第十二章 域和Galois理论
2015年11月16日

# 信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

12. 域和Galois理论

本章, 我们继续讨论域的结构, 特别是Galois 域.

# 12.1 域的扩张

## 12.1.1 域的有限扩张

首先, 我们从集合的包含关系的角度来讨论域的性质.

**定义12.1.1** 设$\mathbf{F}$ 是一个域. 如果$\mathbf{K}$ 是$\mathbf{F}$ 的子域, 则称$\mathbf{F}$ 为$\mathbf{K}$ 的**扩域**.

**例12.1.1** 有理数域$\mathbf{Q}$ 是实数域$\mathbf{R}$ 和复数域$\mathbf{C}$ 的子域. 复数域$\mathbf{C}$ 是实数域$\mathbf{R}$ 的扩域. 实数域$\mathbf{R}$ 是有理数域$\mathbf{Q}$ 的扩域.

**例12.1.2** $\mathbf{F}_{2^8} = \mathbf{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$ 是$\mathbf{F}_2$ 的扩域.

其次, 我们从线性空间的角度来讨论域的性质.

如果$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, 则$1_{\mathbf{F}} = 1_{\mathbf{K}}$. 而且, $\mathbf{F}$ 可作为$\mathbf{K}$ 上的线性空间.

事实上, 对任意$\alpha, \beta \in \mathbf{F}, k \in \mathbf{K}$, 有

$$\alpha + \beta \in \mathbf{K}, \quad k \cdot \alpha \in \mathbf{K}.$$

我们用$[\mathbf{F} : \mathbf{K}]$ 表示$\mathbf{F}$ 在$\mathbf{K}$ 上线性空间的**维数**. 我们称$\mathbf{F}$ 为$\mathbf{K}$ 的**有限维扩域** 或**无限维扩域**, 如果$[\mathbf{F} : \mathbf{K}]$ 是有限或无限.

**定理12.1.1** 设$\mathbf{E}$ 是$\mathbf{F}$ 的扩域, $\mathbf{F}$ 是$\mathbf{K}$ 的扩域. 则

$$[\mathbf{E}:\mathbf{K}]=[\mathbf{E}:\mathbf{F}][\mathbf{F}:\mathbf{K}].$$

如果$\{\alpha_i\}_{i\in I}$ 是$\mathbf{F}$ 在$\mathbf{K}$ 上的基底, $\{\beta_j\}_{j\in J}$ 是$\mathbf{E}$ 在$\mathbf{F}$ 上的基底, 则$\{\alpha_i\,\beta_j\}_{i\in I,j\in J}$ 是$\mathbf{E}$ 在$\mathbf{K}$ 上的基底.

**证** 首先, 证明$\{\alpha_i\,\beta_j\}_{i\in I,j\in J}$ 是$\mathbf{E}$ 在$\mathbf{K}$ 上的生成元. 事实上, 对任意$c\in\mathbf{E}$, 根据$\{\beta_j\}_{j\in J}$ 是$\mathbf{E}$ 在$\mathbf{F}$ 上的基底, 存在$b_j\in\mathbf{F},\ j\in J$ 使得

$$c=\sum_{j\in J}b_j\,\beta_j.$$

再根据$\{\alpha_i\}_{i\in I}$ 是$\mathbf{F}$ 在$\mathbf{K}$ 上的基底, 存在$a_{ij}\in\mathbf{K},\ i\in I$ 使得

$$b_j=\sum_{i\in I}a_{ij}\,\alpha_i.$$

从而,

$$c=\sum_{j\in J}\left(\sum_{i\in I}a_{ij}\,\alpha_i\right)\beta_j=\sum_{i\in I,j\in J}a_{ij}\,\alpha_i\,\beta_j.$$

其次, 证明$\{\alpha_i\,\beta_j\}_{i\in I,j\in J}$ 在$\mathbf{K}$ 上线性无关. 事实上, 若存在$a_{ij}\in\mathbf{K},\ i\in I, j\in J$ 使得

$$\sum_{i\in I,j\in J} a_{ij}\,\alpha_i\,\beta_j=0 \quad \text{或} \quad \sum_{j\in J}\left(\sum_{i\in I} a_{ij}\,\alpha_i\right)\beta_j=0.$$

因为$\sum_{i\in I} a_{ij}\,\alpha_i\in\mathbf{F}$, 且$\{\beta_j\}_{j\in J}$ 是$\mathbf{E}$ 在$\mathbf{F}$ 上的基底, 所以

$$\sum_{i\in I} a_{ij}\,\alpha_i=0,\quad j\in J.$$

又因为$a_{ij}\in\mathbf{K}$, 以及$\{\alpha_i\}_{i\in I}$ 是$\mathbf{F}$ 在$\mathbf{K}$ 上的基底, 得到

$$a_{ij}=0\quad i\in I,\ j\in J.$$

因此, 我们有

$$[\mathbf{E}:\mathbf{K}]=[\mathbf{E}:\mathbf{F}][\mathbf{F}:\mathbf{K}].$$

定理成立. 证毕

**推论** 域$\mathbf{E}$ 是$\mathbf{K}$ 的有限扩域的充要条件是$\mathbf{E}$ 是$\mathbf{F}$ 的有限扩域, 以及$\mathbf{F}$ 是$\mathbf{K}$ 的有限扩域.

**例12.1.3** 实数域$\mathbf{R}$是有理数域$\mathbf{Q}$ 的扩域, 复数域$\mathbf{C}$是实数域$\mathbf{R}$ 的扩域.

**例12.1.4** 数域$\mathbf{Q}(\sqrt{2})$ 是$\mathbf{Q}$ 的有限扩张, 且$[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.

最后, 我们讨论域的子域的生成.

**定理12.1.2** 设$\{\mathbf{E}_j\}_{j\in J}$ 是域**F** (对应地, 环$R$ ) 中的一族子域(对应地, 子环). 则$\bigcap\limits_{j\in J} E_j$ 也是一个子域(对应地, 子环) .

**证** 令$E = \bigcap\limits_{j\in J} E_j$. 根据定理8.1.3, $E$ 是一个交换加法群, 而$E^* = \bigcap\limits_{j\in J} E_j^*$ 是一个交换乘群(对应地, $E$ 也满足子环的乘法运算条件), 因此, $E$ 是域**F** 的子域(对应地, 子环). 证毕

设$\mathbf{F}$ 是一个域, $X \subset \mathbf{F}$, 则包含$X$ 的所有子域(对应地. 子环)的交集仍是包含$X$ 的子域, 叫做由$X$ **生成的子域** (对应地. **子环**). 如果$\mathbf{F}$ 是$\mathbf{K}$ 的扩域及$X \subset \mathbf{F}$, 则由$\mathbf{K} \cup X$ 生成的子域(对应地. 子环)叫做$X$ **在$\mathbf{K}$ 上生成的子域** (对应地. **子环**), 记为$\mathbf{K}(X)$ (对应地. $\mathbf{K}[X]$). 注意到$\mathbf{K}[X]$ 是一个整环.

如果$X = \{u_1, \ldots, u_n\}$, 则$\mathbf{F}$ 的子域$\mathbf{K}(X)$ (对应地. 子环$\mathbf{K}[X]$) 记为$\mathbf{K}(u_1, \ldots, u_n)$ (对应地. $\mathbf{K}[u_1, \ldots, u_n]$). 域$\mathbf{K}(u_1, \ldots, u_n)$ 叫做$\mathbf{K}$ 的**有限扩张**. 如果$X = \{u\}$, 则$\mathbf{K}(u)$ 称为$\mathbf{K}$ 的**单扩张**.

下面给出域中元素的表示.

**定理12.1.3** 设$\mathbf{F}$ 是域$\mathbf{K}$ 的扩域, $u,\ u_1,\ \ldots,\ u_n \in \mathbf{F}$, 以及$X \subset \mathbf{F}$, 则

(i) 子环$\mathbf{K}[u]$ 由形为$f(u)$ 的元素组成, 其中$f$ 是系数在$\mathbf{K}$ 的多项式(就是$f \in \mathbf{K}[x]$).

(ii) 子环$\mathbf{K}[u_1, \ldots, u_n]$ 由形为$f(u_1, \ldots, u_n)$ 的元素组成, 其中$f$ 是系数在$\mathbf{K}$ 的$n$ 元多项式(就是$f \in \mathbf{K}[x_1, \ldots, x_n]$).

(iii) 子环$\mathbf{K}[X]$ 由形为$f(u_1, \ldots, u_n)$ 的元素组成, 其中$n \in \mathbf{N},\ u_1,\ \ldots,\ u_n \in X,\ f$ 是系数在$\mathbf{K}$ 的$n$ 元多项式(就是$f \in \mathbf{K}[x_1, \ldots, x_n]$).

(iv) 子域$\mathbf{K}(u)$ 由形为$\dfrac{f(u)}{g(u)}$ 的元素组成, 其中$f,\ g \in \mathbf{K}[x],\ g(u) \neq 0$.

(v) 子域$\mathbf{K}(u_1, \ldots, u_n)$ 由形为$\dfrac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)}$ 的元素组成, 其中$f,\ g \in \mathbf{K}[x_1, \ldots, x_n],\ g(u_1, \ldots, u_n) \neq 0$.

(vi) 子域$\mathbf{K}(u_1, \ldots, u_n)$ 由形为$\dfrac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)}$ 的元素组成, 其中$n \in \mathbf{N},\ f,\ g \in \mathbf{K}[x_1, \ldots, x_n],\ u_1, \ldots, u_n \in X,\ g(u_1, \ldots, u_n) \neq 0$.

(vii) 对每个$v \in \mathbf{K}(X)$ (对应地. $\mathbf{K}[X]$), 存在一个有限子集$X' \subset X$, 使得$v \in \mathbf{K}(X')$ (对应地. $\mathbf{K}[X']$).

**证** (i) 令

$$\mathbf{E} = \{a_0 + a_1 u + \cdots + + a_m u^m \mid m \in \mathbf{N},\ a_i \in \mathbf{K}\}. \qquad (1)$$

易知, $\mathbf{E}$ 是一个整环. 又对任意$\alpha \in \mathbf{E}$, 有

$$\alpha = a_0 + a_1 u + \cdots + + a_m u^m, \quad m \in \mathbf{N},\ a_i \in \mathbf{K}.$$

因为 $u,\ a_i \in \mathbf{K}[u]$, 所以 $u^i \in \mathbf{K}[u],\ a_i u^i \in \mathbf{K}[u]$. 从而$\alpha \in \mathbf{K}[u]$ 以及$\mathbf{E} \subset \mathbf{K}[u]$. 故$\mathbf{K}[u] = \mathbf{E}$.

(ii) 令

$$\mathbf{E}=\{\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n}u_1^{i_1}\cdots u_n^{i_n}\mid a_{i_1,\ldots,i_n}\in\mathbf{K}\}. \tag{2}$$

易知, $\mathbf{E}$ 是一个整环. 又对任意$\alpha\in\mathbf{E}$, 有

$$\alpha=\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n}u_1^{i_1}\cdots u_n^{i_n},\quad a_{i_1,\ldots,i_n}\in\mathbf{K}.$$

因为 $u_1,\ \ldots,\ u_n,\ a_{i_1,\ldots,i_n}\in\mathbf{K}[u_1,\ldots,u_n]$, 所以 $u_1^{i_1},\ \ldots,\ u_n^{i_n},\ a_{i_1,\ldots,i_n}\in\mathbf{K}[u_1,\ldots,u_n]$, $a_{i_1,\ldots,i_n}u_1^{i_1}\cdots u_n^{i_n}\in\mathbf{K}[u_1,\ldots,u_n]$. 从而$\alpha\in\mathbf{K}[u_1,\ldots,u_n]$ 以及$\mathbf{E}\subset\mathbf{K}[u_1,\ldots,u_n]$. 故$\mathbf{K}[u_1,\ldots,u_n]=\mathbf{E}$.

(iii) 令

$$\mathbf{E}=\{\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n}u_1^{i_1}\cdots u_n^{i_n}\mid n\in\mathbf{N},u_1,\ldots,u_n\in X,a_{i_1,\ldots,i_n}\in\mathbf{K}\}. \tag{3}$$

易知, $\mathbf{E}$ 是一个整环. 又对任意$\alpha\in\mathbf{E}$, 有

$$\alpha=\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n}u_1^{i_1}\cdots u_n^{i_n},\quad a_{i_1,\ldots,i_n}\in\mathbf{K}.$$

因为 $u_1,\ \ldots,\ u_n,\ a_{i_1,\ldots,i_n}\in\mathbf{K}[X]$, 所以 $u_1^{i_1},\ \ldots,\ u_n^{i_n},\ a_{i_1,\ldots,i_n}\in\mathbf{K}[X]$, $a_{i_1,\ldots,i_n}u_1^{i_1}\cdots u_n^{i_n}\in\mathbf{K}[X]$. 从而$\alpha\in\mathbf{K}[X]$ 以及$\mathbf{E}\subset\mathbf{K}[X]$. 故$\mathbf{K}[X]=\mathbf{E}$.

(iv) 令

$$\mathbf{E}=\left\{\frac{f(u)}{g(u)}\ \mid\ f(x),\ g(x)\in\mathbf{K}[x],\ g(u)\neq 0\right\}. \tag{4}$$

易知, $\mathbf{E}$ 是一个子域. 又对任意$\alpha\in\mathbf{E}$, 有

$$\alpha=\frac{f(u)}{g(u)}.$$

根据(i), 有 $f(u),\ g(u)\in\mathbf{K}(u)$, 所以$\alpha\in\mathbf{K}(u)$ 以及$\mathbf{E}\subset\mathbf{K}(u)$. 故$\mathbf{K}(u)=\mathbf{E}$.

(v) 令

$$\mathbf{E}=\left\{\frac{f(u_1,\ldots,u_n)}{g(u_1,\ldots,u_n)}\ \mid\ f,\ g\in\mathbf{K}[x_1,\ldots,x_n],\ g(u_1,\ldots,u_n)\neq 0\right\}. \tag{5}$$

易知, $\mathbf{E}$ 是一个子域. 又对任意$\alpha\in\mathbf{E}$, 有

$$\alpha=\frac{f(u_1,\ldots,u_n)}{g(u_1,\ldots,u_n)}.$$

根据(ii), 有 $f(u_1,\ldots,u_n),\ g(u_1,\ldots,u_n)\in\mathbf{K}(u_1,\ldots,u_n)$, 所以$\alpha\in\mathbf{K}(u_1,\ldots,u_n)$ 以及$\mathbf{E}\subset\mathbf{K}(u_1,\ldots,u_n)$. 故$\mathbf{K}(u_1,\ldots,u_n)=\mathbf{E}$.

(vi) 令

$$\mathbf{E}=\left\{\frac{f(u_1,\ldots,u_n)}{g(u_1,\ldots,u_n)} \;\middle|\; n\in\mathbf{N},\ u_1,\ldots,u_n\in X,\ f,\ g\in\mathbf{K}[x_1,\ldots,x_n],\ g(u_1,\ldots,u_n)\neq 0\right\}. \tag{6}$$

易知, $\mathbf{E}$ 是一个子域. 又对任意$\alpha\in\mathbf{E}$, 有

$$\alpha=\frac{f(u_1,\ldots,u_n)}{g(u_1,\ldots,u_n)}.$$

根据(iii), 有 $f(u_1,\ldots,u_n),\ g(u_1,\ldots,u_n)\in\mathbf{K}(X)$, 所以$\alpha\in\mathbf{K}(X)$ 以及$\mathbf{E}\subset\mathbf{K}(X)$. 故$\mathbf{K}(X)=\mathbf{E}$. 证毕

## 0.1. 域的代数扩张

本节, 我们从多项式的根的角度来讨论扩域.

**定义12.1.2** 设$R$ 是一个整环, **K** 是包含$R$ 的一个域, **F** 是**K** 的一个扩域.

1) **F** 的元素$u$ 称为整环$R$ 上的**代数数**, 如果存在一个非零多项式$f \in R[x]$ 使得$f(u) = 0$.

2) **F** 的元素$u$ 称为整环$R$ 上的**代数整数**, 如果存在一个非零的首一多项式$f \in R[x]$ 使得$f(u) = 0$.

3) **F** 的元素$u$ 称为整环$R$ 上的**超越数**, 如果不存在任何非零多项式$R$ 使得$f(u) = 0$.

进一步, 当**K** 是整环$R$ 的分式域时, 人们有时就称**K** 上的代数数和超越数. 这时, 与代数相关的多项式就可以要求其是首一的多项式. **F** 称为**K** 的**代数扩张**, 如果**F** 的每个元素都是**K** 上的代数数. **F** 称为**K** 上的**超越扩张**, 如果**F** 中至少有一个元素是**K** 上的超越数.

易知, 对于$u \in \mathbf{K}$, 有$u$ 是一次多项式$f(x) = x - u \in \mathbf{K}[x]$ 的根, 因此, $u$ 是**K** 上的代数数.



**例12.1.5**

(i) $u=\sqrt{2}$ 是整数环$\mathbf{Z}$ 上代数整数, 因为有首一多项式

$$f(x)=(x-\sqrt{2})(x+\sqrt{2})=x^2-2\in\mathbf{Z}[x]$$

使得$f(u)=0$. $\mathbf{Q}(\sqrt{2})$ 是代数扩张.

(ii) $u=\dfrac{1+\sqrt{5}}{2}$ 是整数环$\mathbf{Z}$ 上代数整数, 因为有首一多项式

$$f(x)=(x-\frac{1+\sqrt{5}}{2})(x-\frac{1-\sqrt{5}}{2})=x^2-x-1\in\mathbf{Z}[x]$$

使得$f(u)=0$. $\mathbf{Q}(\dfrac{1+\sqrt{5}}{2})$ 是代数扩张.

**例12.1.6**

(i) 圆周率$\pi = 3.14159265\cdots$ 是有理数域$\mathbf{Q}$ 上的超越数.

(ii) 自然对数底$e = 2.71828182\cdots$ 是有理数域$\mathbf{Q}$ 上的超越数.

(iii) $2^{\sqrt{2}}$ 是有理数域$\mathbf{Q}$ 上的超越数.

(iv) $\displaystyle\sum_{n=1}^{\infty}\frac{1}{2^{n!}}$ 是有理数域$\mathbf{Q}$ 上的超越数.

下面建立多项式环和多项式分式域与域扩张之间的关系.

设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $u \in \mathbf{F}$, 则我们可以构造$\mathbf{K}[x]$ 到$\mathbf{K}[u]$ 一个同态:

$$\begin{array}{rccc} \varphi: & \mathbf{K}[x] & \longrightarrow & \mathbf{K}[u] \\ & h(x) & \longmapsto & h(u) \end{array}$$

且上述环同态可拓展为$\mathbf{K}(x)$ 到$\mathbf{K}(u)$ 一个域同态:

$$\begin{array}{rccc} \varphi: & \mathbf{K}(x) & \longrightarrow & \mathbf{K}(u) \\ & \dfrac{h(x)}{g(x)} & \longmapsto & \dfrac{h(u)}{g(u)} \end{array}$$

根据环同态分解定理, 我们有同构:

$$\overline{\varphi}: \ \mathbf{K}[x]/\ker(\varphi) \longrightarrow \mathbf{K}[u]$$

其中$\ker(\varphi) = \{h(x) \mid \in \mathbf{K}[x],\ h(u) = 0\}$.

分两种情况讨论.

1) $u$ 是$\mathbf{K}$ 上的超越数. 这时, $\ker(\varphi) = \{0\}$. 因此, $\varphi$ 是环同构, 也是域同构. 即有定理12.1.4.

2) $u$ 是$\mathbf{K}$ 上的代数数. 这时, $\ker(\varphi) \neq \{0\}$ 是素理想. 因为$\mathbf{K}[x]$ 是主理想环, 所以存在次数最小的首一不可约多项式$f(x)$ 使得$\ker(\varphi) = (f(x))$. 即引理12.1.1.



**定理12.1.4** 如果$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $u \in \mathbf{F}$ 是$\mathbf{K}$ 上的超越数, 则存在一个在$\mathbf{K}$ 上为恒等映射的域同构$\mathbf{K}(u) \cong \mathbf{K}(x)$.

**引理12.1.1** 设$\mathbf{F}$ 是域$\mathbf{K}$ 的扩域, $u \in \mathbf{F}$ 是$\mathbf{K}$ 上的代数数, 则存在惟一的$\mathbf{K}$ 上的首一不可约多项式$f(x)$ 使得$f(u) = 0$.

借助引理, 我们可以建立代数数与多项式的对应关系.

**定义12.1.3** 设F 是域K 的扩域, $u \in$ F 是K 上的代数数. 引理中的首一不可约多项式$f(x)$ 称为 $u$ 的**定义多项式** (或**极小多项式**或**不可约多项式**). $u$ 在K 上的**次数** 定义为$u$ 的定义多项式$f(x)$ 的次数$\deg\ f$. $u$ 的定义多项式$f(x)$ 的其它根叫做$u$ 的**共轭根**.

**例12.1.7** $\sqrt{2}$ 在Q 上的定义多项式是$f(x) = x^2 - 2$, 次数为2, 共轭根为$-\sqrt{2}$.

下面考虑由代数数生成的域.

**定理12.1.5** $\mathbf{F}$ 是域$\mathbf{K}$ 的扩域, $u \in \mathbf{F}$ 是$\mathbf{K}$ 上的代数数, 则

(i) $\mathbf{K}(u) = \mathbf{K}[u]$.

(ii) $\mathbf{K}(u) \cong \mathbf{K}[x]/(f(x))$ , 其中$f(x) \in \mathbf{K}[x]$ 是$u$ 的定义多项式, $n = \deg\ f$.

(iii) $[\mathbf{K}(u) : \mathbf{K}] = n$.

(iv) $\{1, u, u^2, \ldots, u^{n-1}\}$ 是$\mathbf{K}$ 上向量空间$\mathbf{K}(u)$ 的基底.

(v) $\mathbf{K}(u)$ 的每个元素可惟一地表示为$a_0 + a_1u + \cdots + a_{n-1}u^{n-1},\ a_i \in \mathbf{K}$ .

**证** 设$u$ 的定义多项式为$f(x), n = \deg\ f$.

(i) 对任意$\dfrac{h(u)}{g(u)} \in \mathbf{K}(u),\ g(u) \neq 0$, 有多项式$g(x)$ 与$f(x)$ 互素. 根据多项式广义欧几里得除法(定理11.3.6), 存在$s(x),\ t(x) \in \mathbf{K}[x]$ 使得

$$s(x) \cdot g(x) + t(x) \cdot f(x) = 1.$$

从而, $s(u)g(u) = 1$. 因此,

$$\frac{h(u)}{g(u)} = \frac{s(u) \cdot h(u)}{s(u) \cdot g(u)} = s(u) \cdot h(u) \in \mathbf{K}[u],$$

$\mathbf{K}(u) \subset \mathbf{K}[u]$. 这说明, $\mathbf{K}(u) = \mathbf{K}[u]$.

(ii) 考虑$\mathbf{K}[x]$ 到$\mathbf{K}[u]$ 的映射

$$\varphi : g(x) \longmapsto g(u).$$

易知, $\sigma$ 是满的环同态. 根据定理10.5.9, 我们有$\mathbf{K}[x]/\ker(\varphi) \cong \mathbf{K}(u)$ . 但$\ker(\varphi) = (f)$, 故结论成立.

(iv) 对任意$g(x) \in \mathbf{K}[x]$, 根据多项式欧几里得除法(定理11.3.1), 存在$q(x),\ r(x) \in \mathbf{K}[x]$ 使得

$$g(x) = q(x) \cdot f(x) + r(x), \quad 0 \leq \deg\ r < \deg\ f.$$

因此, $g(u) = r(u)$. 这说明, $\{1, u, u^2, \ldots, u^{n-1}\}$ 是$\mathbf{K}(u)$ 的生成元. 又因为$f(x)$ 是使得$f(u) = 0$ 的次数最小的多项式, 所以$\{1, u, u^2, \ldots, u^{n-1}\}$ 在$\mathbf{K}$ 上线性无关. 因此, $\{1, u, u^2, \ldots, u^{n-1}\}$ 是$\mathbf{K}$ 上向量空间$\mathbf{K}(u)$ 的基底.

(iii) 和(v) 由(iv) 得到. 证毕



**例12.1.8** 多项式$x^2 - x - 1$ 是**Q** 上的不可约多项式.

**例12.1.9** 多项式$x^3 - 3x - 1$ 是**Q** 上的不可约多项式.




上海交通大学 SHANGHAI JIAO TONG UNIVERSITY 信息安全工程学院


下面的定理将从域的同构扩充到扩域的同构.

设$\sigma : \mathbf{K} \to \mathbf{L}$ 是域同构. 对于$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbf{K}[x]$, 我们记

$$\sigma(f)(x) = \sigma(a_n)x^n + \sigma(a_{n-1})x^{n-1} + \cdots + \sigma(a_1)x + \sigma(a_0)$$

易知$f$ 和$\sigma(f)$ 同为可约或不可约多项式.

**定理12.1.6** 设$\sigma : \mathbf{K} \to \mathbf{L}$ 是域同构. 设$u$ 是$\mathbf{K}$ 的某一扩域中的元素, $v$ 是$\mathbf{L}$ 的某一扩域中的元素. 假设

(i) $u$ 是$\mathbf{K}$ 上的超越元, $v$ 是$\mathbf{L}$ 上的超越元, 或者

(ii) $u$ 是$\mathbf{K}$ 上的代数数, $u$ 的定义多项式为$f \in \mathbf{K}[x]$ , $v$ 是多项式$\sigma(f) \in \mathbf{L}[x]$ 的根.

则$\sigma$ 可扩充为扩域$\mathbf{K}(u)$ 到$\mathbf{L}(v)$ 的同构$\varphi$, 并将$u$ 映到$v = \varphi(u)$.

**证** 考虑$\mathbf{K}(u)$ 到$\mathbf{L}(v)$ 的映射

$$\varphi : \frac{h(u)}{g(u)} \longrightarrow \frac{\sigma(h)(v)}{\sigma(g)(v)}.$$

这个$\varphi$ 是$\mathbf{K}(u)$ 到$\mathbf{L}(v)$ 的同构, 且满足$\varphi|_{\mathbf{K}} = \sigma$, $\varphi(u) = v$. 事实上, 只需说明$\varphi$ 是一对一的. 若$\sigma(h)(v) = 0$, 根据假设条件, 在情形(i), 有$\sigma(h) = 0$, 从而$h = 0$. 在情形(ii), 有$\sigma(f) \mid \sigma(h)$, 从而$f \mid h$, $h(u) = 0$. 定理成立. 证毕

**定理12.1.7** 设$\mathbf{E}$ 和$\mathbf{F}$ 都是域$\mathbf{K}$ 的扩域, $u \in \mathbf{E}$ 以及$v \in \mathbf{F}$. 则$u$ 和$v$ 是同一不可约多项式$f \in \mathbf{K}[x]$ 的根当且仅当存在一个$\mathbf{K}$ 的同构$\mathbf{K}(u) \cong \mathbf{L}(v)$, 其将$u$ 映到$v$.

**证** 取$\sigma = id_{\mathbf{K}}$ 为$\mathbf{K}$ 上的恒等变换, $\sigma$ 是$\mathbf{K}$ 到自身的同构, 且$\sigma(f) = f$. 应用定理12.1.6 即得到定理12.1.7 . 证毕

**定理12.1.8** 设$\mathbf{K}$ 是一个域, $f \in \mathbf{K}[x]$ 是次数为$n$ 的多项式. 则存在$\mathbf{K}$ 的单扩域$\mathbf{F} = \mathbf{K}(u)$ 使得

(i) $u \in \mathbf{F}$ 是$f$ 的根.

(ii) $[\mathbf{K}(u) : \mathbf{K}] \leq n$, 等式成立当且仅当$f$ 是$\mathbf{K}[x]$ 中的不可约多项式.

**证** 不妨设$f \in \mathbf{K}[x]$ 是不可约多项式, 根据定理11.4.4, 商环$\mathbf{K}[x]/(f)$ 是一个域. 考虑$\mathbf{K}[x]$ 到$\mathbf{K}[x]/(f) = \mathbf{F}$ 的自然同态

$$s : \ g(x) \longmapsto (g(x) \ (\mathrm{mod}\ f(x))).$$

易知, $s|_{\mathbf{K}}$ 是$\mathbf{K}$ 到$s(\mathbf{K})$ 的同构, 且$\mathbf{F}$ 是$s(\mathbf{K})$ 的扩域. 对于$x \in \mathbf{K}[x]$, 令$u = s(x)$, 我们有$\mathbf{F} = \mathbf{K}(u)$ 及$f(u) = 0$. (i) 成立. 从定理12.1.5 即可推出(ii) . 证毕

**推论** 设$\mathbf{K}$ 是一个域, $f \in \mathbf{K}[x]$ 是次数为$n$ 的不可约多项式. 设$\alpha$ 是$f(x)$ 的根, 则$\alpha$ 在$\mathbf{K}$ 上生成的域为$\mathbf{F} = \mathbf{K}(\alpha)$, 且$[\mathbf{K}(\alpha) : \mathbf{K}] = n$.

# 12.2 Galois 基本定理

## 12.2.1 K-同构

本小节先讨论$K-$同构及其性质. 本小节先讨论$K-$同构及其性质.

**定义12.2.1** 设$\mathbf{E}$ 和$\mathbf{F}$ 是$\mathbf{K}$ 的扩域. 一个非零映射$\sigma : \mathbf{E} \to \mathbf{F}$ 叫做**K-同态**, 如果$\sigma$ 是一个域同态, 且$\sigma$ 在$\mathbf{K}$ 上为恒等映射. 特别, 当$\sigma$ 是一个域同构时, $\sigma$ 叫做**K-同构**.

**注** K-同态和K-同构都要求$\mathbf{K}$ 中的元素是不变元, 即在同态或同构映射下保持不变.

一个自同构$\sigma : \mathbf{F} \to \mathbf{F}$ 叫做**K-自同构**, 如果$\sigma$ 是K-同构. $\mathbf{F}$ 的所有K-自同构组成的群叫做$\mathbf{F}$ 在$\mathbf{K}$ 上的**伽略华(Galois)群**, 记为$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$.

对于中间域$\mathbf{E}$ : $\mathbf{K} \subset \mathbf{E} \subset F$, 也有$\mathbf{F}$ 在$\mathbf{E}$ 上的伽略华(Galois)群$\mathrm{Aut}_{\mathbf{E}}\mathbf{F}$.

**定理12.2.1** 设$\mathbf{F}$是$\mathbf{K}$的扩域, $f \in \mathbf{K}[x]$. 如果$u \in \mathbf{F}$是$f$的根, $\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$, 则$\sigma(u)$也是$f$的根.

**证** 设$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{K}[x]$. 对于$u \in \mathbf{F}$及$\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$, 我们有

$$\begin{aligned} \sigma(f(u)) &= \sigma(a_n)\sigma(u)^n + \cdots + \sigma(a_1)\sigma(u) + \sigma(a_0) \\ &= a_n\sigma(u)^n + \cdots + a_1\sigma(u) + a_0 \\ &= f(\sigma(u)). \end{aligned}$$

因此, 当$f(u) = 0$, 有$f(\sigma(u)) = 0$. 定理成立. 证毕

为了更清楚地描述Galois 基本定理关于有限域的中间域与其Galois 群的子群之间的关系, 我们引进符号:

设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $\mathbf{E}$ 是中间域, 设$H$ 是$G = \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的子群. 我们定义

$$I(H) = \{v \in \mathbf{F} \mid \sigma(v) = v,\ \sigma \in H\} \tag{7}$$

和

$$A(\mathbf{E}) = \{\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F} \mid \sigma(u) = u,\ u \in \mathbf{E}\} \tag{8}$$

$I(H)$ 是由$\mathbf{F}$ 中在子群$H$ 中的自同构下保持不变的元素组成的集合. 下面的定理12.2.2 (i) 将证明$I(H)$ 是扩域$\mathbf{F}$ 的中间域. 易知,

$$I(G) = \mathbf{K}, \quad I(\{e\}) = \mathbf{F}.$$

$A(\mathbf{E})$ 是由$G = \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 中使得中间域$\mathbf{E}$ 中元素保持不变的自同构组成的集合. 下面的定理12.2.2 (ii) 将证明$I(H)$ 是$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的子群. 易知,

$$A(\mathbf{F}) = \{e\}, \quad A(\mathbf{K}) = G.$$



**定理12.2.2** 设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $\mathbf{E}$ 是中间域以及$H$ 是$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的子群. 则

(i) $I(H)$ 是扩域$\mathbf{F}$ 的中间域.

(ii) $A(\mathbf{E})$ 是$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的子群.

**证** (i) (1)先证明$I(H)$是$\mathbf{F}$的子环. 事实上,对任意$a, b \in I(H)$, 以及对任意$\sigma \in H$, 有

$$\sigma(a-b) = \sigma(a) - \sigma(b) = a - b,$$

所以, $a - b \in I(H)$. 又

$$\sigma(ab) = \sigma(a)\sigma(b) = ab,$$

所以$ab \in I(H)$.

(2)$I(H)$ 有单位元为$e$. 事实上,对任意$\sigma \in H$, 有$\sigma(e) = e$.

(3) 最后证明$I(H)$ 中的非零元都是可逆元. 事实上, 对于$I(H)$中任一非零元$a$, 以及对任意$\sigma \in H$, 有

$$a\sigma(a^{-1}) = \sigma(a)\sigma(a^{-1}) = \sigma(aa^{-1}) = \sigma(e) = e,$$

以及

$$\sigma(a^{-1})a = \sigma(a^{-1})\sigma(a) = \sigma(a^{-1}a) = \sigma(e) = e.$$

所以$\sigma(a^{-1}) = a^{-1}$, $a^{-1} \in I(H)$.

因此, $I(H)$ 是$\mathbf{F}$ 的子域.

(ii) 要证$A(\mathbf{E})$ 是$Aut_{\mathbf{K}}\mathbf{F}$的子群. 事实上, 对任意$\sigma, \tau \in A(\mathbf{E})$, 有

$$(\sigma\tau^{-1})(u) = \sigma(\tau^{-1}(\tau(u))) = \sigma(u) = u, \quad u \in \mathbf{E}$$

因此, $\sigma\tau^{-1} \in A(\mathbf{E})$. 证毕

中间域$I(H)$ 叫做$H$ 在$\mathbf{F}$ 中的**不变域**.

我们进一步讨论不变域的性质.

**引理12.2.1** 设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $\mathbf{E}$, $\mathbf{E}_1$, $\mathbf{E}_2$ 是中间域. 设$H$, $H_1$, $H_2$ 是$G = \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的子群. 则

i) $I(G) = \mathbf{K}$, $I(\{e\}) = \mathbf{F}$.

ii) $A(\mathbf{F}) = \{e\}$, $A(\mathbf{K}) = G$.

iii) 若$H_1 < H_2$, 则$I(H_1) \supset I(H_2)$.

iv) 若$\mathbf{E}_1 \subset \mathbf{E}_2$, 则$A(\mathbf{E}_1) > A(\mathbf{E}_2)$.

v) $H < A(I(H))$.

vi) $\mathbf{E} \subset I(A(\mathbf{E}))$.

vii) $I(H) = I(A(I(H)))$.

viii) $A(\mathbf{E}) = A(I(A(\mathbf{E})))$.

ix) 若$\mathbf{E} = I(A(\mathbf{E}))$ , 则$H = A(\mathbf{E})$ 满足$\mathbf{E} = I(H)$, 且$H = A(I(H))$.

v) 若$H = A(I(H))$ , 则$\mathbf{E} = I(H)$ 满足$H = A(\mathbf{E})$, 且$\mathbf{E} = I(A(\mathbf{E}))$ .

**证** 根据定义, 直接得到i), ii).

iii) 设$H_1 < H_2$. 则对任意的$v \in I(H_2)$, 有

$$\sigma(v) = v, \quad \sigma \in H_2,$$

当然有 $\sigma(v) = v, \quad \sigma \in H_1$

因此, $v \in I(H_1)$, $I(H_2) \subset I(H_1)$.

iv) 设$\mathbf{E}_1 \subset \mathbf{E}_2$. 则对任意的$\sigma \in A(\mathbf{E}_2)$, 有

$$\sigma(v) = v, \quad v \in \mathbf{E}_2,$$

当然有 $\sigma(v) = v, \quad v \in \mathbf{E}_1$

因此, $\sigma \in A(\mathbf{E}_1)$, $A(\mathbf{E}_2) < A(\mathbf{E}_1)$.

v) 对任意的$\sigma \in H$, 以及任意$v \in I(H)$ , 有

$$\sigma(v) = v, \quad v \in I(H),$$

这意味着$\sigma \in A(I(H))$, $H \subset A(I(H))$.



vi) 对任意的$v \in \mathbf{E}$, 以及任意$\sigma \in A(\mathbf{E})$ , 有

$$\sigma(v) = v, \quad \sigma \in A(\mathbf{E}),$$

这意味着$v \in I(A(\mathbf{E})), E \subset I(A(\mathbf{E}))$.

vii) 由v) 和iii) 推出 $I(A(I(H))) \subset I(H)$.

而在vi) 中取$\mathbf{E} = I(H)$, 得

$$I(H) \subset I(A(I(H))).$$

故$I(H) = I(A(I(H)))$.

viii) 由vi) 和iv) 推出 $A(I(A(\mathbf{E}))) < A(\mathbf{E})$.

而在v) 中取$H = A(\mathbf{E})$, 得

$$A(\mathbf{E}) < A(I(A(\mathbf{E}))).$$

故$A(\mathbf{E}) = A(I(A(\mathbf{E})))$. 证毕

**定义12.2.2** 设$\mathbf{F}$是$\mathbf{K}$的扩域. $\mathbf{F}$叫做**K-的Galois 扩张**, 如果Galois群$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$的不变域是$\mathbf{K}$.

对于中间域$\mathbf{E}$: $\mathbf{K} \subset \mathbf{E} \subset F$, $\mathbf{F}$叫做**E-的Galois 扩张**, 如果Galois群$\mathrm{Aut}_{\mathbf{E}}\mathbf{F}$的不变域是$\mathbf{E}$.

**注1**

- 设域$\mathbf{F}$是$\mathbf{K}$的Galois 扩张, 则对于任意的$u \in \mathbf{F} \setminus \mathbf{K}$, 存在$\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$使得$\sigma(u) \neq u$.
- 设域$\mathbf{F}$是$\mathbf{E}$的Galois 扩张, 则对于任意的$u \in \mathbf{F} \setminus \mathbf{E}$, 存在$\sigma \in \mathrm{Aut}_{\mathbf{E}}\mathbf{F}$使得$\sigma(u) \neq u$.

**注2** 给定$\mathbf{E}$, 可得$A(\mathbf{E})$, 进而得$I(A(\mathbf{E}))$, 它使得$A(\mathbf{E}) = \mathrm{Aut}_{I(A(\mathbf{E}))}\mathbf{F}$. 因此,

$$A(E) = \mathrm{Aut}_{\mathbf{E}}\mathbf{F} \Longleftrightarrow I(A(\mathbf{E})) = \mathbf{E}.$$

这意味着, $E$有Galois 子群$\mathrm{Aut}_{\mathbf{E}}\mathbf{F}$的充要条件是$I(A(\mathbf{E})) = \mathbf{E}$.

**注3** 给定$H < G$, 可得$I(H)$, 进而得$A(I(H))$, 它使得$A(I(H)) = \mathrm{Aut}_{I(H)}\mathbf{F}$, 因此,

$$H = \mathrm{Aut}_{I(H)}\mathbf{F} \Longleftrightarrow A(I(H)) = H$$

这意味着, $H$ 是其不变域$I(H)$ 上Galois 子群$\mathrm{Aut}_{I(H)}\mathbf{F}$ 的充要条件是$A(I(H)) = H$.

中间域$\mathbf{E}$ 叫做闭的, 如果$\mathbf{E} = I(A(\mathbf{E}))$.

$$\begin{array}{ccc} \mathbf{E} & \subset & I(A(\mathbf{E})) \\ \downarrow & \nearrow & \downarrow \\ A(\mathbf{E}) & = & A(I(A(\mathbf{E}))) \end{array}$$

例如, $\mathbf{K}$ 和$\mathbf{F}$ 都是闭域.

子群$H$ 叫做闭的, 如果$H = A(I(H))$.

$$\begin{array}{ccc} I(H) & = & I(A(I(H))) \\ \uparrow & \searrow & \uparrow \\ H & \subset & A(I(H)) \end{array}$$

例如, $\{e\}$ 和$G$ 都是闭子群.

此外,由引理12.2.1, 立得 $\mathbf{E} = I(A(\mathbf{E})) \Longleftrightarrow H = A(I(H))$.

根据引理12.2.1 vii) 和viii), 我们可推出:

**定理12.2.3** 设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域. 则在这个扩张的闭中间域与其Galois群$G = \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的闭子群之间存在一一对应的映射:

$$E \longmapsto A(E) = \mathrm{Aut}_{\mathbf{E}}\mathbf{F}.$$

定理12.2.1 可以推广为:

**定理12.2.4** 设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $\mathbf{E}$ 是$\mathbf{F}$ 的中间域, $f \in \mathbf{E}[x]$. 如果$u \in \mathbf{F}$ 是$f$ 的根, $\sigma \in A(\mathbf{E})$, 则$\sigma(u)$ 也是$f$ 的根.

**证** 设$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{E}[x]$. 对于$u \in \mathbf{F}$ 及$\sigma \in A(\mathbf{E})$, 我们有

$$\sigma(f(u)) = \sigma(a_n)\sigma(u)^n + \cdots + \sigma(a_1)\sigma(u) + \sigma(a_0) = a_n\sigma(u)^n + \cdots + a_1\sigma(u) + a_0 = f(\sigma(u)).$$

因此, 当$f(u) = 0$, 有$f(\sigma(u)) = 0$. 定理成立. 证毕

### 12.2.2 Galois 基本定理

现在我们给出Galois 基本定理:

**定理12.2.5** (Galois 理论的基本定理) 如果$\mathbf{F}$ 是$\mathbf{K}$ 的有限维Galois扩张, 则在所有中间扩域集到Galois 群$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的所有子群集之间存在一个一一对应的映射

$$\mathbf{E} \longmapsto A(\mathbf{E}) = \mathrm{Aut}_{\mathbf{E}}\mathbf{F} \tag{9}$$

使得: (i) $\mathbf{F}$ 是每个中间域$\mathbf{E}$ 上的Galois 域.

(ii) 两个中间域$\mathbf{E}_1 \subset \mathbf{E}_2$ 的相关维数$[\mathbf{E}_2 : \mathbf{E}_1]$ 等于对应子群$A(\mathbf{E}_1) > A(\mathbf{E}_2)$ 的相关指标$[A(\mathbf{E}_1) : A(\mathbf{E}_2)]$, 特别, $\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 有阶$[\mathbf{F} : \mathbf{K}]$.

(iii) 中间域$\mathbf{E}$ 是$\mathbf{K}$ 上的Galois 域当且仅当对应的子群$A(\mathbf{E}) = \mathrm{Aut}_{\mathbf{E}}\mathbf{F}$ 是$G = \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的正规子群, 在这个情况下, $G/A(\mathbf{E})$ (同构意义下) 是$\mathbf{E}$ 在$\mathbf{K}$ 上的Galois 群$\mathrm{Aut}_{\mathbf{K}}\mathbf{E}$.

在给出Galois 基本定理的证明之前, 我们先讨论几个引理.

**引理12.2.2** 设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $\mathbf{E}_1$, $\mathbf{E}_2$ 是中间域, 且$\mathbf{E}_1 \subset \mathbf{E}_2$ . 如果$[\mathbf{E}_2 : \mathbf{E}_1]$ 有限, 则

$$[A(\mathbf{E}_1) : A(\mathbf{E}_2)] \leq [\mathbf{E}_2 : \mathbf{E}_1]. \tag{10}$$

特别地, 如果$[\mathbf{F} : \mathbf{K}]$ 有限, $|\mathrm{Aut}_{\mathbf{K}}\mathbf{F}| \leq [\mathbf{F} : \mathbf{K}]$.

**注** 这意味着: 在变换$A$ 下, 子群之间的指标不会增加.

**证** 对$n = [\mathbf{E}_2 : \mathbf{E}_1]$ 用数学归纳法. $n = 1$ 时, 命题显然成立. $n > 1$ 时, 假设命题对所有$i < n$ 都成立. 取$u \in \mathbf{E}_2, u \notin \mathbf{E}_1$. 因为$[\mathbf{E}_2 : \mathbf{E}_1]$ 有限, 所以$u$ 是$\mathbf{E}_1$ 上的代数元, $u$ 的定义多项式$f(x) \in \mathbf{E}_1[x]$ 具有次数$k > 1$. 考虑如下的中间域及相应的子群:

$$\begin{array}{ccccc} \mathbf{E_1} & \subset & E_1(u) & \subset & \mathbf{E}_2 \\ \downarrow & & \downarrow & & \downarrow \\ A(\mathbf{E_1}) & > & A(E_1(u)) & > & A(\mathbf{E}_2) \end{array}$$

分两种情形. 若$k < n$, 则$1 < n/k < n$. 根据归纳假设, 我们有

$$[A(\mathbf{E}_1) : A(\mathbf{E}_1(u))] \leq [\mathbf{E}_2 : \mathbf{E}_1(u)], \quad [A(\mathbf{E}_1(u)) : A(\mathbf{E}_2)] \leq [\mathbf{E}_2 : \mathbf{E}_1(u)].$$

从而

$$\begin{aligned} [A(\mathbf{E}_1) : A(\mathbf{E}_2)] &\leq [A(\mathbf{E}_1) : A(\mathbf{E}_1(u))] \cdot [A(\mathbf{E}_1(u)) : A(\mathbf{E}_2)] \\ &\leq [\mathbf{E}_2 : \mathbf{E}_1(u)][\mathbf{E}_1(u) : \mathbf{E}_1] \\ &\leq [\mathbf{E}_2 : \mathbf{E}_1(u)]. \end{aligned}$$

若$k = n$, 则$[\mathbf{E}_2 : \mathbf{E}_1(u)] = 1$, 即有$\mathbf{E}_2 = \mathbf{E}_1(u)$. 由定理12.2.4, 可构造商集$A(\mathbf{E}_1)/A(\mathbf{E}_2)$ 到$f$ 在$\mathbf{F}$ 中的根集$\mathrm{Roots}(f)_{\mathbf{F}} = \{v \in \mathbf{F} \mid f(v) = 0\}$ 的映射: $\varphi : \sigma \cdot A(\mathbf{E}_2) \longmapsto \sigma(u)$

$\varphi$ 是一对一的. 事实上, 若 $\varphi(\sigma_1 A(\mathbf{E}_2)) = \varphi(\sigma_2 A(\mathbf{E}_2))$,
则$\sigma_1(u) = \sigma_2(u)$. 从而, $\sigma_2^{-1}\sigma_1(u) = u$, $\sigma_2^{-1}\sigma_1 \in A(\mathbf{E}_1(u)) = A(\mathbf{E}_2)$.
由此得到$\sigma_1 A(\mathbf{E}_2) = \sigma_2 A(\mathbf{E}_2)$.

因为$\varphi$ 是一对一的, 所以$|A(\mathbf{E}_1)/A(\mathbf{E}_2)| \leq |\mathrm{Roots}(f)_{\mathbf{F}}|$. 而$|\mathrm{Roots}(f)_{\mathbf{F}}| \leq n$. 故

$$[A(\mathbf{E}_1) : A(\mathbf{E}_2)] = |A(\mathbf{E}_1)/A(\mathbf{E}_2)| \leq n = [\mathbf{E}_2 : \mathbf{E}_1].$$

特别地, 令$\mathbf{E}_1 = \mathbf{K}$, $\mathbf{E}_2 = \mathbf{F}$. 我们有

$$|\mathrm{Aut}_{\mathbf{K}}\mathbf{F}| = [\mathrm{Aut}_{\mathbf{K}}\mathbf{F} : \{e\}] = [A(\mathbf{K}) : A(\mathbf{F})] \leq [\mathbf{F} : \mathbf{K}].$$

证毕

**引理12.2.3** 设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域. 设$H_1,\ H_2$ 是$G = \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的子群, 且$H_1 < H_2$. 如果$[H_2 : H_1]$ 有限, 则

$$[I(H_1)) : I(H_2)] \leq [H_2 : H_1]. \tag{11}$$

**注** 这意味着: 在变换$I$ 下, 子空间之间的维数不会增加.

**证** 反证法. 设$[H_2 : H_1] = n$, $[I(H_1)) : I(H_2)] > n$. 则存在$u_1, u_2, \ldots, u_n, u_{n+1} \in I(H_1)$, 它们在$I(H_2)$ 上线性无关. 设$H_2/H_1$ 中的代表元为$\sigma_1 \in H_1, \sigma_2, \ldots, \sigma_n$. 在$\mathbf{F}$ 中考虑$n+1$ 元的$n$ 个方程的齐次方程组:

$$\begin{cases} \sigma_1(u_1)\,x_1 + \sigma_1(u_2)\,x_2 + \cdots + \sigma_1(u_n)\,x_n + \sigma_1(u_{n+1})\,x_{n+1} = 0 \\ \sigma_2(u_1)\,x_1 + \sigma_2(u_2)\,x_2 + \cdots + \sigma_2(u_n)\,x_n + \sigma_2(u_{n+1})\,x_{n+1} = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cdots \\ \sigma_n(u_1)\,x_1 + \sigma_n(u_2)\,x_2 + \cdots + \sigma_n(u_n)\,x_n + \sigma_n(u_{n+1})\,x_{n+1} = 0 \end{cases} \tag{12}$$

因为未知变量个数 $n+1$ 大于方程个数 $n$, 所以这个方程组有非零解$\xi$. 适当改变$\sigma_1, \sigma_2, \ldots, \sigma_n$ 的排序, 可设在所有非零解中, 有一组解$\xi = (a_1, a_2, \ldots, a_n, a_{n+1})$, 其不为零的分量$a_i$ 的个数最少. 不妨设

$$\xi_1 = (a_1, a_2, \ldots, a_r, 0, \ldots, 0)$$

其中 $(a_1 = 1,\ a_i \neq 0,\ 2 \leq i \leq r)$.

$$\begin{cases} \sigma_1(u_1)\,x_1+\sigma_1(u_2)\,x_2+\cdots+\sigma_1(u_n)\,x_n+\sigma_1(u_{n+1})\,x_{n+1}=0 \\ \sigma_2(u_1)\,x_1+\sigma_2(u_2)\,x_2+\cdots+\sigma_2(u_n)\,x_n+\sigma_2(u_{n+1})\,x_{n+1}=0 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\cdots \\ \sigma_n(u_1)\,x_1+\sigma_n(u_2)\,x_2+\cdots+\sigma_n(u_n)\,x_n+\sigma_n(u_{n+1})\,x_{n+1}=0 \end{cases} \tag{12}$$

现在, 我们构造一个$\tau \in H_2$, 使得

$$\xi_2 = (\tau(a_1), \tau(a_2), \ldots, \tau(a_r), 0, \ldots, 0)$$

是(12) 的解, 满足$\tau(a_2) \neq a_2$.

因为$\sigma_1 \in H_1$, 所以$\sigma_1(u_i) = u_i,\ 1 \leq i \leq n+1$. 由(12) 的第一个方程, 有

$$u_1a_1 + u_2a_2 + \cdots + u_ra_r = 0.$$

因为$u_1, u_2, \ldots, u_n, u_{n+1} \in I(H_1)$ 在$I(H_2)$ 上线性无关, 所以必有一个$a_i \notin I(H_2)$. (不妨设为$a_2$, 若必要就交换$u_1, u_2, \ldots, u_n, u_{n+1}$ 的次序) 这样, 存在$\tau \in H_2$, 使得$\tau(a_2) \neq a_2$.

现在考虑线性方程组:

$$\begin{cases} \tau\sigma_1(u_1)\,x_1 + \tau\sigma_1(u_2)\,x_2 + \cdots + \tau\sigma_1(u_n)\,x_n + \tau\sigma_1(u_{n+1})\,x_{n+1} = 0 \\ \tau\sigma_2(u_1)\,x_1 + \tau\sigma_2(u_2)\,x_2 + \cdots + \tau\sigma_2(u_n)\,x_n + \tau\sigma_2(u_{n+1})\,x_{n+1} = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cdots \\ \tau\sigma_n(u_1)\,x_1 + \tau\sigma_n(u_2)\,x_2 + \cdots + \tau\sigma_n(u_n)\,x_n + \tau\sigma_n(u_{n+1})\,x_{n+1} = 0 \end{cases} \tag{13}$$

因为$\xi_1 = (a_1, a_2, \ldots, a_r, 0, \ldots, 0)$是(12)的解, 所以$\xi_2 = (\tau(a_1), \tau(a_2), \ldots, \tau(a_r), 0, \ldots, 0)$是(13)的解.

注意到, $\tau \in H_2$时, $\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_n$也是$H_2/H_1$中的代表元. 这样, 对于$1 \le k \le n$, 有$\tau\sigma_k = \sigma_{i_k}\tau'$, $\tau' \in H_1$. 从而, 由$\tau'(u_j) = u_j$, $1 \le j \le n+1$, 得到 $\tau\sigma_k(u_j) = \sigma_{i_k}\tau'(u_j) = \sigma_{i_k}(u_j)$.

而$\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_n}$是$\sigma_1, \sigma_2, \ldots, \sigma_n$的一个排列, 所以方程组(13)与方程组(12)等价. 由此, $\xi_2$也是(12)的解. 从而,

$$\xi_2 - \xi_1 = (0, \tau(a_2) - a_2, \ldots, \tau(a_r) - a_r, 0, \ldots, 0)$$

是(12)的解. 这与$\xi$的非零分量个数最少的选取矛盾.

故$[I(H_1)) : I(H_2)] \le [H_2 : H_1]$. 证毕



**引理12.2.4** 设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $\mathbf{E}_1$, $\mathbf{E}_2$ 是中间域, 且$\mathbf{E}_1 \subset \mathbf{E}_2$ . 设$H_1$, $H_2$ 是$G = \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的子群, 且$H_1 < H_2$. 则

i) 若$\mathbf{E}_1$ 是闭的且$[\mathbf{E}_2 : \mathbf{E}_1]$有限, 那么$\mathbf{E}_2$ 是闭的, 且$[A(\mathbf{E}_1) : A(\mathbf{E}_2)] = [\mathbf{E}_2 : \mathbf{E}_1]$.

ii) 若$H_1$ 是闭的, 且$[H_2 : H_1]$ 有限, 那么$H_2$ 是闭的, 且$[I(H_1)) : I(H_2)] = [H_2 : H_1]$.

iii) 若$\mathbf{F}$ 是$\mathbf{K}$ 的有限维Galois 扩张, 那么每个中间域和其Galois 子群都是闭的, 且$Aut_{\mathbf{K}}\mathbf{F}$ 阶为$[\mathbf{F} : \mathbf{K}]$.

**证** i) 设$\mathbf{E}_1$ 是闭的, 则有$E_1 = I(A(\mathbf{E}_1))$, $E_2 \subset I(A(\mathbf{E}_2))$, 根据引理12.2.2 和引理12.2.3 , 有

$$\begin{aligned}[\mathbf{E}_2 : \mathbf{E}_1] &\leq [I(A(\mathbf{E}_2)) : \mathbf{E}_1] = [I(A(\mathbf{E}_2)) : I(A(\mathbf{E}_1))] \\ &\leq [A(\mathbf{E}_1) : A(\mathbf{E}_2)] \leq [\mathbf{E}_2 : \mathbf{E}_1].\end{aligned}$$

从而, $[I(A(\mathbf{E}_2)) : \mathbf{E}_2] = [I(A(\mathbf{E}_2)) : \mathbf{E}_1]/[\mathbf{E}_2 : \mathbf{E}_1] = 1$, $I(A(\mathbf{E}_2)) = \mathbf{E}_2$, 以及

$$[A(\mathbf{E}_1)) : A(\mathbf{E}_2)] = [\mathbf{E}_2 : \mathbf{E}_1].$$

ii) 设$H_1$ 是闭的,则 有$H_1 = A(I(H_1)), H_2 \subset A(I(H_2))$, 根 据 引理12.2.2 和引理12.2.3, 有

$$\begin{aligned}[H_2 : H_1] &\leq [A(I(H_2)) : H_1] = [A(I(H_2)) : A(I(H_1))] \\ &\leq [I(H_1) : I(H_2)] \leq [H_2 : H_1].\end{aligned}$$

从而, $[A(I(H_2)) : H_2] = [A(I(H_2)) : H_1]/[H_2 : H_1] = 1$, $A(I(H_2)) = H_2$, 以及

$$[I(H_1)) : I(H_2)] = [H_2 : H_1].$$

iii) 设$\mathbf{E}$ 是中间域. 因为$\mathbf{F}$ 是$\mathbf{K}$ 的有限维Galois 扩张, 所以$[\mathbf{E} : \mathbf{K}]$ 是有限的. 而$\mathbf{F}$ 在$\mathbf{K}$ 上是Galois 的, 因此, $\mathbf{K}$ 是闭的. 由i) 推出$\mathbf{E}$ 是闭的, 且$[A(\mathbf{K}) : A(\mathbf{E})] = [\mathbf{E} : \mathbf{K}]$. 特别, 当$\mathbf{E} = \mathbf{F}$ 时, 有

$$|\mathrm{Aut}_{\mathbf{K}}\mathbf{F}| = [\mathrm{Aut}_{\mathbf{K}}\mathbf{F} : \{e\}] = [A(\mathbf{K}) : A(\mathbf{F})] = [\mathbf{F} : \mathbf{K}]$$

是有限的. 从而$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的每个子群$H$ 是有限的. 因为$\{e\}$ 是闭的, 由ii) 得到$H$ 是闭的. 证毕

设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $\mathbf{E}$ 是中间域. 称$\mathbf{E}$ (对于$\mathbf{K}$ 和$\mathbf{F}$) 是稳定的, 如果每个$\mathbf{K}$-自同构$\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 在$\mathbf{E}$ 上的限制都是$\mathbf{E}$ 到$\mathbf{E}$ 自身的映射.

即: 对于$\mathbf{K}$-自同构$\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ ,

$$\sigma : \mathbf{F} \mapsto \mathbf{F} \Rightarrow \sigma|_{\mathbf{E}} : \mathbf{E} \mapsto \mathbf{E}.$$

由此, 可建立$\mathbf{F}$ 的稳定的中间域集$\{\mathbf{E}\}$ 到$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的正规子群集$\{A(\mathbf{E}) = \mathrm{Aut}_{\mathbf{E}}\mathbf{F}\}$ 之间的一一对应关系.

**引理12.2.5** 设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域.

i) 若$\mathbf{E}$ 是稳定的中间扩域, 那么$A(\mathbf{E}) = \mathrm{Aut}_{\mathbf{E}}\mathbf{F}$ 是Galois群$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$的正规子群;

ii) 若$H$ 是$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的正规子群,那么$H$ 的不变域$I(H)$ 是稳定的中间扩域.

**证** i) 设$u \in \mathbf{E}$, $\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$. 根据$\mathbf{E}$ 的稳定性, 有$\sigma(u) \in \mathbf{E}$, 从而, 对于每个$\tau \in A(E)$, 有$(\tau\sigma)(u) = \tau(\sigma(u)) = \sigma(u)$. 因此, 对于任意的$\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ , $\tau \in A(\mathbf{E})$, 以及$u \in \mathbf{E}$, 有

$$(\sigma^{-1}\tau\sigma)(u) = \sigma^{-1}(\tau\sigma(u)) = \sigma^{-1}(\sigma(u)) = u.$$

从而, $\sigma^{-1}\tau\sigma \in A(\mathbf{E})$. $A(\mathbf{E})$ 是$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$的正规子群.

ii) 设$H$ 是$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的正规子群, 那么对任意的$\tau \in H$, $\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ , 有$\sigma^{-1}\tau\sigma \in H$. 因此, 对于任意的$u \in I(H)$, 有$\sigma^{-1}\tau\sigma(u) = u$. 从而, $\tau(\sigma(u)) = \sigma(u)$. 故$\sigma(u) \in I(H)$, $I(H)$ 是稳定的中间扩域. 证毕

**引理12.2.6** 若F 是K 的Galois 扩域, 且E 是稳定的中间扩域, 则E 也是K 的Galois 扩张.

**证** 对于$u \in \mathrm{E} \setminus \mathrm{K}$, 由F 是K 的Galois 扩域, 知存在$\sigma \in \mathrm{Aut}_{\mathrm{K}}\mathrm{F}$, 使得$\sigma(u) \neq u$. 但E 是稳定的, 从而$\sigma|_{\mathrm{E}} \in \mathrm{Aut}_{\mathrm{K}}\mathrm{E}$, 使得$\sigma(u) \neq u$. 因此, E 也是K 的Galois 扩张. 证毕

**引理12.2.7** 若$\mathbf{F}$ 是$\mathbf{K}$ 的某个扩域, $\mathbf{E}$ 是一个中间扩域, 且$\mathbf{E}$ 是$\mathbf{K}$ 的代数扩张和Galois扩张, 那么$\mathbf{E}$ (相对于$\mathbf{F}$ 和$\mathbf{K}$ ) 是稳定的.

**注** 假设条件: $\mathbf{E}$ 是$\mathbf{K}$ 的代数扩张, 是不可缺少的.

**证** 设$u \in \mathbf{E}$, $f \in \mathbf{K}[x]$ 是$u$ 的定义多项式. 令$u_1 = u, u_2, \ldots, u_r$ 是$f$ 在$\mathbf{E}$ 中的不同的根, 则$r \leq \deg f = n$. 如果$\tau \in \mathrm{Aut}_{\mathbf{K}}\mathbf{E}$, 则$\{u_1, u_2, \ldots, u_r\}$ 在$\tau$ 下的像$\{\tau(u_1), \tau(u_2), \ldots, \tau(u_r)\}$ 是$\{u_1, u_2, \ldots, u_r\}$ 的一个置换, 从而, $\mathbf{E}[x]$ 中的多项式$g(x) = (x-u_1)(x-u_2)\cdots(x-u_r)$ 在$\tau$ 的作用下保持不变. 因为, $\mathbf{E}$ 在$\mathbf{K}$ 上是Galois 扩张, 所以$g(x) \in \mathbf{K}[x]$.

由$u_1 = u$ 是$g(x)$ 的根, 得到$f \mid g$. 因为$g$ 是首一多项式,且$\deg g \leq \deg f$, 所以$f = g$, $f$ 的所有根是两两不同的, 且都落在$\mathbf{E}$ 中.

现在, 对于$\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$, 有$\sigma(u)$ 是$f$ 的根, 从而$\sigma(u) \in \mathbf{E}$ . 因此, $\mathbf{E}$ (相对于$\mathbf{F}$ 和$\mathbf{K}$ ) 是稳定的. 证毕



设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $\mathbf{E}$ 是稳定的中间扩域. $\mathbf{K}$-自同构$\tau \in \mathrm{Aut}_{\mathbf{K}}\mathbf{E}$ 叫做可拓展到$\mathbf{F}$, 如果存在$\sigma \in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ , 使得$\sigma|_{\mathbf{E}} = \tau$. 易知, 可拓展的$\mathbf{K}-$ 自同构全体所组成的集合是$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的子群. 特别, 当$\mathbf{E}$ 是稳定时, $A(E) = \mathrm{Aut}_{\mathbf{E}}\mathbf{F}$ 是$G = \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 的正规子群, 从而可以定义商群$G/A(E)$.

**引理12.2.8** 设$\mathbf{F}$ 是$\mathbf{K}$ 的扩域, $\mathbf{E}$ 是稳定的中间扩域, 那么商群$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}/\mathrm{Aut}_{\mathbf{E}}\mathbf{F}$ 同构于可拓展到$\mathbf{F}$ 的$\mathbf{E}$ 的所有$\mathbf{K}$ -自同构所组成的群.

**证** 因为$\mathbf{E}$ 是稳定的中间扩域, 所以映射$\varphi : \sigma \longmapsto \sigma|_{\mathbf{E}}$ 是$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$到$\mathrm{Aut}_{\mathbf{K}}\mathbf{E}$. 显然, 像集合是可拓展到$\mathbf{F}$ 的$\mathbf{K}$-自同构所构成的群, 而核是$\mathrm{Aut}_{\mathbf{E}}\mathbf{F}$ . 因此,商群$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}/\mathrm{Aut}_{\mathbf{E}}\mathbf{F}$ 同构于可拓展到$\mathbf{F}$ 的$\mathbf{E}$ 的所有$\mathbf{K}$ -自同构所组成的群. 证毕

## 12.2.3 基本定理之证明

**Galois 基本定理之证明**: 考虑$\mathbf{F}$ 的中间扩域集到Galois 群$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$的所有子群集之间的映射(9) $\varphi: E \longmapsto A(E)$. 根据引理12.2.1, 我们有

$$\begin{array}{ccccccc} \mathbf{K} & \subset & \mathbf{E} & \subset & I(A(\mathbf{E})) & \subset & \mathbf{F}. \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ A(\mathbf{K}) = Aut_{\mathbf{K}}\mathbf{F} & > & A(\mathbf{E}) & > & A(I(A(\mathbf{E}))) & > & A(\mathbf{F}) = \{id_{\mathbf{F}}\}. \end{array}$$

且$I(A(\mathbf{E})) = \mathbf{E}$ 的充要条件是$H = A(E)$ 满足$A(I(H)) = H$. 这表明(定理12.2.3 ): 闭的中间扩域和闭的Galois 子群之间存在着一个一一对应的关系.

又考虑关系式 $\mathbf{K} \subset \mathbf{E}_1 \subset \mathbf{E}_2 \subset \mathbf{F}$.

我们有(引理12.2.2)

$$[A(\mathbf{K}) : A(\mathbf{E}_1)] \leq [\mathbf{E}_1 : \mathbf{K}], \quad [A(\mathbf{E}_1) : A(\mathbf{E}_2)] \leq [\mathbf{E}_2 : \mathbf{E}_1].$$

因为$\mathbf{K}$ 是闭的, 且$\mathbf{E}_1$ 在$\mathbf{K}$ 上是有限维的(因为$\mathbf{F}$ 是有限维的), 所以$\mathbf{E}_1$ 是闭的, 根据引理12.2.4, 所有的中间域(包括$\mathbf{E}_2$) 和子群都是闭的, 这说明映射$\varphi$ 是一一对应的. 而且, $\mathbf{F}$ 是$\mathbf{E}$ 的Galois 扩张. 并且有$[A(\mathbf{E}_1) : A(\mathbf{E}_2)] = [\mathbf{E}_2 : \mathbf{E}_1]$.

(iii) 必要性. 假设$\mathbf{E}$ 是$\mathbf{K}$ 的Galois 扩张. 因为$\mathbf{F}$ 是有限维的, 所以根据$[\mathbf{F}:\mathbf{K}]=n$, 对任意$u\in F$, 都有$\{1_K,u,u^2,\cdots,u^{n-1}\}$ 成一线性相关组这一事实, 即可知$\mathbf{E}$ 是$\mathbf{K}$ 的代数扩张. 根据引理12.2.7, $\mathbf{E}$ 是稳定的. 即每个$\mathbf{K}$ 自同构$\sigma\in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 在$\mathbf{E}$ 上的限制$\sigma|_{\mathbf{E}}$ 是$\mathbf{E}$ 到自身的同构, 即$\sigma|_{\mathbf{E}}\in \mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ . 由引理12.2.5 i), $A(\mathbf{E})=\mathrm{Aut}_{\mathbf{E}}\mathbf{F}$ 在$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$中是正规的.

充分性. 假设$A(\mathbf{E})$ 在$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 中正规, 那么$I(A(\mathbf{E}))$是一个稳定中间域(引理12.2.5 ii)). 但所有中间域都是闭的, 因此$\mathbf{E}=I(A(\mathbf{E}))$ 是一个稳定中间域, 再由引理12.2.6, 得到$\mathbf{E}$ 是$\mathbf{K}$ 的Galois 域.

假设中间域$\mathbf{E}$ 是$\mathbf{K}$ 的Galois扩张, (从而$A(\mathbf{E})$在$\mathrm{Aut}_{\mathbf{K}}\mathbf{F}$ 中正规), 因为$\mathbf{E}$ 和$A(\mathbf{E})$ 都是闭的, 且$I(G) = \mathbf{K}$ ( $\mathbf{F}$ 是$\mathbf{K}$的Galois 扩张), 由引理12.2.4 得到

$$|G/A(E)| = [G : A(E)] = [I(A(E)) : I(G)] = [\mathbf{E} : \mathbf{K}].$$

由引理12.2.8 , $G/A(E) = \mathrm{Aut}_{\mathbf{K}}\mathbf{F}/\mathrm{Aut}_{\mathbf{E}}\mathbf{F}$ 和$\mathrm{Aut}_{\mathbf{K}}\mathbf{E}$ 的某个阶为$[\mathbf{E} : \mathbf{K}]$ 的子群同构, 但基本定理的i) 表明$|\mathrm{Aut}_{\mathbf{K}}\mathbf{E}| = [\mathbf{E} : \mathbf{K}]$ (因为$\mathbf{E}$ 是$\mathbf{K}$ 的Galois 扩张), 这说明$G/A(\mathbf{E}) \cong \mathrm{Aut}_{\mathbf{K}}\mathbf{E}$. 证毕

# 12.3 可分域 代数闭包

## 12.3.1 可分域

**定义12.3.1** 设$\mathbf{K}$ 是一个域, $f \in \mathbf{K}[x]$ 是次数$\geq 1$ 的多项式. $\mathbf{K}$ 的一个扩域$\mathbf{F}$ 叫做**多项式$f$ 在$\mathbf{K}$ 上的分裂域**, 如果$f$ 在$\mathbf{F}[x]$ 中可分解, 即

$$f(x) = \alpha(x - u_1)(x - u_2)\cdots(x - u_n),$$

且$\mathbf{F} = \mathbf{K}(u_1, \ldots, u_n)$, 其中$\alpha \in \mathbf{K}$, $u_1, \ldots, u_n$ 是$f$ 在$\mathbf{F}$ 中的根.

设$S$ 是$\mathbf{K}[x]$ 中一些次数$\geq 1$ 的多项式组成的集合. $\mathbf{K}$ 的一个扩域$\mathbf{F}$ 叫做**多项式集合$S$ 在$\mathbf{K}$ 上的分裂域**, 如果$S$ 中的每个多项式$f$ 在$\mathbf{F}[x]$ 中可分解, 且$\mathbf{F}$ 由$S$ 中的所有多项式的根在$\mathbf{K}$ 上生成.

**例12.3.1** 设$x^p - x$ 在$\mathbf{F}_p$ 的分裂域就是$\mathbf{F}_p$.

**证** 因为在$\mathbf{F}_p$ 上有$x^p - x = x(x-1)\cdots(x-(p-1))$.

**例12.3.2** 设$E$ 是$q$ 元有限域, 其素域是$\mathbf{F}_p$. 则$x^q - x$ 在$\mathbf{F}_p$ 的分裂域就是$\mathbf{E}$.

**定理12.3.1** 设$\mathbf{K}$ 是一个域, $f \in \mathbf{K}[x]$ 的次数为$n \geq 1$. 则存在$f$ 一个分裂域$\mathbf{F}$ 具有$[\mathbf{F} : \mathbf{K}] \leq n!$.

**证** 我们对$n = \deg\ f$ 作数学归纳法.

如果$n = 1$, 或如果$\mathbf{F}$ 在$\mathbf{K}$ 上可分解, 则$\mathbf{F} = \mathbf{K}$ 是分裂域.

如果$n > 1$, $f$ 在$\mathbf{K}$ 上不能分解, 设$g \in \mathbf{K}[x]$ 是$f$ 的次数大于1 的不可约因式. 则存在$K$ 的一个简单扩张$\mathbf{K}(u)$ 使得$u$ 是$g$ 的根, 且$[\mathbf{K}(u) : \mathbf{K}] = \deg\ g > 1$. 因此, 在$\mathbf{K}(u)[x]$ 中有分解式$f(x) = (x-u)h(x)$, 其中$\deg\ h = n-1$. 由归纳假设, 存在一个$h$ 在$\mathbf{K}(u)$ 上的维数$\leq (n-1!)$ 的分裂域$F$. 易知, $\mathbf{F}$ 在$K$ 上的次数$[\mathbf{F} : \mathbf{K}] = [\mathbf{F} : \mathbf{K}(u)][\mathbf{K}(u) : \mathbf{K}] \leq (n-1)!n = n!$. 证毕

## 12.3.2 代数闭包

下面讨论不能进行代数扩张的域, 也是一个在该域上的多项式总有解的域.

**定理12.3.2** 在域$\mathbf{F}$ 上的如下条件等价:

(i) 每个非常数多项式$f \in \mathbf{F}[x]$ 在$\mathbf{F}$ 中有根.

(ii) 每个非常数多项式$f \in \mathbf{F}[x]$ 在$\mathbf{F}$ 中可分解.

(iii) 每个不可约多项式$f \in \mathbf{F}[x]$ 的次数为一.

(iv) 不存在$\mathbf{F}$ 的代数扩张(除了$\mathbf{F}$ 自己以外).

**证** (i) 推(ii). 对$f$ 的次数$\deg\ f = n$ 作数学归纳法.

$n = 1$ 时, $f(x)$ 为一次多项式, 结论成立.

假设结论对次数$\leq n-1$ 的多项式成立.

对于非零$n \geq 2$ 次多项式$f(x)$, 由(i), $f(x)$ 在$\mathbf{F}$ 中有根$x = a$. 根据定理12.3.1 之推论2, 我们有$x - a \mid f(x)$, 或$f(x) = f_1(x)(x-a)$, 其中$\deg\ f_1 = n-1$. 根据归纳假设, $f_1(x)$ 在$\mathbf{F}$ 中可分解. 故$f \in \mathbf{F}[x]$ 在$\mathbf{F}$ 中可分解.

(ii) 推(iii). 结论显然成立.

(iii) 推(iv). 设$\mathbf{E}$ 是$\mathbf{F}$ 的一个代数扩张, 则对于任意$u \in \mathbf{E}$, 因为$u$ 是$\mathbf{F}$ 上的代数元, 定理12.1.5, 存在不可约多项式$f(x) \in \mathbf{F}[x]$ 使得$f(u) = 0$. 根据(iii), $f(x) = a_1x + a_2,\ a_1, a_2 \in \mathbf{F}$. 从而, $u = -a_2/a_1 \in \mathbf{F}$. 这说明, $\mathbf{E} \subset \mathbf{F},\ \mathbf{E} = \mathbf{F}$. 结论成立.

(iv) 推(i). 设$f(x)$ 是$\mathbf{F}$ 上的非常数多项式, 根据定理12.1.5, 存在$f(x)$ 的一个根$u$, 使得$\mathbf{F}(u)$ 为$\mathbf{F}$ 的代数扩张. 根据(iv), $\mathbf{F}(u) = \mathbf{F}$. 因此, $u \in \mathbf{F}$. 结论成立. 证毕



**定义12.3.2** 设F 是一个域. F 叫做**代数闭包**, 如果域F 满足定理12.3.2 的等价条件.

**定义12.3.3** 设K 是一个域, $f$ 是K 上的不可约多项式. 如果$F$ 是$f$ 在K 上的一个分裂域, 且$f$ 在$F$ 中的根都是单根, 则称$f$ 是**可分**的.

**定义12.3.4** 设F 是域K 的一个扩域, $u$ 是K 上的代数数. 如果$u$ 在$K$ 上的定义多项式是可分的, 则称$u$ 在K 上是可分的. 如果$F$ 中的每个元素$u$ 在K 上都是可分的, 则称$F$ 为K 的**可分扩张**.