

近世代数之十

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

- ① 域扩张的概念
- ② 单扩张

狭义域扩张

- ① 狭义域扩张: $k \subseteq K$, 其中 K 为域, k 为其子域;
- ② 很多例子**不是**狭义域扩张, 只是域同态;
- ③ 回顾: 域之间的同态总是单的。

域扩张

定义

域扩张是指域的同态 $\theta: k \hookrightarrow K$, 简记为 K/k 。

警告：记号 K/k 很危险，不是商环！域扩张本质是同态 θ ，而此记号“真事隐”！

K/k 的理由： $k \simeq \theta(k) \subseteq K$, k “等同”于 $\theta(k)$ ，后者为 K 的子域。于是，域扩张 $\theta: k \hookrightarrow K$ “等同”于狭义域扩张 $\theta(k) \subseteq K$ 。

上述等同： $\lambda \in k$ “等同”于 $\theta(\lambda) \in \theta(k) \subseteq K$ 。

基本例子

例子

(1) 给定不可约多项式 $f(x) \in k[x]$, 考虑 $K = k[x]/(f(x))$, 令 $u = x + (f(x)) \in K$. 则有域扩张

$$k \hookrightarrow K, \quad \lambda \mapsto \lambda + (f(x))$$

右边的 λ 为常值多项式。

(2) 考虑 $k[x]$ 的分式域 $k(x)$, 称为有理函数域 (暂时, 它们还不是“函数”!). 则典范嵌入 $k[x] \hookrightarrow k(x)$ 诱导域扩张

$$k \hookrightarrow k(x), \quad \lambda \mapsto \frac{\lambda}{1}$$

域扩张的同构

比较两域扩张 $\theta: k \rightarrow K$ 以及 $\theta': k \rightarrow K'$?

定义

域扩张 θ 以及 θ' 之间的同构是指域同构 $\phi: K \rightarrow K'$ 使得 $\phi \circ \theta = \theta'$ 。

若 $\theta = \theta'$ ，则 θ 的自同构 $\phi: K \rightarrow K$ 又称为域扩张 K/k 的自同构。

于是， $\text{Aut}(K/k) \subseteq \text{Aut}(K)$ 为子群。

- ① 设 $R \subseteq S$ 为子环, $\alpha \in S$ 。记 $R[\alpha]$ 为包含 R 及 α 的最小子环
- ② 则有 $R[\alpha] = \{\sum r_i \alpha^i \mid \text{有限和 } r_i \in R\}$
- ③ 更一般地, 环的单同态 $\theta: R \hookrightarrow S$, 记 $R[\alpha] = \theta(R)[\alpha] \subseteq S$
- ④ 设 $k \subseteq K$ 为子域, $\alpha \in K$ 。记 $k(\alpha)$ 为包含 k 及 α 的最小子域
- ⑤ 则有 $k(\alpha) = \{(\sum r_i \alpha^i)(\sum r'_i \alpha^i)^{-1} \mid \text{所有可能}\}$
- ⑥ 域扩张 $\theta: k \hookrightarrow K$ 。同样 $k(\alpha) \subseteq K$ 以及 $k \hookrightarrow k(\alpha)$
- ⑦ 更多记号 $R[\alpha_1, \alpha_2], k(\alpha_1, \alpha_2)$

单扩张

定义

域扩张 K/k 称为单的, 若存在 $\alpha \in K$ 使得 $K = k(\alpha)$ 。

例子

- 1 添根构造 $k \hookrightarrow k[x]/(f(x))$
- 2 有理函数域 $k \subseteq k(x)$
- 3 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-1})$
- 4 $\mathbb{R} \subseteq \mathbb{C}$

定义

$\alpha \in K$ 在 k 上代数, 若存在非零 $f(x) \in k[x]$ 使得 $f(\alpha) = 0_K$ 。否则, 则称 α 为 k 上超越元。

- ① 限定词“ k 上”很关键。
- ② $\mathbb{C}/\mathbb{Q}$, 则 $\sqrt{2}, e^{\frac{2\pi i}{3}}$ 均为代数元
- ③ π (Lindermann 1882) 以及 e (Hermite 1873) 均为超越元
- ④ $k \subseteq k(x)$, 其中 x 在 k 上超越

最小多项式

定理

考虑 K/k 以及 $\alpha \in K$ 在 k 上代数。则唯一存在首一不可约多项式 $f(x) \in k[x]$ 满足:

- ① $f(\alpha) = 0$;
- ② 若 $g(x) \in k[x]$ 满足 $g(\alpha) = 0$, 则 $f(x) | g(x)$.

这样的多项式 $f(x)$ 称为 α 关于 k 的最小多项式。

证明: 考虑在 α 处的赋值同态

$$\text{ev}_\alpha: k[x] \longrightarrow K, \quad g(x) \mapsto g(\alpha)$$

考察其核。

练习

- ① 关于 $\mathbb{C}/\mathbb{Q}$, 计算 $\sqrt[3]{2}$, $\sqrt{2} + \sqrt{3}$ 的最小多项式
- ② 考虑域扩张 $\theta: k \rightarrow K$ 以及 $\theta': k \rightarrow K'$ 。若存在域扩张的同构 $\phi: K \rightarrow K'$ 满足 $\theta(\alpha) = \alpha'$ 。则 α 代数当且仅当 α' 代数, 且最小多项式一样。
- ③ 上例有助于体会条件“ $\phi \circ \theta = \theta'$ ”!

单扩张的结构定理

定理

设有单扩张 K/k 使得 $K = k(\alpha)$ 。

- ① 若 α 代数，最小多项式 $f(x)$ ，次数为 d 。则：

$\dim_k K = d < \infty$ ，基为 $1, \alpha, \dots, \alpha^{d-1}$ 且 $K = k[\alpha]$ ；有域扩张同构 $K \simeq k[x]/(f(x))$ 。

- ② 若 α 超越。则 $\dim_k K = \infty$ ，且 $k[\alpha] \neq K$ ；有域扩张同构 $K \simeq k(x)$ 。

本质上仅有两种单扩张！我们主要研究有限维域扩张！

例子

例子

考虑 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, 有 $\mathbb{Q}$ -基 $1, \sqrt[3]{2}, \sqrt[3]{4}$ 。

考虑 $\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}$, 有 $\mathbb{Q}$ -基 $1, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega^2$ 。

有域扩张同构

$$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \simeq \mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}$$

强调, 作为 $\mathbb{C}$ 的子域, $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{2}\omega)$!

还有 $\mathbb{Q}(\sqrt[3]{2}\omega^2)/\mathbb{Q}$ 呢?