

# Homework 7

冯熙喆

2025 年 12 月 13 日

## A 迹和范数

### A1)

假设  $[L : K] = n$ , 那么映射就是标量乘法, 因此  $\text{Tr}_{L/K}(x) = nx, N_{L/K}(x) = x^n$ 。

由于  $XI - m_x$  的每个元素都属于  $K[X]$ , 自然它的行列式属于  $K[X]$ 。

证明  $P_{L/K,x}(X) \in K[X]$ :

取  $L$  的  $K$ -基  $\{e_1, \dots, e_n\}$ , 设  $m_x$  在此基下的矩阵为  $A = (a_{ij})$ 。由于  $xe_j \in L$  可唯一表示为  $\sum_i a_{ij}e_i$ , 故  $a_{ij} \in K$ 。

特征多项式  $P_{L/K,x}(X) = \det(XI - A)$  的系数是  $A$  中元素的多项式组合, 因此  $P_{L/K,x}(X) \in K[X]$ 。

证明  $P_{L/K,x}(X)$  在  $L$  中有根:

由 Cayley-Hamilton 定理,  $P_{L/K,x}(m_x) = 0$  (作为  $L$  上的线性映射)。

将此零映射作用于  $\mathbf{1} \in L$ :

$$P_{L/K,x}(m_x)(\mathbf{1}) = 0$$

注意到  $m_x^k(\mathbf{1}) = x^k$ , 故

$$P_{L/K,x}(m_x)(\mathbf{1}) = P_{L/K,x}(x) = 0$$

因此  $x$  本身就是  $P_{L/K,x}(X)$  在  $L$  中的根。□

## A2)

$X^2 - d$  的两个根为  $\pm\sqrt{d}$ 。由域同构延拓定理,任意  $K$ -自同构  $\sigma$  必须将  $\sqrt{d}$  映到  $X^2 - d$  的某个根。

因此存在唯一的非恒等  $K$ -自同构  $\sigma$ ,满足  $\sigma(\sqrt{d}) = -\sqrt{d}$ 。

对  $x = a + b\sqrt{d}$  ( $a, b \in K$ ),有  $\sigma(x) = a - b\sqrt{d}$

为了计算  $\text{Tr}, N, P$ ,不妨取一组基  $1, \sqrt{d}$ ,则这组基下  $m_x$  的矩阵为  $\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$

从而自然有  $\text{Tr}_{L/K}(x) = 2a, N_{L/K}(x) = a^2 - db^2, P_{L/K,x}(X) = (X - x)(X - \sigma(x))$

## A3)

将线性算子表示成矩阵形式,两矩阵的迹之和就是两矩阵之迹的和,从而迹映射是加法群同态.

类似的,两矩阵乘积的行列式就是两矩阵行列式的乘积,注意到  $GL(K; L)$  恰好是  $L$  上的单位元素(因为它们可逆),因此行列式映射就是单位元素乘法群的同态.

## A4)

设  $[M : K] = m, [L : M] = n$ , 则  $[L : K] = mn$ 。

取  $M$  的  $K$ -基  $\{e_1, \dots, e_m\}$ ,  $L$  的  $M$ -基  $\{f_1, \dots, f_n\}$ 。

则  $\{e_i f_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$  是  $L$  的  $K$ -基。

对任意  $x \in L$ , 设  $m_x^{L/M}$  在基  $\{f_j\}$  下的矩阵为  $A = (a_{jk})$ , 其中  $a_{jk} \in M$ 。

则  $xf_k = \sum_{j=1}^n a_{jk}f_j$ , 故

$$x(e_i f_k) = e_i \sum_{j=1}^n a_{jk} f_j = \sum_{j=1}^n a_{jk} (e_i f_j)$$

现在  $a_{jk} \in M$ , 设  $m_{a_{jk}}^{M/K}$  在基  $\{e_i\}$  下的矩阵为  $B_{jk}$  ( $m \times m$  矩阵)。

则  $m_x^{L/K}$  在基  $\{e_i f_j\}$  下的矩阵是分块矩阵:

$$\mathcal{A} = (B_{jk})_{1 \leq j, k \leq n}$$

这是一个  $mn \times mn$  矩阵。其迹为：

$$\mathrm{Tr}_{L/K}(x) = \sum_{j=1}^n \mathrm{Tr}(B_{jj}) = \sum_{j=1}^n \mathrm{Tr}_{M/K}(a_{jj})$$

而  $\mathrm{Tr}_{L/M}(x) = \sum_{j=1}^n a_{jj}$ , 故

$$\mathrm{Tr}_{M/K}(\mathrm{Tr}_{L/M}(x)) = \mathrm{Tr}_{M/K}\left(\sum_{j=1}^n a_{jj}\right) = \sum_{j=1}^n \mathrm{Tr}_{M/K}(a_{jj})$$

因此  $\boxed{\mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M} = \mathrm{Tr}_{L/K}}$ 。  $\square$

## A5)

为了利用A4的结论,我们考虑中间域  $M/K = K(x)/K$ ,类似地取基  $\{e_i f_j\}$  就可以得到

$$x \cdot e_i f_j = (x \cdot e_i) f_j = \left( \sum_{k=1}^d a_{ki} e_k \right) f_j = \sum_{k=1}^d a_{ki} (e_k f_j)$$

因此在基  $\{e_i f_j\}$  下,  $m_x$  的矩阵  $B = \underbrace{\{A, A, \dots, A\}}_{n \uparrow A}$

因此特征多项式就是极小多项式的  $n$  次幂.  $\square$

## A6)

为此,只要证明对于  $K(x)/K$ (作为  $K$ -线性空间),我们有

$$\mathrm{Tr}_{K(x)/K}(x) = \sum_{i=1}^d x_i, N_{K(x)/K}(x) = \prod_{i=1}^d x_i$$

$x$  作为  $K$ -线性空间  $K(x)$  中的线性映射,其特征多项式就是极小多项式  $P_{min}(X)$ (因为  $\deg$  都是  $d$ ),由于特征多项式(在分裂域中)的所有根之和就是矩阵的迹,所有根之积就是矩阵的行列式,就得到了证明.  $\square$

## A7)

任给  $\sigma \in \mathrm{Hom}_K(L, \Omega)$ , 它满足  $\sigma|_{K(x)} \in \mathrm{Hom}_K(K(x), \Omega)$

据此,考虑限制映射  $Res : Hom_K(L, \Omega) \rightarrow Hom_K(K(x), \Omega)$ ,  $\sigma \mapsto \sigma|_{K(x)}$

由于  $L/K(x)$  也是可分扩张,所以对于某个  $\varphi \in Hom_K(K(x), \Omega)$  恰有  $[L : K(x)]$  个映射的限制映射等于  $\varphi$ ,因此证明就归结于 A6

□

## A8)

考虑可分闭包  $L_s/K$ ,任取  $x \in L - L_s$ ,它在  $L_s$  上的极小多项式是

$$P_{min}(X) = X^{p^k} - x^{p^k} = (X - x)^{p^k}$$

考虑到特征多项式是极小多项式的幂次,并且特征多项式应该是  $p^n$  阶的,据此特征多项式应该是

$$f(X) = X^{p^n} - x^{p^n}$$

任取  $x \in L_s$ ,它是作为线性映射是标量乘法,因此特征多项式也是

$$f(X) = X^{p^n} - x^{p^n}$$

对于迹,我们证明一个更强的结论:不可分扩张的迹是 0.

对于  $L/L_s$  中的元素  $x$ ,我们知道特征多项式形如  $(X - x)^{p^n}$ ,从而  $Tr_{L/L_s}(x) = 0, \forall x \in L$ ,进一步,利用迹的传递性,  $Tr_{L/K}(x) = 0, \forall x \in L$ ,又已知域的特征是  $p$ ,这给出  $p^n = 0^n = 0$ ,可知等式两段相等.

对于范数,如果  $x \in L_s$ ,那么取  $L_s$  的  $K$ -基和  $L$  的  $L_s$  基  $\{e_i\}, \{f_i\}$ ,类似 A4,可以得到  $m_x$  再基  $\{e_i f_j\}$  下的矩阵形如  $B = \text{diag}\{\underbrace{A, A, \dots, A}_{n \uparrow A}\}$ ,其中,  $\det A = N_{L_s/K}(x)$   
这说明  $\det B = (\det A)^{p^n}$ ,也就是  $N_{L/K}(x) = N_{L_s/K}(x)^{p^n}$

如果  $x \in L - L_s$ ,那么  $x^{p^n} \in L_s$ ,利用范数的同态性质就可以知道

$$N_{L/K}(x)^{p^n} = N_{L_s/K}(x^{p^n})^{p^n} = (\prod_i \sigma_i(x))^{p^{2n}}$$

等式两端在代数闭包中取  $p^n$  次根(Frobenius 映射的单性说明这是唯一的), 就得到了待证命题

### A9)

对于可分扩张, 我们知道  $N_{L/K}(x) = \prod_{\sigma \in \text{Hom}_K(L, \Omega)} \sigma(x)$ 。

考虑限制映射  $\text{Res} : \text{Hom}_K(L, \Omega) \rightarrow \text{Hom}_K(M, \Omega)$ ,  $\sigma \mapsto \sigma|_M$ 。

由于  $L/M$  可分, 对每个  $\varphi \in \text{Hom}_K(M, \Omega)$ , 恰有  $[L : M]$  个  $\sigma$  满足  $\sigma|_M = \varphi$ 。

对固定的  $\varphi$ , 这些  $\sigma$  恰好对应于  $\varphi$  复合上  $\text{Hom}_M(L, \Omega)$  中的元素。

对于给定的  $\varphi$ , 应用 A7

$$\prod_{\sigma: \sigma|_M = \varphi} \sigma(x) = \prod_{\psi \in \text{Hom}_M(L, \Omega)} \varphi(\psi(x)) = \varphi \left( \prod_{\psi} \psi(x) \right) = \varphi(N_{L/M}(x))$$

因此

$$N_{L/K}(x) = \prod_{\sigma \in \text{Hom}_K(L, \Omega)} \sigma(x) = \prod_{\varphi \in \text{Hom}_K(M, \Omega)} \prod_{\sigma: \sigma|_M = \varphi} \sigma(x) = \prod_{\varphi \in \text{Hom}_K(M, \Omega)} \varphi(N_{L/M}(x))$$

再将 A7 应用于  $M/K$ :

$$= N_{M/K}(N_{L/M}(x))$$

□

### A10)

设  $P(X)$  在  $\bar{K}$  中的所有根为  $\alpha_1, \alpha_2, \dots, \alpha_d$ , 其中  $\alpha = \alpha_1$ 。

由于  $P$  首一, 有:

$$P(X) = \prod_{j=1}^d (X - \alpha_j)$$

$$P'(X) = \sum_{k=1}^d \prod_{j \neq k} (X - \alpha_j)$$

$$P'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$$

$$N_{K(\alpha)/K}(P'(\alpha)) = \prod_{i=1}^d \sigma_i(P'(\alpha)) = \prod_{i=1}^d P'(\alpha_i) = \prod_{i=1}^d \prod_{j \neq i} (\alpha_i - \alpha_j)$$

$$= \prod_{i < j} (\alpha_i - \alpha_j)^2 \cdot (-1)^{\#\{(i,j): i < j\}}$$

因此:

$$N_{K(\alpha)/K}(P'(\alpha)) = (-1)^{\frac{d(d-1)}{2}} \prod_{i < j} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{d(d-1)}{2}} \text{Disc}(P)$$

□

**A11)**

**A12)**

A8中已经证明了A11,A12两个结论

**A13)**

对于  $\text{Char } K = 0$  的域, 必有  $\text{Tr}_{L/K}(1) \neq 0$ , 任意的非零元素  $x$ , 总能找到  $y$  使得  $xy = 1$ , 这就说明特征0的域, 扩张的迹非退化.

对于不可分扩张, 我们知道任意元素的迹都是0, 从而迹退化.

**A14)**

为此, 我们可以考虑  $x$  的极小多项式在  $\bar{K}$  中的  $n$  个根  $\{\alpha_i\}_{1 \leq i \leq n}$ , 据  $L/K$  可分, 它们两两不等, 因此它们对应的 Vandermonde 矩阵非退化

考虑到  $\text{Tr}_{L/K}(x^k) = \sum_{i=1}^n \alpha_i^k$ , 如果  $\forall k, \text{Tr}_{L/K}(x^k) = 0$ , 那么 Vandermonde 矩阵的列向量之和为 0, 这就导出了矛盾!

□

### A15)

如果域扩张可分, 那么  $\forall x \neq 0, (x, x^k) (-1 \leq k \leq n-2)$  中至少一个被迹双线性型映射到非 0 元素

如果迹双线性型非退化, 域扩张一定不是不可分的(A13 中证明), 也就是说域扩张是可分的.

## B 利用 Galois 对应证明代数基本定理

### B1)

给定一个  $\mathbb{R}$  的 2 次扩张, 它一定形如  $\mathbb{R}(\alpha)$ , 其中  $\alpha$  的极小多项式是 2 阶的。据此我们考虑一个二次方程  $X^2 + aX + b = 0$ , 它的解形如

$$x = \frac{-a \pm \sqrt{\Delta}}{2}$$

其中  $\Delta = a^2 - 4b$ 。如果  $\Delta \geq 0$ , 那么根都是实数(自然极小多项式不是 2 阶的)。如果  $\Delta < 0$ , 我们可以将扩张取为  $\mathbb{R}(x_1 - x_2)$ , 这是因为  $x_1 + x_2 \in \mathbb{R}$ 。因为  $\frac{x_1 - x_2}{\sqrt{-\Delta}}$  满足  $X^2 - 1 = 0 \sqrt{-\Delta} \in R$  所以  $\mathbb{R}(x_1 - x_2) \simeq \mathbb{C}$ , 我们就知道任意这样的域扩张都  $\simeq \mathbb{C}$ 。

### B2)

利用反证法: 假设某个扩张  $K/\mathbb{R}$  是奇数次的, 且次数  $n \geq 3$ 。此时, 任取  $\alpha \in K \setminus \mathbb{R}$ , 并且记它的极小多项式

$$P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0,$$

那么  $d \mid n$  (因为  $\mathbb{R}(\alpha)$  是中间域),  $d$  一定是奇数, 进一步  $d$  是不小于3的奇数。因此存在  $\beta \in \mathbb{R}$ , 使得

$$P(X) = (X - \beta)Q(X),$$

其中  $\beta \in \mathbb{R}, Q(X) \in \mathbb{R}[X]$ , 这说明  $P(X)$  是可约的, 这与它是极小多项式矛盾!

因此奇数次扩张只能是1次扩张, 从而是平凡的扩张。

### B3) $\mathbb{C}$ 没有次数为2的扩张

利用反证法, 假设  $\mathbb{C}$  有2次扩张, 那么扩张添加的元素  $\alpha$  满足方程  $X^2 + aX + b = 0 (a, b \in \mathbb{C})$ , 然而, 直接利用求根公式, 可知多项式在  $X^2 + aX + b$  在  $\mathbb{C}$  中可约, 从而  $\alpha$  的极小多项式次数为1, 导出矛盾!

### B4)

(只对有限Galois扩张证明这一点)

我们假设  $\text{Gal}(K/\mathbb{R})$  是一个  $2^n \cdot l$  阶群, 其中  $l$  是奇数。任取 Sylow 2-子群  $H \subseteq \text{Gal}(K/\mathbb{R})$ , 那么  $[G : H] = l$  是奇数。由 Galois 对应定理,  $H$  对应了  $\mathbb{R}$  的一个  $l$  次扩张  $K^H/\mathbb{R}$ , 我们记  $K^H$  为  $K_1$ 。

此时  $\text{Gal}(K/K_1)$  是一个  $2^n$  阶群。考虑到存在子群的序列

$$\{1\} \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G, \quad |G_i| = 2^i$$

由 Galois 对应定理就知道满足要求的中间域序列存在。

### B5)

如果  $[K : R] = 1$  那么  $K = \mathbb{R}$

如果  $[K : R] \geq 2$  考虑  $K/\mathbb{R}$  的正规闭包  $N/\mathbb{R}$ , 那么  $N/\mathbb{R}$  是有限 Galois 扩张, 综合 B1-B4 的结论, 我们可以知道  $N = \mathbb{C}$ , 因此, 这指出  $K = N$

## B6) 代数基本定理

任取 $\mathbb{C}$ 的代数扩张 $L/\mathbb{C}$ ,假设 $L - \mathbb{C} \neq \emptyset$ ,任取 $\alpha \in L - \mathbb{C}$ ,则 $\mathbb{C}(\alpha)/\mathbb{C}$ 是有限扩张,从而是平凡的扩张,这也就是说任取 $\alpha \in L - \mathbb{C}$ 满足 $\alpha \in \mathbb{C}$ ,导出矛盾!

因此 $\mathbb{C}$ 的代数扩张 $L/\mathbb{C}$ 总是平凡的扩张.