抽象代数学

设$\mathbb{F}$是域，$f(x)\in\mathbb{F}[x]$，$\deg f(x)>0$，前面已构造了$f(x)$在$\mathbb{F}$上分裂域．现在使用代数性质来刻划它

定义 设$\mathbb{F}\subseteq K$是代数扩张，若任一不可约多项式$p(x)\in\mathbb{F}[x]$满足：有一个根在K中，则$p(x)$的所有根均在K中．则K称为$\mathbb{F}$的正规扩张．

性质：$K/\mathbb{F}$是正规扩张，则若给定$f(x)\in\mathbb{F}[x]$不可约若存在$\alpha\in K$，$x-\alpha\mid f(x)$（在$K[x]$中），则$f(x)$在$K[x]$中可裂（写成一次因子乘积）

定理 $K/\mathbb{F}$是有限正规扩张$\Leftrightarrow K$是$\mathbb{F}[x]$中某一个多项式在$\mathbb{F}$上的分裂域．

证明："$\Rightarrow$" 设$K=\mathbb{F}(\alpha_1,\cdots,\alpha_m)$ α_i在$\mathbb{F}$上极小多项式为$p_i(x)$，$i=1,\cdots,m$．因为K是$\mathbb{F}$的正规扩张，则K包含$p_i(x)$的所有根，$i=1,\cdots,m$．即$p(x)=\prod_{i=1}^{m}p_i(x)$的所有根．

$\Rightarrow K$包含$p(x)$在$\mathbb{F}$上的分裂域（它显然包含K）

"$\Leftarrow$" 设K是$f(x)$在$\mathbb{F}$上的分裂域．设$p(x)\in\mathbb{F}[x]$不可约，且存在$\alpha\in K$，使$p(\alpha)=0$．需证K包含$p(x)$所有根．

由上一讲记号，$Em_{\mathbb{F}}(K,\overline{K})=\{\sigma: K\to\overline{K} \mid \sigma|_{\mathbb{F}}=id\}$

因为 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$ $\alpha_i\in K$. $\sigma(f(x))=f(x)$.

$\sigma(\alpha_i)$ 仍是 $f(x)$ 的根. σ 是 $\{\alpha_1,\cdots,\alpha_n\}$ 的置换.

$\sigma(K)=\sigma(\mathbb{F}(\alpha_1,\cdots,\alpha_n))=\mathbb{F}(\sigma(\alpha_1),\cdots,\sigma(\alpha_n))=K$ 对于

$\forall\sigma\in Em_{\mathbb{F}}(K,\overline{K})$ 成立.

设 β 是 $p(x)$ 的另一根，$\beta\in\overline{K}$，L 是 $f(x)p(x)$ 在 $\mathbb{F}$ 上分裂域

$\exists\sigma: \mathbb{F}(\alpha)\xrightarrow{\sim}\mathbb{F}(\beta)$ 扩展为 L 的自同构. $K\subseteq L\subseteq\overline{K}$.

$h(\alpha)\longmapsto h(\beta)$

特别地，这给出了一个嵌入 $\tau: K\longrightarrow\overline{K}$，$\tau(\alpha)=\beta$. $\tau|_{\mathbb{F}}=id$

因为 $\tau(K)=K$，$\beta\in K$.

$\overline{\mathbb{F}}$ 是 $\mathbb{F}$ 的代数闭包

推论 设 $\mathbb{E}/\mathbb{F}$ 是有限正规扩张，~~$\mathbb{L}/\mathbb{E}$ 任意域扩张~~，则 ~~$\mathbb{L}$ 的任意 $\mathbb{F}$-自同构把 $\mathbb{E}$ 映到自身，或~~ $Em_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})=Aut_{\mathbb{F}}(\mathbb{E})$

例 $\mathbb{Q}(\sqrt{2})$ 是 $\mathbb{Q}$ 的正规扩张，它是 x^2-2 在 $\mathbb{Q}$ 上分裂域

$\mathbb{Q}(\sqrt[3]{2})$ 不是 $\mathbb{Q}$ 的正规扩张，它只含 x^3-2 的一个根.

定义 $\mathbb{Q}(\sqrt[3]{2})\xrightarrow{\sigma}\overline{\mathbb{Q}}$ （$\mathbb{Q}$ 的代数闭包） $\sigma|_{\mathbb{Q}}=id$

$a+b\sqrt[3]{2}+c\sqrt[3]{4}\longmapsto a+b\sqrt[3]{2}\omega+c\sqrt[3]{4}\omega^2$

$\sigma\in Em_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}),\overline{\mathbb{Q}})$，但 $\sigma\notin Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$.

推论 域$\mathbb{F}$的任一有限扩张必含包含在$\mathbb{F}$的某个正规扩张之中。

定义 设$\mathbb{F}\subseteq\mathbb{E}$代数扩张，$\overline{\mathbb{E}}$是$\mathbb{E}$的代数闭包，令

$$K=\bigcap_{\substack{\mathbb{E}\subseteq M\subseteq\overline{\mathbb{E}}\\ \mathbb{F}\subseteq M\text{ 正规扩张}}} M$$

K称为$\mathbb{E}$在$\mathbb{F}$上的正规闭包，即包含$\mathbb{E}$的$\mathbb{F}$的最小正规扩张.(验证：K是$\mathbb{F}$的正规扩张)

回到以上推论，$\mathbb{E}=\mathbb{F}(\alpha_1,\cdots,\alpha_n)$ 令$f_i(x)$是α_i在$\mathbb{F}$上的极小多项式，则$f(x)=f_1(x)\cdots f_n(x)$在$\mathbb{F}$上的分裂域即是$\mathbb{E}$在$\mathbb{F}$上的正规闭包.

例：$\mathbb{E}=\mathbb{Q}(\sqrt[4]{2})\supseteq\mathbb{Q}$ $\mathbb{E}$在$\mathbb{Q}$上的正规闭包是$\mathbb{Q}(\sqrt[4]{2},\xi)$

$\xi^4=1$， $\mathbb{E}$在$\mathbb{Q}(\sqrt{2})$上的正规闭包$=\mathbb{E}$.

例1. 设$\mathbb{F}$是有限域，$\mathbb{E}$是$\mathbb{F}$的有限扩张，则$\mathbb{E}$是可分且正规扩张.

证明：设$[\mathbb{E}:\mathbb{F}]=n$，则$|\mathbb{E}|=p^n$，其中$|\mathbb{F}|=p$，$p=q^l$

q为素数$(l\geq 1)$. $\forall a\in\mathbb{E}$， $a^{p^n}=a$，即a满足$x^{p^n}-x=0$

又$x^{p^n}-x=0$至多p^n个根，正好对应$\mathbb{E}$的p^n个元素，则$\mathbb{E}$是$\mathbb{F}$上多项式$x^{p^n}-x$的分裂域. $\forall a\in\mathbb{E}$，$a\notin\mathbb{F}$，设a在$\mathbb{F}$上不可约多项式为$p(x)$. 因为有限域是完全域，其上不可约

多项式可分，因此 α 是可分元. 从而 $\mathbb{E}/\mathbb{F}$ 是可分扩张.

例2. 设 $\mathbb{E}$ 是 $\mathbb{F}$ 上可分多项式 $f(x)$ 的分裂域，则 $\mathbb{E}/\mathbb{F}$ 是可分扩张.

设在 $\mathbb{E}[x]$ 中，$f(x)=c(x-\alpha_1)\cdots(x-\alpha_n)$, $c\in\mathbb{F}$, $\alpha_1,\cdots,\alpha_n\in\mathbb{E}$

则 $\mathbb{E}=\mathbb{F}(\alpha_1,\cdots,\alpha_n)$ α_i 均为可分元，由上讲定理

$\mathbb{E}/\mathbb{F}$ 可分. 或直接看嵌入个数，令 $u\in\mathbb{E}$, u 在 $\mathbb{F}$ 上极小多项式为 $p(x)$，$p(x)$ 全部互异根个数为 n_p

$$\underbrace{|\mathrm{Em}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|}_{=[\mathbb{E}:\mathbb{F}]}=\underbrace{|\mathrm{Em}_{\mathbb{F}(u)}(\mathbb{E},\overline{\mathbb{F}})|}_{=[\mathbb{E}:\mathbb{F}(u)]}\,|\mathrm{Em}_{\mathbb{F}}(\mathbb{F}(u),\overline{\mathbb{F}})|.$$

$\Rightarrow n_p=[\mathbb{F}(u):\mathbb{F}]\Rightarrow p(x)$ 可分.

作业 Page151, 2, 3, 4, 5, 6, 7, 8.

注：$\mathrm{Em}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})$ 记作 $\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})$，在上一讲，我们已经给出了递归刻划，回忆如下：

设 $\mathbb{E}/\mathbb{F}$ 有限扩张，$\mathbb{E}=\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_s)$，令 $\mathbb{L}=\mathbb{F}(\alpha_1,\cdots,\alpha_{s-1})$

则 $\mathbb{E}=\mathbb{L}(\alpha_s)$，考虑

$$\begin{aligned}\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}}) &\xrightarrow{\Phi} \mathrm{Hom}_{\mathbb{F}}(\mathbb{L},\overline{\mathbb{F}}).\\ \sigma &\longmapsto \sigma|_{\mathbb{L}}\end{aligned}$$

Φ 是一个满射：给定 $\tau\in\mathrm{Hom}_{\mathbb{F}}(\mathbb{L},\overline{\mathbb{F}})$，$x\in\mathbb{E}$，$x=\sum_{i=0}^{n}a_i\alpha_s^n$

$a_i\in\mathbb{L}$，定义 $\sigma_\tau:\mathbb{E}\to\overline{\mathbb{F}}$，$\sigma_\tau(x)=\sum_{i=0}^{n}\tau(a_i)\alpha_s^n\Rightarrow\sigma_\tau|_{\mathbb{L}}=\tau$.

令 $\Phi^{-1}(\tau)=\{\sigma\in\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})\,|\,\sigma|_{\mathbb{L}}=\tau\}$，$\forall\sigma\in\Phi^{-1}(\tau)$，

$\sigma(\alpha_s)$ 是 α_s 在 $\mathbb{L}[x]$ 中极小多项式 $P_{\mathbb{L}}(x)$ 的根 $\Rightarrow|\Phi^{-1}(\tau)|=$

$P_{\mathbb{L}}(x)$ 互异根个数 $n_{P_{\mathbb{L}}(x)}\Rightarrow|\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|=|\mathrm{Hom}_{\mathbb{F}}(\mathbb{L},\overline{\mathbb{F}})|\cdot n_{P_{\mathbb{L}}(x)}$

α_s和 L 是生成元，而 L 不动因此 σ 完全由α_s决定

$n_{P_{\mathbb{L}}(x)}=|\mathrm{Hom}_{\mathbb{L}}(\mathbb{E},\overline{\mathbb{F}})|=|\mathrm{Hom}_{\mathbb{L}}(\mathbb{L}(\alpha_s),\overline{\mathbb{F}})|$

因此 $|\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|=|\mathrm{Hom}_{\mathbb{F}}(\mathbb{L},\overline{\mathbb{F}})|\cdot|\mathrm{Hom}_{\mathbb{L}}(\mathbb{E},\overline{\mathbb{F}})|$

一般地，归纳可证：$\mathbb{F}\subseteq\mathbb{L}\subseteq\mathbb{E}$ 有限扩张 则

$$|\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|=|\mathrm{Hom}_{\mathbb{F}}(\mathbb{L},\overline{\mathbb{F}})|\cdot|\mathrm{Hom}_{\mathbb{L}}(\mathbb{E},\overline{\mathbb{F}})|.$$

应用这个到147页习题3.

设 $\beta\in\mathbb{F}(\alpha)$，则有 $\mathbb{F}\subseteq\mathbb{F}(\beta)\subseteq\mathbb{F}(\beta)(\alpha)=\mathbb{F}(\alpha)$，$\alpha$ 也是 $\mathbb{F}(\beta)$ 上可分元，

$|\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}(\alpha),\overline{\mathbb{F}})|=[\mathbb{F}(\alpha):\mathbb{F}]$（因为 α 可分）

$|\mathrm{Hom}_{\mathbb{F}(\beta)}(\mathbb{F}(\alpha),\overline{\mathbb{F}})|=[\mathbb{F}(\alpha):\mathbb{F}(\beta)]$（因为 α 可分）

$\Rightarrow|\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}(\beta),\overline{\mathbb{F}})|=[\mathbb{F}(\beta):\mathbb{F}]\Rightarrow\beta$ 可分.