03/01/2021

Norm and trace

$$\begin{array}{l} E \\ | \\ k \end{array} \quad \text{finite extension of fields} \quad \rightsquigarrow \quad \begin{array}{l} Tr_{E/k} : E \longrightarrow k \\ Nm_{E/k} : E \longrightarrow k \end{array}$$

Definition(s)

1. $\forall x \in E$, let $\ell_x : E \longrightarrow E$, $y \mapsto xy$ $\forall y \in E$ ← k-linear endom. of the k-v.sp E/k

$\ell_x \in End_k(V)$

$$Tr_{E/k}(x) \stackrel{def}{=} Tr(\ell_x) \qquad \det(T - \ell_x|_E)$$
$$N_{E/k}(x) \stackrel{def}{=} \det(\ell_x) \qquad = T^{[E:k]} - tr_{E/k}(x)T^{[E:k]-1} + \cdots + (-1)^{[E:k]} \cdot Nm_{E/k}(x)$$

2. Pick/fix an alg. closure E^{alg} of E

$p = char(k)$

$$card\left(Hom_{ring,k}(E, E^a)\right) \cdot \underbrace{p^A}_{\substack{\parallel \\ \begin{cases} 1 & \text{if } char(k) = 0 \\ [E : (\text{separable closure of } k \text{ in } E)] = [E:k]_{insep} \end{cases}}} = [E:k]$$

$\forall x \in E$,

$$tr_{E/k}(x) = \left(\sum_{\sigma \in Hom_{ring,k}(E, E^a)} \sigma(x)\right) \cdot p^A$$

$$Nm_{E/k}(x) = \left(\prod_{\sigma \in Hom_{ring,k}(E, E^a)} \sigma(x)\right)^{p^A}$$

<u>Remark</u>: $\begin{cases} Tr_{E/k} : E \to k \text{ is a polynomial map} \\ \qquad\qquad\qquad\qquad \text{homog. of degree } 1 \\ Nm_{E/k} : E \to k \text{ is a polynomial map} \\ \qquad\qquad\qquad\qquad \text{homog. of degree } [E:k] \end{cases}$

Explicitly, this means:

Pick a k-basis $\xi_1, \dots, \xi_n$ of E over k
$n = [E:k]$

<u>Consider</u>

$$T_1 \otimes \xi_1 + \dots + T_n \otimes \xi_n \in k[T_1 \cdots T_n] \underset{k}{\otimes} E = M$$

where $T_1, \dots, T_n$ are "variables"

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

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

$$\det\left(X \cdot \mathrm{Id}_M - \ell_{T_1 \otimes \xi_1 + \dots + T_n \xi_n}\right) = X^n - \mathrm{TR}_{E/k} X^{n-1} + \dots + (-1)^n \underbrace{\mathrm{NM}_{E/k}}_{\in k[T_1, \dots, T_n]} \in k[T_1, \dots, T_n][X]$$

$\mathrm{TR}_{E/k} \in k[T_1, \dots, T_n]$

$\rightsquigarrow$ $\mathrm{TR}_{E/k}$ & $\mathrm{Nm}_{E/k}$ define functorial maps:

$$S \underset{k}{\otimes} E \longrightarrow S$$

$$S \underset{k}{\otimes} E \longrightarrow S$$

$\forall$ commutative k-algebra S

They specialize to $tr_{E/k}$ and $Nm_{E/k}$ when $S = k$.

<u>Exer.</u> 1) Show that these two definitions are equivalent

2b) $\forall x \in E$, relate $tr_{E/k}(x)$ and $Nm_{E/k}(x)$

to $Irr(x; k) =$ the irreducible polynomial of x over k

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

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

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

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

Properties:

$[E:k] < \infty$

$$\begin{array}{c} E \\ | \\ F \\ | \\ k \end{array}$$

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

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

(Exer.)

Prop 1
An important property of $Tr_{E/k}$.

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

$$tr(?,?) : E \times E \longrightarrow k$$
$$(\alpha, \beta) \longmapsto Tr_{E/k}(\alpha \cdot \beta)$$

is a non-degenerate symmetric k-bilinear pairing

i.e. $tr_{E/k}$ defines a k-linear isom $E \xrightarrow{B} Hom_k(E, k)$

$\alpha \mapsto (\beta \mapsto Tr_{E/k}(\alpha\beta))$

$\Leftrightarrow$ B is injective

$\Leftrightarrow$ B is surjective

Suffices to show: B is injective.

$\iff$ Suppose that $\alpha \in E$ and $Tr_{E/k}(\alpha\beta) = 0 \ \forall \beta \in E$, then $\beta = 0$

$\iff$

where $\{\sigma_1, \ldots, \sigma_n\} = Hom_{ring,k}(E, E^a)$

$n = [E : k]$

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

$$0 = Tr_{E/k}(\alpha \cdot \beta) \qquad \forall \beta \in E$$

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

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

i.e. the map

$$\beta \longmapsto \Big(\sum_{j=1}^{n} \underbrace{\sigma_j(\alpha)}_{\in E^a} \cdot \underbrace{\sigma_j}_{\in Hom_{ring,k}(E : E^a)} \Big)(\beta)$$

an E^a-linear combination of $\sigma_1, \ldots, \sigma_n \in Hom_{ring,k}(E, E^a)$

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

$$\begin{array}{ccc} E & & \Omega \\ & \diagdown \ \diagup & \\ & k & \end{array}$$

field extensions of k

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

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

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

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

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

Clearly: Artin's l. indep of char.. $\Rightarrow$ Prop 1.

Pf: Suppose $\nu_1, \dots, \nu_n \in \Omega$, all $\neq 0$, and

$$\nu_1 \sigma_1 + \dots + \nu_n \sigma_n = 0 \quad \text{in } \mathrm{Hom}_k(E, \Omega)$$

Want a non-trivial linear relation between $\leq n-1$ elements of $\{\sigma_1, \dots, \sigma_n\}$.

$$\nu_1 \sigma_1(x) \sigma_1 + \nu_2 \sigma_1(x) \sigma_2 + \dots + \nu_n \sigma_1(x) \sigma_n = 0$$

$$\nu_1 \sigma_1 + \nu_2 \sigma_2 + \dots + \nu_n \sigma_n = 0 \quad \text{— (1)}$$

$$\nu_1 \underbrace{\sigma_1(xy)}_{\sigma_1(x)\sigma_1(y)} + \nu_2 \underbrace{\sigma_2(xy)}_{\sigma_2(x) \cdot \sigma_2(y)} + \nu_3 \sigma_3(xy) + \dots + \nu_n \sigma_n(xy) = 0 \quad \forall x, y \in E$$

$$\Longleftrightarrow \nu_1 \sigma_1(x) \sigma_1 + \nu_2 \sigma_2(x) \sigma_2 + \dots + \nu_n \sigma_n(x) \sigma_n = 0 \quad \text{— (2)}$$

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

get

$$\underbrace{(\nu_2 \sigma_1(x) - \nu_2 \sigma_2(x))}_{\neq 0} \sigma_2 + \dots + * \sigma_n = 0$$

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)

$$\begin{tikzcd} E \arrow[dr, dash] & & \Omega \arrow[dl, dash] \\ & k & \end{tikzcd}$$

extension of fields.

k : infinite

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

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

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

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

Let

$\#E = q$

$$\begin{tikzcd} E \arrow[d, dash] \\ \mathbb{F}_p \end{tikzcd}$$

finite

$\sigma : E \longrightarrow \mathbb{F}_p^{\text{alg}}$ field embedding of E in $\overline{\mathbb{F}_p}$

? $\exists$ a polynomial $f(T)$

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

$T^q - T$ 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 $\mathrm{Gal}(E/k) =: G$

$$\xleftarrow[\gamma]{\cong} k[G]$$

as k-linear representations!

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

Next time Proof of these

+ Galois cohomology + Hilbert Thm 90.