抽象代数学

设$\mathbb{E}$是域$\mathbb{F}$的扩域，则$\mathbb{E}$是一个$\mathbb{F}$-向量空间. 若$\dim_{\mathbb{F}}\mathbb{E}=[\mathbb{E}:\mathbb{F}]<\infty$，则$\mathbb{E}$是$\mathbb{F}$的有限(维)扩张. 上一讲，已知：若$\mathbb{E}=\mathbb{F}(\alpha)$是$\mathbb{F}$的一个单扩张，则有两种情形：

(1) α是超越元$\Leftrightarrow[\mathbb{E}:\mathbb{F}]=+\infty$

(2) α是代数元$\Leftrightarrow\mathbb{E}=\mathbb{F}(\alpha)=\mathbb{F}[\alpha]$，$[\mathbb{E}:\mathbb{F}]=n=\alpha$在$\mathbb{F}[x]$中极小多项式的次数.

定义 设$\mathbb{E}$是$\mathbb{F}$的扩域，若$\forall\alpha\in\mathbb{E}$，$\alpha$是$\mathbb{F}$上代数元，则$\mathbb{E}$称为$\mathbb{F}$的代数扩张(algebraic extension)

性质1 有限扩张是代数扩张

证明：$\forall\alpha\in\mathbb{E}$，$[\mathbb{F}(\alpha):\mathbb{F}]\leqslant[\mathbb{E}:\mathbb{F}]<\infty$，$\Rightarrow\alpha$是一个代数元$\Rightarrow\mathbb{E}$是$\mathbb{F}$的代数扩张.

性质2. 设$\mathbb{E}$是$\mathbb{F}$的扩域，$\alpha,\beta\in\mathbb{E}$是$\mathbb{F}$上代数元，则$\alpha\pm\beta$，$\alpha\cdot\beta$，$\alpha\beta^{-1}(\beta\neq0)$也是$\mathbb{F}$上代数元.

证明：$\mathbb{F}\subseteq\mathbb{F}(\alpha)\subseteq\mathbb{F}(\alpha)(\beta)=\mathbb{F}(\alpha,\beta)$

α代数元(over $\mathbb{F}$) $\Rightarrow[\mathbb{F}(\alpha):\mathbb{F}]<\infty$

β是$\mathbb{F}$上代数元$\Rightarrow\beta$是$\mathbb{F}(\alpha)$上代数元$\Rightarrow[\mathbb{F}(\alpha)(\beta):\mathbb{F}(\alpha)]<\infty$

$\Rightarrow \mathbb{F}(\alpha,\beta)$中任一元均是$\mathbb{F}$上代数元.

定义 设$\mathbb{E}$是$\mathbb{F}$的扩域，令$K=\{\alpha\in\mathbb{E}\mid\alpha$是$\mathbb{F}$上代数元$\}$

($\mathbb{F}$在$\mathbb{E}$中的代数闭包, algebraic closure of $\mathbb{F}$ in $\mathbb{E}$).

性质3. K是$\mathbb{E}$的子域，是$\mathbb{F}$的一个代数扩张.

证明：由性质2即得.

例1. $\mathbb{F}=\mathbb{Q}$, $\mathbb{E}=\mathbb{C}$, $K=\mathbb{Q}^{alg}=\{\alpha\in\mathbb{C}\mid\alpha$在$\mathbb{Q}$上是代数元$\}$

$\mathbb{Q}^{alg}$作为$\mathbb{Q}$的代数扩张，但不是有限扩张，例如：

$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\cdots)\subseteq\mathbb{Q}^{alg}$ $\quad\mathbb{Q}(\sqrt[n+3]{2})\subseteq\mathbb{Q}^{alg}$ $\quad n\in\mathbb{N}$.

~~否则~~ $\quad\mathbb{Q}(\sqrt[n+3]{2}:\mathbb{Q})=n+3$.

例2. $\mathbb{F}$一个域 $\quad\mathbb{E}=\mathbb{F}(x)=\left\{\frac{f(x)}{g(x)}\,\middle|\,f(x),g(x)\in\mathbb{F}[x],\ g(x)\neq0\right\}$

$K=\mathbb{F}$，即$\mathbb{F}$在$\mathbb{E}$中代数闭包$=\mathbb{F}$.

定理 设$\mathbb{E}$是$\mathbb{F}$的扩域，则$\mathbb{E}$是$\mathbb{F}$的有限扩张$\Longleftrightarrow$

存在$\alpha_1,\cdots,\alpha_n\in\mathbb{E}$，均是$\mathbb{F}$上代数元，且$\mathbb{E}=\mathbb{F}(\alpha_1,\cdots,\alpha_n)$

证明："$\Leftarrow$"关于n作归纳，若$n=1$，α_1是$\mathbb{F}$上代数元，$\mathbb{E}=\mathbb{F}(\alpha_1)$

则$[\mathbb{E}:\mathbb{F}]<\infty$. 假设对于$n=k$，结论成立. 现在设

$\mathbb{E}=\mathbb{F}(\alpha_1,\cdots,\alpha_{k+1})$，$\alpha_1,\cdots,\alpha_{k+1}$均是$\mathbb{F}$上代数元，

$\mathbb{F}\subseteq\mathbb{F}(\alpha_1,\cdots,\alpha_k)\subseteq\mathbb{E}$. 由归纳假设,$[\mathbb{F}(\alpha_1,\cdots,\alpha_k):\mathbb{F}]<\infty$,

α_{k+1}是$\mathbb{F}$上代数元 $\Rightarrow$ 它是$\mathbb{F}(\alpha_1,\cdots,\alpha_k)$上代数元 $\Rightarrow$

$[\mathbb{E}:\mathbb{F}(\alpha_1,\cdots,\alpha_k)]<\infty \Rightarrow [\mathbb{E}:\mathbb{F}]<\infty$.

"$\Rightarrow$" 设$m=[\mathbb{E}:\mathbb{F}]$,关于$m$作归纳. $m=1$,$\mathbb{E}=\mathbb{F}$.

设$m\leqslant l$时,结论成立.

现设$\mathbb{E}$是$\mathbb{F}$的扩域,且$[\mathbb{E}:\mathbb{F}]=l+1$. $\forall\alpha_1\in\mathbb{E}$,$\alpha_1\notin\mathbb{F}$.

则α_1是$\mathbb{F}$上代数元,$1<[\mathbb{F}(\alpha_1):\mathbb{F}]<\infty$

$\Rightarrow[\mathbb{E}:\mathbb{F}(\alpha_1)]\leqslant l$,由归纳假设,存在$\alpha_2,\cdots,\alpha_n$.

$\mathbb{E}=\mathbb{F}(\alpha_1)(\alpha_2,\cdots,\alpha_n)$ $\quad$ $\alpha_2,\cdots,\alpha_n$是$\mathbb{F}(\alpha_1)$上代数元

$[\mathbb{F}(\alpha_i):\mathbb{F}]<[\mathbb{E}:\mathbb{F}]$ $i=2,\cdots,n\Rightarrow\alpha_2,\cdots,\alpha_n$是$\mathbb{F}$上代数元

以上定理给出了有限扩张的刻划:一系列单扩张的复合.

定理证明最后涉及到代数元在不同域上是否传递.

定理 设$\mathbb{F}\subseteq\mathbb{E}\subseteq K$三个域,$\mathbb{E}$在$\mathbb{F}$上是代数扩张.

设$\alpha\in K$,则α在$\mathbb{F}$上代数元$\Leftrightarrow\alpha$在$\mathbb{E}$上是代数元

证明:"$\Rightarrow$"显然,

"$\Leftarrow$"设α是$\mathbb{E}$上代数元,即存在$\overset{\text{不可约}}{f(x)}\in\mathbb{E}[x]$,$f(x)=\sum_{i=0}^{n}a_ix^i$

$a_i \in \mathbb{E}$ 使得 $f(\alpha)=0$，则 a_i 均是 $\mathbb{F}$ 上代数元，从而 $\mathbb{F}(a_0, a_1, \cdots, a_n)$ 是 $\mathbb{F}$ 上有限扩张。

$[\mathbb{F}(\alpha):\mathbb{F}] \leq [\mathbb{F}(a_0, a_1, \cdots, a_n)(\alpha):\mathbb{F}] = [\mathbb{F}(a_0, \cdots, a_n)(\alpha):\mathbb{F}(a_0, \cdots, a_n)]$

$[\mathbb{F}(a_0, a_1, \cdots, a_n):\mathbb{F}] < \infty \Rightarrow \alpha$ 是 $\mathbb{F}$ 上代数元。

推论 设 $\mathbb{F} \subseteq \mathbb{E} \subseteq K$ 三个域，K 是 $\mathbb{F}$ 的代数扩张 $\Leftrightarrow$ K 是 $\mathbb{E}$ 的代数扩张，$\mathbb{E}$ 是 $\mathbb{F}$ 的代数扩张。

证明："$\Rightarrow$" $\forall \alpha \in K$，$[\mathbb{F}(\alpha):\mathbb{F}] < \infty$，$\Rightarrow [\mathbb{E}(\alpha):\mathbb{E}] < \infty$，

$\forall \beta \in \mathbb{E}$，$[\mathbb{F}(\beta):\mathbb{F}] < \infty$（$\beta$ 看作 K 中元素）。

"$\Leftarrow$" $\forall \alpha \in K$，由以上引理。

定义 一个域 K 称为代数闭域，若不存在 $K \subsetneq \mathbb{E}$，$\mathbb{E}$ 是 K 的真代数扩张。例：$\mathbb{C}$ 是一个代数闭域（没有证明，这个结论也称为：代数基本定理）

命题 设 K 是一个域，如下陈述等价：

(i) K 是代数闭域。

(ii) $K[x]$ 中不可约多项式是一次的。

(iii) $\forall f(x) \in K[x]$，$f(x)$ 不是常数，则 $f(x)$ 在 K 中有根。

证明：(i) ⇒ (iii) 设 $f(x) \in K[x]$，$\deg f(x) > 0$ 则存在 K 的扩域 $\mathbb{E}$，使得 $\exists \alpha \in \mathbb{E}$，$f(\alpha) = 0 \Rightarrow \alpha$ 是 K 上代数元 $\Rightarrow$ $\mathbb{F}(\alpha)$ 是 K 的代数扩张，则 $K = \mathbb{F}(\alpha) \Rightarrow \alpha \in K$.

(iii) ⇒ (ii) 设 $f(x) \in K[x]$，且不可约，则存在 $\alpha \in K$，$f(\alpha) = 0$

$f(x) = (x-\alpha)t(x)$，$t(x) \in K[x]$，因为 $f(x)$ 不可约，$t(x) = t_0 \in K^*$

(ii) ⇒ (i) 设 $\mathbb{E}$ 是 K 的一个代数扩张，$\alpha \in \mathbb{E}$，则 α 在 K 上极小多项式为 $p(x) \in K[x]$，$p(x)$ 不可约 $\Rightarrow p(x) = c(x-\alpha)$，$c \in K^*$

$\Rightarrow \alpha \in K \Rightarrow \mathbb{E} = K$.

定义 设 K 是 $\mathbb{F}$ 的代数扩域且 K 是一个代数闭域，则 K 称为 $\mathbb{F}$ 的代数闭包 (algebraic closure)

例 $\mathbb{Q}^{alg}$ 是 $\mathbb{Q}$ 的代数闭包　　$\mathbb{Q} \subseteq \mathbb{Q}^{alg} \subseteq \mathbb{C}$

⇓推广

命题. 设 $\mathbb{F}$ 是一个域，K 是 $\mathbb{F}$ 的扩域，且 K 是代数闭域.
则 $\mathbb{F}$ 在 K 中代数闭包 = $\mathbb{F}$ 的代数闭包

证明：设 $\mathbb{E}$ 是 $\mathbb{F}$ 在 K 中代数闭包，则 $\mathbb{E}$ 是 $\mathbb{F}$ 的代数扩张

$\forall f(x) \in \mathbb{E}[x]$ $\deg f(x) > 0$ 因为 $\mathbb{E}[x] \subseteq K[x]$，由于 K 是代数闭域，存在 $\alpha \in K$，$f(\alpha) = 0$，α 在 $\mathbb{E}$ 上代数元 $\Rightarrow \alpha$ 是 $\mathbb{F}$ 上代数元 $\Rightarrow \alpha \in \mathbb{E}$. 即 $f(x)$ 在 $\mathbb{E}$ 中有一根.

由命题. $\mathbb{C}$的任意子域均有代数闭包.

定理 设$\mathbb{F}$是一个域，则$\mathbb{F}$的代数闭包存在. $\mathbb{F}$的任意两个代数闭包同构，确切地说，$\mathbb{F}\subseteq K_1$，$\mathbb{F}\subseteq K_2$，K_1, K_2代数闭包，则存在$\varphi: K_1 \xrightarrow{\sim} K_2$. $\varphi(a)=a \quad \forall a\in\mathbb{F}$.

例 设p是一个素数，$\mathbb{Q}(\sqrt{p}, \sqrt[3]{p}, \sqrt[4]{p}, \cdots)$是$\mathbb{Q}$上一个无限次代数扩张

证明: $\sqrt[n]{p}$满足$p(x)=x^n-p \Rightarrow$ ~~$\mathbb{Q}$~~ $\sqrt[n]{p}$是代数元

若$[\mathbb{Q}(\sqrt{p}, \sqrt[3]{p}, \cdots):\mathbb{Q}]=m<\infty$，则$[\mathbb{Q}(\sqrt[m+1]{p}):\mathbb{Q}]=m+1$

矛盾!

作业: Page 131-132, 2. 3, 4, 5, 6, 7, 11.