TRACE AND NORM

KEITH CONRAD

1. Introduction

Let L/K be a finite extension of fields, with $n = [L : K]$. We will associate to this extension two important functions $L \to K$, the trace and the norm.

For each $\alpha \in L$, let $m_\alpha \colon L \to L$ be multiplication by α: $m_\alpha(x) = \alpha x$ for $x \in L$. Each m_α is a K-linear map from L to L, so choosing a K-basis of L lets us write m_α as an $n \times n$ matrix.

Example 1.1. If $c \in K$, then with respect to any K-basis of L, $[m_c]$ is the scalar diagonal matrix $c \cdot I_n$.

Example 1.2. Let $L = \mathbf{C}$, $K = \mathbf{R}$, and use basis $\{1, i\}$. For $\alpha = a + bi$, $[m_\alpha]$ equals

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Example 1.3. Let $L = \mathbf{Q}(\sqrt{r})$ for r a nonsquare rational number, $K = \mathbf{Q}$, and use basis $\{1, \sqrt{r}\}$. For $\alpha = a + b\sqrt{r}$, $[m_\alpha]$ equals

$$\begin{pmatrix} a & rb \\ b & a \end{pmatrix}.$$

Example 1.4. Let $L = \mathbf{Q}(\gamma)$ for γ a root of $X^3 - X - 1$, $K = \mathbf{Q}$, and use basis $\{1, \gamma, \gamma^2\}$. For $\alpha = a + b\gamma + b\gamma^2$, $[m_\alpha]$ equals

$$\begin{pmatrix} a & c & b \\ b & a+c & b+c \\ c & b & a+c \end{pmatrix}.$$

Definition 1.5. The *trace* and *norm* of α from L to K are the trace and determinant of m_α as a K-linear map:

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(m_\alpha) \in K, \quad \mathrm{N}_{L/K}(\alpha) = \det(m_\alpha) \in K.$$

The trace and determinant of m_α can be computed from any matrix representation. By Example 1.1,

$$\mathrm{Tr}_{L/K}(c) = nc, \quad \mathrm{N}_{L/K}(c) = c^n$$

for $c \in K$, where $n = [L : K]$. In particular, $\mathrm{Tr}(1) = [L : K]$. By Example 1.2,

$$\mathrm{Tr}_{\mathbf{C}/\mathbf{R}}(a + bi) = 2a, \quad \mathrm{N}_{\mathbf{C}/\mathbf{R}}(a + bi) = a^2 + b^2.$$

By Example 1.3,

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{r})/\mathbf{Q}}(a + b\sqrt{r}) = 2a, \quad \mathrm{N}_{\mathbf{Q}(\sqrt{r})/\mathbf{Q}}(a + b\sqrt{r}) = a^2 - rb^2.$$

By Example 1.4, $\mathrm{Tr}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(a + b\gamma + c\gamma^2) = 3a + 2c$ and

$$\mathrm{N}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(a + b\gamma + c\gamma^2) = a^3 + b^3 + c^3 - ab^2 + ac^2 - bc^2 + 2a^2c - 3abc.$$

Remark 1.6. Sometimes you might see S or Sp used for trace since Spur is the German word for trace.

2. Properties of the trace and norm

The most basic algebraic properties of the trace and norm will follow from the way m_α depends on α.

Theorem 2.1. *The function $\alpha \mapsto m_\alpha$ is an injective K-linear ring homomorphism $L \to \mathrm{Hom}_K(L, L)$.*

Concretely, this says the matrices in the previous examples are embeddings of L into matrix rings over K. For instance, from Example 1.2 the 2×2 real matrices of the special form $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ add and multiply in the same way as complex numbers.

Proof. For α, β, and x in L,

$$m_{\alpha+\beta}(x) = (\alpha + \beta)(x) = \alpha x + \beta x = m_\alpha(x) + m_\beta(x) = (m_\alpha + m_\beta)(x)$$

and

$$(m_\alpha \circ m_\beta)(x) = m_\alpha(\beta x) = \alpha(\beta x) = (\alpha\beta)x = m_{\alpha\beta}(x),$$

so $m_{\alpha+\beta} = m_\alpha + m_\beta$ and $m_{\alpha\beta} = m_\alpha \circ m_\beta$. Easily m_1 is the identity map on L, so $\alpha \mapsto m_\alpha$ is a ring homomorphism. For $c \in K$,

$$m_{c\alpha}(x) = (c\alpha)x = c(\alpha x) = c(m_\alpha(x)) = (cm_\alpha)(x),$$

so $m_{c\alpha} = cm_\alpha$. Therefore $\alpha \mapsto m_\alpha$ is K-linear.

We can recover α from m_α by evaluating at 1: $m_\alpha(1) = \alpha \cdot 1 = \alpha$, so $\alpha \mapsto m_\alpha$ is injective. □

Corollary 2.2. *The trace $\mathrm{Tr}_{L/K} \colon L \to K$ is K-linear and the norm $\mathrm{N}_{L/K} \colon L \to K$ is multiplicative. Moreover, $\mathrm{N}_{L/K}(L^\times) \subset K^\times$.*

Proof. We have equations of linear maps $m_{\alpha+\beta} = m_\alpha + m_\beta$ and $m_{c\alpha} = cm_\alpha$. Taking the trace of both sides, $\mathrm{Tr}_{L/K}(\alpha + \beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$ and $\mathrm{Tr}_{L/K}(c\alpha) = c\mathrm{Tr}_{L/K}(\alpha)$. So the trace is K-linear. Taking the determinant of both sides of the equation $m_{\alpha\beta} = m_\alpha \circ m_\beta$, we get $\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha)\mathrm{N}_{L/K}(\beta)$.

Finally, since $\mathrm{N}_{L/K}(1) = 1$, for nonzero α in L we take norms of both sides of $\alpha \cdot (1/\alpha) = 1$ to get $\mathrm{N}_{L/K}(\alpha)\mathrm{N}_{L/K}(1/\alpha) = 1$, so $\mathrm{N}_{L/K}(\alpha) \neq 0$. □

The next result says the trace and norm are transitive in towers of field extensions.

Theorem 2.3. *Let $L/F/K$ be a tower of finite extensions. For $\alpha \in L$,*

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(\alpha)), \qquad \mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{F/K}(\mathrm{N}_{L/F}(\alpha)).$$

Proof. Let $(e_1, \ldots, e_m)$ be an ordered F-basis of L and $(f_1, \ldots, f_n)$ be an ordered K-basis of F. Thus as an ordered K-basis of L we can use

$$(e_1 f_1, \ldots, e_1 f_n; \ldots; e_m f_1, \ldots, e_m f_n).$$

For $\alpha \in L$, let

$$\alpha e_j = \sum_{i=1}^{m} c_{ij} e_i, \quad c_{ij} f_s = \sum_{r=1}^{n} b_{ijrs} f_r,$$

for $c_{ij} \in F$ and $b_{ijrs} \in K$. Thus $\alpha(e_j f_s) = \sum_i \sum_r b_{ijrs} e_i f_r$. So

$$[m_\alpha]_{L/F} = (c_{ij}), \quad [m_{c_{ij}}]_{F/K} = (b_{ijrs}), \quad [m_\alpha]_{L/K} = ([m_{c_{ij}}]_{F/K}).$$

Thus

$$\begin{aligned} \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(\alpha)) &= \mathrm{Tr}_{L/K}\left(\sum_i c_{ii}\right) \\ &= \sum_i \mathrm{Tr}_{L/F}(c_{ii}) \\ &= \sum_i \sum_r b_{iirr} \\ &= \mathrm{Tr}_{L/K}(\alpha). \end{aligned}$$

The proof of transitivity of the norm is more complicated, and is omitted. □

The trace and norm of α can be expressed in terms of the roots of the minimal polynomial of α over K. To explain this we need another polynomial related to α:

Definition 2.4. For $\alpha \in L$, its *characteristic polynomial* relative to the extension L/K is the characteristic polynomial of $m_\alpha \colon L \to L$ as a K-linear map:

$$\chi_\alpha(X) = \det(X \cdot I_n - [m_\alpha]) \in K[X].$$

Example 2.5. For $c \in K$, $m_c \colon L \to L$ has matrix representation cI_n, so $\chi_c(X) = (X-c)^n = X^n - ncX^{n-1} + \cdots + (-1)^n c^n$.

Example 2.6. For the extension $\mathbf{C}/\mathbf{R}$, the characteristic polynomial of the matrix in Example 1.2 is $\chi_{a+bi}(X) = X^2 - 2aX + a^2 + b^2$.

For any $n \times n$ square matrix A, its characteristic polynomial has the form

$$\det(XI_n - A) = X^n - \mathrm{Tr}(A)X^{n-1} + \cdots + (-1)^n \det A,$$

so

$$\chi_\alpha(X) = X^n - \mathrm{Tr}_{L/K}(\alpha)X^{n-1} + \cdots + (-1)^n \mathrm{N}_{L/K}(\alpha).$$

This tells us we can read off the trace and norm of α from the characteristic polynomial of α, which can be seen in Examples 2.5 and 2.6.

Theorem 2.7. *Every α in L is a root of its characteristic polynomial $\chi_\alpha(X)$.*

Proof. This is a consequence of the Cayley-Hamilton theorem, which says m_α is killed by its characteristic polynomial: $\chi_\alpha(m_\alpha) = O$. Since $\alpha \mapsto m_\alpha$ is a K-linear ring homomorphism $L \to \mathrm{Hom}_K(L, L)$, for any polynomial $f(X) \in K[X]$ we have $f(m_\alpha) = m_{f(\alpha)}$. Therefore $O = \chi_\alpha(m_\alpha) = m_{\chi_\alpha(\alpha)}$, so $\chi_\alpha(\alpha) = 0$. □

Example 2.8. The complex number $a + bi$ is a root of the real polynomial $\chi_{a+bi}(X) = X^2 - 2aX + a^2 + b^2$.

Although α is a root of $\chi_\alpha(X)$ and $\chi_\alpha(X) \in K[X]$, this does *not* mean $\chi_\alpha(X)$ is the minimal polynomial of α in $K[X]$. The degree of $\chi_\alpha(X)$ is $[L : K]$, whereas the minimal polynomial of α in $K[X]$ has degree $[K(\alpha) : K]$, which varies with α. We will see next that the minimal and characteristic polynomials of α are related to each other.

Theorem 2.9. *The characteristic polynomial is a power of the minimal polynomial. For $\alpha \in L$, let $\pi_\alpha(X)$ be the minimal polynomial of α in $K[X]$ and $d = \deg \pi_\alpha(X) = [K(\alpha) : K]$. Then $\chi_\alpha(X) = \pi_\alpha(X)^{n/d}$.*

In other words, $\chi_\alpha(X)$ is the power of the minimal polynomial of α having degree n. As a simple example, for $c \in K$ its minimal polynomial in $K[X]$ is $X - c$ while its characteristic polynomial is $(X - c)^n$.

Proof. A K-basis of $K(\alpha)$ is $\{1, \alpha, \ldots, \alpha^{d-1}\}$. Let $s = [L : K(\alpha)]$ and $\beta_1, \ldots, \beta_s$ be a $K(\alpha)$-basis of L. Then

$$L = \bigoplus_{k=1}^{s} K(\alpha)\beta_k = \bigoplus_{k=1}^{s} \bigoplus_{j=0}^{d-1} K\alpha^j \beta_k.$$

To compute $\chi_\alpha(X)$ we use as an ordered K-basis of L the set

$$\{\beta_1, \alpha\beta_1, \ldots, \alpha^{d-1}\beta_1; \ldots; \beta_s, \alpha\beta_s, \ldots, \alpha^{d-1}\beta_s\}.$$

Let $\alpha \cdot \alpha^j = \sum_{i=0}^{d-1} c_{ij}\alpha^i$ for $0 \leq j \leq d-1$, where $c_{ij} \in K$. The matrix for multiplication by α on $K(\alpha)$ with respect to the basis $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is (c_{ij}). Since $\det(X \cdot I_d - (c_{ij}))$ is the characteristic polynomial for multiplication by α on $K(\alpha)$ (not on L!), it has α as a root by Theorem 2.7 (using $K(\alpha)$ in place of L). Therefore $\det(X \cdot I_d - (c_{ij})) = \pi_\alpha(X)$ because $\pi_\alpha(X)$ is the only monic polynomial in $K[X]$ of degree $d = [K(\alpha) : K]$ with α as a root.

Since $\alpha \cdot \alpha^j\beta_k = \sum_{i=0}^{d-1} c_{ij}\alpha^i\beta_k$, with respect to the above K-basis of L the matrix for m_α is a block diagonal matrix with s repeated $d \times d$ diagonal blocks (c_{ij}), so $\chi_\alpha(X) = \det(X \cdot I_d - (c_{ij}))^s = \pi_\alpha(X)^s = \pi_\alpha(X)^{n/d}$. □

Corollary 2.10. *Let the minimal polynomial for α in $K[X]$ factor as $(X - \alpha_1)\cdots(X - \alpha_d)$ over a large enough field. Then*

$$\mathrm{Tr}_{L/K}(\alpha) = \frac{n}{d}(\alpha_1 + \cdots + \alpha_d), \quad \mathrm{N}_{L/K}(\alpha) = (\alpha_1 \cdots \alpha_d)^{n/d}.$$

Proof. The trace is the negative of the second-highest power coefficient in $\chi_\alpha(X)$ and the norm is the constant term of $\chi_\alpha(X)$ multiplied by $(-1)^n$. Therefore the formulas for $\mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha)$ are immediate from computing these coefficients in $\pi_\alpha(X)^{n/d}$, where $\pi_\alpha(X)$ is the minimal polynomial of α in $K[X]$. □

This is *not* saying the trace and norm of α are the sum and product of the roots of the minimal polynomial of α over K. Those roots have to be repeated n/d times, where $d = [K(\alpha) : K]$, making a total of n terms in the sum and product.

Corollary 2.11. *Suppose in a large enough field extension the characteristic polynomial of α relative to L/K splits completely as*

$$\chi_\alpha(X) = (X - r_1)\cdots(X - r_n).$$

Then for any $g(X) \in K[X]$,

$$\chi_{g(\alpha)}(X) = (X - g(r_1))\cdots(X - g(r_n)),$$

so

$$\mathrm{Tr}_{L/K}(g(\alpha)) = \sum_{i=1}^{n} g(r_i), \quad \mathrm{N}_{L/K}(g(\alpha)) = \prod_{i=1}^{n} g(r_i).$$

In particular, $\chi_{\alpha+1}(X) = \chi_\alpha(X-1)$ and $\chi_{\alpha^m}(X) = (X - r_1^m)\cdots(X - r_n^m)$, so $\mathrm{N}_{L/K}(\alpha+1) = (-1)^n\chi_\alpha(-1)$ and $\mathrm{Tr}_{L/K}(\alpha^m) = \sum_{i=1}^{n} r_i^m$.

Proof. By Theorem 2.9, $\chi_\alpha(X)$ is a power of the minimal polynomial of α in $K[X]$, so every r_i has the same minimal polynomial over K as α.

Set $f(X) = (X - g(r_1)) \cdots (X - g(r_n))$. We want to show this is the characteristic polynomial of $g(\alpha)$. The coefficients of $f(X)$ are symmetric polynomials in $r_1, \ldots, r_n$ with coefficients in K, so by the symmetric function theorem $f(X) \in K[X]$. Let $M(X)$ be the minimal polynomial of $g(\alpha)$ over K, so $M(X)$ is irreducible in $K[X]$. Since α and each r_i have the same minimal polynomial over K, the fields $K(\alpha)$ and $K(r_i)$ are isomorphic over K. Applying such an isomorphism to the equation $M(g(\alpha)) = 0$ turns it into $M(g(r_i)) = 0$ (because $M(X)$ and $g(X)$ have coefficients in K), so $M(X)$ is the minimal polynomial for $g(r_i)$ over K since $M(X)$ is monic irreducible in $K[X]$.

We have shown all roots of $f(X)$ have minimal polynomial $M(X)$ in $K[X]$, and $f(X)$ is monic, so $f(X)$ is a power of $M(X)$. By Theorem 2.9, $\chi_{g(\alpha)}(X) \in K[X]$ is a power of $M(X)$ with degree $[L : K] = n = \deg(f)$, so $f(X) = \chi_{g(\alpha)}(X)$. □