抽象代数学

回忆域论基本定理 (Kronecker, 1887)

设 $\mathbb{F}$ 是一个域，$f(x)\in\mathbb{F}[x]$，$\deg f(x)>0$. 则存在 $\mathbb{F}$ 的扩域 $\mathbb{E}$. 使得 $\exists\,\alpha\in\mathbb{E}$，$f(\alpha)=0$.

注：$\mathbb{E}$ 的选择不唯一. 通常，任取 $f(x)$ 的一个不可约因式 (在 $\mathbb{F}[x]$ 中不可约) $p(x)$，$\mathbb{E}=\dfrac{\mathbb{F}[x]}{(p(x))}$，这里 $\mathbb{E}$ 看作 $\mathbb{F}$ 的扩域，是通过等同 $\mathbb{F}$ 和 $\mathbb{E}$ 的子域

$$\{a+(p(x))\mid a\in\mathbb{F}\}$$

这一讲的目标：将 $\mathbb{E}$ 扩大使得 $f(x)$ 的所有零点落入扩域中. (这里默认存在 $\mathbb{F}$ 的扩域是代数闭域)

定义 设 $\mathbb{E}$ 是 $\mathbb{F}$ 的扩域. $f(x)\in\mathbb{F}[x]$，$\deg f(x)>0$

满足：(1) 在 $\mathbb{E}[x]$ 中，$f(x)=c(x-\alpha_1)\cdots(x-\alpha_n)$，

$c,\alpha_1,\cdots,\alpha_n\in\mathbb{E}$.

(2) $\mathbb{E}=\mathbb{F}(\alpha_1,\cdots,\alpha_n)$. 则 $\mathbb{E}$ 称为 $f(x)$ 在 $\mathbb{F}$ 上分裂域 (splitting field)

由定义，$\mathbb{E}$ 是包含 $f(x)$ 的全部根的 $\mathbb{F}$ 的最小扩域.

例 $\mathbb{Q}=\mathbb{F}$ $f(x)=x^2+1$，则 $\mathbb{Q}(i)=\{a+bi\mid a,b\in\mathbb{Q}\}$ 是 $f(x)$ 在 $\mathbb{Q}$ 上分裂域.

若取$\mathbb{F}=\mathbb{R}$，则$f(x)$在$\mathbb{R}$上分裂域$=\mathbb{R}(i)=\mathbb{C}$.

分裂域存在性.

定理 设$\mathbb{F}$是一个域，$f(x)\in\mathbb{F}[x]$，$\deg f(x)>0$. 则存在$f(x)$在$\mathbb{F}$上的分裂域$\mathbb{E}$.

证明：关于$\deg f(x)$作归纳. 若$\deg f(x)=1$，则$f(x)=c(x-\alpha)$，$c,\alpha\in\mathbb{F}$. $\mathbb{E}=\mathbb{F}$. 假设对于次数$<\deg f(x)$的任意多项式$g(x)$在任意域$\mathbb{L}$，$g(x)\in\mathbb{L}[x]$，存在$g(x)$在$\mathbb{L}$上分裂域. 对于$f(x)\in\mathbb{F}[x]$，由Kronecker定理，存在$\mathbb{F}$的扩域$\mathbb{E}_0$. 在$\mathbb{E}_0[x]$上，$f(x)=(x-\alpha_1)g(x)$，$\alpha_1\in\mathbb{E}_0$，$g(x)\in\mathbb{E}_0[x]$，因为$\deg g(x)<\deg f(x)$，由假设，存在域K包含$\mathbb{E}_0$和$g(x)$的所有零点，设为$\alpha_2,\cdots,\alpha_n$，则$\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)\subseteq K$是$f(x)$在$\mathbb{F}$上分裂域.

注：设$\mathbb{F}$, $f(x)$如上，若$\mathbb{F}\subseteq K$，K中含$f(x)$的所有零点$a_1,\cdots,a_n$，则$\mathbb{F}(a_1,\cdots,a_n)$即为$f(x)$在$\mathbb{F}$上分裂域.

例 $f(x)=x^4-x^2-2\in\mathbb{Q}[x]$

$f(x)=(x^2-2)(x^2+1)\Rightarrow\mathbb{Q}(\sqrt{2},i)$是$f(x)$在$\mathbb{Q}$上分裂域

例 $f(x)=x^2+x+2\in\mathbb{Z}_3[x]$

$f(x) = [x-(1+i)][x-(1-i)]$

$\Rightarrow \mathbb{Z}_3(i) = \{a+bi \mid a, b \in \mathbb{Z}_3\}$ 是 $f(x)$ 在 $\mathbb{Z}_3$ 上的一个分裂域

存在另一分裂域 $\mathbb{E} = \dfrac{\mathbb{Z}_3[x]}{(x^2+x+2)}$ 则 $\beta \triangleq x + (x^2+x+2)$

是 $f(x) = x^2+x+2 \in \mathbb{Z}_3[x]$ 的一个零点, 另一零点 $-(\beta+1)$

即在 $\mathbb{E}[x]$ 中, $f(x) = (x-\beta)(x+\beta+1)$ $\mathbb{E} = \mathbb{Z}_3(\beta)$

$\mathbb{E}$ 也是 $f(x)$ 在 $\mathbb{Z}_3$ 上一个分裂域.

显然 $\mathbb{E} \cong \mathbb{Z}_3(i)$. 且 $\phi|_{\mathbb{Z}_3} = id_{\mathbb{Z}_3}$

一般地, 有分裂域的唯一性(保持底域 $\mathbb{F}$ 不动).

定理. 设 $\phi: \mathbb{F} \to \mathbb{F}'$ 是域同构, $f(x) \in \mathbb{F}[x]$. $\mathbb{E}$ 是 $f(x)$ 在 $\mathbb{F}$ 上分裂域. $\mathbb{E}'$ 是 $\phi(f(x))$ 在 $\mathbb{F}'$ 上分裂域, 则存在域同构 $\tilde{\phi}: \mathbb{E} \to \mathbb{E}'$ 满足 $\tilde{\phi}|_{\mathbb{F}} = \phi$.

正如下图:

$$\begin{tikzcd}
\mathbb{E} \arrow[r, dashed, "\tilde{\phi}=?"] & \mathbb{E}' \\
\mathbb{F}, f(x) \arrow[u, "\subseteq"] \arrow[r, "\phi"] & \mathbb{F}', \phi(f(x)) \arrow[u, "\subseteq"']
\end{tikzcd}$$

证明: 关于 $\dim_{\mathbb{F}} \mathbb{E}$ 作归纳. (注记: 分裂域是有限扩张, 习题11, 143页) 若 $\dim_{\mathbb{F}} \mathbb{E} = 1$, 则 $\mathbb{E} = \mathbb{F}$, $\mathbb{E}' = \mathbb{F}'$, $\phi(f(x))$ 是一次多项式. $\tilde{\phi} = \phi$.

假设 $\mathbb{F}\subseteq K\subseteq \mathbb{E}$, $\mathbb{F}'\subseteq K'\subseteq \mathbb{E}'$ 是域扩张, $\phi_m: K\to K'$ 是域同构, $\phi_m|_{\mathbb{F}}=\phi$. $\dim_K \mathbb{E} < n=\dim_{\mathbb{F}}\mathbb{E}$, 则存在域同构 $\tilde{\phi}: \mathbb{E}\to\mathbb{E}'$ 使得 $\tilde{\phi}|_K=\phi_m$.

现在, 因为 $\dim_{\mathbb{F}}\mathbb{E}=n>1$, 存在 ~~有一个~~ $f(x)$的 次数 >1 的不可约 ~~多项式~~ 因子 $p(x)$, $\phi(p(x))\in\mathbb{F}'[x]$ 也是不可约的. 令 $\alpha=x+(p(x))\in\frac{\mathbb{F}[x]}{(p(x))}\subseteq\mathbb{E}$, $\beta=x+\phi(p(x))\in\frac{\mathbb{F}'[x]}{(\phi(p(x)))}\subseteq\mathbb{E}'$, $\mathbb{F}\xrightarrow{\phi}\mathbb{F}'$ 诱导了环同构 $\phi_{[x]}:\mathbb{F}[x]\to\mathbb{F}'[x]$, 进一步诱导了域同构 $\mathbb{F}(\alpha)\xrightarrow{\phi_m}\mathbb{F}'(\beta)$, 正如下图.

$$
\begin{tikzcd}
\mathbb{F}(\alpha) \arrow[r, "\sim"] \arrow[rrr, bend left, "\phi_m"] & \frac{\mathbb{F}[x]}{(p(x))} \arrow[r, "\tilde{\phi}_{[x]}"] & \frac{\mathbb{F}'[x]}{(\phi(p(x)))} \arrow[r] & \mathbb{F}'(\beta) \\
& \mathbb{F}[x] \arrow[u] \arrow[r, "\phi_{[x]}"] & \mathbb{F}'[x] \arrow[u] & \\
& \mathbb{F} \arrow[u] \arrow[r, "\phi"] \arrow[uul] & \mathbb{F}' \arrow[u] \arrow[uur] &
\end{tikzcd}
$$

由归纳假设, 存在 $\tilde{\phi}:\mathbb{E}\to\mathbb{E}'$, 使得下图交换

$$
\begin{tikzcd}
\mathbb{E} \arrow[r, "\exists\tilde{\phi}"] & \mathbb{E}' \\
K=\mathbb{F}(\alpha) \arrow[u, "\subseteq"] \arrow[r, "\phi_m"] & K'=\mathbb{F}'(\beta) \arrow[u, "\subseteq"'] \\
\mathbb{F} \arrow[u] \arrow[r, "\phi"] & \mathbb{F}' \arrow[u]
\end{tikzcd}
$$

推论 设$\mathbb{F}$是一个域，$f(x)\overset{\text{不可约}}{\in}\mathbb{F}[x]$，$\deg f(x)>0$，设$\mathbb{E}$是$f(x)$在$\mathbb{F}$上分裂域，若$\alpha,\beta$是$f(x)$在$\mathbb{E}$中两个根，则存在域同构$\tilde{\varphi}:\mathbb{E}\to\mathbb{E}$，$\tilde{\varphi}(\alpha)=\beta$，$\tilde{\varphi}|_{\mathbb{F}}=id$

是否存在同构使一个根 不能映为根?

证明：以上定理证明中，令$\mathbb{F}=\mathbb{F}'$，$\varphi=id_{\mathbb{F}}$。$f(x)$不可约 $f(x)=p(x)$.

$\mathbb{F}(\alpha)$，$\mathbb{F}(\beta)$ 正如上.

例. $f(x)=x^3-2\in\mathbb{Q}[x]$　$f(x)$在$\mathbb{C}$上有三个根：$\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$

其中$\omega=\dfrac{-1+\sqrt{-3}}{2}$　则$f(x)$在$\mathbb{Q}$上分裂域$=\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})=\mathbb{E}$

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{2},\sqrt{-3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "3"] & & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & \mathbb{Q}(\omega\sqrt[3]{2}) \arrow[d, dash, "3"] & \mathbb{Q}(\omega^2\sqrt[3]{2}) \arrow[dl, dash, "3"] & \mathbb{Q}(\sqrt{-3}) \arrow[dll, dash, "2"] \\
 & \mathbb{Q} & &
\end{tikzcd}$$

数字表示维数

例如

$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$
$=\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})=3$.

$\mathbb{E}$上自同构，保持$\mathbb{Q}$不动

$|Aut_{\mathbb{Q}}(\mathbb{E})|=[\mathbb{E}:\mathbb{Q}]=6$

保持$\mathbb{Q}(\sqrt{-3})$的同构.　$\tilde{\varphi}_1:\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})\longrightarrow\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})$

$$\sqrt[3]{2}\longmapsto\sqrt[3]{2}\,\omega.$$
$$\omega\longmapsto\omega.$$

$\tilde{\varphi}_1^3=id$；$\tilde{\varphi}_1^2(\sqrt[3]{2})=\omega^2\sqrt[3]{2}$.

保持~~$\sqrt{-3}$~~$\mathbb{Q}(\sqrt[3]{2})$的自同构　$\tilde{\varphi}_2(\omega)=\omega^2$　$\tilde{\varphi}_2(\omega\sqrt[3]{2})=\omega^2\sqrt[3]{2}$.

例 $\mathbb{F}=\mathbb{Z}_p$,（p为素数）$f(x)\in\mathbb{F}[x]$, n次不可约多项式 $n\geq 1$.

$\frac{\mathbb{F}[x]}{(f(x))}$ 是 $\mathbb{F}$ 的扩域，记作 $\mathbb{E}$. $[\mathbb{E}:\mathbb{F}]=\deg f(x)=n\geq 1$

则 $|\mathbb{E}|=p^n$，令 $\beta=x+(f(x))\in\mathbb{E}$. $f(\beta)=0$

$\mathbb{E}$是有限域，非零元成为一个 p^n-1 阶循环群. β是一个生成元. $\beta^{p^n}=\beta$, $\beta,\beta^p,\beta^{p^2},\cdots,\beta^{p^{n-1}}$ 均是 $f(x)=0$ 的根. $\deg f(x)=n$, 即 $\{\beta,\beta^p,\cdots,\beta^{p^{n-1}}\}$ 是 $f(x)$ 全部根.

即 $\mathbb{E}$ 是 $f(x)$ 在 $\mathbb{F}$ 上的分裂域. $\mathbb{E}=\mathbb{F}(\beta)$.

作业：Page 143, 1, 4, 7, 8, 9, 10, 11.