Galois Theory - Trace and Norm

Abigail Tan
March 22, 2023

Consider a degree-n extension L/K. We view L as an n-dimensional K-vector space. The map $u_x : L \to L$, $u_x(y) = xy$ is K-linear, so we can work with its linear-algebraic properties such as determinant and trace. Define $\mathrm{Tr}_{L/K}(x) = \operatorname{tr} u_x$ and $\mathrm{N}_{L/K}(x) = \det u_x$.

The main result of this chapter is: L/K is separable if and only if $\mathrm{Tr}_{L/K}$ is surjective.

Proposition 1. Let L/K be finite and separable, with degree n. Let $\sigma_1, \dots, \sigma_n : L \to M$ be the n distinct K-homomorphisms into a normal closure M for L/K. Then

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x), \quad N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x), \quad f_{x,L/K} = \prod_{i=1}^{n} (T - \sigma_i(x)).$$

Proof. Proving the result for $f_{x,L/K}$ is sufficient. Let $\{e_i\}$ be a basis for L/K and $P = (\sigma_i(e_j)) \in \mathrm{Mat}_{n\times n}(M)$. The σ_i are linearly independent, so P is not singular.
Now if the matrix of u_x is $A = (a_{ij})$, then $xe_j = \sum_r a_{rj} e_r$ so $\sigma_i(x)\sigma_i(e_j) = \sum_r \sigma_i(e_r) a_{rj}\ \forall i, j$. Writing S for the diagonal matrix of $\sigma_i(x)$, this is $SP = PA$, so $S = PAP^{-1}$ so S and A have the same characteristic polynomial. □

For the following main result, the major observation is that $\mathrm{Tr}_{L/K} : L \to K$ is either the zero map or surjective, because it is K-linear.

Theorem 2. Let L/K be finite. Then L/K is separable if and only if $\mathrm{Tr}_{L/K}$ is surjective.
Proof. Let $n = [L : K]$. If $\operatorname{char} K = 0$, then $\mathrm{Tr}_{L/K}(1) = n \neq 0$ so it follows immediately.
Otherwise, consider $\operatorname{char} K = p > 0$. Suppose L/K is separable, and write $\mathrm{Hom}_K(L, M) = \{\sigma_1, \dots, \sigma_n\}$ for M a normal closure for L/K. Then $\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$. Since the σ_i are linearly independent, there is some x with $\sum \sigma_i(x) \neq 0$, so $\mathrm{Tr}_{L/K}$ is nonzero, so surjective. For the converse, suppose L/K is inseparable. Then there exists some $x \in L$ such that $K(x) \supsetneq K(x^p)$ (by a standard result). Hence $\mathrm{Tr}_{K(x)/K(x^p)} = 0$ by Cor. 5, so Prop. 3 gives $\mathrm{Tr}_{M/K} = 0$. □

Preliminary results used in proving Theorem 2 are given below.

Proposition 3. For $M/L/K$ finite extensions, $\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x)) = \mathrm{Tr}_{M/K}(x)$.

Proposition 4. Let $L = K(x)$ and $f = m_{x,K} = T^n + c_{n-1}T^{n-1} + \dots + c_0 \in K[T]$. Then $f_{x,L/K} = f$.

Corollary 5. Let $\operatorname{char} K = p > 0$ and $L = K(x)$ where $x \notin K$ and $x^p \in K$. Then $\forall y \in L$, $\mathrm{Tr}_{L/K}(y) = 0$ and $N_{L/K}(y) = y^p$.