2021年8月11日 11:48

代数数域

$\mathbb{Q} \subset \mathbb{C}$

Def $\hookrightarrow$ = $\mathbb{Q}$的有限扩张（看作$\mathbb{C}$的子域） $K/\mathbb{Q}$

$\forall \alpha \in K \quad \exists f \in \mathbb{Q}[X] \quad f(\alpha)=0$

↑首一，最小次数的 称作 α在$\mathbb{Q}$上的极小多项式

$\mathbb{C} \supset \overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{是代数数}\}$ = $\mathbb{Q}$的代数闭包

α是某个$\mathbb{Q}$-系数多项式f的根.

Rk $e, \pi \in \mathbb{C} \setminus \overline{\mathbb{Q}}$ 是超越数

$\mathrm{char} K = 0$ L/K 有限扩张 $\Rightarrow$ 单扩张

$\exists \alpha \in L \quad L = K(\alpha)$

也即 $\exists f \in K[X]$ 不可约(首-)多项式 $L = K[X]/(f)$

$K(\alpha) \xrightarrow{\sim} K[X]/(f)$, $\alpha \mapsto \bar{X} = X \bmod (f) = X + (f)$

取 β为f的任一个复根

$\tau : {}_K L \hookrightarrow \mathbb{C}$, $X+(f) \mapsto \beta$，若 $\tau_K = id_K$ 则称为 K-嵌入

Th L/K $[L:K]=n$ 则每个嵌入 $\sigma : K \hookrightarrow \mathbb{C}$ 总可以有n个不同的延拓 $\tau_i : L \hookrightarrow \mathbb{C}$ ($\tau_i|_K = \sigma$)

Pf 令 $L = K(\gamma)$

γ 极小多项式 $f = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + x^n \in K[x]$

L: K-向量空间 基 $(1, \gamma, \gamma^2, \cdots, \gamma^{n-1})$

$\forall \alpha \in L$ 唯一写成 $\alpha = k_0 + k_1 \gamma + \cdots + k_{n-1}\gamma^{n-1}$ $(k_i \in K)$

若 $\tau : L \hookrightarrow \mathbb{C}$ 使 $\tau_K = \sigma$ 则

$\tau(\alpha) = \tau(k_0 + \cdots + k_{n-1}\gamma^{n-1}) = \sigma(k_0) + \sigma(k_1)\tau(\gamma) + \cdots + \sigma(k_{n-1})\tau(\gamma)^{n-1}$

由 $\tau(\gamma)$唯一决定

$\sigma : K \hookrightarrow \mathbb{C}$ $\sigma : K \xrightarrow{\simeq} \sigma(K)$

$\sigma f = \sigma(c_0) + \sigma(c_1) x + \cdots + \sigma(c_{n-1}) x^{n-1} + x^n \in \sigma(K)[x]$

σf是$\sigma(K)$上的不可约多项式，有n个不同复根 $\rho_1, \cdots, \rho_n \in \mathbb{C}$

又 $\sigma f(\tau(\gamma)) = \sigma(c_0) + \sigma(c_1)\tau(\gamma) + \cdots + \sigma(c_{n-1})\tau(\gamma)^{n-1} + \tau(\gamma)^n$

σf 是 $\sigma(K)$ 上的不可约多项式，有 n 个不同复根 $\rho_1, \cdots, \rho_n \in \mathbb{C}$

又 $\sigma f(\tau(\gamma)) = \sigma(c_0) + \sigma(c_1)\tau(\gamma) + \cdots + \sigma(c_{n-1})\tau(\gamma)^{n-1} + \tau(\gamma)^n$

$= \tau(f\gamma) = \tau(0) = 0$

$\tau(\gamma)$ 是 σf 的根，是某个 ρ_i，延拓 τ 至多有 n 种取法.

定义 $\tau_i : L \to \mathbb{C}$

$k_0 + k_1\gamma + \cdots + k_{n-1}\gamma^{n-1} \longmapsto \sigma(k_0) + \sigma(k_1)\rho_i + \cdots + \sigma(k_{n-1})\rho_i^{n-1}$

τ_i 这样的确是域的同态，且 $\tau_i|_K = \sigma$. #

Cor 从 L 到 $\mathbb{C}$ 正好有 $[L:K]$ 个不同的 K-嵌入.

(即在 τ_i 中取 $\sigma: K \to \mathbb{C}$ 为 K 的恒等嵌入)

Rk $L = K(\gamma)$ $f \in K[x]$ 为 γ 的极小多项式

$\deg f = n = [L:K]$ f 在 $\mathbb{C}$ 中 n 个不同根 $\gamma_1, \gamma_2, \cdots, \gamma_n$ ($\gamma_1 = \gamma$)

称作 γ 的 K-共轭元

$\tau_i : L = K(\gamma) \xrightarrow{\simeq} K(\gamma_i) \subseteq \mathbb{C}$ n 个不同的 K-嵌入

$\gamma \longmapsto \gamma_i$

$\tau_1 = id_L$

$i \neq 1$ $K(\gamma_i)$ 可能与 $K(\gamma) = L$ 不相同(也可能相同)

若全是相同的，称 L/K 是 Galois 扩张. $Gal(L/K) = \{\tau_1, \cdots, \tau_n\} = Aut_K L$

$L = K(\gamma_1) = \cdots = K(\gamma_n)$

一般情况，$K(\gamma_1, \gamma_2, \cdots, \gamma_n) \supseteq L$

称作 L/K 的 Galois 闭包/正规闭包

Def $K = \mathbb{Q}$ $f \in \mathbb{Q}[x]$ r 个实根 $\gamma_1, \cdots, \gamma_r$ ($2s + r = n$)

和 s 对共轭复根 $\gamma_{r+1} = \overline{\gamma}_{r+s+1}$

$\gamma_{r+2} = \overline{\gamma}_{r+s+2}$

$\vdots$

$\gamma_{r+s} = \overline{\gamma}_{r+2s}$

$\mathbb{Q}[x]/(f)$ $=$ L

相应地有 $\tau_i : L \longrightarrow \mathbb{Q}(\gamma_i) \subset \mathbb{R} \subset \mathbb{C}$ r 个实嵌入

($i = 1, \cdots, r$) $\bar{x} \longmapsto \gamma_i$

$j = 1, \cdots, s$ $\tau_{r+j} : L \longrightarrow \mathbb{Q}(\gamma_{r+j}) \subset \mathbb{C}$ s 对共轭复嵌入.

$\bar{x} \longmapsto \gamma_{r+j}$

$\tau_{r+s+j} : L \longrightarrow \mathbb{Q}(\overline{\gamma}_{r+j}) \subset \mathbb{C}$

$\bar{x} \longmapsto \overline{\gamma}_{r+j}$

$= c \circ \tau_{r+j}$ $\overline{\gamma}_{r+j} = \gamma_{r+s+j}$

其中 $c : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$

例 $d \in \mathbb{Z}$ 无平方因子

$d>0$ $K=\mathbb{Q}(\sqrt{d})$ 称为 实二次域 (Galois 论)

$id: \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}) \subset \mathbb{R} \subset \mathbb{C}$

$\sigma: \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}) \subset \mathbb{R} \subset \mathbb{C}$

$a+b\sqrt{d} \mapsto a-b\sqrt{d}$

$n=r=2$

$\sqrt{d}$ $x^2-d=(x+\sqrt{d})(x-\sqrt{d})$

$d<0$ $K=\mathbb{Q}(\sqrt{d})$ 虚二次域

$n=\overset{0}{\overset{\|}{r}}+2s$

一对复嵌入 $id: \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$

$\sigma: \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$

$a+b\sqrt{d} \mapsto a-b\sqrt{d}$

$-\sqrt{d}=\sqrt{d}$

例 $f=X^3-2 \in \mathbb{Q}[X]$ 不可约

三个根 $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ $\omega=e^{\frac{2\pi i}{3}}$

$K=\mathbb{Q}[X]/(f)$ 不是 Galois /$\mathbb{Q}$. $[K:\mathbb{Q}]=3=n=r+2s$ $r=1, s=1$

一个实嵌入: $K \to \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R} \subset \mathbb{C}$

$X+(f) \mapsto \sqrt[3]{2}$

一对共轭复嵌入: $\begin{cases} \tau: K \to \mathbb{Q}(\sqrt[3]{2}\omega) \subset \mathbb{C} \\ X+(f) \mapsto \sqrt[3]{2}\omega \\ \sigma\circ\tau=\bar{\tau}: K \to \mathbb{Q}(\sqrt[3]{2}\omega^2) \subset \mathbb{C} \\ X+(f) \mapsto \sqrt[3]{2}\omega^2 \end{cases}$ $\bar{\omega}=\omega^2$

范与迹 norm, trace

$[L:K]=n$ $\sigma_i: L \to \mathbb{C}$ n 个 K-嵌入.

$\forall \alpha \in L$ 定义 $N_{L/K}(\alpha):=\prod_{i=1}^{n}\sigma_i(\alpha)$ norm 范

$T_{L/K}(\alpha):=\sum_{i=1}^{n}\sigma_i(\alpha)$ trace 迹.

Prop ① $N_{L/K}$ 保持乘法, $T_{L/K}$ 保加法

$N(\alpha\beta)=N(\alpha)N(\beta)$ $T(\alpha+\beta)=T(\alpha)+T(\beta)$

② 若 $\alpha \in K$ 则 $N_{L/K}(\alpha)=\alpha^n$, $T_{L/K}(\alpha)=n\alpha$

再加上以下 Th 可知 N, T 的像 $\subset K$ 从而

再加上以下 Th 可知 N, T 的像 $\subset K$ 以及

③ $N_{L/K}: L^* \to K^*$ 与 $T_{L/K}: L \to K$ 也是满射

Th $\alpha \in L$ 在 K 上的极小多项式 $f = x^m - c_1 x^{m-1} + \cdots + (-1)^m c_m \in K[x]$

$m = [K(\alpha):K]$ $(\Rightarrow m \mid n)$ 则有：

$N_{L/K}(\alpha) = c_m^{n/m}$, $T_{L/K}(\alpha) = \frac{n}{m} \cdot c_1 \in K$

证. f 有 m 个根 $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_m$

由定 $T_{K(\alpha)/K}(\alpha) = \alpha_1 + \alpha_2 + \cdots + \alpha_m = c_1$

$N_{K(\alpha)/K}(\alpha) = \alpha_1 \cdots \alpha_m = c_m$

$T_{L/K}(\alpha) = ?$
$N_{L/K}(\alpha) = ?$

K 的每个 K-嵌入 $\tau_i: K(\alpha) \longrightarrow \mathbb{C}$, $\alpha \mapsto \alpha_i$ 分别延拓成 $[L:K(\alpha)] = \frac{n}{m}$ 个

嵌入 $\sigma_{ij}: L \to \mathbb{C}$ $\left(1 \le j \le \frac{n}{m}\right)$

易验证 $\{\sigma_{ij} \mid 1 \le i \le m,\ 1 \le j \le \frac{n}{m}\}$ 两两相互不等，从而这是 L 到 $\mathbb{C}$ 的所有 K-嵌入.

$$N_{L/K}(\alpha) = \prod_{i=1}^{m} \prod_{j=1}^{\frac{n}{m}} \sigma_{ij}(\alpha) = \prod_i \prod_j \tau_i(\alpha) = \prod_i \prod_j \alpha_i = \prod_j (\alpha_1 \cdots \alpha_m)$$

$$= \prod_{j=1}^{n/m} c_m = c_m^{\frac{n}{m}}$$

把 Π 换 Σ $\rightsquigarrow$ $T_{L/K}(\alpha) = \frac{n}{m} c_1$ #

---

exer $\forall \alpha \in L$ 定义 $\varphi_\alpha: L \longrightarrow L$, $\beta \mapsto \alpha\beta$ ① K-线性

② 证明 $T_{L/K}(\alpha) = Tr(\varphi_\alpha)$

$N_{L/K}(\alpha) = \det(\varphi_\alpha)$

Th $L/M/K$ 数域扩张 $\forall \alpha \in L$ 有：

$$N_{L/K}(\alpha) = N_{M/K}(N_{L/M}(\alpha)) \text{ 及 } T_{L/K}(\alpha) = T_{M/K}(T_{L/M}(\alpha))$$

元素的判别式 discriminant.

$[L:K] = n$ $\sigma_i: L \hookrightarrow \mathbb{C}$ K-嵌入

$\alpha_1, \cdots, \alpha_n \in L$

定义 $d_{L/K}(\alpha_1, \cdots, \alpha_n) = \left[\det(\sigma_i(\alpha_j))\right]^2$

定义 $d_{L/K}(\alpha_1,\cdots,\alpha_n)=\left[\det(\sigma_i(\alpha_j))\right]^2$

称作 $\alpha_1,\cdots,\alpha_n$ 的 L/K 的判别式

Lem1 $d_{L/K}(\alpha_1,\cdots,\alpha_n)=\det(T_{L/K}(\alpha_i\alpha_j))\in K$

证 $A=(\sigma_i(\alpha_j))^t$

$$d_{L/K}=\det(A\cdot A^t)=\det\left(\begin{pmatrix}\sigma_1(\alpha_1)&\cdots&\sigma_n(\alpha_1)\\ &&\\ \sigma_1(\alpha_n)&&\sigma_n(\alpha_n)\end{pmatrix}\begin{pmatrix}\sigma_1(\alpha_1)&&\sigma_1(\alpha_n)\\ &&\\ \sigma_n(\alpha_1)&\cdots&\sigma_n(\alpha_n)\end{pmatrix}\right)$$

$$=\det\left(\sum_{k=1}^{n}\sigma_k(\alpha_i\alpha_j)\right)=\det\left(T_{L/K}(\alpha_i\alpha_j)\right)\qquad\#$$

Lem2 $d_{L/K}(\alpha_1,\cdots,\alpha_n)\neq 0\iff\alpha_1,\cdots,\alpha_n$ K-线性无关.

证：$\Rightarrow$. 若 α_n 是其他的 α_i 的 K-线性组合. A^t 的第 n 列是其他列的线性组合 $\det A^t=0=\det(A)$

$\Leftarrow$：若 $d_{L/K}(\alpha_1,\cdots,\alpha_n)=0=\det(T_{L/K}(\alpha_i\alpha_j))$

$(T_{L/K}(\alpha_i\alpha_j))$ 的 n 个行 $R_1,\cdots,R_n$ K-线性相关.

$\exists\ k_i\in K$ 不全0，$k_1R_1+\cdots+k_nR_n=0$

记 $\alpha=k_1\alpha_1+\cdots+k_n\alpha_n\neq 0$ $=\sum k_i\alpha_i$

第一方面 $T_{L/K}(\alpha\alpha_j)=0$ （右边其实是 $k_1R_1+\cdots+k_nR_n$ 中的第 j 分量）$=0$

$\alpha_1,\cdots,\alpha_n$ 是 L 的一组 K-线性基

于是 $T_{L/K}(\alpha\beta)=0\ \forall\beta\in L$，特别地取 $\beta=\alpha^{-1}$ $0=T(\alpha\alpha^{-1})=T(1)=n\cdot 1\neq 0$ #

Rk 此证明同时说明了 $L\times L\longrightarrow K$，$(\alpha,\beta)\mapsto T_{L/K}(\alpha\beta)$ 是非退化的对称双线性型

Rk. $\forall\alpha\in L$（不一定有 $L=K(\alpha)$）

记 $d_{L/K}(\alpha):=d_{L/K}(1,\alpha,\alpha^2,\cdots,\alpha^{n-1})$ 其中 $n=[L:K]$

记 $d_{L/K}(\alpha) := d_{L/K}(1, \alpha, \alpha^2, \cdots, \alpha^{n-1})$ 其中 $n = [L:K]$

称为 α 对于 L/K 的判别式

由 Lem2 知 $d_{L/K}(\alpha) \neq 0 \Leftrightarrow 1, \alpha, \cdots, \alpha^{n-1}$ K-线性无关 $\Leftrightarrow L = K(\alpha)$

Lem3 $L = K(\alpha)$ $n = [L:K]$ $f \in K[x]$ 为 α 的极小多项式.

设 $\alpha_1 = \alpha, \alpha_2, \alpha_3, \cdots, \alpha_n$

则 $d_{L/K}(\alpha) = d_{L/K}(1, \alpha, \cdots, \alpha^{n-1}) = \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s)^2 = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha))$

pf $\sigma_i(\alpha) = \alpha_i$

左边 $= \det(\sigma_i(\alpha^j))^2 = \det\left((\alpha_i^j)_{\substack{1 \le i \le n \\ 0 \le j \le n-1}}\right)^2$ Vandermonde 行列式

$$= \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s)^2$$

$(\alpha_r - \alpha_s)^2 = -(\alpha_s - \alpha_r)(\alpha_r - \alpha_s)$

$1 \le r < s \le n$ 的 (r, s) 共 $\frac{n(n-1)}{2}$ 对

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{r=1}^{n} \prod_{\substack{s=1 \\ s \neq r}}^{n} (\alpha_r - \alpha_s)$$

$f = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$

$f'(\alpha_r) = \prod_{\substack{s=1 \\ s \neq r}}^{n} (\alpha_r - \alpha_s)$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{r=1}^{n} f'(\alpha_r) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha))$$

($\alpha_r = \sigma_r(\alpha)$) #

数域中的单位根

K $G_m(K) = GL_1(K) = K^\times$

$n \in \mathbb{N}_{>1}$ $\quad \mu_n(K) = \{\alpha \in K^* \mid \alpha^n = 1\} \subset G_n(K)$

有限

$$\mu(K) = \bigcup_{n \geq 2} \mu_n(K) \subset G_m(K) = K^*$$

有限？ ($\Leftrightarrow$ 有限个根可解)

$K = \mathbb{Q}$ $\quad \mu(\mathbb{Q}) = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$

Th $\mu(K)$ 有限循环群 $\quad n = [K:\mathbb{Q}]$

Pf $\forall l$ 取 $\omega \in \mu_l(K)$ $\quad \omega$ 满足 $x^l - 1 = 0$

一根本多项式 $\quad f = x^m + c_1 x^{m-1} + \cdots + c_m \in \mathbb{Q}[x]$

$\in \mathbb{Z}[x]$ (下节课讲证)

ω 的共轭元 ω_i 也是 l 次单位根 $\quad \omega_i^l = 1$

$|\omega_i| \leq 1 \Rightarrow \quad |c_j| \leq \binom{m}{j} \leq \binom{n}{j}$

$c_j \in \mathbb{Z}$. $\Rightarrow f$ 取法只有有限个

$\Rightarrow \mu(K)$ 有限元群 #

例 $d > 0$ 无平方因子 $\quad K = \mathbb{Q}(\sqrt{d})$

① 实 $\quad K \subset \mathbb{R}$ $\quad \mu(\mathbb{Q}) \subset \mu(K) \subset \mu(\mathbb{R}) \Rightarrow \mu(K) = \{\pm 1\}$

② 虚, $K = \mathbb{Q}(\sqrt{-d})$ $\quad \zeta_n = e^{2\pi i/n} \in K$

$n = \prod p^m$

$K \supset \mathbb{Q}(\zeta_n) \supset \mathbb{Q}(\zeta_{p^m}) \supset \mathbb{Q}$

$2 = [K:\mathbb{Q}] \geq [\mathbb{Q}(\zeta_{p^m}):\mathbb{Q}] = \varphi(p^m) = p^{m-1}(p-1)$

不可约(分圆多项式)

$\Rightarrow \quad n = 6, 3, 2, 4.$

$\mu(\mathbb{Q}(\sqrt{-1})) = \{\pm 1, \pm i\}$

$\mu(\mathbb{Q}(\sqrt{-3})) = \{\pm 1, \pm\omega, \pm\omega^2\}$ $\quad \omega = -\frac{1}{2} - \frac{\sqrt{3}}{2} i$

$\mu(\mathbb{Q}(\sqrt{3})) = \{\pm 1, \pm w, \pm w^2\}$ $w = -2$ 2.

$d = 2$ 及 $d > 3$ 时 $\mu(\mathbb{Q}(\sqrt{d})) = \{\pm 1\}$