近世代数之十二

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

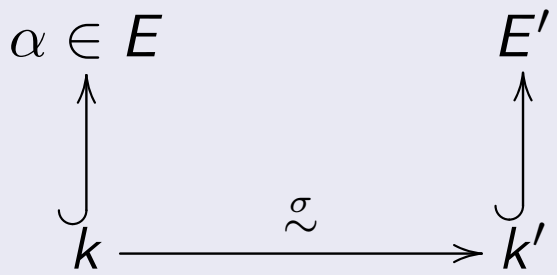
1. 域同态的延拓
2. 分裂域

延拓同态

问题：考虑E/k及E'/k', 域嵌入$\sigma\colon k \hookrightarrow k'$延拓至$E \hookrightarrow E'$?

引理 (关键引理)

考虑下图, α/k的最小多项式$f(x) \in k[x]$



1. 设$\beta \in \mathrm{Root}_E(\sigma(f))$, 则唯一存在$\sigma$的延拓

$$\tilde{\sigma}\colon k(\alpha) \xrightarrow{\sim} k'(\beta) \subseteq E', \quad \alpha \mapsto \beta$$

2. 恰好有$|\mathrm{Root}_E(\sigma(f))|$个这样的延拓。

分裂域

定义

多项式$f(x) \in k[x]$的**分裂域**是指域扩张K/k满足：

1. $f(x)$在K上分裂：$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$;
2. $E = k(\alpha_1, \cdots, \alpha_n)$.

例子

设$f(x) \in \mathbb{Q}[x]$。利用代数基本定理：

$$f(x) = (x - z_1) \cdots (x - z_n), \quad z_i \in \mathbb{C}.$$

则$E = \mathbb{Q}(z_1, \cdots, z_n)$为$f(x)$的分裂域。

更多例子

例子

考虑$x^2+x+\bar{1}\in\mathbb{F}_2[x]$的分裂域!

例子

1. 考虑$x^2+\bar{1}\in\mathbb{F}_3[x]$的分裂域!
2. 考虑$x^2-x-\bar{1}\in\mathbb{F}_3[x]$的分裂域!

分裂域的唯一性

定理

给定域同构$\sigma\colon k \xrightarrow{\sim} k'$，$f(x) \in k[x]$以及相应的$\sigma(f) \in k'[x]$。设$E/k$为$f(x)$ 的分裂域，E'/k'为$\sigma(f)$的分裂域。则σ可延拓指域同构

$$\delta\colon E \xrightarrow{\sim} E'.$$

这样的延拓至多有$\dim_k E = \dim_{k'} E'$个!

证明：对$\dim_k E$归纳，延拓至

$$k(\alpha_1) \xrightarrow{\sim} k'(\alpha_1'), \quad \alpha_1 \mapsto \alpha_1'$$

注意到$E/k(\alpha_1)$为$f(x) \in k(\alpha_1)[x]$的分裂域。

第一步延拓中：α_1'至多有$\dim_k k(\alpha_1)$个可能值!

分裂域的自同构

例子

考虑$x^3-2\in\mathbb{Q}[x]$，其分裂域$E=\mathbb{Q}(\omega,\sqrt[3]{2})$。

回顾$\mathrm{Aut}(E/\mathbb{Q})=\mathrm{Aut}(E)$。

利用延拓的方法具体给出其元素！

例子

考虑$\mathbb{F}_4=\mathbb{F}_2[x]/(x^2+x+\bar{1})$的自同构

群$\mathrm{Aut}(\mathbb{F}_4)=\mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2)$。

有重根的多项式

定义

非零多项式$f(x) \in k[x]$称为**有重根**，若存在E/k使得有$(x-a)^2 | f(x)$，某个$a \in E$。

更严格说，在某个**扩域**里有重根。

内蕴刻画：引入**形式微分** $f'(x) \in k[x]$。

引理

$f(x) \in k[x]$有重根当前仅当$\gcd_{k[x]}(f, f') = 1$。

可分多项式

定义

非零多项式$f(x) \in k[x]$称为可分的,若其（在$k[x]$中的）不可约因子均无重根。

WARNING: $f(x)$的可分性与域k有关! 严格说，域k上的多项式$f(x)$可分

引理

若$\mathrm{char}(k) = 0$，则任何多项式可分。

例子

考虑有理函数域$k = \mathbb{F}_q(t)$。则$x^p - t \in k[x]$不可约，但有重根。故，$x^p - t \in k[x]$不可分。

可分性与自同构

定理 (续唯一性定理)

给定域同构$\sigma\colon k \xrightarrow{\sim} k'$，$f(x) \in k[x]$以及相应的$\sigma(f) \in k'[x]$。设$E/k$为$f(x)$ 的分裂域，E'/k'为$\sigma(f)$的分裂域。则多项式$f(x) \in k[x]$可分当且仅当σ恰有$\dim_k E$个延拓。此时，我们有

$$|\mathrm{Aut}(E/k)| = \dim_k E.$$

证明：回到唯一性定理的证明，延拓!

展望

1. 若E/k是某个可分多项式$f(x) \in k[x]$的分裂域，则$\mathrm{Aut}(E/k)$记为$\mathrm{Gal}(E/k)$，称为E/k的**Galois 群**, 也称为**方程**$f(x)=0$的**Galois群**，又记为$\mathrm{Gal}_k(f)$。
2. Galois理论：联系$\mathrm{Gal}(E/k)$的子群与E的子域。
3. 基于Galois理论，证明Galois大定理：若$\mathrm{char}(k)=0$，$f(x)$根式可解当且仅当$\mathrm{Gal}_k(f)$为可解群。