

Lecture 7 The norm and the trace maps

Let E/K be a finite field ext'n. We have the (left) regular K -algebra rep'n

$$\rho: E \longrightarrow \text{End}_K(E)$$

$$\alpha \longmapsto \begin{pmatrix} E \xrightarrow{\rho_\alpha} E \\ y \longmapsto \alpha y \end{pmatrix}$$

and thus the additive group homomorphism

$$\text{Tr} \circ \rho =: \text{Tr}_{E/K}: E \longrightarrow K,$$

known as the trace map as well as the multiplicative group homomorphism

$$\det \circ \rho =: N_{E/K}: E^\times \longrightarrow K^\times,$$

known as the norm map. For each $\alpha \in E$ we define its characteristic polynomial

$$c_{\alpha, E/K}(X) = c_{p_\alpha}(X),$$

where as usual

$$c_A(X) := \det(X I_n - A) \in K[X],$$

with $A = [p_\alpha]_{\mathcal{B}} \in M_n(K)$, for any choice of basis $\mathcal{B}$ for E/K .

(It is well-defined by basic linear algebra.) Let $p_{\alpha/K}(X) \in K[X]$ be the minimal polynomial of $\alpha \in E$.

Prop'n With the above assumptions, for each $\alpha \in E$

$$c_{\alpha, E/K}(X) = p_{\alpha/K}(X)^{[E:K(\alpha)]}$$

Proof

Case 1. $[E : K(\alpha)] = 1$: The Hamilton-Cayley says that $c_A(A) = 0$, thus for each $\alpha \in E$ we have

$$c_{\alpha, E/K}(\rho_\alpha) = 0, \quad *$$

in the endomorphism ring $\text{End}_K(E)$. But the kernel of

$$\rho : E \longrightarrow \text{End}_K(E)$$

is trivial, so $(*)$ gives $c_{\alpha, E/K}(\alpha) = 0$ and thus $\rho_{\alpha/K}(X) \mid c_{\alpha, E/K}(X)$.

As $\deg \rho_{\alpha/K}(X) = \deg c_{\alpha, E/K}(X)$, and both polynomials are monic, we have

$$\rho_{\alpha/K}(X) = c_{\alpha, E/K}(X)$$

and Case 1 follows.

Case 2. $[E : K(\alpha)] > 1$: Let $\mathcal{B} = \{\beta_1, \dots, \beta_d\}$ be a basis of $K(\alpha)/K$,
so by Case 1 the matrix $A = (a_{ij}) \in M_d(K)$ defined by

$$\alpha \beta_1 = a_{11} \beta_1 + \dots + a_{d1} \beta_d$$

$$\vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \vdots$$

$$\alpha \beta_d = a_{d1} \beta_1 + \dots + a_{dd} \beta_d$$

is s.t. $c_A(X) = p_{\alpha/K}(X)$. If $\mathcal{B}' = \{\beta'_1, \dots, \beta'_d\}$ is a basis of $E/K(\alpha)$
then $\mathcal{B}'' = \{\beta_i \beta'_j\}$ is a basis of E/K and thus we get

$$d' = [E : K(\alpha)]$$

blocks of d equations each,

$$\alpha \beta_1 \beta'_1 = a_{11} \beta_1 \beta'_1 + \dots + a_{1d} \beta_d \beta'_1$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$$\alpha \beta_d \beta'_1 = a_{d1} \beta_1 \beta'_1 + \dots + a_{dd} \beta_d \beta'_1$$

$$\vdots$$

$$\alpha \beta_1 \beta'_d = a_{11} \beta_1 \beta'_d + \dots + a_{1d} \beta_d \beta'_d$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$$\alpha \beta_d \beta'_d = a_{d1} \beta_1 \beta'_d + \dots + a_{dd} \beta_d \beta'_d$$

Therefore

$$[p_\alpha]_{\mathcal{B}''} = \begin{bmatrix} A & 0_d & \cdots & 0_d & 0_d \\ 0_d & A & \cdots & 0_d & 0_d \\ \vdots & \vdots & & \vdots & \vdots \\ 0_d & 0_d & \cdots & A & 0_d \\ 0_d & 0_d & \cdots & 0_d & A \end{bmatrix}$$

But we know that $c_A(X) = p_{\alpha/K}(X)$. Hence

$$c_{\alpha, E/K}(X) = p_{\alpha/K}(X)^{[E:K(\alpha)]}$$

and the proposition follows $\square$

Corollary Let $\bar{K}$ be an algebraic closure of K containing E , so

$$p_{\alpha/K}(X) = (X - \alpha_1) \cdots (X - \alpha_d)$$

with $\alpha_1, \dots, \alpha_d \in \bar{K}$. Then

$$N_{E/K}(\alpha) = \left(\prod_{i=1}^d \alpha_i \right)^{[E:K(\alpha)]}$$

$$\text{Tr}_{E/K}(\alpha) = [E:K(\alpha)] \cdot \sum_{i=1}^d \alpha_i$$

Proof

We have $p_{\alpha/K}(X) = X^d + a_{d-1}X^{d-1} + \dots + a_0$, where

$$a_{d-1} = - \sum_{i=1}^d \alpha_i,$$

$$a_0 = (-1)^d \prod_{i=1}^d \alpha_i.$$

Hence

$$p_{\alpha, E/K}(X) \stackrel{\text{Prop'n}}{=} p_{\alpha/K}(X)^{[E:K(\alpha)]}$$

$$= X^n + [E:K(\alpha)] a_{d-1} X^{n-1} + \dots + a_0^{[E:K(\alpha)]}$$

But

$$c_{\alpha, E/K}(X) = X^n - \text{Tr}(\rho_\alpha) X^{n-1} + \dots + (-1)^n \det(\rho_\alpha).$$

Therefore

$$\text{Tr}_{E/K}(\alpha) = -[E:K(\alpha)] a_{d-1} = [E:K(\alpha)] \sum_{i=1}^d \alpha_i$$

$$N_{E/K}(\alpha) = (-1)^n a_0^{[E:K(\alpha)]} = (-1)^n \left((-1)^d \prod_{i=1}^d \alpha_i \right)^{[E:K(\alpha)]}$$

$$= \left(\prod_{i=1}^d \alpha_i \right)^{[E:K(\alpha)]} \quad \square$$

Fix an algebraic closure $\bar{K}$ of K containing E and let $\text{Hom}_K(E, \bar{K})$ be the set of ring homomorphisms $\sigma : E \longrightarrow \bar{K}$ s.t. $\sigma|_K = \text{id}_K$. If E/K is separable, then

$$N_{E/K}(\alpha) = \prod_{\sigma \in \text{Hom}_K(E, \bar{K})} \sigma(\alpha)$$

$$\text{Tr}_{E/K}(\alpha) = \sum_{\sigma \in \text{Hom}_K(E, \bar{K})} \sigma(\alpha)$$

If we further assume that E/K is normal, so that it is Galois with Galois group

$\text{Gal}(E/K) = \text{Hom}_K(E, \bar{K})$, then

$$N_{E/K}(\alpha) = \prod_{\sigma \in \text{Gal}(E/K)} \sigma(\alpha),$$

$$\text{Tr}_{E/K}(\alpha) = \sum_{\sigma \in \text{Gal}(E/K)} \sigma(\alpha).$$