



网络空间安全学院

School of Cyberspace Security, BUPT

信息安全数学基础

—— 域

信数课题组

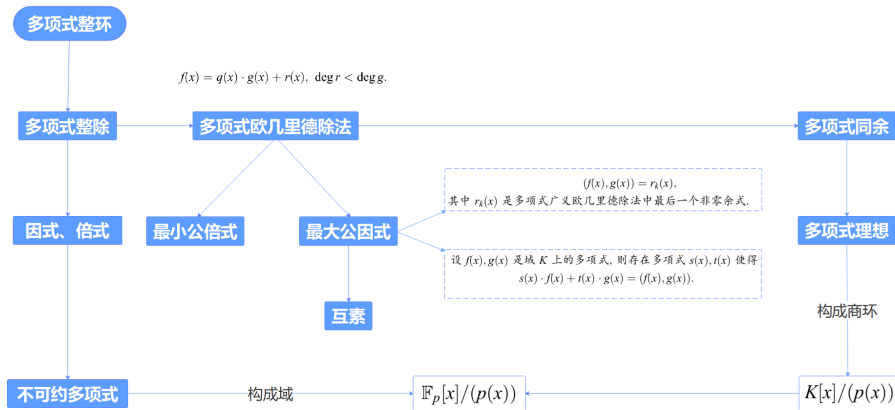
北京邮电大学

传邮万里

国脉所系



上次课回顾



目录

- ① 分式域
- ② 素域与扩域
 - 有限扩域
 - 代数扩域
- ③ Galois 基本定理
- ④ 有限域
 - 有限域的构造
 - 有限域的 Galois 群
 - 有限域的正规基

从整数集 \mathbb{Z} 构造出有理数集 \mathbb{Q} 是经典和重要的方法. 运用该方法可以从整环构造出对应的分式域.

为此, 我们首先介绍等价关系 R .

从整数集 \mathbb{Z} 构造出有理数集 \mathbb{Q} 是经典和重要的方法. 运用该方法可以从整环构造出对应的分式域.

为此, 我们首先介绍等价关系 R .

定理 8.1.1

设 A 是一个整环, 令 $E = A \times A^*$. 在 E 上定义关系 $R: (a, b)R(c, d)$, 如果 $ad = bc$, 则 R 是 E 上的等价关系, 即有

- (i) 自反性: 对任意 $(a, b) \in E$, 有 $(a, b)R(a, b)$.
- (ii) 对称性: 如果 $(a, b)R(c, d)$, 则 $(c, d)R(a, b)$.
- (iii) 传递性: 如果 $(a, b)R(c, d)$ 和 $(c, d)R(e, f)$, 则 $(a, b)R(e, f)$.

从整数集 \mathbb{Z} 构造出有理数集 \mathbb{Q} 是经典和重要的方法. 运用该方法可以从整环构造出对应的分式域.

为此, 我们首先介绍等价关系 R .

定理 8.1.1

设 A 是一个整环, 令 $E = A \times A^*$. 在 E 上定义关系 $R: (a, b)R(c, d)$, 如果 $ad = bc$, 则 R 是 E 上的等价关系, 即有

- (i) 自反性: 对任意 $(a, b) \in E$, 有 $(a, b)R(a, b)$.
- (ii) 对称性: 如果 $(a, b)R(c, d)$, 则 $(c, d)R(a, b)$.
- (iii) 传递性: 如果 $(a, b)R(c, d)$ 和 $(c, d)R(e, f)$, 则 $(a, b)R(e, f)$.

证: (i) 对任意 $(a, b) \in E$, 有 $ab = ba$, 所以 $(a, b)R(a, b)$.

从整数集 \mathbb{Z} 构造出有理数集 \mathbb{Q} 是经典和重要的方法. 运用该方法可以从整环构造出对应的分式域.

为此, 我们首先介绍等价关系 R .

定理 8.1.1

设 A 是一个整环, 令 $E = A \times A^*$. 在 E 上定义关系 $R: (a, b)R(c, d)$, 如果 $ad = bc$, 则 R 是 E 上的等价关系, 即有

- (i) 自反性: 对任意 $(a, b) \in E$, 有 $(a, b)R(a, b)$.
- (ii) 对称性: 如果 $(a, b)R(c, d)$, 则 $(c, d)R(a, b)$.
- (iii) 传递性: 如果 $(a, b)R(c, d)$ 和 $(c, d)R(e, f)$, 则 $(a, b)R(e, f)$.

证: (i) 对任意 $(a, b) \in E$, 有 $ab = ba$, 所以 $(a, b)R(a, b)$.

(ii) 由 $(a, b)R(c, d)$ 知, $ad = bc$, 再由交换性, $cb = da$. 故 $(c, d)R(a, b)$.

从整数集 \mathbb{Z} 构造出有理数集 \mathbb{Q} 是经典和重要的方法. 运用该方法可以从整环构造出对应的分式域.

为此, 我们首先介绍等价关系 R .

定理 8.1.1

设 A 是一个整环, 令 $E = A \times A^*$. 在 E 上定义关系 $R: (a, b)R(c, d)$, 如果 $ad = bc$, 则 R 是 E 上的等价关系, 即有

- (i) 自反性: 对任意 $(a, b) \in E$, 有 $(a, b)R(a, b)$.
- (ii) 对称性: 如果 $(a, b)R(c, d)$, 则 $(c, d)R(a, b)$.
- (iii) 传递性: 如果 $(a, b)R(c, d)$ 和 $(c, d)R(e, f)$, 则 $(a, b)R(e, f)$.

证: (i) 对任意 $(a, b) \in E$, 有 $ab = ba$, 所以 $(a, b)R(a, b)$.

(ii) 由 $(a, b)R(c, d)$ 知, $ad = bc$, 再由交换性, $cb = da$. 故 $(c, d)R(a, b)$.

(iii) 由 $(a, b)R(c, d)$, $(c, d)R(e, f)$ 知, $ad = bc, cf = de$, 进而 $adf = (bc)f = b(de)$, 即 $d(af - be) = 0$. 而 d 是整环 A 中的非零元, 则 $af = be$. 立得.

记 $\frac{a}{b} = C_{(a,b)} = \{(c,d) \in E \mid (c,d)R(a,b)\}$ 为 (a,b) 的等价类.

我们在商集 E/R 上定义加法和乘法如下:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

则 E/R 关于加法构成一个交换群, 零元为 $\frac{0}{1}$, $\frac{a}{b}$ 的负元为 $\frac{-a}{b}$.

$(E/R)^* = (E/R) \setminus \{\frac{0}{b}\}$ 关于乘法构成一个交换群, 单位元为 $\frac{1}{1}$, $\frac{a}{b}$ 的逆元为 $\frac{b}{a}$.

最后, E/R 关于加法和乘法满足分配律.

因此, E/R 构成一个域, 叫做 A 的分式域.

记 $\frac{a}{b} = C_{(a,b)} = \{(c,d) \in E \mid (c,d)R(a,b)\}$ 为 (a,b) 的等价类.
我们在商集 E/R 上定义加法和乘法如下:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

则 E/R 关于加法构成一个交换群, 零元为 $\frac{0}{1}$, $\frac{a}{b}$ 的负元为 $\frac{-a}{b}$.
 $(E/R)^* = (E/R) \setminus \{\frac{0}{b}\}$ 关于乘法构成一个交换群, 单位元为 $\frac{1}{1}$, $\frac{a}{b}$ 的逆元为 $\frac{b}{a}$.

最后, E/R 关于加法和乘法满足分配律.

因此, E/R 构成一个域, 叫做 A 的分式域.

定理 8.1.2

交换环 A 有分式域的充要条件是 A 是整环.

例 8.1.1 取 $A = \mathbb{Z}$, 则 \mathbb{Z} 是一个整环, 从而有分式域, 叫作 \mathbb{Z} 的有理数域, 记作 \mathbb{Q} . 其加法和乘法运算为

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

例 8.1.1 取 $A = \mathbb{Z}$, 则 \mathbb{Z} 是一个整环, 从而有分式域, 叫作 \mathbb{Z} 的有理数域, 记作 \mathbb{Q} . 其加法和乘法运算为

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

例 8.1.2 取 $A = \mathbb{Z}/p\mathbb{Z}$, 其中 p 为素数, 则 A 是一个整环, 从而有分式域, 叫作 $\mathbb{Z}/p\mathbb{Z}$ 的 p -元域, 记作 \mathbb{F}_p 或 $GF(p)$.

例 8.1.1 取 $A = \mathbb{Z}$, 则 \mathbb{Z} 是一个整环, 从而有分式域, 叫作 \mathbb{Z} 的有理数域, 记作 \mathbb{Q} . 其加法和乘法运算为

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

例 8.1.2 取 $A = \mathbb{Z}/p\mathbb{Z}$, 其中 p 为素数, 则 A 是一个整环, 从而有分式域, 叫作 $\mathbb{Z}/p\mathbb{Z}$ 的 p -元域, 记作 \mathbb{F}_p 或 $GF(p)$.

例 8.1.3 设 K 是一个域, 则 $A = K[x]$ 是一个整环, 从而有分式域, 叫作 $K[x]$ 的多项式分式域, 记作 $K(x)$, 即

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

其加法和乘法运算为

$$\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)g_2(x) + g_1(x)f_2(x)}{g_1(x)g_2(x)}, \quad \frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}.$$

上一章已经介绍了一般的域和子域的概念, 本节首先考虑“最小”的子域.

定义 8.2.1

如果一个域不含真子域, 则称其为素域.

上一章已经介绍了一般的域和子域的概念, 本节首先考虑“最小”的子域.

定义 8.2.1

如果一个域不含真子域, 则称其为素域.

例 8.2.1 有理数域 \mathbb{Q} 是素域. $F_p = \mathbb{Z}/p\mathbb{Z}$ 是素域.

上一章已经介绍了一般的域和子域的概念, 本节首先考虑“最小”的子域.

定义 8.2.1

如果一个域不含真子域, 则称其为素域.

例 8.2.1 有理数域 \mathbb{Q} 是素域. $F_p = \mathbb{Z}/p\mathbb{Z}$ 是素域.

定理 8.2.1

设 F 是一个域. 如果 F 的特征为 0, 则 F 有一个与 \mathbb{Q} 同构的素域.
如果 F 的特征为 p , 则 F 有一个与 F_p 同构的素域.

证: 略.

接下来, 从集合的包含关系角度讨论域的性质.

定义 8.2.2

设 F 是一个域. 如果 K 是 F 的子域, 则称 F 是 K 的扩域.

接下来, 从集合的包含关系角度讨论域的性质.

定义 8.2.2

设 F 是一个域. 如果 K 是 F 的子域, 则称 F 是 K 的扩域.

设 F 是一个域, $X \subset F$, 则包含 X 的所有子域的交集仍是包含 X 的子域, 叫作由 X 生成的子域.

如果 F 是 K 的扩域及 $X \subset F$, 则由 $K \cup X$ 生成的子域叫作 X 在 K 上生成的子域, 记作 $K(X)$.

如果 $X = \{u_1, \dots, u_n\}$, 则 F 的子域 $K(X)$ 记作 $K(u_1, \dots, u_n)$.

如果 $X = \{u\}$, 则 $K(u)$ 称为 K 的单扩域.

接下来, 从集合的包含关系角度讨论域的性质.

定义 8.2.2

设 F 是一个域. 如果 K 是 F 的子域, 则称 F 是 K 的扩域.

设 F 是一个域, $X \subset F$, 则包含 X 的所有子域的交集仍是包含 X 的子域, 叫作由 X 生成的子域.

如果 F 是 K 的扩域及 $X \subset F$, 则由 $K \cup X$ 生成的子域叫作 X 在 K 上生成的子域, 记作 $K(X)$.

如果 $X = \{u_1, \dots, u_n\}$, 则 F 的子域 $K(X)$ 记作 $K(u_1, \dots, u_n)$.

如果 $X = \{u\}$, 则 $K(u)$ 称为 K 的单扩域.

例 8.2.2 有理数域 \mathbb{Q} 是实数域 \mathbb{R} 和复数域 \mathbb{C} 的子域, 复数域 \mathbb{C} 是实数域 \mathbb{R} 的扩域, 实数域 \mathbb{R} 是有理数域 \mathbb{Q} 的扩域.

接下来, 从集合的包含关系角度讨论域的性质.

定义 8.2.2

设 F 是一个域. 如果 K 是 F 的子域, 则称 F 是 K 的扩域.

设 F 是一个域, $X \subset F$, 则包含 X 的所有子域的交集仍是包含 X 的子域, 叫作由 X 生成的子域.

如果 F 是 K 的扩域及 $X \subset F$, 则由 $K \cup X$ 生成的子域叫作 X 在 K 上生成的子域, 记作 $K(X)$.

如果 $X = \{u_1, \dots, u_n\}$, 则 F 的子域 $K(X)$ 记作 $K(u_1, \dots, u_n)$.

如果 $X = \{u\}$, 则 $K(u)$ 称为 K 的单扩域.

例 8.2.2 有理数域 \mathbb{Q} 是实数域 \mathbb{R} 和复数域 \mathbb{C} 的子域, 复数域 \mathbb{C} 是实数域 \mathbb{R} 的扩域, 实数域 \mathbb{R} 是有理数域 \mathbb{Q} 的扩域.

例 8.2.3 $F_{2^8} = F_2[x]/(x^8 + x^4 + x^3 + x + 1)$ 是 F_2 的扩域.

目录

- ① 分式域
- ② 素域与扩域
 - 有限扩域
 - 代数扩域
- ③ Galois 基本定理
- ④ 有限域
 - 有限域的构造
 - 有限域的 Galois 群
 - 有限域的正规基

再从线性空间角度讨论域的性质.

如果 F 是 K 的扩域, 则 $1_F = 1_K$. 而且, F 可作为 K 上的线性空间. 事实上, 对任意 $\alpha, \beta \in F, k \in K$, 有 $\alpha + \beta \in F, k \cdot \alpha \in F$.

用 $[F:K]$ 表示 F 在 K 上线性空间的维数. 如果 $[F:K]$ 是有限或无限的, 则称 F 是 K 的有限扩域或无限扩域.

再从线性空间角度讨论域的性质.

如果 F 是 K 的扩域, 则 $1_F = 1_K$. 而且, F 可作为 K 上的线性空间. 事实上, 对任意 $\alpha, \beta \in F, k \in K$, 有 $\alpha + \beta \in F, k \cdot \alpha \in F$.

用 $[F:K]$ 表示 F 在 K 上线性空间的维数. 如果 $[F:K]$ 是有限或无限的, 则称 F 是 K 的有限扩域或无限扩域.

定理 8.2.2

设 E 是 F 的扩域, F 是 K 的扩域, 则 $[E:K] = [E:F][F:K]$. 而且, 如果 $\{\alpha_i\}_{i \in I}$ 是 F 在 K 上的基底, $\{\beta_j\}_{j \in J}$ 是 E 在 F 上的基底, 则 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 是 E 在 K 上的基底.

再从线性空间角度讨论域的性质.

如果 F 是 K 的扩域, 则 $1_F = 1_K$. 而且, F 可作为 K 上的线性空间. 事实上, 对任意 $\alpha, \beta \in F, k \in K$, 有 $\alpha + \beta \in F, k \cdot \alpha \in F$.

用 $[F:K]$ 表示 F 在 K 上线性空间的维数. 如果 $[F:K]$ 是有限或无限的, 则称 F 是 K 的有限扩域或无限扩域.

定理 8.2.2

设 E 是 F 的扩域, F 是 K 的扩域, 则 $[E:K] = [E:F][F:K]$. 而且, 如果 $\{\alpha_i\}_{i \in I}$ 是 F 在 K 上的基底, $\{\beta_j\}_{j \in J}$ 是 E 在 F 上的基底, 则 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 是 E 在 K 上的基底.

证: 首先证明 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 是 E 在 K 上的生成元. 事实上, 对 $\forall c \in E$, 由 $\{\beta_j\}_{j \in J}$ 是 E 在 F 上的基底, 存在 $b_j \in F, j \in J$ 使得 $c = \sum_{j \in J} b_j \beta_j$. 再由 $\{\alpha_i\}_{i \in I}$ 是 F 在 K 上的基底, 存在 $a_{ij} \in K, i \in I$ 使得 $b_j = \sum_{i \in I} a_{ij} \alpha_i$. 从而,

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

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

其次证明 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 在 K 上线性无关.

事实上, 若存在 $a_{ij} \in K, i \in I, j \in J$ 使得 $\sum_{i \in I, j \in J} a_{ij} \alpha_i \beta_j = 0$, 即

$\sum_{j \in J} \left(\sum_{i \in I} a_{ij} \alpha_i \right) \beta_j = 0$. 因为 $\sum_{i \in I} a_{ij} \alpha_i \in F$, 且 $\{\beta_j\}_{j \in J}$ 是 E 在 F 上的基底, 所以 $\sum_{i \in I} a_{ij} \alpha_i = 0, j \in J$. 又因为 $a_{ij} \in K$, 以及 $\{\alpha_i\}_{i \in I}$ 是 F 在 K 上的基底, 得到 $a_{ij} = 0, i \in I, j \in J$.

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

其次证明 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 在 K 上线性无关.

事实上, 若存在 $a_{ij} \in K, i \in I, j \in J$ 使得 $\sum_{i \in I, j \in J} a_{ij} \alpha_i \beta_j = 0$, 即

$\sum_{j \in J} \left(\sum_{i \in I} a_{ij} \alpha_i \right) \beta_j = 0$. 因为 $\sum_{i \in I} a_{ij} \alpha_i \in F$, 且 $\{\beta_j\}_{j \in J}$ 是 E 在 F 上的基底, 所以 $\sum_{i \in I} a_{ij} \alpha_i = 0, j \in J$. 又因为 $a_{ij} \in K$, 以及 $\{\alpha_i\}_{i \in I}$ 是 F 在 K 上的基底, 得到 $a_{ij} = 0, i \in I, j \in J$.

进一步, 有 $[E : K] = [E : F][F : K]$.

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

其次证明 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 在 K 上线性无关.

事实上, 若存在 $a_{ij} \in K, i \in I, j \in J$ 使得 $\sum_{i \in I, j \in J} a_{ij} \alpha_i \beta_j = 0$, 即

$\sum_{j \in J} \left(\sum_{i \in I} a_{ij} \alpha_i \right) \beta_j = 0$. 因为 $\sum_{i \in I} a_{ij} \alpha_i \in F$, 且 $\{\beta_j\}_{j \in J}$ 是 E 在 F 上的基底, 所以 $\sum_{i \in I} a_{ij} \alpha_i = 0, j \in J$. 又因为 $a_{ij} \in K$, 以及 $\{\alpha_i\}_{i \in I}$ 是 F 在 K 上的基底, 得到 $a_{ij} = 0, i \in I, j \in J$.

进一步, 有 $[E : K] = [E : F][F : K]$.

推论 8.2.1

设 E 是 K 的有限扩域的充要条件是 E 是 F 的有限扩域, 且 F 是 K 的有限扩域.

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

其次证明 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 在 K 上线性无关.

事实上, 若存在 $a_{ij} \in K, i \in I, j \in J$ 使得 $\sum_{i \in I, j \in J} a_{ij} \alpha_i \beta_j = 0$, 即

$\sum_{j \in J} \left(\sum_{i \in I} a_{ij} \alpha_i \right) \beta_j = 0$. 因为 $\sum_{i \in I} a_{ij} \alpha_i \in F$, 且 $\{\beta_j\}_{j \in J}$ 是 E 在 F 上的基底, 所以 $\sum_{i \in I} a_{ij} \alpha_i = 0, j \in J$. 又因为 $a_{ij} \in K$, 以及 $\{\alpha_i\}_{i \in I}$ 是 F 在 K 上的基底, 得到 $a_{ij} = 0, i \in I, j \in J$.

进一步, 有 $[E : K] = [E : F][F : K]$.

推论 8.2.1

设 E 是 K 的有限扩域的充要条件是 E 是 F 的有限扩域, 且 F 是 K 的有限扩域.

例 8.2.4 数域 $\mathbb{Q}(\sqrt{2})$ 是 \mathbb{Q} 的有限扩张, 且 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

目录

- ① 分式域
- ② 素域与扩域
 - 有限扩域
 - 代数扩域
- ③ Galois 基本定理
- ④ 有限域
 - 有限域的构造
 - 有限域的 Galois 群
 - 有限域的正规基

再从多项式的根的角度讨论扩域.

定义 8.2.3

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

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

(3) 对于 F 的元素 u , 如果不存在任何非零多项式 $f \in R[x]$ 使得 $f(u) = 0$, 则称 u 为整环 R 上的超越数.

进一步, 当 K 是整环 R 的分式域时, 人们有时就称为 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多项式. 如果 F 的每个元素都是 K 上的代数数, 则 F 称为 K 的代数扩张. 如果 F 中至少有一个元素是 K 上的超越数, 则 F 称为 K 的超越扩张.

再从多项式的根的角度讨论扩域.

定义 8.2.3

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

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

(3) 对于 F 的元素 u , 如果不存在任何非零多项式 $f \in R[x]$ 使得 $f(u) = 0$, 则称 u 为整环 R 上的超越数.

进一步, 当 K 是整环 R 的分式域时, 人们有时就称为 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多项式. 如果 F 的每个元素都是 K 上的代数数, 则 F 称为 K 的代数扩张. 如果 F 中至少有一个元素是 K 上的超越数, 则 F 称为 K 的超越扩张.

注: 对于 $u \in K$, 有 u 是 $f(x) = x - u \in K[x]$ 的根. 故 u 是 K 上的代数数.

例 8.2.5

(1) $u = \sqrt{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

例 8.2.5

(1) $u = \sqrt{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

(2) $u = \frac{1+\sqrt{5}}{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

例 8.2.5

(1) $u = \sqrt{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

(2) $u = \frac{1+\sqrt{5}}{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

例 8.2.6

(1) 圆周率 $\pi = 3.14159265 \dots$ 是有理数域 \mathbb{Q} 上的超越数.

例 8.2.5

(1) $u = \sqrt{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

(2) $u = \frac{1+\sqrt{5}}{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

例 8.2.6

(1) 圆周率 $\pi = 3.14159265 \dots$ 是有理数域 \mathbb{Q} 上的超越数.

(2) 自然对数底 $e = 2.71828182 \dots$ 是有理数域 \mathbb{Q} 上的超越数.

例 8.2.5

(1) $u = \sqrt{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

(2) $u = \frac{1+\sqrt{5}}{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

例 8.2.6

(1) 圆周率 $\pi = 3.14159265 \dots$ 是有理数域 \mathbb{Q} 上的超越数.

(2) 自然对数底 $e = 2.71828182 \dots$ 是有理数域 \mathbb{Q} 上的超越数.

(3) $2^{\sqrt{2}}$ 是有理数域 \mathbb{Q} 上的超越数.

例 8.2.5

(1) $u = \sqrt{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

(2) $u = \frac{1+\sqrt{5}}{2}$ 是整数环 \mathbb{Z} 上的代数整数, 因为有首一多项式

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

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

例 8.2.6

(1) 圆周率 $\pi = 3.14159265 \dots$ 是有理数域 \mathbb{Q} 上的超越数.

(2) 自然对数底 $e = 2.71828182 \dots$ 是有理数域 \mathbb{Q} 上的超越数.

(3) $2^{\sqrt{2}}$ 是有理数域 \mathbb{Q} 上的超越数.

(4) $\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$ 是有理数域 \mathbb{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 F 是 K 的扩域, $u \in F$, 则可以构造 $K[x]$ 到 $K[u]$ 的一个同态.

$$\begin{aligned}\varphi : K[x] &\rightarrow K[u] \\ h(x) &\mapsto h(u)\end{aligned}$$

且上述环同态可拓展为 $K(x)$ 到 $K(u)$ 的一个域同态.

$$\begin{aligned}\varphi : K(x) &\rightarrow K(u) \\ \frac{h(x)}{g(x)} &\mapsto \frac{h(u)}{g(u)}\end{aligned}$$

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 F 是 K 的扩域, $u \in F$, 则可以构造 $K[x]$ 到 $K[u]$ 的一个同态.

$$\begin{aligned}\varphi : K[x] &\rightarrow K[u] \\ h(x) &\mapsto h(u)\end{aligned}$$

且上述环同态可拓展为 $K(x)$ 到 $K(u)$ 的一个域同态.

$$\begin{aligned}\varphi : K(x) &\rightarrow K(u) \\ \frac{h(x)}{g(x)} &\mapsto \frac{h(u)}{g(u)}\end{aligned}$$

根据环同态基本定理, 有同构

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

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

分两种情况讨论:

(1) u 是 K 上超越数. $\ker(\varphi) = \{0\}$. 因此, φ 是环同构, 也是域同构, 即

定理 8.2.3

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

分两种情况讨论:

(1) u 是 K 上超越数. $\ker(\varphi) = \{0\}$. 因此, φ 是环同构, 也是域同构, 即

定理 8.2.3

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

(2) u 是 K 上代数数. $\ker(\varphi) \neq \{0\}$ 是素理想. 而 $K[x]$ 是主理想环, 故存在次数最小首一不可约多项式 $f(x)$ 使得 $\ker(\varphi) = (f(x))$, 即

定理 8.2.4

设 F 是域 K 的扩域, $u \in F$ 是 K 上的代数数, 则存在一个在 K 上的首一不可约多项式 $f(x)$ 使得 $f(u) = 0$.

分两种情况讨论:

(1) u 是 K 上超越数. $\ker(\varphi) = \{0\}$. 因此, φ 是环同构, 也是域同构, 即

定理 8.2.3

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

(2) u 是 K 上代数数. $\ker(\varphi) \neq \{0\}$ 是素理想. 而 $K[x]$ 是主理想环, 故存在次数最小首一不可约多项式 $f(x)$ 使得 $\ker(\varphi) = (f(x))$, 即

定理 8.2.4

设 F 是域 K 的扩域, $u \in F$ 是 K 上的代数数, 则存在一个在 K 上的首一不可约多项式 $f(x)$ 使得 $f(u) = 0$.

由此, 可以建立代数数与多项式的对应关系.

定义 8.2.4

设 F 是域 K 的扩域, $u \in F$ 是 K 上的代数数. 满足 $f(u) = 0$ 的首一不可约多项式 $f(x)$ 称为 u 的极小多项式或定义多项式. 将此不可约多项式 $f(x)$ 的次数 $\deg f$ 定义为 u 在 K 上的次数, 并将此不可约多项式 $f(x)$ 的其他根称作 u 的共轭根.

定义 8.2.4

设 F 是域 K 的扩域, $u \in F$ 是 K 上的代数数. 满足 $f(u) = 0$ 的首一不可约多项式 $f(x)$ 称为 u 的极小多项式或定义多项式. 将此不可约多项式 $f(x)$ 的次数 $\deg f$ 定义为 u 在 K 上的次数, 并将此不可约多项式 $f(x)$ 的其他根称作 u 的共轭根.

例 8.2.7 $\sqrt{2}$ 在 \mathbb{Q} 上的极小多项式是 $f(x) = x^2 - 2$, 次数为 2, 共轭根为 $-\sqrt{2}$.

下面考虑由代数数生成的域.

定理 8.2.5

设 F 是 K 的扩域, $u \in F$ 是 K 上的代数数, 则

- (i) $K(u) = K[u]$.
- (ii) $K(u) \cong K[x]/(f(x))$, 其中 $f(x) \in K[x]$ 是 u 的极小多项式, $n = \deg f$.
- (iii) $[K(u) : K] = n$.
- (iv) $\{1, u, u^2, \dots, u^{n-1}\}$ 是 K 上向量空间 $K(u)$ 的基底.
- (v) $K(u)$ 的每个元素可唯一地表示为 $a_0 + a_1u + \dots + a_{n-1}u^{n-1}$, $a_i \in K$.

下面考虑由代数数生成的域.

定理 8.2.5

设 F 是 K 的扩域, $u \in F$ 是 K 上的代数数, 则

- (i) $K(u) = K[u]$.
- (ii) $K(u) \cong K[x]/(f(x))$, 其中 $f(x) \in K[x]$ 是 u 的极小多项式, $n = \deg f$.
- (iii) $[K(u) : K] = n$.
- (iv) $\{1, u, u^2, \dots, u^{n-1}\}$ 是 K 上向量空间 $K(u)$ 的基底.
- (v) $K(u)$ 的每个元素可唯一地表示为 $a_0 + a_1u + \dots + a_{n-1}u^{n-1}$, $a_i \in K$.

证: 设 u 的极小多项式为 $f(x)$, $n = \deg f$.

(i) 对任意 $\frac{h(u)}{g(u)} \in K(u)$, $g(u) \neq 0$, 有多项式 $g(x)$ 与 $f(x)$ 互素. 根据多项式广义欧几里德除法, 存在 $s(x), t(x) \in K[x]$ 使得 $s(x) \cdot g(x) + t(x) \cdot f(x) = 1$. 从而, $s(u)g(u) = 1$. 因此,

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

故 $K(u) \subset K[u]$. 这说明, $K(u) = K[u]$.

故 $K(u) \subset K[u]$. 这说明, $K(u) = K[u]$.

(ii) 考虑 $K[x]$ 到 $K[u]$ 的映射 $\varphi : g(x) \mapsto g(u)$.

易知, σ 是满的环同态. 根据环同态基本定理, 有

$$K(u) \cong K[x]/\ker(\varphi),$$

而 $\ker(\varphi) = (f)$, 即得.

故 $K(u) \subset K[u]$. 这说明, $K(u) = K[u]$.

(ii) 考虑 $K[x]$ 到 $K[u]$ 的映射 $\varphi : g(x) \mapsto g(u)$.

易知, σ 是满的环同态. 根据环同态基本定理, 有

$$K(u) \cong K[x]/\ker(\varphi),$$

而 $\ker(\varphi) = (f)$, 即得.

(iv) 对任意 $g(x) \in K[x]$, 根据多项式欧几里德除法, 存在 $q(x)$, $r(x) \in K[x]$ 使得 $g(x) = q(x) \cdot f(x) + r(x)$, $0 \leq \deg r < \deg f$.

因此, $g(u) = r(u)$. 这说明, $\{1, u, u^2, \dots, u^{n-1}\}$ 是 $K(u)$ 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 $\{1, u, u^2, \dots, u^{n-1}\}$ 在 K 上线性无关.

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

故 $K(u) \subset K[u]$. 这说明, $K(u) = K[u]$.

(ii) 考虑 $K[x]$ 到 $K[u]$ 的映射 $\varphi : g(x) \mapsto g(u)$.

易知, σ 是满的环同态. 根据环同态基本定理, 有

$$K(u) \cong K[x]/\ker(\varphi),$$

而 $\ker(\varphi) = (f)$, 即得.

(iv) 对任意 $g(x) \in K[x]$, 根据多项式欧几里德除法, 存在 $q(x)$, $r(x) \in K[x]$ 使得 $g(x) = q(x) \cdot f(x) + r(x)$, $0 \leq \deg r < \deg f$.

因此, $g(u) = r(u)$. 这说明, $\{1, u, u^2, \dots, u^{n-1}\}$ 是 $K(u)$ 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 $\{1, u, u^2, \dots, u^{n-1}\}$ 在 K 上线性无关.

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

(iii) 和 (v) 由 (iv) 可得.

例 8.2.8 多项式 $x^2 - x - 1$ 是 \mathbb{Q} 上的不可约多项式.

例 8.2.8 多项式 $x^2 - x - 1$ 是 \mathbb{Q} 上的不可约多项式.

例 8.2.9 多项式 $x^3 - 3x - 1$ 是 \mathbb{Q} 上的不可约多项式.

例 8.2.8 多项式 $x^2 - x - 1$ 是 \mathbb{Q} 上的不可约多项式.

例 8.2.9 多项式 $x^3 - 3x - 1$ 是 \mathbb{Q} 上的不可约多项式.

例 8.2.10 F_2 上的 4 次以下的不可约多项式与可约多项式是:

- (1) 一次不可约多项式: $x, x + 1$;
- (2) 二次不可约多项式: $x^2 + x + 1$;
- (3) 二次可约多项式: $x^2, x^2 + 1 = (x + 1)^2, x^2 + x = x(x + 1)$;
- (4) 三次不可约多项式: $x^3 + x + 1, x^3 + x^2 + 1$;
- (5) 三次可约多项式为: $x^3, x^3 + x, x^3 + x^2, x^3 + x^2 + x,$
 $x^3 + x^2 + x + 1 = (x + 1)^3, x^3 + 1 = (x + 1)(x^2 + x + 1).$

下面从线性空间的角度讨论域中元素间的关系.

定义 8.2.5

设 F 是域 K 的扩域, a_1, a_2, \dots, a_n 是 F 的 n 个元素. 如果存在一个非零多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则称 a_1, a_2, \dots, a_n 在 K 上代数相关. 否则, a_1, a_2, \dots, a_n 叫作代数无关.

下面从线性空间的角度讨论域中元素间的关系.

定义 8.2.5

设 F 是域 K 的扩域, a_1, a_2, \dots, a_n 是 F 的 n 个元素. 如果存在一个非零多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则称 a_1, a_2, \dots, a_n 在 K 上代数相关. 否则, a_1, a_2, \dots, a_n 叫作代数无关.

注: 所谓 a_1, a_2, \dots, a_n 代数无关, 即如果有多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则 $f = 0$.

下面从线性空间的角度讨论域中元素间的关系.

定义 8.2.5

设 F 是域 K 的扩域, a_1, a_2, \dots, a_n 是 F 的 n 个元素. 如果存在一个非零多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则称 a_1, a_2, \dots, a_n 在 K 上代数相关. 否则, a_1, a_2, \dots, a_n 叫作代数无关.

注: 所谓 a_1, a_2, \dots, a_n 代数无关, 即如果有多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则 $f = 0$.

例 8.2.11 $\pi = 3.14 \dots$ 和自然对数底 $e = 2.718 \dots$ 在 \mathbb{Q} 上代数无关.

下面从线性空间的角度讨论域中元素间的关系.

定义 8.2.5

设 F 是域 K 的扩域, a_1, a_2, \dots, a_n 是 F 的 n 个元素. 如果存在一个非零多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则称 a_1, a_2, \dots, a_n 在 K 上代数相关. 否则, a_1, a_2, \dots, a_n 叫作代数无关.

注: 所谓 a_1, a_2, \dots, a_n 代数无关, 即如果有多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则 $f = 0$.

例 8.2.11 $\pi = 3.14\dots$ 和自然对数底 $e = 2.718\dots$ 在 \mathbb{Q} 上代数无关.

定理 8.2.6

设 F 是域 K 的有限生成扩域, 则 F 是 K 的代数扩张, 或者存在代数无关元 $\theta_1, \dots, \theta_t$ 使得 F 是 $K(\theta_1, \dots, \theta_t)$ 的代数扩张.

下面从线性空间的角度讨论域中元素间的关系.

定义 8.2.5

设 F 是域 K 的扩域, a_1, a_2, \dots, a_n 是 F 的 n 个元素. 如果存在一个非零多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则称 a_1, a_2, \dots, a_n 在 K 上代数相关. 否则, a_1, a_2, \dots, a_n 叫作代数无关.

注: 所谓 a_1, a_2, \dots, a_n 代数无关, 即如果有多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则 $f = 0$.

例 8.2.11 $\pi = 3.14\dots$ 和自然对数底 $e = 2.718\dots$ 在 \mathbb{Q} 上代数无关.

定理 8.2.6

设 F 是域 K 的有限生成扩域, 则 F 是 K 的代数扩张, 或者存在代数无关元 $\theta_1, \dots, \theta_t$ 使得 F 是 $K(\theta_1, \dots, \theta_t)$ 的代数扩张.

证: 设 F 在域 K 的有限生成元为 $S = \{a_1, a_2, \dots, a_n\}$. 若 S 中的每个元素在 K 上代数相关, 则 F 是 K 的代数扩张. 否则, S 中有元素在 K 上代数无关, 设为 θ_1 . 用 $K(\theta_1)$ 代替 K 作讨论. 如此下去, 即得.

下面从域的同构扩充到扩域的同构. 设 $\sigma : K \rightarrow L$ 是域同构.

对于 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$, 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 8.2.7

设 $\sigma : K \rightarrow L$ 是域同构. u 是 K 的某个扩域中的元素, v 是 L 的某个扩域中的元素, 假设

- (i) u 是 K 上的超越数, v 是 L 上的超越数, 或者
- (ii) u 是 K 上的代数数, u 的极小多项式为 $f(x) \in K[x]$, v 是多项式 $\sigma(f) \in L[x]$ 的根,

则 σ 可扩充为扩域 $K(u)$ 到 $L(v)$ 的同构 φ , 并将 u 映射到 $v = \varphi(u)$.

下面从域的同构扩充到扩域的同构. 设 $\sigma : K \rightarrow L$ 是域同构.

对于 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$, 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 8.2.7

设 $\sigma : K \rightarrow L$ 是域同构. u 是 K 的某个扩域中的元素, v 是 L 的某个扩域中的元素, 假设

- (i) u 是 K 上的超越数, v 是 L 上的超越数, 或者
- (ii) u 是 K 上的代数数, u 的极小多项式为 $f(x) \in K[x]$, v 是多项式 $\sigma(f) \in L[x]$ 的根,

则 σ 可扩充为扩域 $K(u)$ 到 $L(v)$ 的同构 φ , 并将 u 映射到 $v = \varphi(u)$.

证: 考虑 $K(u)$ 到 $L(v)$ 映射 $\varphi : \frac{h(u)}{g(u)} \rightarrow \frac{\sigma(h)(v)}{\sigma(g)(v)}$. 这个 φ 是 $K(u)$ 到 $L(v)$ 的同构, 且满足 $\varphi|_K = \sigma, \varphi(u) = v$. 事实上, 只需说明 φ 是一对一的.

若 $\sigma(h)(v) = 0$, 根据假设条件, 在情形 (i) 下, 有 $\sigma(h) = 0$, 从而 $h = 0$. 在情形 (ii) 下, 有 $\sigma(f) \mid \sigma(h)$, 从而 $f \mid h$, 即有 $h(u) = 0$.

定理 8.2.8

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

若 $\sigma(h)(v) = 0$, 根据假设条件, 在情形 (i) 下, 有 $\sigma(h) = 0$, 从而 $h = 0$. 在情形 (ii) 下, 有 $\sigma(f) \mid \sigma(h)$, 从而 $f \mid h$, 即有 $h(u) = 0$.

定理 8.2.8

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

证: 取 $\sigma = id_K$ 为 K 上的恒等变换, σ 是 K 到自身的同构, 且 $\sigma(f) = f$. 应用定理 8.2.7 即得.

若 $\sigma(h)(v) = 0$, 根据假设条件, 在情形 (i) 下, 有 $\sigma(h) = 0$, 从而 $h = 0$. 在情形 (ii) 下, 有 $\sigma(f) \mid \sigma(h)$, 从而 $f \mid h$, 即有 $h(u) = 0$.

定理 8.2.8

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

证: 取 $\sigma = id_K$ 为 K 上的恒等变换, σ 是 K 到自身的同构, 且 $\sigma(f) = f$. 应用定理 8.2.7 即得.

定理 8.2.9

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

- (i) $u \in F$ 是 f 的根.
- (ii) $[K(u) : K] \leq n$, 等式成立当且仅当 f 是 $K[x]$ 中的不可约多项式.

证：不妨设 $f \in K[x]$ 是不可约多项式，根据商环 $K[x]/(f)$ 是一个域。

考虑 $K[x]$ 到 $K[x]/(f) = F$ 的自然同态

$$s : g(x) \mapsto g(x) \bmod f(x).$$

易知, $s|_K$ 是 K 到 $s(K)$ 的同构, 且 F 是 $s(K)$ 的扩域.

对于 $x \in K[x]$, 令 $u = s(x)$, 有

$$F = K(u) \text{ 及 } f(u) = 0.$$

则 (i) 成立.

从定理 8.2.5 即可推出 (ii).

证：不妨设 $f \in K[x]$ 是不可约多项式，根据商环 $K[x]/(f)$ 是一个域。

考虑 $K[x]$ 到 $K[x]/(f) = F$ 的自然同态

$$s : g(x) \mapsto g(x) \bmod f(x).$$

易知, $s|_K$ 是 K 到 $s(K)$ 的同构, 且 F 是 $s(K)$ 的扩域.

对于 $x \in K[x]$, 令 $u = s(x)$, 有

$$F = K(u) \text{ 及 } f(u) = 0.$$

则 (i) 成立.

从定理 8.2.5 即可推出 (ii).

推论 8.2.2

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

定义 8.2.6

设 K 是一个域, $f \in K[x]$ 是次数为 $n \geq 1$ 的多项式. 对于 K 的一个扩域 F , 如果 f 在 $F[x]$ 中可完全分解成一次因式的乘积, 即

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

且 $F = K(u_1, \cdots, u_n)$, 其中 $\alpha \in K$, u_1, \cdots, u_n 是 f 在 F 中的根, 则称 F 为多项式 f 在 K 上的分裂域或根域.

定义 8.2.6

设 K 是一个域, $f \in K[x]$ 是次数为 $n \geq 1$ 的多项式. 对于 K 的一个扩域 F , 如果 f 在 $F[x]$ 中可完全分解成一次因式的乘积, 即

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

且 $F = K(u_1, \cdots, u_n)$, 其中 $\alpha \in K$, u_1, \cdots, u_n 是 f 在 F 中的根, 则称 F 为多项式 f 在 K 上的分裂域或根域.

注: 设 S 是 $K[x]$ 中一些次数 ≥ 1 的多项式组成的集合. 对于 K 的一个扩域 F , 如果 S 中的每一个多项式 f 在 $F[x]$ 中可完全分解成一次因式的乘积, 且 F 由 S 中的所有多项式的根在 K 上生成, 则称 F 为多项式集合 S 在 K 上的分裂域.

定义 8.2.6

设 K 是一个域, $f \in K[x]$ 是次数为 $n \geq 1$ 的多项式. 对于 K 的一个扩域 F , 如果 f 在 $F[x]$ 中可完全分解成一次因式的乘积, 即

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

且 $F = K(u_1, \cdots, u_n)$, 其中 $\alpha \in K$, u_1, \cdots, u_n 是 f 在 F 中的根, 则称 F 为多项式 f 在 K 上的分裂域或根域.

注: 设 S 是 $K[x]$ 中一些次数 ≥ 1 的多项式组成的集合. 对于 K 的一个扩域 F , 如果 S 中的每一个多项式 f 在 $F[x]$ 中可完全分解成一次因式的乘积, 且 F 由 S 中的所有多项式的根在 K 上生成, 则称 F 为多项式集合 S 在 K 上的分裂域.

例 8.2.12 设 $x^p - x$ 在 F_p 的分裂域就是 F_p .

定义 8.2.6

设 K 是一个域, $f \in K[x]$ 是次数为 $n \geq 1$ 的多项式. 对于 K 的一个扩域 F , 如果 f 在 $F[x]$ 中可完全分解成一次因式的乘积, 即

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

且 $F = K(u_1, \cdots, u_n)$, 其中 $\alpha \in K$, u_1, \cdots, u_n 是 f 在 F 中的根, 则称 F 为多项式 f 在 K 上的分裂域或根域.

注: 设 S 是 $K[x]$ 中一些次数 ≥ 1 的多项式组成的集合. 对于 K 的一个扩域 F , 如果 S 中的每一个多项式 f 在 $F[x]$ 中可完全分解成一次因式的乘积, 且 F 由 S 中的所有多项式的根在 K 上生成, 则称 F 为多项式集合 S 在 K 上的分裂域.

例 8.2.12 设 $x^p - x$ 在 F_p 的分裂域就是 F_p .

证: 在 F_p 上有 $x^p - x = x(x - 1) \cdots (x - (p - 1))$.

定义 8.2.6

设 K 是一个域, $f \in K[x]$ 是次数为 $n \geq 1$ 的多项式. 对于 K 的一个扩域 F , 如果 f 在 $F[x]$ 中可完全分解成一次因式的乘积, 即

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

且 $F = K(u_1, \cdots, u_n)$, 其中 $\alpha \in K$, u_1, \cdots, u_n 是 f 在 F 中的根, 则称 F 为多项式 f 在 K 上的分裂域或根域.

注: 设 S 是 $K[x]$ 中一些次数 ≥ 1 的多项式组成的集合. 对于 K 的一个扩域 F , 如果 S 中的每一个多项式 f 在 $F[x]$ 中可完全分解成一次因式的乘积, 且 F 由 S 中的所有多项式的根在 K 上生成, 则称 F 为多项式集合 S 在 K 上的分裂域.

例 8.2.12 设 $x^p - x$ 在 F_p 的分裂域就是 F_p .

证: 在 F_p 上有 $x^p - x = x(x - 1) \cdots (x - (p - 1))$.

例 8.2.13 设 E 是 q 元有限域, 则 $x^q - x$ 在 E 的素域 F_p 的分裂域是 E .

定理 8.2.10

设 K 是一个域, $f \in K[x]$ 的次数为 $n \geq 1$, 则存在 f 的一个分裂域 F 且 $[F : K] \leq n!$.

定理 8.2.10

设 K 是一个域, $f \in K[x]$ 的次数为 $n \geq 1$, 则存在 f 的一个分裂域 F 且 $[F : K] \leq n!$.

证: 对 $n = \deg f$ 作数学归纳法.

如果 $n = 1$, 或如果 f 在 K 上可完全分解, 则 $F = K$ 是分裂域.

定理 8.2.10

设 K 是一个域, $f \in K[x]$ 的次数为 $n \geq 1$, 则存在 f 的一个分裂域 F 且 $[F : K] \leq n!$.

证: 对 $n = \deg f$ 作数学归纳法.

如果 $n = 1$, 或如果 f 在 K 上可完全分解, 则 $F = K$ 是分裂域.

如果 $n > 1$, f 在 K 上不能完全分解, 设 $g \in K[x]$ 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 $K(u)$ 使得 u 是 g 的根, 且 $[K(u) : K] = \deg g > 1$. 因此, 在 $K(u)[x]$ 中有分解式 $f(x) = (x - u)h(x)$, 其中 $\deg h = n - 1$. 由归纳假设, 存在 h 在 $K(u)$ 上的维数 $\leq (n - 1)!$ 的分裂域 F . 易知, F 在 K 上的次数

$$[F : K] = [F : K(u)][K(u) : K] \leq (n - 1)!n = n!.$$

定理 8.2.10

设 K 是一个域, $f \in K[x]$ 的次数为 $n \geq 1$, 则存在 f 的一个分裂域 F 且 $[F : K] \leq n!$.

证: 对 $n = \deg f$ 作数学归纳法.

如果 $n = 1$, 或如果 f 在 K 上可完全分解, 则 $F = K$ 是分裂域.

如果 $n > 1$, f 在 K 上不能完全分解, 设 $g \in K[x]$ 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 $K(u)$ 使得 u 是 g 的根, 且 $[K(u) : K] = \deg g > 1$. 因此, 在 $K(u)[x]$ 中有分解式 $f(x) = (x - u)h(x)$, 其中 $\deg h = n - 1$. 由归纳假设, 存在 h 在 $K(u)$ 上的维数 $\leq (n - 1)!$ 的分裂域 F . 易知, F 在 K 上的次数

$$[F : K] = [F : K(u)][K(u) : K] \leq (n - 1)!n = n!.$$

下面讨论不能进行代数扩张的域, 也就是一个在该域上的多项式总有解的域.

定理 8.2.11

在域 F 上的以下条件等价:

- (i) 每个非常数多项式 $f \in F[x]$ 在 F 中有根.
- (ii) 每个非常数多项式 $f \in F[x]$ 在 F 中可完全分解.
- (iii) 每个不可约多项式 $f \in F[x]$ 的次数为 1.
- (iv) 除了 F 以外, 不存在 F 的代数扩张.

定理 8.2.11

在域 F 上的以下条件等价:

- (i) 每个非常数多项式 $f \in F[x]$ 在 F 中有根.
- (ii) 每个非常数多项式 $f \in F[x]$ 在 F 中可完全分解.
- (iii) 每个不可约多项式 $f \in F[x]$ 的次数为 1.
- (iv) 除了 F 以外, 不存在 F 的代数扩张.

证: (i) \Rightarrow (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) 知, $f(x)$ 在 F 中有根 $x = a$. 根据多项式欧几里德除法可得到 $x - a \mid f(x)$, 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 F 中可完全分解, 故 $f \in F[x]$ 在 F 中可完全分解.

定理 8.2.11

在域 F 上的以下条件等价:

- (i) 每个非常数多项式 $f \in F[x]$ 在 F 中有根.
- (ii) 每个非常数多项式 $f \in F[x]$ 在 F 中可完全分解.
- (iii) 每个不可约多项式 $f \in F[x]$ 的次数为 1.
- (iv) 除了 F 以外, 不存在 F 的代数扩张.

证: (i) \Rightarrow (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) 知, $f(x)$ 在 F 中有根 $x = a$. 根据多项式欧几里德除法可得到 $x - a \mid f(x)$, 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 F 中可完全分解, 故 $f \in F[x]$ 在 F 中可完全分解.

(ii) \Rightarrow (iii). 结论显然成立.

定理 8.2.11

在域 F 上的以下条件等价:

- (i) 每个非常数多项式 $f \in F[x]$ 在 F 中有根.
- (ii) 每个非常数多项式 $f \in F[x]$ 在 F 中可完全分解.
- (iii) 每个不可约多项式 $f \in F[x]$ 的次数为 1.
- (iv) 除了 F 以外, 不存在 F 的代数扩张.

证: (i) \Rightarrow (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) 知, $f(x)$ 在 F 中有根 $x = a$. 根据多项式欧几里德除法可得到 $x - a \mid f(x)$, 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 F 中可完全分解, 故 $f \in F[x]$ 在 F 中可完全分解.

(ii) \Rightarrow (iii). 结论显然成立. (iii) \Rightarrow (iv). 设 E 是 F 的一个代数扩张, 则对于任意 $u \in E$, 因为 u 是 F 上的代数元, 由定理 8.2.5, 存在不可约多项式 $f(x) \in F[x]$ 使得 $f(u) = 0$. 由 (iii), $f(x) = a_1x + a_2, a_1, a_2 \in F$. 从而,

$u = -(a_1^{-1})a_2 \in F$. 这说明, $E \subset F$, 故 $E = F$, 结论成立.

$u = -(a_1^{-1})a_2 \in F$. 这说明, $E \subset F$, 故 $E = F$, 结论成立.

(iv) \Rightarrow (i). 设 $f(x)$ 是 F 上的非常数多项式, 由定理 8.2.5, 存在 $f(x)$ 的根 u 使 $F(u)$ 为 F 的代数扩张. 由 (iv), $F(u) = F$. 故, $u \in F$, 结论成立.

$u = -(a_1^{-1})a_2 \in F$. 这说明, $E \subset F$, 故 $E = F$, 结论成立.

(iv) \Rightarrow (i). 设 $f(x)$ 是 F 上的非常数多项式, 由定理 8.2.5, 存在 $f(x)$ 的根 u 使 $F(u)$ 为 F 的代数扩张. 由 (iv), $F(u) = F$. 故, $u \in F$, 结论成立.

定义 8.2.7

设 F 是一个域. 如果域 F 满足定理 8.2.11 的等价条件, 则称 F 为代数闭包.

$u = -(a_1^{-1})a_2 \in F$. 这说明, $E \subset F$, 故 $E = F$, 结论成立.

(iv) \Rightarrow (i). 设 $f(x)$ 是 F 上的非常数多项式, 由定理 8.2.5, 存在 $f(x)$ 的根 u 使 $F(u)$ 为 F 的代数扩张. 由 (iv), $F(u) = F$. 故, $u \in F$, 结论成立.

定义 8.2.7

设 F 是一个域. 如果域 F 满足定理 8.2.11 的等价条件, 则称 F 为代数闭包.

定义 8.2.8

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.

$u = -(a_1^{-1})a_2 \in F$. 这说明, $E \subset F$, 故 $E = F$, 结论成立.

(iv) \Rightarrow (i). 设 $f(x)$ 是 F 上的非常数多项式, 由定理 8.2.5, 存在 $f(x)$ 的根 u 使 $F(u)$ 为 F 的代数扩张. 由 (iv), $F(u) = F$. 故, $u \in F$, 结论成立.

定义 8.2.7

设 F 是一个域. 如果域 F 满足定理 8.2.11 的等价条件, 则称 F 为代数闭包.

定义 8.2.8

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 8.2.9

设 F 是域 K 是一个扩域, u 是 K 上的代数数. 如果 u 在 K 上的极小多项式是可分的, 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.

定义 8.3.1

设 E 和 F 是域 K 的扩域. 对于一个非零映射 $\sigma: E \rightarrow F$, 如果 σ 是一个域同态, 且 σ 在 K 上为恒等映射, 则称 σ 为 K -同态. 特别地, 当 σ 是一个域同构时, 则称 σ 为 K -同构.

定义 8.3.1

设 E 和 F 是域 K 的扩域. 对于一个非零映射 $\sigma: E \rightarrow F$, 如果 σ 是一个域同态, 且 σ 在 K 上为恒等映射, 则称 σ 为 K -同态. 特别地, 当 σ 是一个域同构时, 则称 σ 为 K -同构.

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

定义 8.3.1

设 E 和 F 是域 K 的扩域. 对于一个非零映射 $\sigma : E \rightarrow F$, 如果 σ 是一个域同态, 且 σ 在 K 上为恒等映射, 则称 σ 为 K -同态. 特别地, 当 σ 是一个域同构时, 则称 σ 为 K -同构.

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

对于一个自同构 $\sigma : F \rightarrow F$, 如果 σ 是 K -同构, 则称 σ 为 K -自同构. F 的所有 K -自同构组成的群叫作 F 在 K 上的伽罗瓦 (Galois) 群, 记作 $\text{Aut}_K F$.

定义 8.3.1

设 E 和 F 是域 K 的扩域. 对于一个非零映射 $\sigma : E \rightarrow F$, 如果 σ 是一个域同态, 且 σ 在 K 上为恒等映射, 则称 σ 为 K -同态. 特别地, 当 σ 是一个域同构时, 则称 σ 为 K -同构.

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

对于一个自同构 $\sigma : F \rightarrow F$, 如果 σ 是 K -同构, 则称 σ 为 K -自同构. F 的所有 K -自同构组成的群叫作 F 在 K 上的伽罗瓦 (Galois) 群, 记作 $\text{Aut}_K F$.

对于中间域 $E : K \subset E \subset F$, 也有 F 在 E 上的 Galois 群 $\text{Aut}_E F$.

定义 8.3.1

设 E 和 F 是域 K 的扩域. 对于一个非零映射 $\sigma : E \rightarrow F$, 如果 σ 是一个域同态, 且 σ 在 K 上为恒等映射, 则称 σ 为 K -同态. 特别地, 当 σ 是一个域同构时, 则称 σ 为 K -同构.

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

对于一个自同构 $\sigma : F \rightarrow F$, 如果 σ 是 K -同构, 则称 σ 为 K -自同构. F 的所有 K -自同构组成的群叫作 F 在 K 上的伽罗瓦 (Galois) 群, 记作 $\text{Aut}_K F$.

对于中间域 $E : K \subset E \subset F$, 也有 F 在 E 上的 Galois 群 $\text{Aut}_E F$.

定理 8.3.1

设 F 是 K 的扩域, $f \in K[x]$. 如果 $u \in F$ 是 f 的根, $\sigma \in \text{Aut}_K F$, 则 $\sigma(u)$ 也是 f 的根.

定义 8.3.1

设 E 和 F 是域 K 的扩域. 对于一个非零映射 $\sigma : E \rightarrow F$, 如果 σ 是一个域同态, 且 σ 在 K 上为恒等映射, 则称 σ 为 K -同态. 特别地, 当 σ 是一个域同构时, 则称 σ 为 K -同构.

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

对于一个自同构 $\sigma : F \rightarrow F$, 如果 σ 是 K -同构, 则称 σ 为 K -自同构. F 的所有 K -自同构组成的群叫作 F 在 K 上的伽罗瓦 (Galois) 群, 记作 $\text{Aut}_K F$.

对于中间域 $E : K \subset E \subset F$, 也有 F 在 E 上的 Galois 群 $\text{Aut}_E F$.

定理 8.3.1

设 F 是 K 的扩域, $f \in K[x]$. 如果 $u \in F$ 是 f 的根, $\sigma \in \text{Aut}_K F$, 则 $\sigma(u)$ 也是 f 的根.

设 F 是 K 的扩域, E 是中间域. 设 H 是 $G = \text{Aut}_K F$ 的子群. 定义

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

和

$$A(E) = \{\sigma \in \text{Aut}_K F \mid \sigma(u) = u, u \in E\}.$$

$I(H)$ 是由 F 中在子群 H 的自同构下保持不变的元素组成的集合. $A(E)$ 是由 $G = \text{Aut}_K F$ 中使中间域 E 中的元素保持不变的自同构组成的集合.

设 F 是 K 的扩域, E 是中间域. 设 H 是 $G = \text{Aut}_K F$ 的子群. 定义

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

和

$$A(E) = \{\sigma \in \text{Aut}_K F \mid \sigma(u) = u, u \in E\}.$$

$I(H)$ 是由 F 中在子群 H 的自同构下保持不变的元素组成的集合. $A(E)$ 是由 $G = \text{Aut}_K F$ 中使中间域 E 中的元素保持不变的自同构组成的集合.

定理 8.3.2

设 F 是 K 的扩域, E 是中间域以及 H 是 $\text{Aut}_K F$ 的子群, 则

- (i) $I(H)$ 是扩域 F 的中间域.
- (ii) $A(E)$ 是 $\text{Aut}_K F$ 的子群.

设 F 是 K 的扩域, E 是中间域. 设 H 是 $G = \text{Aut}_K F$ 的子群. 定义

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

和

$$A(E) = \{\sigma \in \text{Aut}_K F \mid \sigma(u) = u, u \in E\}.$$

$I(H)$ 是由 F 中在子群 H 的自同构下保持不变的元素组成的集合. $A(E)$ 是由 $G = \text{Aut}_K F$ 中使中间域 E 中的元素保持不变的自同构组成的集合.

定理 8.3.2

设 F 是 K 的扩域, E 是中间域以及 H 是 $\text{Aut}_K F$ 的子群, 则

- (i) $I(H)$ 是扩域 F 的中间域.
- (ii) $A(E)$ 是 $\text{Aut}_K F$ 的子群.

注: 中间域 $I(H)$ 叫作 H 在 F 中的**不变域**. 易知,

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

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

定义 8.3.2

设 F 是 K 的扩域. 如果 Galois 群 $\text{Aut}_K F$ 的不变域是 K , 则 F 叫作 K 的 Galois 扩张.

定义 8.3.2

设 F 是 K 的扩域. 如果 Galois 群 $\text{Aut}_K F$ 的不变域是 K , 则 F 叫作 K 的 Galois 扩张.

注: 对于中间域 $E : K \subset E \subset F$, 如果 Galois 群 $\text{Aut}_E F$ 的不变域是 E , 则 F 叫作 E 的 Galois 扩张.

定义 8.3.2

设 F 是 K 的扩域. 如果 Galois 群 $\text{Aut}_K F$ 的不变域是 K , 则 F 叫作 K 的 Galois 扩张.

注: 对于中间域 $E: K \subset E \subset F$, 如果 Galois 群 $\text{Aut}_E F$ 的不变域是 E , 则 F 叫作 E 的 Galois 扩张.

注: 设域 F 是 K 的 Galois 扩张, 则对任意的 $u \in F \setminus K$, 存在 $\sigma \in \text{Aut}_K F$ 使得 $\sigma(u) \neq u$. 设域 F 是 E 的 Galois 扩张, 则对任意的 $u \in F \setminus E$, 存在 $\sigma \in \text{Aut}_E F$ 使得 $\sigma(u) \neq u$.

定义 8.3.2

设 F 是 K 的扩域. 如果 Galois 群 $\text{Aut}_K F$ 的不变域是 K , 则 F 叫作 K 的 Galois 扩张.

注: 对于中间域 $E: K \subset E \subset F$, 如果 Galois 群 $\text{Aut}_E F$ 的不变域是 E , 则 F 叫作 E 的 Galois 扩张.

注: 设域 F 是 K 的 Galois 扩张, 则对任意的 $u \in F \setminus K$, 存在 $\sigma \in \text{Aut}_K F$ 使得 $\sigma(u) \neq u$. 设域 F 是 E 的 Galois 扩张, 则对任意的 $u \in F \setminus E$, 存在 $\sigma \in \text{Aut}_E F$ 使得 $\sigma(u) \neq u$.

注: 给定 E , 可得 $A(E)$, 进而得 $I(A(E))$, 它使得 $A(E) = \text{Aut}_{I(A(E))} F$. 故

$$A(E) = \text{Aut}_E F \Leftrightarrow I(A(E)) = E.$$

即 E 有 Galois 子群 $\text{Aut}_E F$ 的充要条件是 $I(A(E)) = E$.

定义 8.3.2

设 F 是 K 的扩域. 如果 Galois 群 $\text{Aut}_K F$ 的不变域是 K , 则 F 叫作 K 的 Galois 扩张.

注: 对于中间域 $E: K \subset E \subset F$, 如果 Galois 群 $\text{Aut}_E F$ 的不变域是 E , 则 F 叫作 E 的 Galois 扩张.

注: 设域 F 是 K 的 Galois 扩张, 则对任意的 $u \in F \setminus K$, 存在 $\sigma \in \text{Aut}_K F$ 使得 $\sigma(u) \neq u$. 设域 F 是 E 的 Galois 扩张, 则对任意的 $u \in F \setminus E$, 存在 $\sigma \in \text{Aut}_E F$ 使得 $\sigma(u) \neq u$.

注: 给定 E , 可得 $A(E)$, 进而得 $I(A(E))$, 它使得 $A(E) = \text{Aut}_{I(A(E))} F$. 故

$$A(E) = \text{Aut}_E F \Leftrightarrow I(A(E)) = E.$$

即 E 有 Galois 子群 $\text{Aut}_E F$ 的充要条件是 $I(A(E)) = E$.

注: 给定 $H < G$, 可得 $I(H)$, 进而得 $A(I(H))$ 使得 $A(I(H)) = \text{Aut}_{I(H)} F$. 故

$$H = \text{Aut}_{I(H)} F \Leftrightarrow A(I(H)) = H.$$

如果 $E = I(A(E))$, 则称中间域 E 是闭的. 例如 K 和 F 都是闭域.
如果 $H = A(I(H))$, 则称子群 H 是闭的. 例如 $\{e\}$ 和 G 都是闭子群.

如果 $E = I(A(E))$, 则称中间域 E 是闭的. 例如 K 和 F 都是闭域.

如果 $H = A(I(H))$, 则称子群 H 是闭的. 例如 $\{e\}$ 和 G 都是闭子群.

定理 8.3.3

设 F 是 K 的扩域, 则在其闭中间域与 Galois 群 $G = \text{Aut}_K F$ 的闭子群之间存在一一对应的映射:

$$E \mapsto A(E) = \text{Aut}_E F$$

如果 $E = I(A(E))$, 则称中间域 E 是闭的. 例如 K 和 F 都是闭域.

如果 $H = A(I(H))$, 则称子群 H 是闭的. 例如 $\{e\}$ 和 G 都是闭子群.

定理 8.3.3

设 F 是 K 的扩域, 则在其闭中间域与 Galois 群 $G = \text{Aut}_K F$ 的闭子群之间存在一一对应的映射:

$$E \mapsto A(E) = \text{Aut}_E F$$

由此, 定理 8.3.1 可以推广为:

定理 8.3.4

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

定理 8.3.5 (Galois 理论的基本定理)

如果 F 是 K 的有限维 Galois 扩张, 则在所有中间扩域集到 Galois 群 $\text{Aut}_K F$ 的所有子群集之间存在一个一一对应的映射

$$E \mapsto A(E) = \text{Aut}_E F$$

使得:

- (i) F 是每个中间域 E 上的 Galois 域.
- (ii) 两个中间域 $E_1 \subset E_2$ 的相关维数 $[E_2 : E_1]$ 等于对应子群 $A(E_1) > A(E_2)$ 的相关指标 $[A(E_1) : A(E_2)]$. 特别地, $\text{Aut}_K F$ 有阶 $[F : K]$.
- (iii) 中间域 E 是 K 上的 Galois 域当且仅当对应的子群 $A(E) = \text{Aut}_E F$ 是 $G = \text{Aut}_K F$ 的正规子群, 在这个情况下, $G/A(E)$ (同构意义下) 是 E 在 K 上的 Galois 群 $\text{Aut}_K E$.

目录

- ① 分式域
- ② 素域与扩域
 - 有限扩域
 - 代数扩域
- ③ Galois 基本定理
- ④ 有限域
 - 有限域的构造
 - 有限域的 Galois 群
 - 有限域的正规基

设 F_q 是 q 元有限域, 其特征 p 为素数, 则 F_q 包含素域 $F_p = \mathbb{Z}/p\mathbb{Z}$, 是 F_p 上的有限维线性空间. 设 $n = [F_q : F_p]$, 则 $q = p^n$, 即 q 是其特征 p 的方幂. 根据定理 8.2.5 有

设 F_q 是 q 元有限域, 其特征 p 为素数, 则 F_q 包含素域 $F_p = \mathbb{Z}/p\mathbb{Z}$, 是 F_p 上的有限维线性空间. 设 $n = [F_q : F_p]$, 则 $q = p^n$, 即 q 是其特征 p 的方幂. 根据定理 8.2.5 有

定理 8.4.1

设 $K = \mathbb{Z}/p\mathbb{Z}$ 是一个有限域, 其中 p 是素数. 设 $p(x)$ 是 $K[x]$ 中的 n 次不可约多项式, 则

$$K[x]/((p(x))) = \{a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \mid a_i \in K\}$$

构成一个域, 记作 F_{p^n} . 这个域的元素个数为 p^n .

设 F_q 是 q 元有限域, 其特征 p 为素数, 则 F_q 包含素域 $F_p = \mathbb{Z}/p\mathbb{Z}$, 是 F_p 上的有限维线性空间. 设 $n = [F_q : F_p]$, 则 $q = p^n$, 即 q 是其特征 p 的方幂. 根据定理 8.2.5 有

定理 8.4.1

设 $K = \mathbb{Z}/p\mathbb{Z}$ 是一个有限域, 其中 p 是素数. 设 $p(x)$ 是 $K[x]$ 中的 n 次不可约多项式, 则

$$K[x]/((p(x))) = \{a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \mid a_i \in K\}$$

构成一个域, 记作 F_{p^n} . 这个域的元素个数为 p^n .

注: F_{p^n} 中的加法和乘法是:

$$f(x) + g(x) = (f + g)(x) \mod p(x),$$

$$f(x)g(x) = (fg)(x) \mod p(x).$$

例 8.4.1 设 $F_2 = \mathbb{Z}/2\mathbb{Z}$, 则 $p(x) = x^8 + x^4 + x^3 + x + 1$ 是 $F_2[x]$ 中的 8 次不可约多项式.

事实上, 我们有

$$F_{2^8} = F_2[x]/(x^8 + x^4 + x^3 + x + 1) = \{a_7x^7 + \cdots + a_1x + a_0 \mid a_i \in \{0, 1\}\}.$$

F_{2^8} 中的加法和乘法是:

$$f(x) + g(x) = (f + g)(x) \mod (x^8 + x^4 + x^3 + x + 1),$$

$$f(x)g(x) = (fg)(x) \mod (x^8 + x^4 + x^3 + x + 1).$$

另一方面, 单独考虑非零元, 可以证明: $F_q^* = F_q \setminus \{0\}$ 是 $q - 1$ 阶循环乘群. 为此, 先讨论 F_q^* 的一些性质.

定理 8.4.2

F_q^* 的任意元 a 的阶整除 $q - 1$.

另一方面, 单独考虑非零元, 可以证明: $F_q^* = F_q \setminus \{0\}$ 是 $q - 1$ 阶循环乘群. 为此, 先讨论 F_q^* 的一些性质.

定理 8.4.2

F_q^* 的任意元 a 的阶整除 $q - 1$.

证: (方法一) 设 $H = \langle a \rangle$ 是 a 生成的循环群, 根据推论 8.2.1, 有 $\text{ord}(a) = |H|$ 且 $|H| \mid |F_q^*|$, 即 $\text{ord}(a) \mid q - 1$.

另一方面, 单独考虑非零元, 可以证明: $F_q^* = F_q \setminus \{0\}$ 是 $q - 1$ 阶循环乘群. 为此, 先讨论 F_q^* 的一些性质.

定理 8.4.2

F_q^* 的任意元 a 的阶整除 $q - 1$.

证: (方法一) 设 $H = \langle a \rangle$ 是 a 生成的循环群, 根据推论 8.2.1, 有 $\text{ord}(a) = |H|$ 且 $|H| \mid |F_q^*|$, 即 $\text{ord}(a) \mid q - 1$.

(方法二) 设 $F_q^* = \{a_1, a_2, \dots, a_{q-1}\}$, 则 $a \cdot a_1, a \cdot a_2, \dots, a \cdot a_{q-1}$ 是 a_1, a_2, \dots, a_{q-1} 的一个排列, 其中 $a \in F_q^*$. 因此,
 $(a \cdot a_1)(a \cdot a_2) \cdots (a \cdot a_{q-1}) = a_1 a_2 \cdots a_{q-1}$, 即 $a^{q-1}(a_1 \cdots a_{q-1}) = a_1 \cdots a_{q-1}$.
两端右乘 $(a_1 a_2 \cdots a_{q-1})^{-1}$, 得 $a^{q-1} = 1$. 类似于定理 4.1.1 的证明, 有 $\text{ord}(a) \mid q - 1$.

定义 8.4.1

如果有限域 F_q 的元素 g 是 F_q^* 的生成元, 即阶为 $q-1$, 则称 g 为 F_q 的本原元. 此时, 有 $F_q = \{0\} \cup \langle g \rangle = \{0, g^0 = 1, g, \dots, g^{q-2}\}$. 同时, 称本原元 g 的极小多项式为本原多项式.

定义 8.4.1

如果有限域 F_q 的元素 g 是 F_q^* 的生成元, 即阶为 $q-1$, 则称 g 为 F_q 的本原元. 此时, 有 $F_q = \{0\} \cup \langle g \rangle = \{0, g^0 = 1, g, \dots, g^{q-2}\}$. 同时, 称本原元 g 的极小多项式为本原多项式.

定理 8.4.3

每个有限域都有本原元. 如果 g 是 F_q 的本原元, 则 g^d 是 F_q 的本原元当且仅当 $(d, q-1) = 1$. 特别地, F_q 有 $\varphi(q-1)$ 个本原元.

定义 8.4.1

如果有限域 F_q 的元素 g 是 F_q^* 的生成元, 即阶为 $q-1$, 则称 g 为 F_q 的本原元. 此时, 有 $F_q = \{0\} \cup \langle g \rangle = \{0, g^0 = 1, g, \dots, g^{q-2}\}$. 同时, 称本原元 g 的极小多项式为本原多项式.

定理 8.4.3

每个有限域都有本原元. 如果 g 是 F_q 的本原元, 则 g^d 是 F_q 的本原元当且仅当 $(d, q-1) = 1$. 特别地, F_q 有 $\varphi(q-1)$ 个本原元.

推论 8.4.1

设 $q = p^n$, p 为素数, $d \mid q-1$, 则有限域 F_q 中有阶为 d 的元素.

定义 8.4.1

如果有限域 F_q 的元素 g 是 F_q^* 的生成元, 即阶为 $q-1$, 则称 g 为 F_q 的本原元. 此时, 有 $F_q = \{0\} \cup \langle g \rangle = \{0, g^0 = 1, g, \dots, g^{q-2}\}$. 同时, 称本原元 g 的极小多项式为本原多项式.

定理 8.4.3

每个有限域都有本原元. 如果 g 是 F_q 的本原元, 则 g^d 是 F_q 的本原元当且仅当 $(d, q-1) = 1$. 特别地, F_q 有 $\varphi(q-1)$ 个本原元.

推论 8.4.1

设 $q = p^n$, p 为素数, $d \mid q-1$, 则有限域 F_q 中有阶为 d 的元素.

推论 8.4.2

设 p 为素数, 则存在整数 g 遍历模 p 简化剩余系, 即存在模 p 原根.

类似于模 p 原根的构造方法 (定理 4.2.7), 也有有限域 F_{p^n} 的本原元构造方法.

定理 8.4.4

给定有限域 F_{p^n} , 其中 p 为素数. 设 $p^n - 1$ 的所有不同素因数是 q_1, \dots, q_s , 则 g 是 F_{p^n} 中本原元的充要条件是

$$g^{\frac{p^n-1}{q_i}} \neq 1, \quad i = 1, \dots, s.$$

目录

- ① 分式域
- ② 素域与扩域
 - 有限扩域
 - 代数扩域
- ③ Galois 基本定理
- ④ 有限域
 - 有限域的构造
 - 有限域的 Galois 群
 - 有限域的正规基

定理 8.4.5

设 F_q 是 $q = p^n$ 元有限域, σ 是 F_q 到自身的映射, $\sigma: a \mapsto a^p$, 则 σ 是 F_q 的自同构, 且 F_q 中在 σ 下的不动元是素域 F_p 的元素, 而 σ 的 n 次幂是恒等映射.

定理 8.4.5

设 F_q 是 $q = p^n$ 元有限域, σ 是 F_q 到自身的映射, $\sigma: a \mapsto a^p$, 则 σ 是 F_q 的自同构, 且 F_q 中在 σ 下的不动元是素域 F_p 的元素, 而 σ 的 n 次幂是恒等映射.

证: 根据定理 7.2.1 以及定理 8.3.4, 有

$$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b),$$

$$\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b).$$

因此, σ 是 F_q 的自同构. 因为

$\sigma^2(a) = \sigma(a^p) = a^{p^2}, \dots, \sigma^j(a) = \sigma(a^{p^{j-1}}) = a^{p^j}, \dots, \sigma^n(a) = a^{p^n} = a$, 所以 σ^j 的不动元是 $x^{p^j} - x$ 的根. 特别地, 当 $j=1$ 时, σ 的不动元是 $x^p - x$ 的根, 这些根就是素域 F_p 的 p 个元素. 而当 $j=n$ 时, σ 的不动元是 $x^q - x$ 的根, 这些根就是域 F_q 的所有 q 个元素. 因此, σ^n 是恒等映射, σ 的逆映射是 σ^{n-1} .

定理 8.4.5

设 F_q 是 $q = p^n$ 元有限域, σ 是 F_q 到自身的映射, $\sigma: a \mapsto a^p$, 则 σ 是 F_q 的自同构, 且 F_q 中在 σ 下的不动元是素域 F_p 的元素, 而 σ 的 n 次幂是恒等映射.

证: 根据定理 7.2.1 以及定理 8.3.4, 有

$$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b),$$

$$\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b).$$

因此, σ 是 F_q 的自同构. 因为

$\sigma^2(a) = \sigma(a^p) = a^{p^2}, \dots, \sigma^j(a) = \sigma(a^{p^{j-1}}) = a^{p^j}, \dots, \sigma^n(a) = a^{p^n} = a$, 所以 σ^j 的不动元是 $x^{p^j} - x$ 的根. 特别地, 当 $j=1$ 时, σ 的不动元是 $x^p - x$ 的根, 这些根就是素域 F_p 的 p 个元素. 而当 $j=n$ 时, σ 的不动元是 $x^q - x$ 的根, 这些根就是域 F_q 的所有 q 个元素. 因此, σ^n 是恒等映射, σ 的逆映射是 σ^{n-1} .

注: 定理 8.4.5 中的映射 σ 叫作 Frobenius 自同构.

推论 8.4.3

设 F_q 是 $q = p^n$ 元有限域, 设 $\sigma: a \mapsto a^p$ 是 F_q 到自身的映射, $\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ 是 F_q 的子集, 且在 σ 下保持不变, 即 $\{\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_d)\}$ 是 $\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ 的一个置换, 则 $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$ 是 F_p 上的多项式.

推论 8.4.3

设 F_q 是 $q = p^n$ 元有限域, 设 $\sigma : a \mapsto a^p$ 是 F_q 到自身的映射, $\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ 是 F_q 的子集, 且在 σ 下保持不变, 即 $\{\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_d)\}$ 是 $\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ 的一个置换, 则 $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$ 是 F_p 上的多项式.

证: 因为多项式 f 的系数是 $\alpha_1, \alpha_2, \dots, \alpha_d$ 的对称多项式, 所以它们在 σ 下保持不变, 即它们属于 $I(\langle \sigma \rangle) = F_p$.

推论 8.4.3

设 F_q 是 $q = p^n$ 元有限域, 设 $\sigma : a \mapsto a^p$ 是 F_q 到自身的映射, $\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ 是 F_q 的子集, 且在 σ 下保持不变, 即 $\{\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_d)\}$ 是 $\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ 的一个置换, 则 $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$ 是 F_p 上的多项式.

证: 因为多项式 f 的系数是 $\alpha_1, \alpha_2, \dots, \alpha_d$ 的对称多项式, 所以它们在 σ 下保持不变, 即它们属于 $I(\langle \sigma \rangle) = F_p$.

定理 8.4.6

设 F_q 是 $q = p^n$ 元有限域, σ 是 F_q 到自身的映射, $\sigma : a \mapsto a^p$. 如果 α 是 F_q 的任意元, 则 α 在 F_p 上的共轭元是元素 $\sigma^j(\alpha) = \alpha^{p^j}$.

推论 8.4.3

设 F_q 是 $q = p^n$ 元有限域, 设 $\sigma : a \mapsto a^p$ 是 F_q 到自身的映射, $\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ 是 F_q 的子集, 且在 σ 下保持不变, 即 $\{\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_d)\}$ 是 $\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ 的一个置换, 则 $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$ 是 F_p 上的多项式.

证: 因为多项式 f 的系数是 $\alpha_1, \alpha_2, \dots, \alpha_d$ 的对称多项式, 所以它们在 σ 下保持不变, 即它们属于 $I(\langle \sigma \rangle) = F_p$.

定理 8.4.6

设 F_q 是 $q = p^n$ 元有限域, σ 是 F_q 到自身的映射, $\sigma : a \mapsto a^p$. 如果 α 是 F_q 的任意元, 则 α 在 F_p 上的共轭元是元素 $\sigma^j(\alpha) = \alpha^{p^j}$.

证: 设 $d = [F_p(\alpha) : F_p]$, 则 $F_p(\alpha)$ 可作为有限域 F_{p^d} (在同构意义下). 因此, α 满足 $x^{p^d} = x$, 但不满足 $x^{p^j} = x, 1 \leq j < d$. 由此, 重复应用 σ , 就得到 d 个不同元 $\alpha, \sigma(\alpha) = \alpha^p, \dots, \sigma^{d-1}(\alpha) = \alpha^{p^{d-1}}$. 断言: 这些元素是 α 的共轭元.

的极小多项式的全部根. 事实上, 设 α 的极小多项式为

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0, \quad a_i \in F_p,$$

则 $f(\alpha) = \alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = 0$. 两端作 p 次方, 根据定理 7.2.1, 并注意到 $a_i^p = a_i, 0 \leq i < d$, 有

$$f(\alpha^p) = (\alpha^p)^d + a_{d-1}(\alpha^p)^{d-1} + \cdots + a_1\alpha^p + a_0 = f(\alpha)^p = 0.$$

依次继续作 p 次方, 对于 $1 \leq j < d$, 有

$$f(\alpha^{p^j}) = (\alpha^{p^j})^d + a_{d-1}(\alpha^{p^j})^{d-1} + \cdots + a_1\alpha^{p^j} + a_0 = f(\alpha)^{p^j} = 0.$$

的极小多项式的全部根. 事实上, 设 α 的极小多项式为

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0, \quad a_i \in F_p,$$

则 $f(\alpha) = \alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = 0$. 两端作 p 次方, 根据定理 7.2.1, 并注意到 $a_i^p = a_i, 0 \leq i < d$, 有

$$f(\alpha^p) = (\alpha^p)^d + a_{d-1}(\alpha^p)^{d-1} + \cdots + a_1\alpha^p + a_0 = f(\alpha)^p = 0.$$

依次继续作 p 次方, 对于 $1 \leq j < d$, 有

$$f(\alpha^{p^j}) = (\alpha^{p^j})^d + a_{d-1}(\alpha^{p^j})^{d-1} + \cdots + a_1\alpha^{p^j} + a_0 = f(\alpha)^{p^j} = 0.$$

推论 8.4.4

设 F_q 是 $q = p^n$ 元有限域, σ 是 F_q 到自身的映射, $\sigma: a \mapsto a^p$. 设 $f(x)$ 是 F_p 上的 d 次首一不可约多项式. 如果 α 是 $f(x)$ 在 F_q 中的根, 则 $\alpha, \sigma(\alpha) = \alpha^p, \cdots, \sigma^{d-1}(\alpha) = \alpha^{p^{d-1}}$ 是 F_q 中的全部根, 其中 d 是使得 $\sigma^d(\alpha) = \alpha$ 的最小正整数.

定理 8.4.7

F_{q^n} 在 F_q 上的自同构集是一个阶为 n 的循环群, 其生成元为自同构 $\sigma_q(\alpha) = \alpha^q$.

定理 8.4.7

F_{q^n} 在 F_q 上的自同构集是一个阶为 n 的循环群, 其生成元为自同构 $\sigma_q(\alpha) = \alpha^q$.

证: 设 β 是 F_{q^n} 中的本原元, 则 β 在 F_q 上的阶为 $q^n - 1$, 且其极小多项式 $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F_q[x]$ 有根

$$\beta, \sigma_q(\beta) = \beta^q, \sigma_q^2(\beta) = \beta^{q^2}, \dots, \sigma_q^{n-1}(\beta) = \beta^{q^{n-1}}.$$

定理 8.4.7

F_{q^n} 在 F_q 上的自同构集是一个阶为 n 的循环群, 其生成元为自同构 $\sigma_q(\alpha) = \alpha^q$.

证: 设 β 是 F_{q^n} 中的本原元, 则 β 在 F_q 上的阶为 $q^n - 1$, 且其极小多项式 $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F_q[x]$ 有根

$$\beta, \sigma_q(\beta) = \beta^q, \sigma_q^2(\beta) = \beta^{q^2}, \dots, \sigma_q^{n-1}(\beta) = \beta^{q^{n-1}}.$$

设 $f(x)$ 是 F_q 上的多项式. 因为 F_{q^n} 在 F_q 上的自同构 τ 保持 $f(x)$ 的系数不变, 所以 $f(\alpha) = 0$ 的充要条件是 $f(\tau(\alpha)) = 0$. 换句话说, τ 对 $f(x)$ 在 F_{q^n} 中的根进行了置换. 特别地, 对于 $p(x)$ 的根 β , 存在 i 使得 $\tau(\beta) = \beta^{q^i}$. 故

$$\sigma_q^i(\beta) = \sigma_q(\sigma_q^{i-1}(\beta)) = \beta^{q^i} = \tau(\beta).$$

定理 8.4.7

F_{q^n} 在 F_q 上的自同构集是一个阶为 n 的循环群, 其生成元为自同构 $\sigma_q(\alpha) = \alpha^q$.

证: 设 β 是 F_{q^n} 中的本原元, 则 β 在 F_q 上的阶为 $q^n - 1$, 且其极小多项式 $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F_q[x]$ 有根

$$\beta, \sigma_q(\beta) = \beta^q, \sigma_q^2(\beta) = \beta^{q^2}, \dots, \sigma_q^{n-1}(\beta) = \beta^{q^{n-1}}.$$

设 $f(x)$ 是 F_q 上的多项式. 因为 F_{q^n} 在 F_q 上的自同构 τ 保持 $f(x)$ 的系数不变, 所以 $f(\alpha) = 0$ 的充要条件是 $f(\tau(\alpha)) = 0$. 换句话说, τ 对 $f(x)$ 在 F_{q^n} 中的根进行了置换. 特别地, 对于 $p(x)$ 的根 β , 存在 i 使得 $\tau(\beta) = \beta^{q^i}$. 故

$$\sigma_q^i(\beta) = \sigma_q(\sigma_q^{i-1}(\beta)) = \beta^{q^i} = \tau(\beta).$$

因为 β 是 F_{q^n} 的本原元, 得 $\tau = \sigma_q^i$. 因此, F_{q^n} 在 F_q 上的自同构集是一个阶为 n 的循环群, 其生成元为自同构 $\sigma_q(\alpha) = \alpha^q$.

目录

- ① 分式域
- ② 素域与扩域
 - 有限扩域
 - 代数扩域
- ③ Galois 基本定理
- ④ 有限域
 - 有限域的构造
 - 有限域的 Galois 群
 - 有限域的正规基

最后, 再次从向量空间的基底角度考虑有限域. 易知,

设 α 是 F_q 上次数为 n 的 F_{q^n} 中的元素, 则 $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ 构成 F_{q^n} 在 F_q 上的一组基底, 称作**多项式基底**.

结合上述知识, 我们可以找到另外一种形式的基底.

最后, 再次从向量空间的基底角度考虑有限域. 易知,

设 α 是 F_q 上次数为 n 的 F_{q^n} 中的元素, 则 $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ 构成 F_{q^n} 在 F_q 上的一组基底, 称作**多项式基底**.

结合上述知识, 我们可以找到另外一种形式的基底.

定义 8.4.2

F_{q^n} 在 F_q 上形如 $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}$ 的基底叫作 F_{q^n} 在 F_q 上的**正规基**.

最后, 再次从向量空间的基底角度考虑有限域. 易知,

设 α 是 F_q 上次数为 n 的 F_{q^n} 中的元素, 则 $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ 构成 F_{q^n} 在 F_q 上的一组基底, 称作**多项式基底**.

结合上述知识, 我们可以找到另外一种形式的基底.

定义 8.4.2

F_{q^n} 在 F_q 上形如 $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}$ 的基底叫作 F_{q^n} 在 F_q 上的**正规基**.

定理 8.4.8

有限域 F_{q^n} 在其子域 F_q 上有正规基存在.

证: 略.

例 8.4.2 求 $F_{2^4} = F_2[x]/(x^4 + x + 1)$ 中的正规基.

例 8.4.2 求 $F_{2^4} = F_2[x]/(x^4 + x + 1)$ 中的正规基.

解: (i) 对于 $\beta = x$, 有

$$\beta = x,$$

$$\beta^2 = x^2,$$

$$\beta^4 = x + 1,$$

$$\beta^8 = x^2 + 1,$$

所以, $\beta, \beta^2, \beta^{2^2}, \beta^{2^3}$ 不构成一组基底.

例 8.4.2 求 $F_{2^4} = F_2[x]/(x^4 + x + 1)$ 中的正规基.

解: (i) 对于 $\beta = x$, 有

$$\beta = x,$$

$$\beta^2 = x^2,$$

$$\beta^4 = x + 1,$$

$$\beta^8 = x^2 + 1,$$

所以, $\beta, \beta^2, \beta^{2^2}, \beta^{2^3}$ 不构成一组基底.

(ii) 对于 $\beta = x^3$, 有

$$\beta = x^3 = x^3,$$

$$\beta^2 = x^6 = x^3 + x^2,$$

$$\beta^4 = x^{12} = x^3 + x^2 + x + 1,$$

$$\beta^8 = x^9 = x^3 + x,$$

所以, $\beta, \beta^2, \beta^{2^2}, \beta^{2^3}$ 构成一组基底, 是正规基.

本课作业

1. 证明: $x^3 + x + 1$ 是 $F_2[x]$ 中的不可约多项式,
从而 $F_{2^3} = F_2[x]/(x^3 + x + 1)$ 是一个域.
2. 计算由 $F_2[x]/(x^3 + x + 1)$ 得到的有限域 F_{2^3} .
3. $g(x) = x$ 是否为 F_{2^3} 的生成元?
4. 证明: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
5. 设 K 是 F 的扩域, E_1 和 E_2 包含于 K 中, 且都是 F 的扩域. 证明:
如果 $[E_1 : F]$ 和 $[E_2 : F]$ 都是素数, 则 $E_1 = E_2$ 或 $E_1 \cap E_2 = F$.

交流与讨论



电子邮箱:

陈秀波: xb_chen@bupt.edu.cn

徐国胜: guoshengxu@bupt.edu.cn

金正平: zhpjin@bupt.edu.cn