

我们已经知道添加一元多项式环 $F[x]$ 中不可约元的一个根得到的单代数扩张的结构，

而根据第三章推论 9.1 可知，对于 $F[x]$ 中的 n 次多项式 $f(x)$ 来说，一定存在 F 的扩域 E ，使得 $f(x)$ 在 E 上有 n 个根，

如果我们将 $f(x)$ 的这 n 个根都添加到 F 中，

那么将得到 F 的一个扩域，这就是分裂域，

分裂域与 n 次代数方程的求解问题密切相关，

本节重点研究分裂域的存在性、唯一性及其与正规扩张的关系等问题，

定义 4.1 设 F 是域， $f(x)$ 是 $F[x]$ 中 $n(n \geq 1)$ 次多项式，

若 F 的扩域 E 满足下面两个条件：

(1) $f(x)$ 在 $E[x]$ 中能分解成一次因子的乘积，

即 $f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ ， α_i 属于 E ， $i = 1, 2, \dots, n$ ， a 属于 F ，

(2) $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ ，

则称 E 是 $f(x)$ 在 F 上的分裂域，

若 $f(x)$ 是域 F 上的 $n(n \geq 1)$ 次多项式，则由第三章推论 9.1 可知，

存在 F 的扩域 K ，使得 $f(x)$ 在 $K[x]$ 中能分解成一次因子的乘积

$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ ， a 属于 F ， α_i 属于 K ， $i = 1, 2, \dots, n$ ，

从而 $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ 是 $f(x)$ 在 F 上的分裂域，

定理 4.1 域 F 上任意一个 $n(n \geq 1)$ 次多项式 $f(x)$ 在 F 上都有分裂域，

定理 4.2 设 φ 是域 F 到域 $\bar{F}$ 的域同构, $f(x)$ 是 $F[x]$ 中的 $n(n \geq 1)$ 次多项式,

若 E 和 $\bar{E}$ 分别是 $f(x)$ 在 F 上和 $f^\varphi(x)$ 在 $\bar{F}$ 上的分裂域,

则存在 E 到 $\bar{E}$ 的域同构 ψ , 使得 $\psi|_F = \varphi$

证: 用数学归纳法证明,

当 $n=1$ 时, φ 为所求, 假设定理结论对 $n-1$ 次多项式成立,

下面证明定理结论对 n 次多项式 $f(x)$ 成立,

设 $p(x)$ 是 $f(x)$ 的一个不可约因子, 且属于 E 的 α 是 $p(x)$ 的一个根,

若令 β 是 $p^\varphi(x)$ 的一个根,

则由本章定理 2.2 可知, 存在 $F(\alpha)$ 到 $\bar{F}(\beta)$ 的域同构 τ , 使得 $\tau(\alpha) = \beta, \tau|_F = \varphi$,

令 $f(x) = (x - \alpha)g(x)$, 则 $g(x)$ 属于 $F(\alpha)[x]$, $f^\tau(x) = (x - \beta) \cdot g^\tau(x)$,

由于 $\deg g(x) < \deg f(x)$, 因此由归纳假设可知,

存在 $g(x)$ 在 $F(\alpha)$ 上的分裂域 E 到 $g^\tau(x)$ 在 $\bar{F}(\beta)$ 上的分裂域 $\bar{E}$ 的域同构 ψ ,

使得 $\psi|_{F(\alpha)} = \tau$, 进而, $\psi|_F = \tau|_F = \varphi$,

在上述定理中, 若令 $\bar{F} = F, \varphi = \text{id}_F$, 则有:

推论 4.1 设 F 是域,

则 $F[x]$ 中 n 次多项式 $f(x)$ 在 F 上的分裂域在同构意义下是唯一的 ($n \geq 1$)

例 4.1 设 $f(x) = x^4 - x^2 - 2$ 属于 $\mathbb{Q}[x]$,

分别求 $f(x)$ 在有理数域 $\mathbb{Q}$ 和在实数域 $\mathbb{R}$ 上的分裂域,

解: 因为 $f(x) = x^4 - x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i)$,

所以 $f(x)$ 在有理数域上的分裂域是 $\mathbb{Q}(\pm\sqrt{2}, \pm i) = \mathbb{Q}(\sqrt{2}, i)$

易知, 包含 $\mathbb{Q}$ 的扩张 $\mathbb{Q}(\sqrt{2}, i)$ 的本原元是 $\sqrt{2} + i$,

因此, $f(x)$ 在有理数域上的分裂域是 $\mathbb{Q}(\sqrt{2} + i)$,

$f(x)$ 在实数域上的分裂域是 $\mathbb{R}(\pm\sqrt{2}, \pm i)$, 而易知 $\mathbb{R}(\pm\sqrt{2}, \pm i) = \mathbb{R}(i) = \mathbb{C}$,

例 4.2 求多项式 x^5-1 在有理数域 Q 上的分裂域 ,

解: 设 $\alpha = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$, 则 $x^5-1 = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)$,

所以 x^5-1 在有理数域 Q 上的分裂域为 $Q(\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5) = Q(\alpha) = Q[\alpha]$,

例 4.3 设 $f(x) = x^2 + x + 2$ 属于 $Z_3[x]$, 试证明 $Z_3[i]$ 是 $f(x)$ 在 Z_3 上的分裂域

证: 由 $f(x) = (x-1+i)(x-1-i)$ 可知 , $f(x)$ 在 Z_3 上的分裂域是 $Z_3(1+i, 1-i)$,

因为 $1-(1\pm i) = \mp i$, 所以 $Z_3(1+i, 1-i) = Z_3(i)$,

又因为 i (i 是 x^2+1 的根) 是 Z_3 上的代数元 , 所以 $Z_3(i) = Z_3[i]$,

即 $Z_3[i]$ 是 $f(x)$ 在 Z_3 上的分裂域 ,

例 4.4 设 F 是域 , 且 $\text{Char } F = p > 0$,

试证明若 α 是 $F[x]$ 中多项式 x^p-t 的一个根 , 则 $F(\alpha)$ 是 x^p-t 在 F 上的分裂域 ,

证: 因为 $\alpha^p - t = 0$, 所以 $x^p - t = x^p - \alpha^p = (x-\alpha)^p$, 即 α 是 x^p-t 的 p 重根 ,

因此 , x^p-t 在 F 上的分裂域为 $F[\alpha]$,

下面来讨论与分裂域相关的正规扩张的性质 ,

定义 4.2 设包含 F 的 E 是域的有限扩张 ,

如果当 $F[x]$ 中的不可约元的一个根属于 E 时 , 该不可约元的其他根也属于 E ,

那么称包含 F 的 E 是正规扩张 ,

包含 F 的正规扩张 E 的概念也可以等价地定义为 :

E 中任意元素 α 在 F 上的极小多项式在 $E[x]$ 中能分解成一次因子的乘积 ,

定理 4.3 设包含 F 的 E 是域扩张，

则当且仅当 E 是 $F[x]$ 中某个多项式在 F 上的分裂域时，包含 F 的 E 是正规扩张，

证: (必要性) 若包含 F 的 E 是正规扩张，则包含 F 的 E 是有限扩张，

根据本章定理 3.3(2) 可知，

存在 F 上的代数元 $\alpha_1, \alpha_2, \dots, \alpha_n$ ，使得 $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ ，

设 $\alpha_1, \alpha_2, \dots, \alpha_n$ 在 F 上的极小多项式分别是 $f_1(x), f_2(x), \dots, f_n(x)$ ，

$f_1(x), f_2(x), \dots, f_n(x)$ 在 F 上的分裂域为 K ，

因为包含 F 的 E 是正规扩张，所以， $f_1(x), f_2(x), \dots, f_n(x)$ 的所有根都在 E 中，

从而， $f_1(x), f_2(x), \dots, f_n(x)$ 的所有根都在 E 中，那么 K 包含于 E

但是， $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ 包含于 K ，因而 $K = E$ ，

即 E 是多项式 $f_1(x)f_2(x)\cdots f_n(x)$ 在 F 上的分裂域，

(充分性) 假设 E 是 $F[x]$ 中多项式 $f(x)$ 在 F 上的分裂域，

则存在属于 E 的 $\alpha_1, \alpha_2, \dots, \alpha_n$ 使得 $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ ，

且 $f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$ ，

由本章定理 3.3(1) 可知，包含 F 的 E 是有限扩张

接下来我们仅需要指出：对于 $F[x]$ 中任一不可约元 $p(x)$ ，

若属于 E 的 α 是 $p(x)$ 的根，则 $p(x)$ 的任意一个根 β 属于 E ，

因为 α, β 都是 $p(x)$ 的根，因此由本章推论 2.1 可知，

存在 $F(\alpha)$ 到 $F(\beta)$ 的域同构 φ ，使得 $\varphi|_F = \text{id}_F$ ，且 $\varphi(\alpha) = \beta$ ，

再由 $f(x) \in F[x] \subseteq F(\alpha)[x], F(\beta)[x]$ 及定理 4.2 可知，

存在 $F(\alpha)(\alpha_1, \alpha_2, \dots, \alpha_n)$ 到 $F(\beta)(\alpha_1, \alpha_2, \dots, \alpha_n)$ 的同构 τ ，

从而， $|F(\alpha)(\alpha_1, \alpha_2, \dots, \alpha_n) : F| = |F(\beta)(\alpha_1, \alpha_2, \dots, \alpha_n) : F|$ ，

因为 α 属于 E ， $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ ，

所以 $F(\alpha)(\alpha_1, \alpha_2, \dots, \alpha_n) = E$ ， $F(\beta)(\alpha_1, \alpha_2, \dots, \alpha_n) = E(\beta)$ ，

进而 $|E : F| = |E(\beta) : F| = |E(\beta) : E| |E : F|$ ，

因此， $|E(\beta) : E| = 1$ ，即属于 E ，证毕，

推论 4.2 设 $K \supseteq E \supseteq F$ 是域的扩张，

若包含 F 的 K 是正规扩张，则包含 E 的 K 是正规扩张，

证： 因为包含 F 的 K 是正规扩张，所以包含 F 的 K 是有限扩张，

但是， E 在 F 上的向量空间是 K 在 F 上的向量空间的子空间，

因此，包含 F 的 E 是有限扩张，

根据定理 4.3 可知，

存在属于 $F[x]$ 的 $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ ，使得 $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ ，

因为 E 包含 F ，所以 $f(x)$ 属于 $E[x]$ ，

且 $K = F(\alpha_1, \alpha_2, \dots, \alpha_n) = E(\alpha_1, \alpha_2, \dots, \alpha_n)$ ，即 K 是 $f(x)$ 在 E 上的分裂域，

因此，包含 E 的 K 是正规扩张，

注意，在推论 4.2 中，包含 F 的扩张 E 不一定是正规扩张，

例如， $x^3 - 2$ 是 $\mathbb{Q}[x]$ 中的不可约元，

若设 K 是 $x^3 - 2$ 在 $\mathbb{Q}$ 上的分裂域，则包含 $\mathbb{Q}$ 的 K 是正规扩张，

但是包含 $\mathbb{Q}$ 的 $\mathbb{Q}(\sqrt[3]{2})$ 不是正规扩张(因为 $\sqrt[3]{2}\omega$ 不属于 $\mathbb{Q}(\sqrt[3]{2})$ ，其中 $\omega = \frac{-1 + \sqrt{3}i}{2}$)

下例说明，在扩张 $K \supseteq E \supseteq F$ 中，

即使包含 E 的 K 和包含 F 的 E 都是正规扩张，包含 F 的 K 也不一定是正规扩张，

例 4.5 因为 $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ ，所以包含 $\mathbb{Q}$ 的 $\mathbb{Q}(\sqrt{2})$ 是正规扩张，

又因为 $x^2 - \sqrt{2} = (x - \sqrt[4]{2})(x + \sqrt[4]{2})$ ，所以包含 $\mathbb{Q}(\sqrt{2})$ 的 $\mathbb{Q}(\sqrt[4]{2})$ 也是正规扩张，

但是 $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)$ ，

所以包含 $\mathbb{Q}$ 的 $\mathbb{Q}(\sqrt[4]{2})$ 不是正规扩张