois} \mid \\ E \\ \text{Galois} \mid \\ K \end{array}\right) \text{Galois}$$

proof: • $N_{L/K}(a) = \prod_{\sigma \in Gal(L/K)} \sigma(a) = \prod_{\tau \in Gal(E/K)} \left(\prod_{\substack{\sigma \in Gal(L/K) \\ \sigma|_E = \tau}} \sigma(a) \right)$

$$= \prod_{\tau \in Gal(E/K)} \tau\left(\prod_{\sigma \in Gal(L/E)} \sigma(a) \right) = N_{E/K} \circ N_{L/E}(a)$$

• $Tr_{L/K}(a) = \sum_{\sigma \in Gal(L/K)} \sigma(a) = \sum_{\tau \in Gal(E/K)} \left(\sum_{\substack{\sigma \in Gal(L/K) \\ \sigma|_E = \tau}} \sigma(a) \right)$

$$= \sum_{\tau \in Gal(E/K)} \tau\left(\sum_{\sigma \in Gal(L/E)} \sigma(a) \right) = Tr_{E/K} \circ Tr_{L/E}(a).$$

$\square$

Lemma 2: $L = K(a)/K$ Galois

$f = \sum c_i T^i$ minimal polynomial of a

$n = \deg f = [L:K]$

Then $N_{L/K}(a) = (-1)^n c_0$ and $Tr_{L/K}(a) = -c_{n-1}$.

proof: Let $G = Gal(L/K)$. Then over L

$$f = \prod_{\sigma \in G} (T - \sigma(a)) = T^n - \underbrace{\sum_{\sigma \in G} \sigma(a)}_{= Tr_{L/K}(a)} T^{n-1} + \dots + (-1)^n \underbrace{\prod_{\sigma \in G} \sigma(a)}_{= N_{L/K}(a)}.$$

$\square$

Def: G group

K field

• A <u>character of G in K</u> is a multiplicative function $\chi : G \to K$ with image in $K^\times$.

• A set of functions $f_1, \dots, f_n : G \to K$ is <u>linearly independent</u> (<u>over K</u>) if a relation

$a_1 f_1 + \dots + a_n f_n = 0$ with $a_1, \dots, a_n \in K$ implies $a_1 = \dots = a_n = 0$.

<u>Thm 3</u>: G group

K field

$\chi_1, \dots, \chi_n$ pairwise distinct characters

Then $\chi_1, \dots, \chi_n$ are linearly independent.

<u>proof</u>: Assume there is a non-trivial relation

$$a_1\chi_1 + \dots + a_n\chi_n = 0,$$

and assume that n is minimal s.t. such a non-trivial relation exists.

• If $n=1$, then $a_1\chi_1 = 0$ with $a_1 \neq 0$. ↯

• If $n>1$, then there is a $g \in G$ such that $\chi_1(g) \neq \chi_2(g)$ since $\chi_1 \neq \chi_2$. Since

$$a_1\chi_1(g)\chi_1(h) + \dots + a_n\chi_n(g)\chi_n(h) = a_1\chi_1(gh) + \dots + a_n\chi_n(gh) = 0$$

for all $h \in G$, we have

$$(a_1\chi_1(g))\cdot\chi_1 + \dots + (a_n\chi_n(g))\cdot\chi_n = 0$$

Thus

$$0 = a_1\chi_1 + \dots + a_n\chi_n - \frac{1}{\chi_1(g)}\cdot\left[(a_1\chi_1(g))\chi_1 + \dots + (a_n\chi_n(g))\chi_n\right]$$

$$= \underbrace{\left[a_2 - a_2\frac{\chi_2(g)}{\chi_1(g)}\right]}_{\neq 0}\cdot\chi_2 + a_3'\chi_3 + \dots + a_n'\chi_n$$

is non-trivial with $n-1$ terms. ↯ □

Cor 4: L/K finite Galois

Then $Tr_{L/K} : L \to K$ is not constant 0.

proof: Let $Gal(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. By Thm. 3,

$\sigma_1 + \ldots + \sigma_n \neq 0$ as maps $\sigma_i : L^\times \to L$, i.e.

$\exists a \in L^\times$ s.t.

$$Tr_{L/K}(a) = \sigma_1(a) + \ldots + \sigma_n(a) \neq 0.$$

$\square$

Def: A finite extension L/K is <u>cyclic</u> if it is Galois with cyclic Galois group.

Thm 5: (Hilbert's Theorem 90)

L/K cyclic

$Gal(L/K) = \langle \sigma \rangle$

Then $N_{L/K}(a) = 1$ if and only if there is a $b \in L^\times$ such that $a = \frac{b}{\sigma(b)}$.

proof: "$\Leftarrow$": If $a = \frac{b}{\sigma(b)}$, then $N_{L/K}(a) = \prod_{\tau \in Gal(L/K)} \frac{\tau(b)}{\tau\sigma(b)} = 1.$

"$\Rightarrow$": If $N_{L/K}(a) = 1$ and $n = [L:K]$, then by Thm. 3,

$$\varphi = id_L + a \cdot \sigma + (a \cdot \sigma(a)) \sigma^2 + \ldots + (a \cdot \sigma(a) \cdot \ldots \cdot \sigma^{n-2}(a)) \cdot \sigma^{n-1}$$

is a non-constant map $L^\times \to L$, i.e. there is a $c \in L^\times$ s.t. $b = \varphi(c) \neq 0$. Thus

$$a \cdot \sigma(b) = a \cdot \sigma(c) + a \cdot \sigma(a) \sigma^2(c) + \ldots + \underbrace{(a \cdot \sigma(a) \ldots \sigma^{n-1}(a))}_{= N_{L/K}(a) = 1} \underbrace{\sigma^n(c)}_{= c}$$

$$= \varphi(c) = b,$$

thus $a = b / \sigma(b)$.

$\square$

Thm 6: L/K cyclic

$Gal(L/K) = \langle \sigma \rangle$

Then $Tr_{L/K}(a) = 0$ if and only if there is a $b \in L$

s.t. $a = b - \sigma(b)$.

proof: "$\Leftarrow$": If $a = b - \sigma(b)$, then $Tr_{L/K}(a) = \sum_{\tau \in Gal(L/K)} (\tau(b) - \tau\sigma(b)) = 0$.

"$\Rightarrow$": Assume that $Tr_{L/K}(a) = 0$. By Cor. 4, there is a $c \in L$ s.t. $Tr_{L/K}(c) \neq 0$. Let $n = [L:K]$ and

$$b = \frac{1}{Tr_{L/K}(c)} \cdot \left[a\,\sigma(c) + (a + \sigma(a))\,\sigma^2(c) + \ldots + (a + \ldots + \sigma^{n-2}(a))\,\sigma^{n-1}(c) \right].$$

Then

$$b - \sigma(b) = \frac{1}{Tr_{L/K}(c)} \cdot \Big[a\sigma(c) + \ldots + (a + \ldots + \sigma^{n-2}(a))\,\sigma^{n-1}(c)$$

$$- \sigma(a)\,\sigma^2(c) - \ldots - \underbrace{(\sigma(a) + \ldots + \sigma^{n-1}(a))}_{= Tr_{L/K}(a) - a = -a}\,\underbrace{\sigma^n(c)}_{= c} \Big]$$

$$= \frac{1}{Tr_{L/K}(c)} \cdot \Big[\underbrace{a\sigma(c) + a\sigma^2(c) + \ldots + a\sigma^{n-1}(c) + ac}_{a \cdot Tr_{L/K}(c)} \Big]$$

$$= a. \qquad \square$$