

## 0.1 域的单扩张

### 定义 0.1 (环的特征)

设  $R$  为环. 如果存在最小的正整数  $n$ , 使得对所有的  $a \in R$ , 有  $na = 0$ , 则称  $n$  为环  $R$  的**特征**. 如果这样的正整数不存在, 则称环  $R$  的**特征**为 0. 环  $R$  的特征记作  $\text{Char } R$ .



**例题 0.1**  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  的特征都等于 0.

### 命题 0.1

设  $\mathbb{Z}_m$  是模  $m$  剩余类环, 则  $\text{Char } \mathbb{Z}_m = m, \text{Char } \mathbb{Z}_m[x] = m$ .



**证明** 对每个  $\bar{n} \in \mathbb{Z}_m$ , 有

$$m\bar{n} = \overline{mn} = \bar{0}.$$

而对于任何正整数  $k < m$ , 有

$$k\bar{1} = \bar{k} \neq \bar{0},$$

所以  $\text{Char } \mathbb{Z}_m = m$ . 类似地可以证明, 对于  $\mathbb{Z}_m$  上的一元多项式环  $\mathbb{Z}_m[x]$ , 也有  $\text{Char } \mathbb{Z}_m[x] = m$ .



### 定理 0.1

设  $R$  是有单位元  $e$  的环. 如果  $e$  关于加法的阶为无穷大, 那么  $R$  的特征等于 0. 如果  $e$  关于加法的阶等于  $n$ , 那么  $\text{Char } R = n$ .



**证明** 如果  $e$  关于加法的阶为无穷大, 那么不存在正整数  $n$ , 使得  $ne = 0$ . 所以由特征的定义知,  $R$  的特征等于 0.

如果  $e$  关于加法的阶等于正整数  $n$ , 则  $ne = 0$ . 而且  $n$  是满足这一性质的最小正整数. 因此, 对于任意的  $a \in R$ , 有

$$na = n(e \cdot a) = (ne) \cdot a = 0 \cdot a = 0.$$

于是  $R$  的特征等于  $n$ .



### 定理 0.2

整环的特征是 0 或者是一个素数.



**证明** 由定理 0.1, 只要证明, 如果整环  $R$  的单位元  $e$  关于加法的阶有限, 则它必为素数.

设  $e$  关于加法的阶为  $n$ . 显然  $n > 1$ . 假设  $n = p_1 p_2 \cdots p_s, 1 \leq p_i \leq n$  且  $p_i$  都是素数. 则

$$0 = ne = (p_1 p_2 \cdots p_s)e = (p_1 e) \cdot (p_2 e) \cdots (p_s e).$$

由  $R$  是整环和命题????可知存在  $i_0 \in [1, s] \cap \mathbb{N}$ , 使  $p_{i_0} e = 0$ . 因为  $n$  是使得  $ne = 0$  成立的最小正整数, 所以  $p_{i_0} = n$ . 因此  $n$  是素数.



### 定义 0.2 (素域/素体)

不包含任何平凡子体的体称为**素体**或**素域**, 即子体只有自身的体.



### 定理 0.3

设  $K$  是一个体, 则  $K$  的所有子体之交就是  $K$  包含的唯一素域 (素体), 也是  $K$  的子体.



**注** 这个定理表明: 每个体可以看成是某个素域 (素体) 的扩张.

**证明** 记  $K$  的所有子体之交为  $R$ , 则由命题 0.3 知  $R$  仍为  $K$  的子体. 设  $R_1$  是  $R$  的子体且  $R_1 \subseteq R$ , 则  $R_1$  也是  $K$  的子体, 从而由  $R$  的定义知  $R \subseteq R_1$ , 故  $R_1 = R$ . 故  $R$  是  $K$  的素域.

若  $K$  还包含一个素域  $R'$ , 则  $R'$  也是  $K$  的子体, 从而  $R' \supseteq R$ . 又因为  $R'$  是素域, 所以  $R' = R$ . 故唯一性得证.  $\square$

#### 定理 0.4

- (1)  $\mathbb{Z}_p, \mathbb{Q}$  都是素域 (素体).
- (2) 设  $\Pi$  是一个素域 (素体), 则  $\Pi \cong \mathbb{Z}_p$  ( $p$  为素数) 或  $\Pi \cong \mathbb{Q}$ . 进而素域 (素体) 一定是域.

**证明**

- (1)  $\mathbb{Z}_p$  对于加法是素数阶群. 由 Lagrange 定理知  $\mathbb{Z}_p$  无非平凡子群, 故  $\mathbb{Z}_p$  无非平凡子体, 因而  $\mathbb{Z}_p$  是素域 (素体).

若  $F$  为域  $\mathbb{Q}$  的子体, 于是  $1 \in F$ , 从而  $\mathbb{Z} \subset F$ , 由命题 0.3 知  $\mathbb{Z}$  的分式域是  $\mathbb{Q}$ . 因而由定理 0.3 知  $\mathbb{Q} \subseteq F$ , 故  $F = \mathbb{Q}$ , 所以  $\mathbb{Q}$  为素域 (素体).

- (2) 设  $e$  为  $\Pi$  的么元, 于是易知  $\mathbb{Z}e = \{ne | n \in \mathbb{Z}\}$  为  $\Pi$  的可交换子环且有  $\mathbb{Z}$  到  $\mathbb{Z}e$  的同态  $\pi : \pi(n) = ne (n \in \mathbb{Z})$ . 于是由环的同态基本定理知

$$\mathbb{Z}e \cong \mathbb{Z} / \ker \pi.$$

由于  $\mathbb{Z}$  为 Euclid 环, 进而也是主理想整环, 故有  $p \in \mathbb{Z}$ , 使得  $\ker \pi = \langle p \rangle$ . 因为  $\Pi$  为体, 故由命题 0.3 知  $\mathbb{Z}e$  为交换整环, 即  $\mathbb{Z} / \ker \pi = \mathbb{Z} / \langle p \rangle$  也是交换整环. 因此由定理 0.3 知  $\langle p \rangle$  为素理想, 再由定理 0.3 知  $p$  为  $\mathbb{Z}$  中的素元素, 进而  $p$  只能为素数或零.

当  $p$  为素数时, 由命题 0.3 知  $\mathbb{Z}e \cong \mathbb{Z} / \langle p \rangle = \mathbb{Z} / p\mathbb{Z} = \mathbb{Z}_p$  为域, 从而  $\mathbb{Z}e$  是  $\Pi$  的子体. 又  $\Pi$  无非平凡子体, 故  $\Pi = \mathbb{Z}e \cong \mathbb{Z}_p$ .

当  $p = 0$  时, 有  $\mathbb{Z}e \cong \mathbb{Z} / \langle 0 \rangle = \mathbb{Z}$ . 由命题 0.3 知  $\mathbb{Z}$  的分式域是  $\mathbb{Q}$ . 记  $\mathbb{Z}e$  的分式域为  $F$ , 则由推论 0.3 知  $F \cong \mathbb{Q}$ . 又  $\mathbb{Z}e \subset \Pi$ , 故由定理 0.3 知  $F \subseteq \Pi$ . 再由  $\Pi$  是素域知  $\Pi = F \cong \mathbb{Q}$ .  $\square$

#### 定义 0.3 (体的特征)

若体  $K$  包含的素域与  $\mathbb{Q}$  同构, 则称  $K$  的**特征**为零. 若体  $K$  包含的素域与  $\mathbb{Z}_p$  ( $p$  为素数) 同构, 则称  $K$  的**特征**为  $p$ . 记  $K$  的特征为  $\text{ch } K$  或  $\text{Char } K$ .

**注** 由定理 0.3 知  $K$  只包含唯一的素域, 又由定理 0.4 知  $K$  的素域只可能同构于  $\mathbb{Q}$  或  $\mathbb{Z}_p$  ( $p$  为素数), 因此  $\text{ch } K$  只能是 0 或素数.

#### 定理 0.5

设  $K$  是一个体,  $p$  为素数, 则

- (1)  $\text{ch } K = p \iff pa = 0, \forall a \in K$ ;
- (2)  $\text{ch } K = 0 \iff na \neq 0, \forall n \in \mathbb{N}, a \in K^* = K \setminus \{0\}$ .

**证明** 记  $K$  的么元为  $e$ ,  $K$  中素域为  $\Pi$ . 显然  $\mathbb{Z}e = \{ne | n \in \mathbb{Z}\}$  为  $\Pi$  的可交换子环且有  $\mathbb{Z}$  到  $\mathbb{Z}e$  的同态  $\pi : \pi(n) = ne (n \in \mathbb{Z})$ . 于是由环的同态基本定理知

$$\mathbb{Z}e \cong \mathbb{Z} / \ker \pi. \quad (1)$$

由于  $\mathbb{Z}$  为 Euclid 环, 进而也是主理想整环, 故有  $p' \in \mathbb{Z}$ , 使得  $\ker \pi = \langle p' \rangle$ . 因为  $\Pi$  为体, 故由命题 0.3 知  $\mathbb{Z}e$  为交换整环, 即  $\mathbb{Z} / \ker \pi = \mathbb{Z} / \langle p' \rangle$  也是交换整环. 因此由定理 0.3 知  $\langle p' \rangle$  为素理想, 再由定理 0.3 知  $p'$  为  $\mathbb{Z}$  中的素元素, 进而  $p'$  只能为素数或零.

- (1) 若  $\text{ch } K = p$ , 即  $\Pi \cong \mathbb{Z}_p$ , 又因为在  $\mathbb{Z}_p$  中有  $p \cdot 1 = 0$ , 所以在  $\Pi$  中有  $pe = 0$ , 因而  $pa = pe \cdot a = 0, \forall a \in K$ .

反之, 若  $pa = 0, \forall a \in K$ , 则  $pe = 0$ . 从而对  $\forall z \in \mathbb{Z}$ , 有  $\pi(pz) = pze = z \cdot pe = 0$ . 故  $\langle p \rangle = p\mathbb{Z} \subseteq \ker \pi$ . 若

$p' \neq p$ , 则  $\langle p \rangle \not\subseteq \langle p' \rangle = \ker \pi$  矛盾! 因此  $p = p'$ , 即

$$\ker \pi = \langle p \rangle.$$

又因为  $p$  为素数, 所以由(1)式及命题??知  $\mathbb{Z}e \cong \mathbb{Z}/\langle p \rangle = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$  为域, 从而  $\mathbb{Z}e$  是  $\Pi$  的子域, 也是子体. 又  $\Pi$  无非平凡子体, 故  $\Pi = \mathbb{Z}e \cong \mathbb{Z}_p$ , 即  $\text{ch } K = p$ .

- (2) 若  $\text{ch } K = 0$ , 即  $\Pi \cong \mathbb{Q}$ . 记  $\mathbb{Z}e$  的分式域为  $F$ , 又  $\mathbb{Z}e \subset \Pi$ , 故由定理??知  $F \subseteq \Pi$ . 再由  $\Pi$  是素域知  $\Pi = F \cong \mathbb{Q}$ . 于是由推论??知  $\mathbb{Z} \cong \mathbb{Z}e$ . 因此由  $n \cdot 1 \neq 0, \forall n \in \mathbb{N}$  知  $ne \neq 0, \forall n \in \mathbb{N}$ . 又由命题????知  $K$  是整环, 故  $\forall a \in K^*, na = ne \cdot a \neq 0$ .

反之,  $\forall n \in \mathbb{N}, a \in K^*$  有  $na \neq 0$ . 特别地,  $\pi(n) = ne \neq 0, \pi(-n) = -ne \neq 0$ . 于是  $\ker \pi = \{0\} = \langle 0 \rangle$ . 故由(1)式知  $\mathbb{Z}e \cong \mathbb{Z}/\langle 0 \rangle = \mathbb{Z}$ , 即  $\text{ch } K = 0$ .

□

### 推论 0.1

数域的特征都是零.

♡

证明

□

### 定义 0.4

设  $K$  为域  $F$  的扩域,  $S$  为  $K$  的子集.  $K$  中所有包含  $F \cup S$  的子域之交, 称为由  $F$  与  $S$  生成的子域, 也称为  $F$  上添加  $S$  所得的域, 亦称为  $S$  在  $F$  上生成的域, 记为  $F(S)$ .

显然有  $K = F(K)$ , 因而讨论域的扩张实质上是讨论在域上添加一个集合所得的域. 为清楚起见, 以  $F[S]$  表示下列形式的一切有限和:

$$\sum_{i_1, i_2, \dots, i_n \geq 0} \alpha_{i_1 i_2 \dots i_n} a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n},$$

其中  $\alpha_j \in S, j = 1, 2, \dots, n, \alpha_{i_1 i_2 \dots i_n} \in F$  所构成的集合, 显然  $F[S]$  是  $K$  的子环, 它的分式域恰为  $F(S)$ . 特别当  $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$  为有限集时, 分别记

$$F[S] = F[\alpha_1, \alpha_2, \dots, \alpha_n], \quad F(S) = F(\alpha_1, \alpha_2, \dots, \alpha_n).$$

♣

### 定理 0.6

设  $K$  为域  $F$  的扩域,  $S \subseteq K$ , 则

- (1)  $F(S) = \bigcup_{S' \subseteq S} F(S')$ , 此处  $S'$  取遍  $S$  的所有有限子集;  
 (2) 若  $S = S_1 \cup S_2$ , 则  $F(S) = F(S_1)(S_2)$ .

♡

证明

- (1) 显然  $F(S') \subseteq F(S)$ , 因而

$$\bigcup_{S' \subseteq S} F(S') \subseteq F(S).$$

反之,  $\forall a \in F(S)$  有  $a = \frac{f}{g}, f, g \in F[S]$ , 由于  $f, g$  的表达式均为有限和的形式, 因而存在  $S$  的有限子集  $S'_0$ , 使  $f, g \in F[S'_0]$ . 于是  $a = \frac{f}{g} \in F[S'_0] \subseteq \bigcup_{S' \subseteq S} F(S')$ , 故结论 (1) 成立.

- (2) 由于  $F(S_1 \cup S_2)$  是  $K$  中包含  $F, S_1 \cup S_2$  的最小子域, 而  $F, S_1, S_2 \subseteq F(S_1)(S_2)$ , 故有

$$F(S_1 \cup S_2) \subseteq F(S_1)(S_2).$$

反之,  $F(S_1)(S_2)$  是包含  $F(S_1), S_2$  的最小子域, 而

$$F(S_1) \subseteq F(S_1 \cup S_2), \quad S_2 \subseteq F(S_1 \cup S_2),$$

故  $F(S_1)(S_2) \subseteq F(S_1 \cup S_2)$ , 因而结论 (2) 成立. □

### 推论 0.2

$$F(\alpha_1, \alpha_2, \dots, \alpha_n) = F(\alpha_1)(\alpha_2) \cdots (\alpha_n).$$

从定理 3.1.3 及推论 3.1.2 可知在一个域上添加一个有限集合  $S$  可转化成添加有限个元素的问题, 而添加有限个元素的问题, 可转化成添加一个元素的问题.

### 定义 0.5

设  $K$  是  $F$  的扩域. 若  $\exists \alpha \in K$ , 使得

$$K = F(\alpha),$$

称  $K$  是  $F$  的单扩域.

若  $\alpha$  是  $F$  上的代数元, 称  $K = F(\alpha)$  为  $F$  的单代数扩张.

若  $\alpha$  是  $F$  上的超越元, 称  $K = F(\alpha)$  为  $F$  的单超越扩张.

从定理 2.8.5 可知当  $\alpha$  为超越元时,  $F(\alpha)$  同构于  $F$  上一元多项式环  $F[x]$  的分式域  $F(x)$ . 由 2.1 节知此分式域存在且唯一, 故一个域  $F$  的单超越扩张存在且唯一, 因而  $F(\alpha)$  就是  $F$  上的一元多项式环的分式域. 今后将侧重讨论单代数扩张的情形.

同样从定理 2.8.5 可知当  $\alpha$  为代数元时,

$$F(\alpha) \cong F[x]/\langle p(x) \rangle,$$

其中,  $p(x)$  是  $F[x]$  中的不可约多项式且满足  $p(\alpha) = 0$ . 此时  $F[\alpha]$  是域, 因而有  $F[\alpha] = F(\alpha)$ . 由于  $F$  是域, 故可知  $p(x)$  与一个首一多项式相伴, 因而不妨设  $p(x)$  为首一多项式且这样的  $p(x)$  由  $\alpha$  唯一确定.

### 定义 0.6

设  $K$  是  $F$  的扩域,  $\alpha \in K$ ,  $\alpha$  是  $F$  上的代数元.  $F[x]$  中以  $\alpha$  为根的不可约首一多项式称为  $\alpha$  在  $F$  上的不可约多项式, 记为  $\text{Irr}(\alpha, F)$ . 它的次数称为  $\alpha$  在  $F$  上的次数, 记为  $\deg(\alpha, F)$ , 即  $\deg(\alpha, F) = \deg(\text{Irr}(\alpha, F))$ .

由 2.2 节与 2.8 节的讨论知若  $\alpha$  是  $F$  上的代数元, 则

$$\langle \text{Irr}(\alpha, F) \rangle = \{f(x) \in F[x] \mid f(\alpha) = 0\} = \{f(x) \in F[x] \mid \text{Irr}(\alpha, F) \mid f(x)\}.$$

### 定理 0.7

设  $F(\alpha)$  是  $F$  的单代数扩张, 又  $\deg(\alpha, F) = n$ , 则  $F(\alpha)$  是  $F$  上的  $n$  维线性空间且  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  是一组基<sup>①</sup>.

**证明** 根据 1.6 节中域  $F$  上的线性空间的定义, 可直接验证  $F(\alpha)$  是  $F$  上的线性空间. 回忆 2.2 节曾指出在  $F[x]$  与  $F[\alpha] = F(\alpha)$  之间有满同态  $\eta$  满足

$$\eta(f(x)) = f(\alpha), \quad \forall f(x) \in F[x],$$

而

$$\ker \eta = \langle \text{Irr}(\alpha, F) \rangle.$$

由  $\deg(\alpha, F) = n$ , 故  $\exists q(x), r(x) \in F[x]$ , 使得

$$f(x) = q(x)\text{Irr}(\alpha, F) + r(x), \quad \deg r(x) < \deg(\alpha, F)$$

(注意  $\deg 0 = -\infty$ ), 因而  $f(\alpha) = r(\alpha)$ . 于是  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  生成  $F(\alpha)$ . 又若  $\deg s(x) < \deg(\alpha, F)$ , 而  $s(\alpha) = 0$ , 则  $\eta(s(x)) = 0$ . 故  $\text{Irr}(\alpha, F) \mid s(x)$ , 因而  $s(x) = 0$ , 即  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  线性无关, 故  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  是  $F(\alpha)$  的一组基, 故  $F(\alpha)$  的维数为  $n$ .

□

**定义 0.7**

设  $K_1, K_2$  都是域  $F$  的扩域. 若有  $K_1$  到  $K_2$  上的同构  $\eta$ , 使  $\eta|_F = \text{id}_F$ , 则称  $K_1$  与  $K_2$  是  $F$  的等价扩张,  $\eta$  称为  $F$  同构. 特别地, 若  $K_1 = K_2$ , 则称  $\eta$  为  $F$  自同构.

♣

**例题 0.2**  $F(\alpha), F(\beta)$  都是  $F$  的单超越扩张, 则  $F(\alpha)$  与  $F(\beta)$  是  $F$  的等价扩张. 这时它们与一元多项式环  $F[x]$  的分式域都是  $F$  的等价扩张.

**例题 0.3**  $F(\alpha), F(\beta)$  都是  $F$  的单代数扩张且  $\text{Irr}(\alpha, F) = \text{Irr}(\beta, F)$ , 则  $F(\alpha)$  与  $F(\beta)$  是  $F$  的等价扩张.

事实上, 记  $p(x) = \text{Irr}(\alpha, F) = \text{Irr}(\beta, F)$ , 则  $F(\alpha), F(\beta)$  与  $F[x]/\langle p(x) \rangle$  都是  $F$  的等价扩张, 故  $F(\alpha)$  与  $F(\beta)$  是  $F$  的等价扩张.

由此例知对  $F[x]$  中的任一不可约多项式  $p(x)$  在等价定义下存在唯一单代数扩张. 事实上,  $F[x]/\langle p(x) \rangle = F(x + \langle p(x) \rangle)$ . 令  $\alpha = x + \langle p(x) \rangle$ , 则  $\text{Irr}(\alpha, F)$  与  $p(x)$  相伴.

但是, 对  $F$  的两个等价的单代数扩张  $F(\alpha), F(\beta)$ , 不一定有  $\text{Irr}(\alpha, F) = \text{Irr}(\beta, F)$ .

**例题 0.4** 设  $F = \mathbb{R}, \alpha = \sqrt{-1}, \beta = 1 + \sqrt{-1}$ . 显然  $F(\alpha) = \mathbb{C}, F(\beta) = \mathbb{C}$ , 故  $F(\alpha)$  与  $F(\beta)$  是  $F$  的等价扩张, 但  $\text{Irr}(\alpha, F) = x^2 + 1, \text{Irr}(\beta, F) = x^2 - 2x + 2$ , 故  $\text{Irr}(\alpha, F) \neq \text{Irr}(\beta, F)$ .

**例题 0.5** 定义  $\mathbb{C}$  到  $\mathbb{C}$  的映射  $\tau$ :

$$\tau(a + b\sqrt{-1}) = a - b\sqrt{-1}, \quad \forall a, b \in \mathbb{R},$$

则容易验证  $\tau$  是  $\mathbb{C}$  的  $\mathbb{R}$  自同构.

比等价扩张更特殊一点的概念是共轭.

**定义 0.8**

设  $K, K_1, K_2$  都是域  $F$  的扩域且

$$K \supseteq K_i \supseteq F, \quad i = 1, 2.$$

若  $K_1$  与  $K_2$  是  $F$  等价扩张, 则称  $K_1, K_2$  是  $K$  (对  $F$ ) 共轭的子域.

又若  $\alpha, \beta \in K$  且  $\text{Irr}(\alpha, F) = \text{Irr}(\beta, F)$ , 则称  $\alpha$  与  $\beta$  是 (对  $F$ ) 的共轭元素.

从例 3.1.2 知  $\alpha, \beta$  是共轭元素, 则  $F(\alpha)$  与  $F(\beta)$  共轭. 从例 3.1.3 知反之不成立.

♣