Lecture 23 The norm and the trace maps

Let E/K be a finite field extn. We have the (left) regular K-algebra repn

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

$$\alpha \longmapsto \left(E \xrightarrow{\rho_\alpha} E \right) \quad \left(y \longmapsto \alpha y \right)$$

and thus the additive group homomorphism

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

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*

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

where as usual

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

with $A = [\rho_\alpha]_{\mathcal{B}} \in M_n(K)$, 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

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

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

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

is trivial, so $(*)$ gives $c_{\alpha, E/K}(\alpha) = 0$ and thus $p_{\alpha/K}(X) \mid c_{\alpha, E/K}(X)$. As $\deg p_{\alpha/K}(X) = \deg c_{\alpha, E/K}(X)$, and both polynomials are monic, we have

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

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

$$\alpha\beta_1 = a_{11}\beta_1 + \cdots + a_{1d}\beta_d$$

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

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

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,

$$
\begin{aligned}
\alpha\beta_1\beta_1' &= a_{11}\beta_1\beta_1' + \cdots + a_{1d}\beta_d\beta_1' \\
&\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
\alpha\beta_d\beta_1' &= a_{d1}\beta_1\beta_1' + \cdots + a_{dd}\beta_d\beta_1'
\end{aligned}
$$

$$\vdots$$

$$
\begin{aligned}
\alpha\beta_1\beta_{d'}' &= a_{11}\beta_1\beta_{d'}' + \cdots + a_{1d}\beta_d\beta_{d'}' \\
&\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
\alpha\beta_d\beta_{d'}' &= a_{d1}\beta_1\beta_{d'}' + \cdots + a_{dd}\beta_d\beta_{d'}'
\end{aligned}
$$

Therefore

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

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 $\overline{K}$ be an algebraic closure of K containing E, so

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

with $\alpha_1, \ldots, \alpha_d \in \overline{K}$. Then

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

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

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

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

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

But

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

Therefore

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

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

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

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

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

$$Tr_{E/K}(\alpha) = \sum_{\sigma \in \mathrm{Hom}_K(E, \bar{K})} \sigma(\alpha)$$

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

$Gal(E/K) = Hom_K(E, \bar{K})$, then

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

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