有限扩张

定义 1 (有限扩张, 无限扩张)**.** 设域扩张 K/F，把 K 看作 F 上的线性空间时，称线性空间的维数为 K 对 F 的**扩张次数**，记作 $[K:F]$，当扩张次数有限时，称 K 是 F 的**有限扩张**，否则称 K 是 F 的**无限扩张**.

命题 1. 单代数扩张 $F(\alpha)$ 的扩张次数 $[F(\alpha):F]=\deg(\alpha,F)$.

定义 2 (代数扩张, 超越扩张)**.** 设域扩张 K/F，若任意 $\alpha\in K$ 都是 F 上的代数元，则称 K 是 F 的**代数扩张**，否则称 K 是 F 的**超越扩张**.

定理 1. 有限扩张一定是代数扩张.

证明. 设域扩张 K/F，则存在 $n\in\mathbb{N}$ 使得 $[K:F]=n$. 对任意 $\alpha\in K$，$1,\alpha,\cdots,\alpha^n$ 线性相关. 于是存在不全为零的 $a_0,a_1,\cdots,a_n\in F$ 使得 $\sum\limits_{i=0}^{n}a_i\alpha^i=0$，故 α 是 F 上的代数元. □

推论 1. 若 α 是超越元，则 $F(\alpha)$ 是无限扩张.

定理 2. 设域扩张 K/F，$\alpha\in K$，则下列条件等价.

1. $F(\alpha)$ 是 F 的代数扩张.
2. α 是 F 上的代数元.
3. $F(\alpha)$ 是 F 的有限扩张.

定义 3 (中间域)**.** 设域扩张 $K/E,E/F$. 则称 E 为扩张 K/F 的**中间域**.

定理 3. 设 E 是域扩张 K/F 的中间域，则扩张 K/F 有限当且仅当扩张 K/E 和 E/F 都有限，且有

$$[K:F]=[K:E]\,[E:F]\,.$$

证明. 若 K/F 有限，则 F 上线性空间 K 是有限维的，其子空间 E 也是有限维的，故 E/F 有限. 设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是线性空间 K 在域 F 上的一组基，由于 $F\subset E$，于是 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 K 在 E 上的生成组，可以从中选出线性无关元组成一组基，自然是有限的，即 K/E 有限.

反之，若 K/E 和 E/F 都有限，可设 K 在 E 上的一组基为 $\alpha_1,\alpha_2,\cdots,\alpha_n$，$E$ 在 F 上的一组基为 $\beta_1,\beta_2,\cdots,\beta_m$，则由线性空间张量积的性质可知 $\alpha_1\beta_1,\cdots,\alpha_1\beta_m,\alpha_2\beta_1,\cdots,\cdots,\alpha_n\beta_m$ 是 K 在 F 上的一组基，于是 K/F 有限，且

$$[K:F]=[K:E]\,[E:F]\,.$$

□

推论 2. 设 $K/E_1/E_2/\cdots/E_n/F$，则

$$[K:F]=[K:E_1]\,[E_1:E_2]\cdots[E_n:F]\,.$$

推论 3. 若 $[K:F]$ 是素数，则 K 与 F 间无真中间域.

下面将说明代数扩张的代数扩张仍为代数扩张，先给出一个引理.

引理 1. 域扩张 K/F 有限当且仅当存在**单代数扩张升链**

$$F=F_0\subset F_1\subset\cdots\subset F_r=K.$$

其中 F_{i+1} 是 F_i 的单代数扩张.

证明. 若 K/F 是有限扩张，则由定理1，K/F 是代数扩张. 于是任意 $\alpha\in K$ 都是 F 上的代数元. 取 $\alpha_1\in K-F$，$F_1=F(\alpha_1)$，则 $F=F_0\subset F_1$. 若 $K=F_1$，则完成证明，否则取 $\alpha_2\in K-F_1$，$F_2=F_1(\alpha_2)$，则 $F=F_0\subset F_1\subset F_2$，若 $K=F_2$，则完成证明，否则以此类推，经有限次后总能得到 $r\in\mathbb{N}$ 使得 $K=F_r$. 反之，由于每个单代数扩张次数有限，于是 $[K:F]$ 作为单扩张次数之积也有限. □

定理 4. 设域扩张 K/E，E/F 是代数扩张，则域扩张 K/F 也是代数扩张.

证明. 对任意 $\alpha\in K$，由于 K/E 是代数扩张，于是 α 是 E 上的代数元. 记

$$\mathrm{Irr}(\alpha,E)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n,\quad a_i\in E.$$

于是 $\mathrm{Irr}(\alpha,E)\in F(a_1,a_2,\cdots,a_n)\,[x]$.

因为 E/F 是代数扩张，于是 $a_1,a_2,\cdots,a_n$ 都是 F 上的代数元，记

$$F=F_0,\ F_i=F(a_1,a_2,\cdots,a_i),\ i=1,2,\cdots,n$$

又因为 $\mathrm{Irr}(\alpha,E)$ 是 α 的零化多项式，于是 α 是 $F(a_1,a_2,\cdots,a_n)$ 上的代数元，则有单代数扩张升链

$$F=F_0\subset F_1\subset\cdots\subset F_n\subset F(a_1,a_2,\cdots,a_n)(\alpha),$$

于是由引理1，$F(a_1,a_2,\cdots,a_n)(\alpha)$ 是有限扩张，由定理1，$F(a_1,a_2,\cdots,a_n)(\alpha)$ 是代数扩张，于是 α 是 F 上的代数元，又因为 α 的任意性，故 K/F 是代数扩张. □

上述定理的逆命题依然成立.

命题 2. 设域扩张 K/F 是代数扩张，E 是中间域，则 E/F，K/E 都是代数扩张.

证明. 因为 K/F 是代数扩张，任意 $\alpha\in E\subset K$ 都是 F 上的代数元，故 E/F 是代数扩张. 对任意 $\beta\in K$ 是 F 上代数元，而 $\mathrm{Irr}(\beta,F)\in F\,[x]\subset E\,[x]$，故 β 是 E 上代数元，所以 K/E 是代数扩张. □

定义 4 (代数闭包)**.** 设域扩张 K/F，K 中 F 上全体代数元的集合 $\overline{F}$ 称为 F 在 K 中的**代数闭包**.

定理 5. 设域扩张 K/F，则 F 在 K 中的代数闭包 $\overline{F}$ 是包含于 K 的 F 的最大代数扩张，且任意 $\delta \in K - \overline{F}$ 都是 $\overline{F}$ 上的超越元.

证明. 对任意 $\alpha, \beta \in \overline{F}$，由于 $\overline{F} \subset K$，于是满足有关运算的公理，下证四则运算封闭即可. 而 $\alpha, \beta \in F(\alpha, \beta) = F(\alpha)(\beta)$，其中 $F(\alpha)(\beta)$ 是 $F(\alpha)$ 的代数扩张，$F(\alpha)$ 是 F 的代数扩张，于是 $F(\alpha)(\beta)$ 是 F 的代数扩张. 则 $\alpha \pm \beta$ 和 $\alpha\beta^{\pm 1}$ 均为 F 上的代数元，于是 $\alpha \pm \beta$ 和 $\alpha\beta^{\pm 1} \in \overline{F}$. 故 $\overline{F}$ 是 F 的扩域.

对任意 $\delta \in K - \overline{F}$，假设 δ 是 $\overline{F}$ 上的代数元，则 $\overline{F}(\delta)/\overline{F}$ 和 $\overline{F}/F$ 都是代数扩张，则 $\overline{F}(\delta)/F$ 也是代数扩张，这与 $\overline{F}$ 是最大的代数扩张矛盾. □

定义 5 (代数数, 超越数)**.** 若 $\alpha \in \mathbb{C}$ 是 $\mathbb{Q}[x]$ 中某多项式的根，则称 α 为**代数数**，否则称 α 为**超越数**.

定义 6 (代数整数)**.** 若 $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$，则称 α 为**代数整数**.

定义 7 (代数数域)**.** $\mathbb{Q}$ 在 $\mathbb{C}$ 上的代数闭包 $\overline{\mathbb{Q}}$ 称为**代数数域**.

命题 3. 代数数只有可数多个.

命题 4 (Hermite,1873)**.** e 是超越数.

命题 5 (Lindeman,1882)**.** π 是超越数.

注. 从而否定了“化圆为方”作图的可能性.

例 1. 设域扩张 K/F，$\alpha \in K$ 是 F 上代数元且 $\deg(\alpha, F)$ 为奇数，证明 $F(\alpha^2) = F(\alpha)$.

证明. 一方面，$F(\alpha^2) \subset F(\alpha)$. 而

$$[F(\alpha) : F] = \left[F(\alpha) : F(\alpha^2)\right] \left[F(\alpha^2) : F\right],$$

因为 $\deg(\alpha, F) = [F(\alpha) : F]$ 是奇数，于是 $\left[F(\alpha) : F(\alpha^2)\right]$ 也是奇数. 而 $x^2 - \alpha^2 \in F(\alpha^2)$ 把 α 化零，则 $\deg(\alpha, F(\alpha^2)) \leqslant 2$. 又 $\left[F(\alpha) : F(\alpha^2)\right]$ 是奇数，于是 $\left[F(\alpha) : F(\alpha^2)\right] = 1$，故 $F(\alpha^2) = F(\alpha)$. □