群与 Galois 理论

作业 7

陈宏泰

2024011131

清华大学数学科学系

cht24@mails.tsinghua.edu.cn

2025 年 12 月 24 日

目录

A. 迹与范数

L/K 是域的有限扩张, 对任意的 $x \in L$, 考虑乘法映射：

$$m_x : L \longrightarrow L, \quad y \mapsto x \cdot y$$

这是 K-线性空间 L 上的 K-线性映射, 它的迹、行列式和特征多项式分别记作：

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}\,(m_x)\,, \quad \mathrm{N}_{L/K}(x) = \det\,(m_x)\,, \quad P_{L/K,x}(X) = \det\,(X \cdot I - m_x)\,.$$

1. 假设 $x \in K$, 试计算 $\mathrm{Tr}_{L/K}(x), \mathrm{N}_{L/K}(x)$ 和 $P_{L/K,x}(X)$. 对一般的 $x \in L$, 证明 $P_{L/K,x}(X) \in K[X]$ 并且 $P_{L/K,x}(X)$ 在 L 中有根.

证明：不妨设 $[L : K] = n$.

当 $x \in K$ 时, 乘法映射 m_x 是 L 上的数乘映射, 因此它的矩阵表示为 xI , 其中 I 是 L 的任意一组基下的单位矩阵. 于是,

$$\begin{aligned}
&\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(xI) = nx,\\
&\mathrm{N}_{L/K}(x) = \det(xI) = x^n,\\
&P_{L/K,x}(X) = \det(XI - xI) = (X - x)^n.
\end{aligned}$$

对于一般的 $x \in L$, 设 $\{e_1, e_2, \cdots, e_n\}$ 是 L 作为 K-线性空间的一组基, 则乘法映射 m_x 在该基下的矩阵表示为 $M = (m_{ij})$, 其中 $m_{ij} \in K$ 满足

$$xe_j = \sum_{i=1}^{n} m_{ij} e_i, \forall\ 1 \leqslant j \leqslant n.$$

因此, $P_{L/K,x}(X) = \det(XI - M)$ 是 $K[X]$ 中的多项式. 记 $v = (e_1, e_2, \cdots, e_n)^T$, 进一步写成

$$M^T v = xv.$$

于是 x 是 M^T 的特征值, 于是

$$\det(X \cdot I - M) = \det(X \cdot I - M^T) = 0,$$

即 $P_{L/K,x}(X)$ 在 L 中有根, 并为 x 自身. □

2. 假设 $d \in K$ 但是 $d \notin K^2, L = K(\sqrt{d}), x = a + b\sqrt{d}$. 证明, 存在唯一的域同构 $\sigma \in \mathrm{Aut}_K(L)$, 使得 $\sigma(\sqrt{d}) = -\sqrt{d}$ 并且

$$\mathrm{Tr}_{L/K}(x) = 2a = x + \sigma(x), \mathrm{N}_{L/K}(x) = a^2 - db^2 = x \cdot \sigma(x), P_{L/K,x}(X) = (X - x)(X - \sigma(x)).$$

证明：由于 $d \notin K^2$, 因此 $L = K(\sqrt{d})$ 是 K 的二次扩张. 定义映射 σ:

$$L \to L, \quad a + b\sqrt{d} \mapsto a - b\sqrt{d}.$$

并且对于任意的 $x_1, x_2 \in L$, 有 (具体的计算与复数的共轭类似):

$$\sigma(x_1 + x_2) = \sigma(x_1) + \sigma(x_2),$$
$$\sigma(x_1 x_2) = \sigma(x_1)\sigma(x_2).$$
$$\sigma(k) = k, \quad \forall\, k \in K.$$

因此 σ 是 K-同态, 从而是域同构, 即 $\sigma \in \mathrm{Aut}_K(L)$. 显然 $\sigma(\sqrt{d}) = -\sqrt{d}$.

若存在 $\overline{\sigma} \in \mathrm{Aut}_K(L)$ 也满足条件, 则 $\forall\, c, e \in K$,

$$\overline{\sigma}(c + e\sqrt{d}) = \overline{\sigma}(c) - \overline{\sigma}(e)\overline{\sigma}(\sqrt{d}) = c - e\sqrt{d} = \sigma(c + e\sqrt{d}),$$

因此 $\overline{\sigma} = \sigma$, 唯一性得证.

由于 $[L : K] = 2$, 由乘法映射的定义可知, 在基 $\{1, \sqrt{d}\}$ 下, 乘法映射 m_x 的矩阵表示为

$$M = \begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

因此,

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(M) = 2a = x + \sigma(x),$$
$$\mathrm{N}_{L/K}(x) = \det(M) = a^2 - db^2 = x \cdot \sigma(x),$$
$$P_{L/K,x}(X) = \det(X \cdot I - M) = (X - x)(X - \sigma(x)).$$

□

3. 证明, 以下映射为群同态:

$$\mathrm{Tr}_{L/K} : (L, +) \to (K, +), \quad \mathrm{N}_{L/K} : \left(L^\times, \cdot\right) \to \left(K^\times, \cdot\right)$$

证明: 对任意的 $x, y \in L$, 由乘法映射的定义可知,

$$m_{x+y}(z) = (x + y)z = xz + yz = m_x(z) + m_y(z), \forall\, z \in L.$$

因此,

$$m_{x+y} = m_x + m_y.$$

由线性映射的迹的性质可知,

$$\mathrm{Tr}_{L/K}(x + y) = \mathrm{Tr}(m_{x+y}) = \mathrm{Tr}(m_x + m_y) = \mathrm{Tr}(m_x) + \mathrm{Tr}(m_y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y).$$

同理, 对任意的 $x, y \in L^\times$, 有

$$m_{xy}(z) = (xy)z = x(yz) = m_x(m_y(z)), \forall\, z \in L.$$

因此,

$$m_{xy} = m_x \circ m_y.$$

由线性映射的行列式的性质可知,

$$\mathrm{N}_{L/K}(xy) = \det(m_{xy}) = \det(m_x \circ m_y) = \det(m_x) \cdot \det(m_y) = \mathrm{N}_{L/K}(x) \cdot \mathrm{N}_{L/K}(y).$$

由 m_x 为 K-线性映射知, $\mathrm{Tr}_{L/K}, \mathrm{N}_{L/K} \in K$. 又当 $x \in L^\times$ 时, m_x 为可逆映射 (因为存在逆元素 x^{-1} 使得 $m_x \circ m_{x^{-1}} = m_{x^{-1}} \circ m_x = \mathrm{id}_L$), 因此 $\mathrm{N}_{L/K}(x) = \det(m_x) \neq 0$, 即 $\mathrm{N}_{L/K}(x) \in K^\times$.

综上所述, 两个映射均为群同态. □

4. (迹的传递性) 如果 $K \subset M \subset L$ 是中间域. 证明,

$$\mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M} = \mathrm{Tr}_{L/K}.$$

(提示：选取 $\{e_i\}_{i\leqslant m}$ 和 $\{f_j\}_{j\leqslant n}$ 分别为 M/K 和 L/M 的基, 此时 $\{e_i f_j\}_{i\leqslant m, j\leqslant n}$ 为 L/K 的基. 那么,

$$x \cdot f_j = \sum_{j'=1}^{n} m_{jj'} f_{j'}, m_{jj'} \in M; m_{jj'} \cdot e_i = \sum_{i'=1}^{m} k_{jj',ii'} e_{i'}, k_{jj',ii'} \in K.$$

利用上述公式计算)

证明：设 $[M:K] = m, [L:M] = n$, 则 $[L:K] = mn$. 设 $\{e_1, e_2, \cdots, e_m\}$ 是 M 作为 K-线性空间的一组基, $\{f_1, f_2, \cdots, f_n\}$ 是 L 作为 M-线性空间的一组基. 则 $\{e_i f_j \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$ 是 L 作为 K-线性空间的一组基.

对任意的 $x \in L$, 存在 $m_{jj'} \in M$ 满足

$$x \cdot f_j = \sum_{j'=1}^{n} m_{jj'} f_{j'}, \quad \forall\, 1 \leqslant j \leqslant n.$$

同时, 对任意的 $m_{jj'} \in M$, 存在 $k_{jj',ii'} \in K$ 满足

$$m_{jj'} \cdot e_i = \sum_{i'=1}^{m} k_{jj',ii'} e_{i'}, \quad \forall\, 1 \leqslant i \leqslant m.$$

因此, 在基 $\{e_i f_j\}$ 下,

$$x \cdot (e_i f_j) = (x \cdot f_j) e_i = \left(\sum_{j'=1}^{n} m_{jj'} f_{j'} \right) e_i = \sum_{j'=1}^{n} (m_{jj'} \cdot e_i) f_{j'} = \sum_{j'=1}^{n} \sum_{i'=1}^{m} k_{jj',ii'} e_{i'} f_{j'}.$$

于是乘法映射 m_x 的矩阵表示为 $M = (M_{(i,j),(i',j')})$, 其中

$$M_{(i,j),(i',j')} = k_{jj',ii'}.$$

由矩阵的迹的定义可知,

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(M) = \sum_{j=1}^{n} \sum_{i=1}^{m} k_{jj,ii}.$$

注意到

$$\mathrm{Tr}_{L/M}(x)=\mathrm{Tr}\left((m_{jj'})_{j,j'}\right)=\sum_{j=1}^{n}m_{jj},\mathrm{Tr}_{M/K}(m_{jj})=\mathrm{Tr}\left((k_{jj,ii'})_{i,i'}\right)=\sum_{i=1}^{m}k_{jj,ii}.$$

因此,

$$\mathrm{Tr}_{L/K}(x)=\sum_{j=1}^{n}\sum_{i=1}^{m}k_{jj,ii}=\sum_{j=1}^{n}\mathrm{Tr}_{M/K}(m_{jj})=\mathrm{Tr}_{M/K}\left(\sum_{j=1}^{n}m_{jj}\right)=\mathrm{Tr}_{M/K}\left(\mathrm{Tr}_{L/M}(x)\right).$$

即有

$$\mathrm{Tr}_{M/K}\circ\mathrm{Tr}_{L/M}=\mathrm{Tr}_{L/K}.$$

□

5. 对于 $x\in L$, 令 $P_{\min}(X)$ 为其在 K 上的极小多项式. 证明,

$$P_{L/K,x}(X)=P_{\min}(X)^{[L:K(x)]}$$

(提示：选取 $\{e_i\}_{i\leqslant m}$ 和 $\{f_j\}_{j\leqslant n}$ 分别为 $K(x)/K$ 和 $L/K(x)$ 的基, 此时 $\{e_if_j\}_{i\leqslant m,j\leqslant n}$ 为 L/K 的基)

证明： 设 $[K(x):K]=m,[L:K(x)]=n$, 则 $[L:K]=mn$. 设 $\{e_1,e_2,\cdots,e_m\}$ 是 $K(x)$ 作为 K-线性空间的一组基, $\{f_1,f_2,\cdots,f_n\}$ 是 L 作为 $K(x)$-线性空间的一组基. 则 $\{e_if_j\mid 1\leqslant i\leqslant m,1\leqslant j\leqslant n\}$ 是 L 作为 K-线性空间的一组基.

首先考察在 $K(x)/K$ 上的乘法映射 m_x 的特征多项式, 这显然就是 x 在 K 上的极小多项式 $P_{\min}(X)$.

(不妨取一组基为 $\{1,x,x^2,\cdots,x^{m-1}\}$, 则在该基下, 乘法映射 m_x 的矩阵表示为

$$A=\begin{pmatrix}0&0&\cdots&0&-a_0\\1&0&\cdots&0&-a_1\\0&1&\cdots&0&-a_2\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&-a_{m-1}\end{pmatrix},$$

其中 $P_{\min}(X)=X^m+a_{m-1}X^{m-1}+\cdots+a_1X+a_0$. 由此可知, $P_{\min}(X)=\det(X\cdot I-M)$.)

再考虑 m_x 在 L/K 上的特征多项式, 直接考虑 m_x 在 e_if_j 上的作用并且记 m_x 在 $\{e_1,e_2,\cdots,e_m\}$ 上的矩阵为 A, 则有:

$$x\cdot(e_if_j)=(x\cdot e_i)f_j=\left(\sum_{i'=1}^{m}a_{ii'}e_{i'}\right)f_j=\sum_{i'=1}^{m}a_{ii'}e_{i'}f_j.$$

因此, 在基 $\{e_if_j\}$ 下, 乘法映射 m_x 的矩阵表示为 $M=(M_{(i,j),(i',j')})$, 其中

$$M_{(i,j),(i',j')}=\begin{cases}a_{ii'},&\text{if } j=j',\\0,&\text{if } j\neq j'.\end{cases}$$

也即, 乘法映射 m_x 在基 $\{e_if_j\}$ 下的矩阵表示为分块对角阵:

$$M=\begin{pmatrix}A&0&\cdots&0\\0&A&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&A\end{pmatrix}_{mn}.$$

由此可知,

$$P_{L/K,x}(X)=\det(X\cdot I-M)=\det(X\cdot I-A)^n=P_{\min}(X)^{[L:K(x)]}.$$

□

注：仔细比较与第 4 小问的证明过程, 4. 中的证明过程 x 只能作用在中间域 M 上, 而 5. 中的证明过程 x 可以作用在 K 上. 这样就导致 5 中的表示矩阵为分块对角阵.

6. 对于 $x\in L,P_{\min}(X)$ 为其在 K 上的极小多项式，$x_1,x_2,\cdots,x_d$ 为 $P_{\min}(X)$ 在 K 的某个分裂域中所有的根（即 $P_{\min}(X)=\prod_{i=1}^{d}(X-x_i)$ ）。证明，

$$\mathrm{Tr}_{L/K}(x)=[L:K(x)]\left(\sum_{i=1}^{d}x_i\right),\quad \mathrm{N}_{L/K}(x)=\left(\prod_{i=1}^{d}x_i\right)^{[L:K(x)]}.$$

证明：由第 5 小问的结论可知,

$$P_{L/K,x}(X)=P_{\min}(X)^{[L:K(x)]}=\left(\prod_{i=1}^{d}(X-x_i)\right)^{[L:K(x)]}=\prod_{i=1}^{d}(X-x_i)^{[L:K(x)]}.$$

因此, 由特征多项式的系数和迹与行列式的关系可知,

$$\mathrm{Tr}_{L/K}(x)=-\text{系数}(X^{nd-1})=[L:K(x)]\left(\sum_{i=1}^{d}x_i\right),$$
$$\mathrm{N}_{L/K}(x)=(-1)^{nd}\text{常数项}=\left(\prod_{i=1}^{d}x_i\right)^{[L:K(x)]}.$$

□

7. L/K 为有限可分扩张，Ω/K 为域扩张并且 Ω 是代数封闭的。那么，对任意的 $x\in L$ ，

$$\mathrm{Tr}_{L/K}(x)=\sum_{\sigma\in\mathrm{Hom}_K(L,\Omega)}\sigma(x),\mathrm{N}_{L/K}(x)=\prod_{\sigma\in\mathrm{Hom}_K(L,\Omega)}\sigma(x),$$

以及

$$P_{L/K,x}(X)=\prod_{\sigma\in\mathrm{Hom}_K(L,\Omega)}(X-\sigma(x)).$$

提示：证明思路参考讲义的 166 页. 借助中间域 $K(x)$.

证明：设 L/K 为有限可分扩张, Ω/K 为代数封闭域扩张, $x \in L$. 记

$$\Sigma := \mathrm{Hom}_K(L, \Omega).$$

由于 L/K 可分, $K(x)/K$ 与 $L/K(x)$ 亦为有限可分扩张, 因此任意 $\tau \in \mathrm{Hom}_K(K(x), \Omega)$ 都可以延拓为某个 $\sigma \in \mathrm{Hom}_K(L, \Omega)$, 从而限制映射

$$\mathrm{res} : \Sigma \longrightarrow \mathrm{Hom}_K(K(x), \Omega), \quad \sigma \longmapsto \sigma|_{K(x)},$$

是满射. 设 $\alpha \in \Omega$ 是 x 的一个 K-共轭元, 即

$$\alpha = \tau(x) \quad \text{对某个} \tau \in \mathrm{Hom}_K(K(x), \Omega).$$

则

$$\{\sigma \in \Sigma \mid \sigma(x) = \alpha\} = \{\sigma \in \Sigma \mid \sigma|_{K(x)} = \tau\} = \mathrm{res}^{-1}(\tau).$$

由于 $L/K(x)$ 是有限可分扩张，对每个固定的 τ，满足 $\sigma|_{K(x)} = \tau$ 的 K-嵌入 $\sigma : L \to \Omega$ 的个数等于扩张次数 $[L : K(x)]$，即

$$\#\mathrm{res}^{-1}(\tau) = [L : K(x)].$$

这说明：对每一个 K-共轭元 α，恰有 $[L : K(x)]$ 个 $\sigma \in \Sigma$ 满足 $\sigma(x) = \alpha$. 设 $P_{\min}(X)$ 为 x 在 K 上的最小多项式，则

$$P_{\min}(X) = \prod_{\alpha} (X - \alpha),$$

其中 α 遍历 x 的所有 K-共轭元. 由上面的计数结果可得

$$\prod_{\sigma \in \Sigma} (X - \sigma(x)) = \prod_{\alpha} (X - \alpha)^{[L:K(x)]} = P_{\min}(X)^{[L:K(x)]}.$$

而由第 5 小问, 知

$$P_{L/K, x}(X) = P_{\min}(X)^{[L:K(x)]},$$

故

$$P_{L/K, x}(X) = \prod_{\sigma \in \mathrm{Hom}_K(L, \Omega)} (X - \sigma(x)).$$

由特征多项式与迹、范数的定义, 类似第 6 小题有

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \mathrm{Hom}_K(L, \Omega)} \sigma(x), \qquad \mathrm{N}_{L/K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(L, \Omega)} \sigma(x).$$

□

8. L/K 为有限扩张，Ω/K 如上。那么，对任意的 $x \in L$，

$$\mathrm{Tr}_{L/K}(x) = p^n \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x), \mathrm{N}_{L/K}(x) = \left(\prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x) \right)^{p^n},$$

其中，$p^n = \frac{[L,K]}{[L,K]_s}$ 为扩张的不可分次数。

证明： 设 $P_{\min}(X) = (X-\alpha_1)\cdots(X-\alpha_d)$ 设其中有 d' 个互不相同 $\{\beta_1, \cdots, \beta_{d'}\}$ 则 $d' = [K(x):K]_s$ 且每个根重数均为 $\frac{[K(x):K]}{[K(x):K]_s} =: p^m$. 又有

$$\mathrm{Ext}_{L/K}(\Omega, \mathrm{id}_K) = \prod_{\psi \in \mathrm{Ext}_{K(x)/K}(\Omega, \mathrm{id}_K)} \mathrm{Ext}_{L/K(x)}(\Omega, \psi),$$

即 $\mathrm{Hom}_K(L,\Omega) = \prod_{\psi \in \mathrm{Ext}_{K(x)/K}(\Omega,\mathrm{id}_K)} \mathrm{Ext}_{L/K(x)}(\Omega,\psi)$. 而有对应 $\mathrm{Hom}_K(L,\Omega) = \{\tau_1, \cdots, \tau_{d'}\}$. 且 $\tau_i(x) = \beta_i, 1 \leqslant i \leqslant d'$. $\forall \sigma \in \mathrm{Ext}_{L/K(x)}(\Omega, \tau_i), \sigma|_{K(x)} = \tau_i$ 故 $\sigma(x) = \tau_i(x) = \beta_i, 1 \leq i \leq d'$.

又 $|\mathrm{Ext}_{L/K(x)}(\Omega, \tau_i)| = [L : K(x)]_s = \frac{[L:K]_s}{[K(x):K]_s}$. 故对于每个 β_i，恰有 $[L : K(x)]_s$ 个 $\sigma \in \mathrm{Hom}_K(L,\Omega)$ 满足 $\sigma(x) = \beta_i$. 由第 5 小问的结论可知

$$P_{L/K,x}(X) = P_{\min}(X)^{[L:K(x)]} = \prod_{i=1}^{d} (X-\alpha_i)^{[L:K(x)]} = \prod_{i=1}^{d'} (X-\beta_i)^{p^m[L:K(x)]}.$$

又有

$$\begin{aligned} p^m[L:K(x)] &= \frac{[K(x):K]}{[K(x):K]_s}[L:K(x)] \\ &= \frac{[L:K]}{[K(x):K]_s} = \frac{[L:K]_s \cdot p^n}{[K(x):K]_s} \\ &= p^n \cdot [L:K(x)]_s. \end{aligned}$$

于是

$$P_{L/K,x}(X) = \prod_{i=1}^{d'} (X-\beta_i)^{p^n[L:K(x)]_s} = \left(\prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} (X - \sigma(x)) \right)^{p^n}.$$

类似于第 6 小问的证明过程, 可得

$$\mathrm{Tr}_{L/K}(x) = p^n \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x), \quad \mathrm{N}_{L/K}(x) = \left(\prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x) \right)^{p^n}.$$

□

9. （迹和范数的传递性）如果 $K \subset M \subset L$ 是中间域。证明，

$$\mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M} = \mathrm{Tr}_{L/K}, \quad \mathrm{N}_{M/K} \circ \mathrm{N}_{L/M} = \mathrm{N}_{L/K}.$$

（为简单起见，你可以只对可分情形进行证明）

证明： 由于 L/K 可分, 因此 M/K 和 L/M 亦为可分扩张. 设 $x \in L$, 则由第 7 小问的结论可知,

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x), \quad \mathrm{N}_{L/K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x).$$

同理,

$$\mathrm{Tr}_{L/M}(x) = \sum_{\tau \in \mathrm{Hom}_M(L,\Omega)} \tau(x), \quad \mathrm{N}_{L/M}(x) = \prod_{\tau \in \mathrm{Hom}_M(L,\Omega)} \tau(x).$$

对任意的 $\tau \in \mathrm{Hom}_M(L,\Omega)$, 其限制映射 $\tau|_M$ 属于 $\mathrm{Hom}_K(M,\Omega)$. 由此可知,

$$\begin{aligned}
\mathrm{Tr}_{M/K}(\mathrm{Tr}_{L/M}(x)) &= \mathrm{Tr}_{M/K}\left(\sum_{\tau \in \mathrm{Hom}_M(L,\Omega)} \tau(x)\right) \\
&= \sum_{\tau \in \mathrm{Hom}_M(L,\Omega)} \mathrm{Tr}_{M/K}(\tau(x)) \\
&= \sum_{\tau \in \mathrm{Hom}_M(L,\Omega)} \sum_{\substack{\sigma \in \mathrm{Hom}_K(L,\Omega) \\ \sigma|_M = \tau|_M}} \sigma(x) \\
&= \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x) = \mathrm{Tr}_{L/K}(x).
\end{aligned}$$

同理,

$$\begin{aligned}
\mathrm{N}_{M/K}(\mathrm{N}_{L/M}(x)) &= \mathrm{N}_{M/K}\left(\prod_{\tau \in \mathrm{Hom}_M(L,\Omega)} \tau(x)\right) \\
&= \prod_{\tau \in \mathrm{Hom}_M(L,\Omega)} \mathrm{N}_{M/K}(\tau(x)) \\
&= \prod_{\tau \in \mathrm{Hom}_M(L,\Omega)} \prod_{\substack{\sigma \in \mathrm{Hom}_K(L,\Omega) \\ \sigma|_M = \tau|_M}} \sigma(x) \\
&= \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x) = \mathrm{N}_{L/K}(x).
\end{aligned}$$

□

注： 如果是不可分的情况, 则需要借助第 8 小问的结论进行类似的证明. 如下：由于 L/K 为有限扩张, 因此 M/K 和 L/M 亦为有限扩张. 设 $[M : K]_s = m, [L : M]_s = n$, 则

$[L:K]_s = m+n$. 设 $x \in L$, 则由第 8 小问的结论可知,

$$\begin{aligned}
\mathrm{Tr}_{M/K}(\mathrm{Tr}_{L/M}(x)) &= \mathrm{Tr}_{M/K}\left(p^n \sum_{\tau\in \mathrm{Hom}_M(L,\Omega)} \tau(x)\right) \\
&= p^n \sum_{\tau\in \mathrm{Hom}_M(L,\Omega)} \mathrm{Tr}_{M/K}(\tau(x)) \\
&= p^n \sum_{\tau\in \mathrm{Hom}_M(L,\Omega)} \left(p^m \sum_{\substack{\sigma\in \mathrm{Hom}_K(L,\Omega)\\ \sigma|_M=\tau|_M}} \sigma(x)\right) \\
&= p^{m+n} \sum_{\sigma\in \mathrm{Hom}_K(L,\Omega)} \sigma(x) = \mathrm{Tr}_{L/K}(x).
\end{aligned}$$

同理,

$$\begin{aligned}
\mathrm{N}_{M/K}(\mathrm{N}_{L/M}(x)) &= \mathrm{N}_{M/K}\left(\left(\prod_{\tau\in \mathrm{Hom}_M(L,\Omega)} \tau(x)\right)^{p^n}\right) \\
&= \left(\prod_{\tau\in \mathrm{Hom}_M(L,\Omega)} \mathrm{N}_{M/K}(\tau(x))\right)^{p^n} \\
&= \left(\prod_{\tau\in \mathrm{Hom}_M(L,\Omega)} \left(\prod_{\substack{\sigma\in \mathrm{Hom}_K(L,\Omega)\\ \sigma|_M=\tau|_M}} \sigma(x)\right)^{p^m}\right)^{p^n} \\
&= \left(\prod_{\sigma\in \mathrm{Hom}_K(L,\Omega)} \sigma(x)\right)^{p^{m+n}} = \mathrm{N}_{L/K}(x).
\end{aligned}$$

10. K 是域，$P(X) \in K[X]$ 为首一的不可约多项式，$d = \deg(P), \alpha$ 为 P 在 $\overline{K}$ 中的一个根。证明，

$$\mathrm{Disc}(P) = (-1)^{\frac{1}{2}d(d-1)} \mathrm{N}_{K(\alpha)/K}(P'(\alpha))$$

以上，$\mathrm{Disc}(P) := \prod_{i<j}(\alpha_i - \alpha_j)^2$ ，其中，$\{\alpha_i\}$ 为 P 在 $\overline{K}$ 中的所有根（包括重根）。

证明： 设 $P(X) = \prod_{i=1}^{d}(X - \alpha_i)$, 则

$$P'(X) = \sum_{i=1}^{d} \prod_{\substack{1\leqslant j\leqslant d\\ j\neq i}} (X - \alpha_j).$$

因此,

$$P'(\alpha_i) = \prod_{\substack{1\leqslant j\leqslant d\\ j\neq i}} (\alpha_i - \alpha_j).$$

由此可得,

$$\prod_{i=1}^{d} P'(\alpha_i) = \prod_{i=1}^{d} \prod_{\substack{1\leqslant j\leqslant d\\ j\neq i}} (\alpha_i - \alpha_j) = (-1)^{\frac{1}{2}d(d-1)} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

因此,

$$\mathrm{Disc}(P)=\prod_{i<j}(\alpha_i-\alpha_j)^2=(-1)^{\frac{1}{2}d(d-1)}\prod_{i=1}^{d}P'(\alpha_i).$$

由于 $K(\alpha)$ 是 K 的有限扩张, 由第 7 小问的结论可知,

$$\mathrm{N}_{K(\alpha)/K}(P'(\alpha))=\prod_{\sigma\in\mathrm{Hom}_K(K(\alpha),\overline{K})}\sigma(P'(\alpha))=\prod_{i=1}^{d}P'(\alpha_i).$$

因此,

$$\mathrm{Disc}(P)=(-1)^{\frac{1}{2}d(d-1)}\mathrm{N}_{K(\alpha)/K}(P'(\alpha)).$$

□

11. L/K 为有限扩张，$x\in L$ 在 K 上不可分。证明，$\mathrm{Tr}_{L/K}(x)=0$ 。

证明：由第 8 小问的结论可知,

$$\mathrm{Tr}_{L/K}(x)=p^n\sum_{\sigma\in\mathrm{Hom}_K(L,\Omega)}\sigma(x),$$

这还隐含了 $\mathrm{Char}(K)=p>0$. 由于 x 在 K 上不可分, 因此任意的 $\sigma\in\mathrm{Hom}_K(L,\Omega)$ 都满足 $\sigma(x)=x$. 由此可知,

$$\mathrm{Tr}_{L/K}(x)=p^n\sum_{\sigma\in\mathrm{Hom}_K(L,\Omega)}x=p^n\cdot[L:K]_s\cdot x=0.$$

□

12. L/K 为有限扩张并且不是可分的。证明，$\mathrm{Tr}_{L/K}\equiv 0$ 。

证明：由于 L/K 不是可分扩张, 因此存在 $x\in L$ 在 K 上不可分. 由第 11 小问的结论可知,

$$\mathrm{Tr}_{L/K}(x)=0.$$

由于乘法映射 m_x 是 K-线性映射, 对任意的 $y\in L$, 有

$$\mathrm{Tr}_{L/K}(xy)=\mathrm{Tr}(m_{xy})=\mathrm{Tr}(m_x\circ m_y)=\mathrm{Tr}(m_y\circ m_x)=\mathrm{Tr}(m_y)\cdot\mathrm{Tr}(m_x)=\mathrm{Tr}_{L/K}(y)\cdot 0=0.$$

由于 $\{xy\mid y\in L\}$ 张成了整个 L, 因此对任意的 $z\in L$, 有

$$\mathrm{Tr}_{L/K}(z)=0.$$

即有

$$\mathrm{Tr}_{L/K}\equiv 0.$$

□

13. 考虑对称 K-双线性的二次型

$$L\times L\longrightarrow K,\quad (x,y)\mapsto\mathrm{Tr}_{L/K}(x\cdot y)$$

对任意的 $x \in L$，存在 $y \in L$，使得 $\mathrm{Tr}_{L/K}(x \cdot y) \neq 0$，我们就称这个二次型是**非退化的**，否则是**退化的**。证明，如果 $\mathrm{char}(K) = 0$，以上二次型非退化；如果 L/K 不是可分的，以上二次型退化。

证明： 如果 $\mathrm{char}(K) = 0, \forall x \in L^{\times}$,

$$\mathrm{Tr}_{L/K}(x \cdot x^{-1}) = \mathrm{Tr}_{L/K}(1) = [L : K] \neq 0.$$

如果 L/K 不是可分扩张, 则由第 12 小问的结论可知,

$$\mathrm{Tr}_{L/K} \equiv 0.$$

即二次型是退化的. □

14. 假设 L/K 是可分的，从而，$L = K(x), n = [L : K]$。证明，$\mathrm{Tr}_{L/K}\left(x^k\right)$ 中至少有一个非零，其中，$k = 0, 1, \cdots, n-1$.

证明： 设 $P_{\min}(X)$ 为 x 在 K 上的极小多项式, 则 $\deg(P_{\min}) = n$. 由于 L/K 是可分扩张, 因此 $P_{\min}(X)$ 在某个分裂域中有 n 个互异的根, 记为 $x_1, x_2, \cdots, x_n$.(根与 K-同态是一一对应的) 由第 7 小问的结论可知,

$$\mathrm{Tr}_{L/K}\left(x^k\right) = \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x^k) = \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x)^k = \sum_{i=1}^{n} x_i^k, \quad k = 0, 1, \cdots, n-1.$$

如果 $\mathrm{Tr}_{L/K}\left(x^k\right) = 0$ 对所有的 $k = 0, 1, \cdots, n-1$ 都成立, 则由范德蒙行列式可知,

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i) = 0,$$

这与 $x_1, x_2, \cdots, x_n$ 互异矛盾. 因此, 存在某个 k , 使得 $\mathrm{Tr}_{L/K}\left(x^k\right) \neq 0$. □

15. 证明，L/K 是可分的等价于二次型

$$L \times L \longrightarrow K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(x \cdot y)$$

非退化。

证明： 如果 L/K 是可分扩张, 则由第 14 小问的结论可知,

$$\mathrm{Tr}_{L/K}\left(x^k\right) \neq 0,$$

对某个 $k = 0, 1, \cdots, n-1$. 因此, 对任意的 $x' \in L^{\times}$，存在 $y = \frac{x^{k-1}}{x'} \in L$, 使得

$$\mathrm{Tr}_{L/K}(x \cdot y) \neq 0.$$

再由 13 小问的结论可知, 如果 L/K 是不是可分的, 则二次型是退化的.

综上, L/K 是可分的等价于二次型非退化. □

B. 利用 Galois 对应证明代数基本定理

给定有限扩张 $K/\mathbb{R}$。

1. 证明，若 $[K:\mathbb{R}]=2$，则 $K\simeq\mathbb{C}$。

证明： 设 $K=\mathbb{R}(\alpha)$, 则 α 在 $\mathbb{R}$ 上的极小多项式 $P_{\min}(X)$ 的次数为 2. 由于 $\mathbb{R}$ 是实数域, 因此 $P_{\min}(X)$ 在 $\mathbb{R}$ 上没有实根. 于是, $P_{\min}(X)$ 的形式为

$$P_{\min}(X)=X^2+bX+c,$$

其中 $b,c\in\mathbb{R}$ 且判别式 $b^2-4c<0$. 设 $\Delta=\sqrt{4c-b^2}>0$, 则 $P_{\min}(X)$ 在 $\mathbb{C}$ 中的根为

$$\alpha_1=\frac{-b+i\Delta}{2},\quad \alpha_2=\frac{-b-i\Delta}{2}.$$

定义映射

$$\varphi: K\longrightarrow\mathbb{C},\quad f(\alpha)\mapsto f(\alpha_1),$$

其中 $f(X)\in\mathbb{R}[X]$. φ 是一个域同构. 这是因为, 对任意的 $f(X),g(X)\in\mathbb{R}[X]$, 有

$$\varphi(f(\alpha)+g(\alpha))=f(\alpha_1)+g(\alpha_1)=\varphi(f(\alpha))+\varphi(g(\alpha)),$$
$$\varphi(f(\alpha)\cdot g(\alpha))=f(\alpha_1)\cdot g(\alpha_1)=\varphi(f(\alpha))\cdot\varphi(g(\alpha)).$$

从而 φ 是域同态, 从而是域同构.

因此, $K\simeq\mathbb{C}$. □

2. 证明，若 $[K:\mathbb{R}]$ 为奇数，则 $K\simeq\mathbb{R}$。（提示：这是证明中唯一使用连续性的地方）

证明： 任取 $\alpha\in K$, 设 $P_{\min}(X)$ 为 α 在 $\mathbb{R}$ 上的极小多项式, 则 $\deg(P_{\min})=2n+1$. 由于 $\mathbb{R}$ 是实数域, 由连续性知 $P_{\min}(X)$ 在 $\mathbb{R}$ 上至少有一个实根, 记为 r. 由于 $P_{\min}(X)$ 是不可约多项式, 因此 $P_{\min}(X)=X-r$. 于是, $\alpha=r\in\mathbb{R}$. 因此, $K=\mathbb{R}$. 即有 $K\simeq\mathbb{R}$. □

3. 证明，$\mathbb{C}$ 没有次数为 2 的扩张。

证明： 假设存在次数为 2 的扩张 $L/\mathbb{C}$. 则存在 $\alpha\in L$, 使得 $L=\mathbb{C}(\alpha)$. 设 $P_{\min}(X)$ 为 α 在 $\mathbb{C}$ 上的极小多项式, 则 $\deg(P_{\min})=2$. 但次数为 2 的代数扩张都为正规扩张 (证明使用韦达定理), 因此 $P_{\min}(X)$ 在 $\mathbb{C}$ 上分裂, 这与 $P_{\min}(X)$ 不可约矛盾. 因此, $\mathbb{C}$ 没有次数为 2 的扩张. □

4. 如果 $K/\mathbb{R}$ 是 Galois 扩张。证明，存在中间域的序列：

$$\mathbb{R}\subset K_1\subset K_2\subset\cdots\subset K_n=K$$

使得 $[K_1:\mathbb{R}]$ 为奇数并且对每个 $i=1,\cdots,n-1,[K_{i+1}:K_i]=2$。

（提示：可以使用（证明）群论中的结论：G 是 p-群，其中 p 是素数，$|G|=p^n,n\in\mathbb{Z}_{\geqslant 1}$ ，则存在子群的序列

$$G_1<G_2<\cdots<G_n=G,$$

其中 $|G_i| = p^i$ 且 G_i 在 G 中正规。）

注：先证明群论中的结论. 设 G 是 p-群, 其中 p 是素数, $|G| = p^n, n \in \mathbb{Z}_{\geqslant 1}$. 通过归纳法证明该结论.

当 $n = 1$ 时, G 本身就是所需的子群序列.

假设当 $n = k$ 时结论成立. 当 $n = k + 1$ 时, 由于 G 是 p-群, 因此其中心 $Z(G)$ 非平凡. 取 $Z(G)$ 中的一个阶为 p 的循环子群 H, 则 H 在 G 中正规. 考虑商群 G/H, 则 $|G/H| = p^k$. 由归纳假设可知, 存在子群的序列

$$G_1 < G_2 < \cdots < G_k = G/H,$$

其中 $|G_i| = p^i$ 且 G_i 在 G/H 中正规.

对每个 $i = 1, 2, \cdots, k$, 定义子群

$$G'_{i+1} = \pi^{-1}(G_i),$$

其中 $\pi : G \longrightarrow G/H$ 是自然投射. 则有

$$|G'_{i+1}| = |H| \cdot |G_i| = p^{i+1}.$$

因此, 存在子群的序列

$$G'_1 < G'_2 < \cdots < G'_{k+1} = G,$$

其中 $|G'_i| = p^i$ 且 G'_i 在 G 中正规.

综上, 群论中的结论得证.

证明：设 $G = \mathrm{Gal}(K/\mathbb{R})$. 设 $|G| = 2^n \cdot l$, 其中 l 为奇数. 由 Sylow 定理, G 有阶为 2^n 的 Sylow 2-子群 H_1. 由群论中的结论可知, 存在子群的序列

$$H_1 \triangleright H_2 \triangleright \cdots \triangleright H_n = 1,$$

其中 $|H_i| = 2^i$ 且 H_i 在 H_1 中正规, 正规包含是因为指数皆为 2. 对每个 $i = 1, 2, \cdots, n$, 定义中间域

$$K_i = K^{H_i} = \{x \in K \mid \sigma(x) = x, \forall \sigma \in H_i\}.$$

则由 Galois 对应可知, 存在中间域的序列

$$\mathbb{R} \subset K_1 \subset K_2 \subset \cdots \subset K_n = K,$$

使得 $[K_1 : \mathbb{R}] = \frac{|G|}{|H_i|} = \frac{2^n \cdot l}{2^n} = l$ 和对每个 $i = 1, \cdots, n-1, [K_{i+1} : K_i] = \frac{|H_i|}{|H_{i+1}|} = 2$. □

5. 证明，给定有限扩张 $K/\mathbb{R}$ ，那么 $K = \mathbb{R}$ 或 $\mathbb{C}$ 。

证明： 设 $[K:\mathbb{R}]=n$. 如果 n 为奇数, 则由第 2 小问的结论可知, $K\simeq\mathbb{R}$. 如果 n 为偶数, 考虑 $K/\mathbb{R}$ 的正规闭包 N, 于是 $N/\mathbb{C}$ 为 Galois 扩张. 则由第 4 小问的结论可知, 存在中间域的序列

$$\mathbb{R}\subset K_1\subset K_2\subset\cdots\subset K_m=N,$$

使得 $[K_1:\mathbb{R}]$ 为奇数并且对每个 $i=1,\cdots,m-1,[K_{i+1}:K_i]=2$.

由于 $[K_1:\mathbb{R}]$ 为奇数, 由第 2 小问的结论可知, $K_1\simeq\mathbb{R}$. 那么 $K_2\simeq\mathbb{C}$(由 n 为偶数, $m\geqslant 2$). 再由第 3 小问的结论可知, $m=2$. 因此, $N=K_2\simeq\mathbb{C}$. 这也意味着 $K=\mathbb{C}$.

综合以上两种情况可知, 给定有限扩张 $K/\mathbb{R}$, 那么 $K=\mathbb{R}$ 或 $\mathbb{C}$. □

6. 证明代数基本定理。

证明： 设 $P(x)\in\mathbb{C}[X]$ 为首一多项式, K 为 $P(X)$ 的分裂域. 那么 $K/\mathbb{C}$ 为有限扩张, 从而 $K/\mathbb{R}$ 也为有限扩张. 由第 5 小问的结论可知, $K=\mathbb{C}$. 因此, 代数基本定理得证. □