Minimal Polynomials in Linear Algebra and Field Theory

Timo Chang
timo65537@protonmail.com

Last edited: December 25, 2025

In this essay, we draw a connection between two notions of "minimal polynomials" in linear algebra and field theory. We also use this to investigate the norm and trace for a finite extension of fields.

1 Characteristic Polynomial and Minimal Polynomial

Recall the following two notions of minimal polynomials in linear algebra and field theory.

Definition 1.1. (1) (Linear algebra) Let T be a linear operator on a finite-dimensional vector space over F. The *minimal polynomial* $p(x) \in F[x]$ of T is the monic polynomial of least positive degree for which $p(T) = T_0$ is the zero operator.

(2) (Field theory) Let E/F be a field extension and $\alpha \in E$ be algebraic over F. The *minimal polynomial* (or *irreducible polynomial*) of α over F, denoted by $\mathrm{Irr}_F(\alpha)$, is the unique monic irreducible polynomial over F which has α as a root.

We also recall that any polynomial $g(x) \in F[x]$ with $g(T) = T_0$ is necessarily divisible by $p(x)$, and any polynomial $g(x) \in F[x]$ with $g(\alpha) = 0$ is necessarily divisible by $\mathrm{Irr}_F(\alpha)$. Due to the similarities between these two notions of minimal polynomials, we expect that there is a connection between them. This is illustrated in the following proposition.

Proposition 1.2. *Let E/F be a finite extension of fields. For each $\alpha \in E$, consider the F-linear operator $T_\alpha : E \to E$ given by $T_\alpha(v) := \alpha \cdot v$ for every $v \in E$.*

(1) The minimal polynomial $p(x)$ of T_α is equal to the minimal polynomial $\mathrm{Irr}_F(\alpha)$ of α over F.

(2) The characteristic polynomial $f(x)$ of T_α is equal to $\mathrm{Irr}_F(\alpha)^{[E:F(\alpha)]}$.

Proof. (1) We write $\mathrm{Irr}_F(\alpha) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in F[x]$. Note that for each $v \in E$,

$$\begin{aligned}\mathrm{Irr}_F(\alpha)(T_\alpha)(v) &= (T_\alpha^n + c_{n-1}T_\alpha^{n-1} + \cdots + c_0 \,\mathrm{id}_E)(v) \\ &= \alpha^n v + c_{n-1}\alpha^{n-1}v + \cdots + c_0 v \\ &= (\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0) \cdot v = 0.\end{aligned}$$

So $\operatorname{Irr}_F(\alpha)(T_\alpha)$ is the zero operator on E. This implies that $p(x) \mid \operatorname{Irr}_F(\alpha)$.

On the other hand, write $p(x) = x^m + d_{m-1}x^{m-1} + \cdots + d_0 \in F[x]$. Then we know $p(T_\alpha)$ is the zero operator on E. In particular,

$$\begin{aligned} 0 &= p(T_\alpha)(1) \\ &= (T_\alpha^m + d_{m-1}T_\alpha^{m-1} + \cdots + d_0 \operatorname{id}_E)(1) \\ &= \alpha^m + d_{m-1}\alpha^{m-1} + \cdots + d_0 \\ &= p(\alpha). \end{aligned}$$

So α is a root of $p(x)$. This implies that $\operatorname{Irr}_F(\alpha) \mid p(x)$.

Since $p(x)$ and $\operatorname{Irr}_F(\alpha)$ are both monic, we can now conclude that $p(x) = \operatorname{Irr}_F(\alpha)$.

(2) Consider the tower of field extensions $F \subseteq F(\alpha) \subseteq E$. We let $\{1, \alpha, \ldots, \alpha^{n-1}\}$ be the canonical F-basis of $F(\alpha)$ and $\{\beta_1, \ldots, \beta_k\}$ be any $F(\alpha)$-basis of E. Then it is straightforward to check that

$$\{\beta_1, \alpha\beta_1, \ldots, \alpha^{n-1}\beta_1, \beta_2, \alpha\beta_2, \ldots, \alpha^{n-1}\beta_2, \ldots, \beta_k, \alpha\beta_k, \ldots, \alpha^{n-1}\beta_k\}$$

is an ordered basis of E over F. Let $\operatorname{Irr}_F(\alpha) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in F[x]$. Then from

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0,$$

one sees that the matrix representation of the linear operator $T_\alpha : E \to E$, $v \mapsto \alpha \cdot v$ with respect to this ordered basis is

$$\underbrace{\begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}}_{k \text{ copies}}, \quad \text{where} \quad A = \begin{pmatrix} & & & & -c_0 \\ 1 & & & & -c_1 \\ & 1 & & & -c_2 \\ & & \ddots & & \vdots \\ & & & 1 & -c_{n-1} \end{pmatrix}_{n\times n}.$$

So the characteristic polynomial of T_α is $f(x) = \det(xI_n - A)^k$. It is a standard exercise that (see [FIS19, Exercise 4.3.24])

$$\det(xI_n - A) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 = \operatorname{Irr}_F(\alpha).$$

This shows that $f(x) = \operatorname{Irr}_F(\alpha)^k = \operatorname{Irr}_F(\alpha)^{[E:F(\alpha)]}$. □

2 Norm and Trace

Recall the following definitions of norm and trace in field theory.

Definition 2.1. Let E/F be a finite extension of fields. For each $\alpha \in E$, let $T_\alpha : E \to E$ be the F-linear operator given by $T_\alpha(v) := \alpha \cdot v$ for every $v \in E$. We define the *norm* $\mathrm{Nr}_{E/F}(\alpha)$ and *trace* $\mathrm{Tr}_{E/F}(\alpha)$ of α to be the determinant and trace of T_α, respectively. That is,

$$\mathrm{Nr}_{E/F}(\alpha) := \det(T_\alpha) \quad \text{and} \quad \mathrm{Tr}_{E/F}(\alpha) := \mathrm{tr}(T_\alpha).$$

Proposition 2.2. *Let E/F be a finite extension of degree n. For any $\alpha \in E$, let $\mathrm{Irr}_F(\alpha) = x^m + c_{m-1}x^{m-1} + \cdots + c_0$ be its minimal polynomial. Then*

$$\mathrm{Nr}_{E/F}(\alpha) = (-1)^n c_0^{n/m} \quad \textit{and} \quad \mathrm{Tr}_{E/F}(\alpha) = -\frac{n}{m} c_{m-1}.$$

Proof. It is a standard exercise in linear algebra (see [FIS19, Exercise 5.1.20 and 21]) that the constant term (resp. the coefficient of x^{n-1}) of the characteristic polynomial $f(x)$ of T_α is $(-1)^n \det(T_\alpha)$ (resp. $-\mathrm{tr}(T_\alpha)$). By Proposition 1.2, we see that

$$\begin{aligned} f(x) &= \mathrm{Irr}_F(\alpha)^{n/m} \\ &= (x^m + c_{m-1}x^{m-1} + \cdots + c_0)^{n/m} \\ &= x^n + \frac{n}{m} c_{m-1} x^{n-1} + \cdots + c_0^{n/m}. \end{aligned}$$

Hence, we have

$$c_0^{n/m} = (-1)^n \det(T_\alpha) = (-1)^n \mathrm{Nr}_{E/F}(\alpha)$$

and

$$\frac{n}{m} c_{m-1} = -\mathrm{tr}(T_\alpha) = -\mathrm{Tr}_{E/F}(\alpha).$$

□

References

[FIS19] Stephen H. Friedberg, Arnold J. Insel, and Lawrence E. Spence. *Linear algebra.* 5th ed. Pearson, 2019.