域的单扩张

定义 1 (素体)**.** 只以自身为子体的体称为**素体**.

命题 1. 每个体中必包含唯一的素体作为其子体.

证明. 对任意体，它的全部子体的交即为素体，因为不包含更小的体了. 又反设有两个素体，那么素体的交一定比这两个素体小，这与素体的定义矛盾，于是每个体包含的素体是唯一的. □

定理 1. 设 p 是素数，则 $\mathbb{Z}_p$ 和 $\mathbb{Q}$ 都是素体. 对任意素体 M，或者 $M \cong \mathbb{Z}_p$，或者 $M \cong \mathbb{Q}$.

证明. $\mathbb{Z}_p$ 的子体作为加群，元素个数只能为 1 或 p，作为体，至少有元素 0 和 1，于是 $\mathbb{Z}_p$ 的元素个数只能为 p，故子体只能为 $\mathbb{Z}_p$.

$\mathbb{Q}$ 的子体 F 至少含有 0 和 1，对四则运算封闭，则 $\mathbb{Z} \subset F$，于是 $\mathbb{Z}$ 的分式域 $\mathbb{Q} \subset F$，故 $F = \mathbb{Q}$.

下设 M 是一个素体，记 e 是 M 的幺元，则 $\mathbb{Z}e = \{ne \mid n \in \mathbb{Z}\}$ 是 M 的子环，且是整环. 作映射 $\pi : \mathbb{Z} \to \mathbb{Z}e, n \mapsto ne$，则 π 是满同态，于是由同态基本定理，

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

而 $\ker \pi$ 是 $\mathbb{Z}$ 的理想，$\mathbb{Z}$ 是 PID，故存在 p 使得 $\ker \pi = \langle p \rangle$. 又因为 $\mathbb{Z}e$ 是整环，于是 $\langle p \rangle$ 是素理想，p 为 0 或素数.

当 p 为素数时，$\mathbb{Z}e \cong \mathbb{Z}_p$ 是域，则 $\mathbb{Z}e$ 是 M 的子体，而 M 是素体，故 $M \cong \mathbb{Z}e \cong \mathbb{Z}_p$.

当 $p = 0$ 时，$\mathbb{Z}e \cong \mathbb{Z}$，则 $\mathbb{Z}e$ 的分式域 $F \cong \mathbb{Q}$. 由于 M 是体，$\mathbb{Z}e$ 是 M 的子环，于是 $F \subset M$. 而 M 是素体，于是 $M = F \cong \mathbb{Q}$. □

注. *素体总是同构于域* $\mathbb{Z}_p$ *或* $\mathbb{Q}$*，于是又称为***素域**.

定义 2 (特征)**.** 若体 K 的素域与 $\mathbb{Q}$ 同构，则称 K 的**特征**为 0. 若体 K 的素域与 $\mathbb{Z}_p$ 同构，则称 K 的**特征**为 p. 记 K 的特征为 $\mathrm{Ch}K$.

定理 2. 设 K 是体，p 为素数，则

1. $\mathrm{Ch}K = p \iff pa = 0, \forall a \in K$.

2. $\mathrm{Ch}K = 0 \iff na \neq 0, \forall n \in \mathbb{N}^+, a \in K^*$.

证明. 设 K 的幺元为 e，K 中素域为 M.

1. 若 $\mathrm{Ch}K = p$，则 $M \cong \mathbb{Z}_p$，于是 $pe = 0$，对任意 $a \in K$，有 $pa = pea = 0$. 反之，若 $pa = 0, \forall a \in K$，则 $pe = 0$，于是 $M \cong \mathbb{Z}_p$，即 $\mathrm{Ch}K = p$.

2. 若 $\mathrm{Ch}K = 0$，则 $\mathbb{Z} \cong \mathbb{Z}e$，故对任意 $n \in \mathbb{N}^+$，$ne \neq 0$，于是对任意 $a \in K^*$，$na = nea \neq 0$. 反之，对任意 $n \in \mathbb{N}^+$，$a \in K^*$，有 $na \neq 0$，则 $ne \neq 0$，于是 $\mathbb{Z} \cong \mathbb{Z}e$，故 $\mathrm{Ch}K = 0$. □

注. 上述定理作为特征的等价条件，可以给出特征的另一定义，并推广到无零因子环上.

推论 1. 数域的特征都是 0.

证明. 由定理2的第 2 条可得. 或者因为任何数域都包含 $\mathbb{Q}$，而 $\mathrm{Ch}\mathbb{Q}=0$ 也可得. □

定义 3 (扩域)**.** 若 F 是域 K 的子域，则称 K 是 F 的**扩域**，记作 K/F.

定义 4. 设域扩张 K/F，S 是 K 的子集.K 中所有包含 $F\cup S$ 的域的交称为 F 上添加 S 所得的域，记作 $F(S)$.

注. 即包含 $F\cup S$ 的最小的域，也称为 F 和 S 生成的子域.

记

$$F\left[S\right]=\left\{\sum_{i_1,i_2,\cdots,i_n\leqslant 0}a_{i_1i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}\;\middle|\;\forall n\in\mathbb{N}^+,\alpha_j\in S,a_{i_1i_2\cdots i_n}\in F\right\}.$$

有下述命题.

命题 2. $F(S)$ 是 $F\left[S\right]$ 的分式域.

证明. 记 $f(\alpha_1,\alpha_2,\cdots,\alpha_n)=\sum a_{i_1i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}$，则

$$\left\{\frac{f(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g(\beta_1,\beta_2,\cdots,\beta_m)}\;\middle|\;f(\alpha_1,\alpha_2,\cdots,\alpha_n),g(\beta_1,\beta_2,\cdots,\beta_m)\in F\left[S\right],g(\beta_1,\beta_2,\cdots,\beta_m)\neq 0\right\}$$

是 $F\left[S\right]$ 的分式域，且包含于 $F(S)$. 又因为 $F(S)$ 是所有包含 $F\cup S$ 的域的交，于是 $F(S)$ 就是 $F\left[S\right]$ 的分式域. □

定理 3. 设域扩张 K/F，$S\subset K$，则

1. $F(S)=\bigcup\limits_{S'\in S}F(S')$，其中 S' 取遍 S 的所有有限子集.
2. $F(S_1\cup S_2)=F(S_1)(S_2)$.

证明. 1. $S'\subset S$，则 $F(S')\subset F(S)$. 对任意 $a\in F(S)$，存在 $f,g\in F\left[S\right]$ 使得 $a=\dfrac{f}{g}$. 而 f,g 均为有限和，故存在 S 的有限子集 S_0' 使得 $f,g\in F\left[S_0'\right]$，则

$$a=\frac{f}{g}\in F(S_0')\subset\bigcup_{S'\subset S}F(S').$$

$F(S_1\cup S_2)$ 是含 $F\cup(S_1\cup S_2)$ 的最小域，而 $F(S_1)(S_2)$ 是含 $F\cup S_1\cup S_2$ 的域，于是 $F(S_1\cup S_2)\subset F(S_1)(S_2)$.

2. $F(S_1)(S_2)$ 是含 $(F\cup S_1)\cup S_2$ 的最小域，而 $F(S_1\cup S_2)$ 是含 $F\cup S_1\cup S_2$ 的域，于是 $F(S_1)(S_2)\subset F(S_1\cup S_2)$. 故 $F(S_1\cup S_2)=F(S_1)(S_2)$. □

推论 2. $F(S_1)(S_2) = F(S_2)(S_1)$.

推论 3. $F(\alpha_1, \alpha_2, \cdots, \alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$.

至此，把在域上添加有限集合转化为添加有限个元素，进一步转化为添加单个元素的问题.

定义 5 (域的单扩张)**.** 设域扩张 K/F. 若存在 $\alpha \in K$ 使得 $K = F(\alpha)$，则称 K 是 F 的**单扩张**或**单扩域**. 若 α 是 F 上的代数元，则称 $K = F(\alpha)$ 是 F 的**单代数扩张**，若 α 是 F 上的超越元，则称 $K = F(\alpha)$ 是 F 的**单超越扩张**.

单超越扩张的构造：由于 α 是超越元，于是 $F[\alpha]$ 是 F 上一元多项式环，在同构意义下唯一，于是它的分式域 $F(\alpha)$ 在同构意义下唯一.

单代数扩张的构造有下述定理.

定理 4. 域 F 的单代数扩张 $F(\alpha) = F[\alpha]$.

证明. 嵌入映射 $i: F \to K$ 为同态映射. 对任意 $\alpha \in K$，有 $\eta: F[x] \to K$ 使得 $\eta(x) = \alpha$. 于是 $\eta(F[x]) = F[\alpha]$. 即 $\eta: F[x] \to F[\alpha]$ 是满同态. 由同态基本定理，

$$F[x] / \ker\eta \cong F[\alpha].$$

由于 $F[x]$ 是域 F 上的多项式环，因而是主理想整环. 而 $\ker\eta$ 是 $F[x]$ 的理想，故存在 $p(x) \in F[x]$ 使得 $\ker\eta = \langle p(x)\rangle$.

又因为 $F[\alpha]$ 是整环，于是 $\langle p(x)\rangle$ 是素理想，$p(x)$ 为不可约多项式. 而 $F[x]$ 是主理想整环，于是 $\langle p(x)\rangle$ 是极大理想，因而 $F[\alpha]$ 是域. 而 $F(\alpha)$ 是 $F[\alpha]$ 的分式域，故 $F(\alpha) = F[\alpha]$. □

注. $F[\alpha]$ 的形式为

$$F[\alpha] = \left\{ f(\alpha) = \sum_{i=0}^{k} a_i\alpha^i \;\middle|\; a_i \in F, \forall k \in \mathbb{N} \right\},$$

于是 $F(\alpha)$ 中的元素更清晰了.

注. $p(x)$ 把 α 化零，即 $p(\alpha) = 0$. 不妨设 $p(x)$ 首一，则这样的首一不可约多项式 $p(x)$ 被 α 唯一确定，称为 α 的极小多项式，即如下定义.

定义 6 (极小多项式)**.** 设 K 是 F 的扩域，$\alpha \in K$ 且为 F 上的代数元，$F[x]$ 中以 α 为根的首一不可约多项式称为 α 在 F 上的**极小多项式**，记作 $\mathrm{Irr}(\alpha, F)$. 称 $\deg(\mathrm{Irr}(\alpha, F))$ 为 α 在 F 上的**次数**，记作 $\deg(\alpha, F)$.

还可以从线性空间的角度看单代数扩张.

定理 5. 设 $F(\alpha)$ 是域 F 的单代数扩张，又若 $\deg(\alpha, F) = n$，则 $F(\alpha)$ 是 F 上的 n 维线性空间，且 $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 是一组基.

证明. 由线性空间定义可以验证 $F(\alpha)$ 是 F 上的线性空间. 下证 $1, \alpha, \cdots, \alpha^{n-1}$ 是一组基.

反设 $1, \alpha, \cdots, \alpha^{n-1}$ 线性相关，则有不全为零的 $a_0, a_1, \cdots, a_{n-1}$ 使 $\sum\limits_{i=0}^{n-1} a_i\alpha^i = 0$，这与 $\deg(\alpha, F) = n$ 矛盾.

由 $\deg(\alpha, F) = n$，对任意 $f(x) \in F[x]$，存在 $q(x), r(x) \in F[x]$ 使得

$$f(x) = q(x)\mathrm{Irr}(\alpha, F) + r(x), \qquad \deg r(x) < \deg(\mathrm{Irr}(\alpha, F)) = n.$$

于是 $f(\alpha) = r(\alpha)$，可被 $1, \alpha, \cdots, \alpha^{n-1}$ 线性表出.

因而 $1, \alpha, \cdots, \alpha^{n-1}$ 是 $F(\alpha)$ 的一组基，故 $F(\alpha)$ 的维数为 n. □

注. 上述定理把 F 的代数单扩张与线性空间联系，元素为 $\sum\limits_{i=0}^{n-1} a_i\alpha^i$，把求和的项数限制住.

注. $F(\alpha)$ 分别看作线性空间和域时，它们的加法是一致的，但乘法有所不同. 线性空间中的乘法是系数域 F 中的元素与 $F(\alpha)$ 中元素相乘，乘积的次数仍小于 n. 而域中的乘法是 $F(\alpha)$ 中的两个元素 $\sum\limits_{i=0}^{n-1} a_i\alpha^i$ 与 $\sum\limits_{i=0}^{n-1} b_i\alpha^i$ 相乘，乘积的次数不一定仍小于 n，这时可以与上述证明中类似作多项式的带余除法，以 $\mathrm{Irr}(\alpha, F)$ 为除式，得到 $r(x)$ 再代入 α，使得乘积与次数小于 n 的 $r(\alpha)$ 相等.

定义 7 (等价扩张)**.** 设 K_1, K_2 都是 F 的扩域，且存在同构 $\eta: K_1 \to K_2$. 若 $\eta\big|_F = \mathrm{id}_F$，则称 K_1 与 K_2 是 ***F*-等价扩张**，称 η 为 K_1 到 K_2 的 ***F*-同构**，若 $K_1 = K_2 = K$，则称 η 为 K 的 ***F*-自同构**.

命题 3. 设 $F(\alpha)$ 和 $F(\beta)$ 都是 F 的单超越扩张，则 $F(\alpha)$ 与 $F(\beta)$ 是 F-等价扩张.

证明. $F(\alpha)$ 与 $F(\beta)$ 都是 F 上一元多项式环的分式域，因此 $F(\alpha) \cong F(\beta)$ 且 $\eta\big|_F = \mathrm{id}_F$. □

命题 4. 设 $F(\alpha)$ 和 $F(\beta)$ 都是 F 的单代数扩张且 $\mathrm{Irr}(\alpha, F) = \mathrm{Irr}(\beta, F)$，则 $F(\alpha)$ 与 $F(\beta)$ 是 F-等价扩张.

证明. 设 $n = \deg(\alpha, F) = \deg(\beta, F)$，作映射

$$\eta: F(\alpha) \to F(\beta), \sum_{i=0}^{n-1} a_i\alpha^i \mapsto \sum_{i=0}^{n-1} a_i\beta^i,$$

则由同一域上相同维数的线性空间同构可知 η 是双射且保持域的加法. 对于乘法，存在 $q(x), r(x) \in F[x]$ 使得

$$\left(\sum_{i=0}^{n-1} a_i x^i\right)\left(\sum_{i=0}^{n-1} b_i x^i\right) = q(x)\mathrm{Irr}(\alpha, F) + r(x), \qquad \deg r(x) < n.$$

于是

$$\left(\sum_{i=0}^{n-1} a_i\alpha^i\right)\left(\sum_{i=0}^{n-1} b_i\alpha^i\right) = r(\alpha).$$

有

$$\eta(r(\alpha)) = \sum_{i=0}^{n-1} c_i\beta^i = q(\beta)\mathrm{Irr}(\beta, F) + r(\beta) = \left(\sum_{i=0}^{n-1} a_i\beta^i\right)\left(\sum_{i=0}^{n-1} b_i\beta^i\right).$$

故 η 是域同构. 对任意 $a_0 \in F$，有

$$\eta(a_0) = \eta\left(\sum_{i=0}^{n-1} a_i\alpha^i\right) = \sum_{i=0}^{n-1} a_i\beta^i = a_0\beta^0 = a_0.$$

于是 $\eta\big|_F = \mathrm{id}_F$，故 $F(\alpha)$ 与 $F(\beta)$ 是 F-等价扩张. $\square$

注. 单代数扩张 $F(\alpha)$ 在 F-等价扩张的意义下，完全由 $\mathrm{Irr}(\alpha, F)$ 决定.

例 1. F-等价的两个单代数扩张 $F(\alpha)$ 和 $F(\beta)$,不一定有 $\mathrm{Irr}(\alpha, F) = \mathrm{Irr}(\beta, F)$. 例如 $\mathbb{R}(\sqrt{-1}) = \mathbb{R}(1+\sqrt{-1}) = \mathbb{C}$，但 $\mathrm{Irr}(\sqrt{-1}, \mathbb{R}) = x^2+1$，$\mathrm{Irr}(1+\sqrt{-1}, \mathbb{R}) = x^2-2x+2$，显然不等. 但它们的次数是相同的.

定义 8 (共轭子域)**.** 设 K_1 和 K_2 是 F-等价扩张，且都是 K 的子域，则称 K_1 和 K_2 是 K 中对 F 的**共轭子域**.

定义 9 (共轭元素)**.** 设域扩张 K/F，$\alpha, \beta \in K$，$\mathrm{Irr}(\alpha, F) = \mathrm{Irr}(\beta, F)$，则称 α 与 β 是对 F 的**共轭元素**.