線性代數和體論中的極小多項式

Timo Chang
timo65537@protonmail.com
譯者: 仙女仙女

最後編輯: 2025 年 12 月 25 日

在本文中, 我們探討線性代數與體論 (域論) 中兩種「極小多項式」概念之間的關聯, 並進一步藉此探討有限體擴張 (域擴張) 下的範數及跡.

1 特徵多項式與極小多項式

讓我們先回顧在線性代數及體論中極小多項式的概念.

定義 1.1 (1) (線性代數) 設 T 爲有限維 F-線性空間上的線性算子, 稱使得 $p(T)=T_0$ 爲零算子的 (正) 次數最低的首一多項式 $p(x)\in F[x]$ 爲 T 的**極小多項式**.

(2) (體論) 設 E/F 爲體擴張, $\alpha\in E$ 爲 F 上的代數元, 稱 $F[x]$ 中唯一具有根 α 之不可約的首一多項式 $\mathrm{Irr}_F(\alpha)$ 爲 α **在** F **上的極小多項式** (或**不可約多項式**).

此外, 值得注意的是: 凡是滿足 $g(T)=T_0$ 的多項式 $g(x)\in F[x]$, 必定可被 $p(x)$ 整除; 同樣地, 凡是滿足 $g(\alpha)=0$ 的多項式 $g(x)\in F[x]$ 也必定可被 $\mathrm{Irr}_F(\alpha)$ 整除. 由於這兩種極小多項式在性質上具有明顯的相似之處, 我們自然會預期它們之間存在某種內在的關聯, 這一點將在以下命題中呈現.

命題 1.2 設 E/F 爲有限體擴張, 對每個 $\alpha\in E$, 考慮 F-線性映射 $T_\alpha: E\to E$, $T_\alpha(v):=\alpha\cdot v$ $(v\in E)$.

(1) T_α 的極小多項式等於 α 在 F 上的極小多項式 $\mathrm{Irr}_F(\alpha)$.

(2) T_α 的特徵多項式 f 等於 $\mathrm{Irr}_F(\alpha)^{[E:F(\alpha)]}$.

證明 (1) 記 $\mathrm{Irr}_F(\alpha)(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_0\in F[x]$. 注意到, 對所有 $v\in E$,

$$\begin{aligned}\mathrm{Irr}_F(\alpha)(T_\alpha)(v)&=(T_\alpha^n+c_{n-1}T_\alpha^{n-1}+\cdots+c_0\,\mathrm{id}_E)(v)\\&=\alpha^n v+c_{n-1}\alpha^{n-1}v+\cdots+c_0v\\&=(\alpha^n+c_{n-1}\alpha^{n-1}+\cdots+c_0)\cdot v=0,\end{aligned}$$

故 $\mathrm{Irr}_F(\alpha)(T_\alpha)$ 是 E 上的零算子, 因此 $p(x)\mid\mathrm{Irr}_F(\alpha)(x)$.

另一方面, 記 $p(x) = x^m + d_{m-1}x^{m-1} + \cdots + d_0 \in F[x]$, 則 $p(T_\alpha)$ 是 E 上的零算子. 特別地,

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

故 α 是 $p(x)$ 的一根, 因此 $\mathrm{Irr}_F(\alpha)(x) \mid p(x)$.

由於 $p(x)$ 和 $\mathrm{Irr}_F(\alpha)(x)$ 均爲首一多項式, 故可推得 $p(x) = \mathrm{Irr}_F(\alpha)(x)$.

(2) 考慮體擴張塔 $F \subseteq F(\alpha) \subseteq E$, 設 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 爲 $F(\alpha)$ 的標準 F-基, $\{\beta_1, \ldots, \beta_k\}$ 爲 E 的任一組 $F(\alpha)$-基, 則可很直接地驗證

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

是 E 在 F 上的有序基. 令 $\mathrm{Irr}_F(\alpha)(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in F[x]$, 則由

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

可看出線性算子 $T_\alpha : E \to E$, $v \mapsto \alpha \cdot v$ 關於該有序基的矩陣表示式爲

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

因此 T_α 的特徵多項式爲 $f(x) = \det(xI_n - A)^k$. 由常見的習題 (見 [FIS19, Exercise 4.3.24]) 可證明

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

於是 $f(x) = \mathrm{Irr}_F(\alpha)(x)^k = \mathrm{Irr}_F(\alpha)(x)^{[E:F(\alpha)]}$. □

2 範數與跡

我們先回顧體論中範數和跡的定義.

定義 2.1 設 E/F 爲有限體擴張, 對於每個 $\alpha \in E$, 考慮 F-線性算子 $T_\alpha : E \to E$, $T_\alpha(v) := \alpha \cdot v$ ($v \in E$), 並分別定義 α 的範數 $\mathrm{Nr}_{E/F}(\alpha)$ 和跡 $\mathrm{Tr}_{E/F}(\alpha)$ 爲 T_α 的行列式和跡, 即

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

命題 2.2　設 E/F 爲次數爲 n 的有限擴張, 對所有 $\alpha \in E$, 設 $\operatorname{Irr}_F(\alpha)(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_0$ 爲其極小多項式, 則

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

證明　線性代數中有常見的習題 (見 [FIS19, Exercise 5.1.20 及 21]) 要我們證明 T_α 的特徵多項式 $f(x)$ 的常數項 (相應地, x^{n-1} 的係數) 爲 $(-1)^n \det(T_\alpha)$ (相應地, $-\operatorname{tr}(T_\alpha)$). 依命題 1.2, 有

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

於是, 有

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

及

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

□

參考資料

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