

03/01/2021

Norm and trace

E finite extension of fields.

$$k \hookrightarrow \text{Tr}_{E/k} : E \longrightarrow k$$

$$\text{Nm}_{E/k} : E \longrightarrow k$$

Definitions

1. $\forall x \in E$, let $l_x : E \rightarrow E$ $\forall y \in E$ $\leftarrow k$ -linear endom. of the k -v.sp E/k
 \Downarrow
 $y \mapsto xy$
 $\text{End}_k(V)$

$$\text{Tr}_{E/k}(x) \stackrel{\text{def}}{=} \text{Tr}(l_x)$$

$$\text{Nm}_{E/k}(x) \stackrel{\text{def}}{=} \det(l_x) = T^{[E:k]} - \text{tr}_{E/k}(x) T^{[E:k]-1} + \dots$$

2. Pick/fix an alg. closure E^{alg} of E $+ (-1)^{[E:k]} \cdot \text{Nm}_{E/k}(x)$

$$\text{card}(\text{Hom}_{\text{ring}, k}(E, E^{\text{alg}})) \cdot \underbrace{p^A}_{=} = [E:k] \quad p = \text{char}(k)$$

$$\begin{cases} 1 & \text{if } \text{char}(k) = 0 \\ [E : (\text{separable closure of } k \text{ in } E)] & = [E:k]_{\text{insep}} \end{cases}$$

$\forall x \in E$,

$$\text{tr}_{E/k}(x) = \left(\sum_{\sigma \in \text{Hom}_{\text{ring}, k}(E, E^{\text{alg}})} \sigma(x) \right) \cdot p^A$$

$$\text{Nm}_{E/k}(x) = \left(\prod_{\sigma \in \text{Hom}_{\text{ring}, k}(E, E^{\text{alg}})} \sigma(x) \right)^{p^A}$$

Remark = $\left\{ \begin{array}{l} \text{Tr}_{E/k} : E \rightarrow k \text{ is a polynomial map} \\ \text{homog. of degree 1} \\ \text{Nm}_{E/k} : E \rightarrow k \text{ is a polynomial map} \\ \text{homog. of degree } [E:k] \end{array} \right.$

Explicitly, this means:

Pick a k -basis ξ_1, \dots, ξ_n of E over k
 $n = [E:k]$

Consider.

$$T_1 \otimes \xi_1 + \dots + T_n \otimes \xi_n \in k[T_1, \dots, T_n] \otimes_k E = M$$

where T_1, \dots, T_n are "variables"

free $k[T_1, \dots, T_n]$ -module of rank n

$$L_{T_1 \otimes \xi_1 + \dots + T_n \otimes \xi_n} \in \text{End}_{k[T_1, \dots, T_n]}(M)$$

$$\det(X \cdot \text{Id}_M - L_{T_1 \otimes \xi_1 + \dots + T_n \otimes \xi_n}) = X^n - \text{Tr}_{E/k} X^{n-1} + \dots + (-1)^n \text{Nm}_{E/k}$$

$\in k[T_1, \dots, T_n][X]$

$k[T_1, \dots, T_n]$ $k[T_1, \dots, T_n]$

\leadsto

$$\begin{array}{l} \text{Tr}_{E/k} \\ \& \\ \text{Nm}_{E/k} \end{array} \begin{array}{l} \text{defns functional} \\ \text{maps} \end{array} \cdot S \otimes_k E \rightarrow S$$

$$\cdot S \otimes_k E \rightarrow S$$

\forall commutative k -algebra S
 They specialize to $\text{tr}_{E/k}$ and $\text{Nm}_{E/k}$ when $S = k$.

Exer. 1) Show that these two definitions are equivalent

2b) $\forall x \in E$, relate $\text{tr}_{E/k}(x)$ and $N_{E/k}(x)$

to $\text{Irr}(x; k) = \text{the irreducible polynomial of } x \text{ over } k$

Ans involves $[E:k(x)]$

$$= T^m - a_1 T^{m-1} + \dots + (-1)^m a_m$$

2a) $\forall x \in k \subseteq E$, $\text{tr}_{E/k}(x) = [E:k] \cdot x$

$$N_{E/k}(x) = x^{[E:k]}$$

Properties:

$$[E:k] < \infty$$



$$\text{Tr}_{E/k} = \text{Tr}_{F/k} \circ \text{Tr}_{E/F}$$

$$N_{E/k} = N_{F/k} \circ N_{E/F}$$

(Exer.)

Prop 1

An important property of $\text{Tr}_{E/k}$.

Suppose E/k is finite separable, then the k -bilinear map

$$\begin{aligned} \text{tr}(?, ?) : E \times E &\longrightarrow k \\ (\alpha, \beta) &\longmapsto \text{Tr}_{E/k}(\alpha \cdot \beta) \end{aligned}$$

is a non-degenerate symmetric k -bilinear pairing

$$\text{i.e. } \text{tr}_{E/k} \text{ defines a } k\text{-linear isom } E \xrightarrow{B} \text{Hom}_k(E, k)$$

$\Leftrightarrow B$ is injective

$\Leftrightarrow B$ is surjective

$$\alpha \mapsto (B \mapsto \text{Tr}_{E/k}(\alpha \beta))$$

Suffices to show: B is injective.

\Leftrightarrow Suppose that $\alpha \in E$ and $\text{Tr}_{E/k}(\alpha \beta) = 0 \quad \forall \beta \in E$,
then $\beta = 0$

\Leftrightarrow

where $\{\sigma_1, \dots, \sigma_n\} = \text{Hom}_{\text{ring}, k}(E, E^a)$
 $n = [E:k]$

Write $\alpha = \sum_{i=1}^n a_i \xi_i \quad a_i \in k$

$$0 = \text{Tr}_{E/k}(\alpha \cdot \beta) \quad \forall \beta \in E$$

$$= \sum_{j=1}^n \sum_{i=1}^n \sigma_j(\alpha \cdot \beta)$$

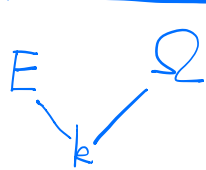
$$= \sum_{j=1}^n \sigma_j(\alpha) \cdot \sigma_j(\beta)$$

i.e. the map

$$\beta \mapsto \left(\underbrace{\sum_{j=1}^n \sigma_j(\alpha)}_{\in E^a} \cdot \underbrace{\sigma_j}_{\in \text{Hom}_{\text{ring}, k}(E, E^a)} \right) (\beta)$$

an E^a -linear combination of
 $\sigma_1, \dots, \sigma_n \in \text{Hom}_{\text{ring}, k}(E, E^a)$

Prop/Lemma 2 (Artin) "linear indep. of characters".



field extensions of k

$\sigma_1, \dots, \sigma_n$ are distinct elements of $\text{Hom}_{\text{lang } k}(E, \Omega)$

Then $\sigma_1, \dots, \sigma_n$ are linearly indep over Ω .

i.e if $\mu_1, \dots, \mu_n \in \Omega$

$$\mu_1 \sigma_1 + \dots + \mu_n \sigma_n = 0 \in \text{Hom}_k(E, \Omega)$$

then $\mu_1 = \dots = \mu_n = 0$

clearly = Artin's l. indep of char. \Rightarrow Prop 1.

Pf: Suppose $v_1, \dots, v_n \in \Omega$, all $\neq 0$, and

$$v_1 \sigma_1 + \dots + v_n \sigma_n = 0 \text{ in } \text{Hom}_k(E, \Omega)$$

Want a non-trivial linear relation between

$\leq n-1$ elements of $\{\sigma_1, \dots, \sigma_n\}$.

$$\begin{cases} v_1 \sigma_1(x) \sigma_1 + v_2 \sigma_1(x) \sigma_2 + \dots + v_n \sigma_1(x) \sigma_n = 0 \\ v_1 \sigma_1 + v_2 \sigma_2 + \dots + v_n \sigma_n = 0 \end{cases} \quad (1)$$

$$v_1 \frac{\sigma_1(xy)}{\sigma_1(x) \sigma_1(y)} + v_2 \frac{\sigma_2(xy)}{\sigma_2(x) \sigma_2(y)} + v_3 \sigma_3(xy) + \dots + v_n \sigma_n(xy) = 0 \quad \forall x, y \in E$$

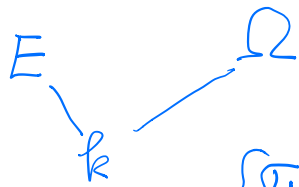
Pick $x \in E$ s.t. $\sigma_1(x) \neq \sigma_2(x)$

$$\text{get } \underbrace{(v_2 \sigma_1(x) - v_2 \sigma_2(x))}_{\neq 0} \sigma_2 + \dots + * \sigma_n = 0$$

a linear relation between $\leq n-1$ elements of $\{\sigma_2, \dots, \sigma_n\}$

Finish by induction! q.e.d.

Thm (Artin, alg. indep. of characters)
extension of fields.



k : infinite

" $T_i^q - T_i = 0$ "
when evaluated
at elts of E

$\{\sigma_1, \dots, \sigma_n\} \subseteq \text{Hom}_{k, \text{ring}}(E, \Omega)$
distinct elts

Then $\sigma_1, \dots, \sigma_n$ are alg. indep. over k .

i.e. If $f(T_1, \dots, T_n) \in k[T_1, \dots, T_n]$

and $f(\sigma_1(\xi_1), \dots, \sigma_n(\xi_n)) = 0 \quad \forall \xi_1, \dots, \xi_n \in E$

then $f(T_1, \dots, T_n) = 0$.

Let $\#E = q$ $E \xleftarrow{\text{finite}} \mathbb{F}_p$
 $\sigma: E \rightarrow \mathbb{F}_p^{\text{alg}}$ field embedding of E in \mathbb{F}_p
 $? \exists$ a polynomial $f(T)$

s.t. $f(\sigma(\xi)) = 0 \quad \forall \xi \in E$?

$T^q - T$ has this property!

Exer How to modify Thm when $\#k < \infty$.

Thm "Normal basis thm".

E finite Galois extension.
 k Then: E/k + the k -linear action of $\text{Gal}(E/k) = G$
 $\xrightarrow{\sim} k[G]$
as k -linear representations!

Exer What does this statement mean in terms of γ ? esp $\gamma(H^1)$

Next time prove of these
+ Galois cohomology + Hilbert Thm 90.