

抽象代数学

回忆域论基本定理 (Kronecker, 1887)

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

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

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

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

定义 设 E 是 F 的扩域, $f(x) \in F[x]$, $\deg f(x) > 0$ 满足: (1) 在 $E[x]$ 中, $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$, $c, \alpha_1, \dots, \alpha_n \in E$.

(2) $E = F(\alpha_1, \dots, \alpha_n)$. 则 E 称为 $f(x)$ 在 F 上分裂域

由定义, E 是包含 $f(x)$ 的全部根的 F 的最小扩域.

(splitting field)

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



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

分裂域存在性.

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

证明: 关于 $\deg f(x)$ 作归纳. 若 $\deg f(x) = 1$, 则 $f(x) = c(x - \alpha)$, $c, \alpha \in F$. $E = F$. 假设对于次数 $< \deg f(x)$ 的任意多项式 $g(x)$ 在任意域 L , $g(x) \in L[x]$, 存在 $g(x)$ 在 L 上分裂域. 对于 $f(x) \in F[x]$, 由 Kronecker 定理, 存在 F 的扩域 E_0 . 在 $E_0[x]$ 上, $f(x) = (x - \alpha_1)g(x)$, $\alpha_1 \in E_0$, $g(x) \in E_0[x]$. 因为 $\deg g(x) < \deg f(x)$, 由假设, 存在域 K 包含 E_0 和 $g(x)$ 的所有零点, 设为 $\alpha_2, \dots, \alpha_n$, 则 $F(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq K$ 是 $f(x)$ 在 F 上分裂域.

注: 设 $F, f(x)$ 如上, 若 $F \subseteq K$, K 中含 $f(x)$ 的所有零点 a_1, \dots, a_n , 则 $F(a_1, \dots, a_n)$ 即为 $f(x)$ 在 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 $\mathbb{E} = \frac{\mathbb{Z}_3[x]}{(x^2+x+2)}$ 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 $\phi|_{\mathbb{Z}_3} = \text{id}_{\mathbb{Z}_3}$

一般地, 有分裂域的唯一性 (保持底域 \mathbb{F} 不动).

定理 设 $\phi: \mathbb{F} \rightarrow \mathbb{F}'$ 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 $\tilde{\phi}: \mathbb{E} \rightarrow \mathbb{E}'$ 满足 $\tilde{\phi}|_{\mathbb{F}} = \phi$.

正如下图:

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{\tilde{\phi}=?} & \mathbb{E}' \\ \uparrow \subseteq & & \uparrow \subseteq \\ \mathbb{F}, f(x) & \xrightarrow{\phi} & \mathbb{F}', \phi(f(x)) \end{array}$$

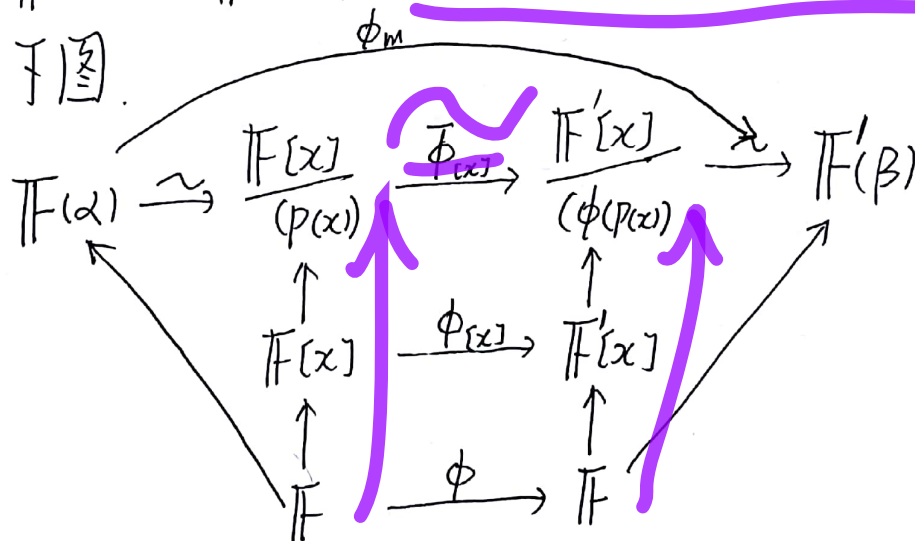
证明: 关于 $\dim_{\mathbb{F}} \mathbb{E}$ 作归纳. (注记: 分裂域是有限扩张, 习题 11, 143 页) 若 $\dim_{\mathbb{F}} \mathbb{E} = 1$, 则 $\mathbb{E} = \mathbb{F}$, $\mathbb{E}' = \mathbb{F}'$, $\phi(f(x))$ 是 \mathbb{F}' 上多项式. $\tilde{\phi} = \phi$.



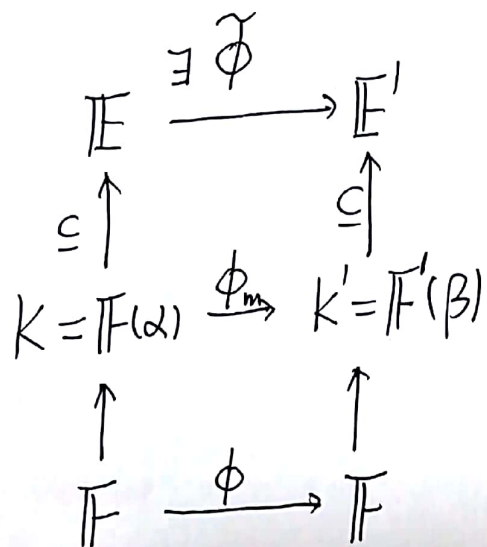
假设 $F \subseteq K \subseteq E$, $F' \subseteq K' \subseteq E'$ 是域扩张, $\phi_m: K \rightarrow K'$ 是域同构, $\phi_m|_F = \phi$. $\dim_K E < n = \dim_F E$, 则存在域同构 $\tilde{\phi}: E \rightarrow E'$ 使得 $\tilde{\phi}|_K = \phi_m$.

现在, 因为 $\dim_F E = n > 1$, 存在 ~~$f(x)$ 的~~ $f(x)$ 次数 > 1 的不可约多项式 $p(x)$, $\phi(p(x)) \in F'[x]$ 也是不可约的. 令 $\alpha = x + (p(x)) \in \frac{F[x]}{(p(x))} \subseteq E$, $\beta = x + \phi(p(x)) \in \frac{F'[x]}{(\phi(p(x)))} \subseteq E'$, $F \xrightarrow{\phi} F'$ 诱导了

环同构 $\phi_{[x]}: F[x] \rightarrow F'[x]$, 进一步诱导了域同构 $F(\alpha) \xrightarrow{\phi_m} F(\beta)$, 正如下图.



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

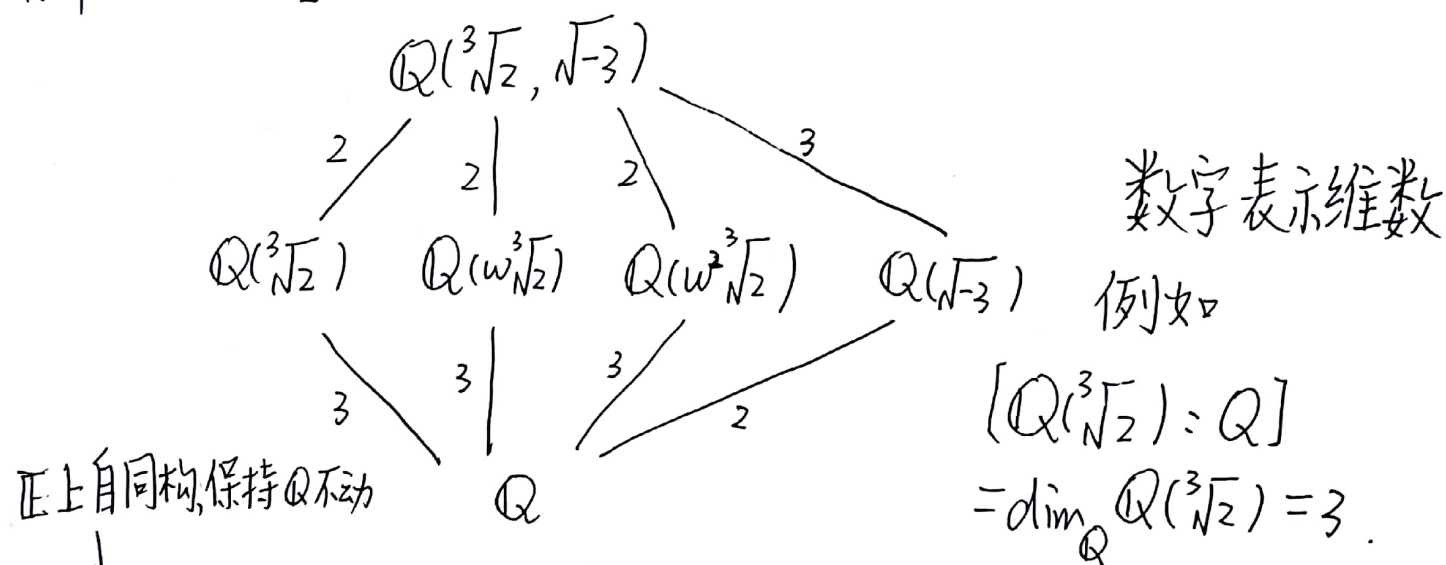


推论 设 \mathbb{F} 是一个域, $f(x) \in \mathbb{F}[x]$, $\deg f(x) > 0$, 设 \mathbb{E} 是 $f(x)$ 在 \mathbb{F} 上分裂域, 若 α, β 是 $f(x)$ 在 \mathbb{E} 中两个根, 则存在域同构 $\tilde{\phi}: \mathbb{E} \rightarrow \mathbb{E}$, $\tilde{\phi}(\alpha) = \beta$, $\tilde{\phi}|_{\mathbb{F}} = \text{id}$. 是否存在同构使一个根不能映为根?

证明: 以上定理证明中, 令 $\mathbb{F} = \mathbb{F}'$, $\phi = \text{id}_{\mathbb{F}}$. $f(x)$ 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 $\omega = \frac{-1 + \sqrt{-3}}{2}$ 则 $f(x)$ 在 \mathbb{Q} 上分裂域 $= \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) = \mathbb{E}$



保持 $\mathbb{Q}(\sqrt{-3})$ 的同构. $\tilde{\phi}_1: \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) \rightarrow \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$
 $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$
 $\omega \mapsto \omega$

$$\tilde{\phi}_1^3 = \text{id}, \quad \tilde{\phi}_1^2(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$$

保持 $\mathbb{Q}(\sqrt[3]{2})$ 的自同构 $\tilde{\phi}_2(\omega) = \omega^2 \quad \tilde{\phi}_2(\omega\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$



例 $F = \mathbb{Z}_p$, $f(x) \in F[x]$, n 次不可约多项式 $n \geq 1$.
 $\frac{F[x]}{(f(x))}$ ^(p 为素数) 是 F 的扩域, 记作 E , $[E:F] = \deg f(x) = n \geq 1$
 则 $|E| = p^n$, 令 $\beta = x + (f(x)) \in E$. $f(\beta) = 0$
 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. $\beta^{p^n} = \beta$, $\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{n-1}}$ 均是 $f(x) = 0$ 的根. $\deg f(x) = n$, 即 $\{\beta, \beta^p, \dots, \beta^{p^{n-1}}\}$ 是 $f(x)$ 全部根.
 即 E 是 F 的分裂域. $E = F(\beta)$.
 $f(x)$ 在

作业: Page 143, 1, 4, 7, 8, 9, 10, 11.

