可分扩张

定义 1 (可分元素)**.** 设域扩张 K/F，$\alpha \in K$ 是 F 上的代数元. 若 $\mathrm{Irr}(\alpha, F)$ 可分，则称 α 是 F 上的**可分元素**，否则称为 F 的**不可分元素**.

定义 2 (可分扩张)**.** 设域扩张 K/F 是代数扩张，若 K 中任一元素都是 F 上的可分元素，则称 K 是 F 的**可分扩张**，否则称为 F 的**不可分扩张**.

命题 1. 完备域的代数扩张是可分扩张.

证明. 由定义即得. □

推论 1. 有限域的代数扩张是可分扩张.

推论 2. 特征为 0 的域的代数扩张是可分扩张.

命题 2. 设域扩张 K/F 是可分扩张，E 是中间域，则 E/F，K/E 都是可分扩张.

证明. 因为 K/F 是可分扩张，故 K/F 是代数扩张，则 E/F，F/E 都是代数扩张. 对任意 $\alpha \in E \subset K$，$\mathrm{Irr}(\alpha, F)$ 可分，故 E/F 是可分扩张.

对任意 $\beta \in K$，$\mathrm{Irr}(\beta, F)$ 可分，且 $\mathrm{Irr}(\beta, E) \mid \mathrm{Irr}(\beta, F)$，则 $\mathrm{Irr}(\beta, E)$ 可分，故 K/E 是可分扩张. □

命题 3. 存在不可分的代数扩张.

证明. 设 p 是素数，α 是 $\mathbb{Z}_p$ 上的超越元，则 $x^p - \alpha \in \mathbb{Z}_p(\alpha)[x]$ 不可约，设 $x^p - \alpha$ 在扩域上的一个根为 θ，则 $x^p - \alpha = x^p - \theta^p = (x - \theta)^p$，有重根，则 $x^p - \alpha$ 不可分. □

定理 1. 设 K 是可分多项式 $f(x) \in F[x]$ 的分裂域，则 K 是 F 的可分扩张.

证明. 因为 K 是 $f(x) \in F[x]$ 的分裂域，故 K/F 是有限扩张，进而是代数扩张. 又 $f(x)$ 是可分多项式，故 K 的不同 F-自同构的个数为 $[K : F]$. 因为 K 是 $f(x) \in F[x]$ 的分裂域，故 K/F 是正规扩张. 对任意 $\alpha \in K$，因为 $f(x)$ 的分裂域是 K，因此 $f(x)$ 的根都在 K 中，又因为 K/F 是正规扩张，所以 $\mathrm{Irr}(\alpha, F)f(x)$ 的根都在 K 中，$\mathrm{Irr}(\alpha, F)f(x) \in F[x]$ 的分裂域仍是 K，又因为 K 的不同 F-自同构的个数为 $[K : F]$，故 $\mathrm{Irr}(\alpha, F)f(x)$ 是 F 上的可分多项式，则 $\mathrm{Irr}(\alpha, F)$ 是 F 上的可分多项式. 由 α 的任意性，K/F 是可分扩张. □

推论 3. 设 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 F 上可分元素，则 $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 是 F 的可分扩张.

证明. 因为 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 F 上可分元素，则 $\mathrm{Irr}(\alpha_1, F), \mathrm{Irr}(\alpha_2, F), \cdots, \mathrm{Irr}(\alpha_n, F)$ 是 F 上的可分多项式，则 $\prod_{i=1}^{n} \mathrm{Irr}(\alpha_i, F)$ 也是 F 上的可分多项式. 设它的分裂域为 K，则由定理1，域扩张 K/F 是可分扩张. 又 $F \subset F(\alpha_1, \alpha_2, \cdots, \alpha_n) \subset K$，故 $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 是 F 的可分扩张. □

定义 3 (本原元素). 设域扩张 K/F 是有限扩张，若存在 $\theta \in K$ 使得 $K = F(\theta)$，则称 θ 是 K 对 F 的**本原元素**.

定理 2. 设 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是域 F 上的可分元素，则 $K = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 中有本原元素 θ 使 $K = F(\theta)$.

证明. 只需证 $n = 2$ 时即可.

当 F 是有限域时，$K = F(\alpha, \beta)$ 也是有限域，于是 K 中非零元关于乘法作成的子群 $(K^*, \cdot)$ 为循环群，存在 $\theta \in K^*$ 使得 $K^* = \langle\theta\rangle$，故 $K = F(\theta)$.

当 F 是无限域时，设 α, β 是 F 上的可分元素，记 $\theta = \beta + c\alpha$，$c \in F$，则 $F(\theta) \subset F(\alpha, \beta)$. 记 $p_1(x) = \mathrm{Irr}(\alpha, F)$，$p_2(x) = \mathrm{Irr}(\beta, F)$，在 $p_1(x)p_2(x) \in F[x]$ 的分裂域中，因为 α, β 是域 F 上的可分元素，于是 $p_1(x), p_2(x)$ 可以分解为互不相同的一次因式

$$p_1(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_t),$$

$$p_2(x) = (x - \beta_1)(x - \beta_2)\cdots(x - \beta_s),$$

不妨设 $\alpha_1 = \alpha$，$\beta_1 = \beta$.

由于

$$p_2(\theta - c\alpha) = p_2(\beta) = 0,$$

于是 α 是 $p_2(\theta - cx)$ 的根. 记

$$f(x) = p_2(\theta - cx) = (\theta - cx - \beta_1)(\theta - cx - \beta_2)\cdots(\theta - cx - \beta_s) \in F(\theta)[x].$$

当 $c \neq \dfrac{\beta_j - \beta}{\alpha - \alpha_i}$ $(i = 2, 3, \cdots, t,\ j = 1, 2, \cdots, s)$ 时，有

$$\beta + c\alpha - c\alpha_i - \beta_j = \theta - c\alpha_i - \beta_j \neq 0,$$

因为 F 是无限域，于是总可以找到这样的 c，此时 $(f(x), \mathrm{Irr}(\alpha, F)) = x - \alpha$，于是 $x - \alpha \in F(\theta)[x]$，$\alpha \in F(\theta)$. 则 $\beta = \theta - c\alpha \in F(\theta)$，故 $F(\alpha, \beta) \subset F(\theta)$. □

注. 定理事实上给出了本原元素的求法，但是求解困难. 对于无限域，可以采用先猜后证的思路. 即任取 c_0，令 $\theta = \beta + c_0\alpha$，只要得出 $\alpha \in F(\theta)$ 或 $\beta \in F(\theta)$ 即可.

定理 3. 一个域的有限可分扩张一定是单代数扩张.

证明. 设有限可分扩张 K/F，$K = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$，其中 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是可分元素，则由定理2可知存在 θ 使得 $K = F(\theta)$. □

下面说明可分扩张的可分扩张仍为可分扩张，先给出一个引理.

引理 1. 设 F 是域，$\mathrm{Ch}F = p \neq 0$，α 是 F 上代数元，则 $F(\alpha)$ 是 F 的可分扩张当且仅当 $F(\alpha) = F(\alpha^p)$.

证明. “⇒”：显然 $F(\alpha^p)\subset F(\alpha)$. 又因为 $F(\alpha)$ 是 F 的可分扩张，所以 α 是 F 上的可分元素，进而是 $F(\alpha^p)$ 上的可分元素. 于是 $\mathrm{Irr}(\alpha,F(\alpha^p))$ 无重根. 而 $x^p-\alpha^p\in F(\alpha)[x]$ 是 α 的零化多项式，于是

$$\mathrm{Irr}(\alpha,F(\alpha^p))\mid x^p-\alpha^p=(x-\alpha)^p.$$

故 $\mathrm{Irr}(\alpha,F(\alpha^p))=x-\alpha$，则 $\alpha\in F(\alpha^p)$，故 $F(\alpha)\subset F(\alpha^p)$.

“⇐”：反设 α 是 F 上的不可分元素，则 $\mathrm{Irr}(\alpha,F)$ 是不可分的不可约多项式，存在不可约多项式 $g(x)\in F[x]$ 使得 $\mathrm{Irr}(\alpha,F)=g(x^p)$，将 α 代入，有 $g(\alpha^p)=0$. 把 α^p 看作一个整体，则 $g(x)$ 把 α^p 化零且首一不可约，故 $\mathrm{Irr}(\alpha^p,F)=g(x)$. 于是 $\deg(\alpha,F)>\deg(\alpha^p,F)$，即 $[F(\alpha):F]>[F(\alpha^p):F]$. 这与 $F(\alpha)=F(\alpha^p)$ 矛盾. □

定理 4. 设域扩张 K/E，E/F 是可分扩张，则域扩张 K/F 也是可分扩张.

证明. 不妨设 $\mathrm{Ch}F=p\neq 0$. 由 K/E，E/F 都是可分扩张，所以都是代数扩张，则 K/F 也是代数扩张. 因为 K/E 可分，故对任意 $\alpha\in K$，α 是 E 上可分元素，则

$$\mathrm{Irr}(\alpha,E):=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

是可分多项式，其中 $a_0,a_1,\cdots,a_{n-1}\in E$. 取 $F(a_0,a_1,\cdots,a_{n-1})$，则

$$\mathrm{Irr}(\alpha,E)\in F(a_0,a_1,\cdots,a_{n-1})[x]$$

无重根. 又因为 E/F 可分，故 $a_0,a_1,\cdots,a_{n-1}$ 都是 F 上可分元，故存在本原元素 $\theta\in F(a_0,a_1,\cdots,a_{n-1})$ 使得 $F(\theta)=F(a_0,a_1,\cdots,a_{n-1})$.

因为

$$\mathrm{Irr}(\theta,F(\alpha))\ \Big|\ \mathrm{Irr}(\theta,F(\alpha^p)),$$

而

$$(\mathrm{Irr}(\theta,F(\alpha)))^p\in F^p(\alpha^p)=F(\alpha^p),$$

故

$$\mathrm{Irr}(\theta,F(\alpha^p))\ \Big|\ (\mathrm{Irr}(\theta,F(\alpha)))^p.$$

因为 θ 是 F 上可分元素，故 θ 是 $F(\alpha^p)$ 上可分元素，$\mathrm{Irr}(\theta,F(\alpha^p))$ 无重根，则

$$\mathrm{Irr}(\theta,F(\alpha^p))\ \Big|\ \mathrm{Irr}(\theta,F(\alpha)).$$

故 $\mathrm{Irr}(\theta,F(\alpha))=\mathrm{Irr}(\theta,F(\alpha^p))$，于是

$$[F(\theta,\alpha^p):F(\alpha^p)]=[F(\theta,\alpha):F(\alpha)].$$

因为 α 是 $F(\theta)$ 上的可分元，由引理1有 $F(\theta,\alpha)=F(\theta,\alpha^p)$. 于是

$$[F(\theta,\alpha):F(\alpha)]\,[F(\alpha):F(\alpha^p)]=[F(\theta,\alpha):F(\alpha^p)]=[F(\theta,\alpha^p):F(\alpha^p)]=[F(\theta,\alpha):F(\alpha)].$$

比较左右两边即得

$$[F(\theta,\alpha):F(\alpha)]=1,$$

因而 $F(\alpha)=F(\alpha^p)$，由引理1即得 $F(\alpha)$ 是 F 的可分扩张，即 α 是 F 上的可分元素，而由 α 的任意性可得 K/F 是可分扩张. □