Norm, Trace and Discriminant in a Number Field

Math4Joy • 2 Feb 2024

This post offers a summary note on the norm, trace, characteristic polynomial and discriminant of an element $\alpha \in K$, a number field of degree n over $\mathbb{Q}$.

► **$\mathbb{Q}$-linear transformation:** For any $\alpha \in K$, we can define a $\mathbb{Q}$-linear transformation $m_\alpha : K \to K$, such that

$$m_\alpha(x) = \alpha x, \tag{1}$$

for some $x \in K$. Such an m_α can be represented as a matrix (with respect to a basis for K over $\mathbb{Q}$), denoted by $[m_\alpha]$. We define the *trace* and *norm* of α as follows:

$$T_{K/\mathbb{Q}}(\alpha) = trace\,[m_\alpha] \tag{2}$$
$$N_{K/\mathbb{Q}}(\alpha) = det\,[m_\alpha] \tag{3}$$

The characteristic polynomial $char(\alpha)$ is defined as,

$$char_{K/\mathbb{Q}}(\alpha) = det\,(XI - [m_\alpha])\,, \tag{4}$$

where X is the indeterminate and I is an $n\times n$ identity matrix.

Example-1: When we exactly know the representation of the algebraic number θ with respect to a basis in the number field $\mathbb{Q}[\sqrt[3]{3}]$,

$$\theta = q_0 + q_1\sqrt[3]{3} + q_2\sqrt[3]{9}, \tag{5}$$

where $q_i \in \mathbb{Q}$, $\forall i \in \{0,1,2\}$. θ acts on the basis elements $\{1, \sqrt[3]{3}, \sqrt[3]{9}\}$ as,

$$\begin{aligned} \theta.1 &= q_0 + q_1\sqrt[3]{3} + q_2\sqrt[3]{9} \\ \theta.\sqrt[3]{3} &= 3q_2 + q_0\sqrt[3]{3} + q_1\sqrt[3]{9} \\ \theta.\sqrt[3]{9} &= 3q_1 + 3q_2\sqrt[3]{3} + q_0\sqrt[3]{9}, \end{aligned}$$

which gives,

$$[m_\theta] = \begin{bmatrix} q_0 & 3q_2 & 3q_1 \\ q_1 & q_0 & 3q_2 \\ q_2 & q_1 & q_0 \end{bmatrix} \implies T(\theta) = 3q_0,\ N(\theta) = det\,[m_\theta]\ \text{(figure this out!)}$$

Example-2: When we do not know the algebraic number θ in terms of its basis elements, but know its minimal polynomial over $\mathbb{Q}$, denoted as $min(\theta, \mathbb{Q})$. Let θ be the root of the irreducible polynomial $X^3 - 3X + 1$. What are the trace and norm of θ? Since $X^3 - 3X + 1$ is irreducible, let's choose the basis $\{1, \theta, \theta^2\}$. θ acts on these basis elements as,

$$\begin{aligned}
&\theta.1 = 0 + \theta + 0 \\
&\theta.\theta = 0 + 0 + \theta^2 \\
&\theta.\theta^2 = -1 + 3\theta + 0,
\end{aligned}$$

which gives,

$$[m_\theta] = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{bmatrix} \implies T(\theta) = 0,\ N(\theta) = det\,[m_\theta] = -1$$

So far so good! What about the characteristic polynomial $char(\theta)$? As per Eq. (4),

$$char(\theta)(X) = \begin{vmatrix} X & 0 & 1 \\ -1 & X & -3 \\ 0 & -1 & X \end{vmatrix} = X(X^2 - 3) + 1 \tag{6}$$

This is not a coincidence that $char(\theta)$ is identical to the minimal polynomial of θ over $\mathbb{Q}$. In fact,

- *Proposition-1:* $char_{K/\mathbb{Q}}(\alpha) = min[\alpha, \mathbb{Q}]^{[K:\mathbb{Q}(\alpha)]}$ for some $\alpha \in K$.

Proof sketch. Prove using Caley-Hamilton theorem for $K = \mathbb{Q}(\alpha)$, then apply induction. □

► **Counting embeddings:** There exist alternative equivalent ways to define *trace* and *norm* via embeddings of a number field K in an algebraic closure, say $\mathbb{C}$. For our purpose here, an *embedding* is an injective homomorphism from K to $\mathbb{C}$ that fix $\mathbb{Q}$ pointwise.

Let $\sigma_1, \ldots, \sigma_n$ be n embeddings of K in $\mathbb{C}$, where $n = [K : \mathbb{Q}]$, we can also define trace and norm of $\alpha \in K$ as,

$$T_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \tag{7}$$

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \tag{8}$$

Well-definedness of trace and norm: How to see that these two definitions (via $\mathbb{Q}$-linear transformation and through embeddings) are equivalent?

Proof sketch. As per Eq. (2), $T_{K/\mathbb{Q}}(\alpha)$ is the sum of eigenvalues of $[m_\alpha]$, which is identical to sum of the roots of $char_{K/\mathbb{Q}}(\alpha)$. As per Eq. (7), $T_{K/\mathbb{Q}}(\alpha)$ is the sum of roots of $min[\alpha, \mathbb{Q}]$. The relationship between characteristic and minimal polynomials of α via proposition-1, therefore, completes the proof. Similar argument works for the norm. □

► **Discriminant:** Two (equivalent) definitions of the *discriminant* of $\alpha_1, \ldots, \alpha_n$, where $\alpha_i \in K$ for all i,

- $disc(\alpha_1, \ldots, \alpha_n) = |T_{K/\mathbb{Q}}(\alpha_i\alpha_j)|$
- $disc(\alpha_1, \ldots, \alpha_n) = |\sigma_i(\alpha_j)|^2$, if we think embeddings only.

Well-definedness of discriminant: $|\sigma_i(\alpha_j)|^2 = |T_{K/\mathbb{Q}}(\alpha_i\alpha_j)|$.

Proof sketch. $[\sigma_i(\alpha_j)]\,[\sigma_j(\alpha_i)] = \sigma_1(\alpha_i\alpha_j) + \ldots + \sigma_n(\alpha_i\alpha_j) = T(\alpha_i\alpha_j)$, and then apply properties of determinant. □