第7章　有限域

7.1 域的有限扩张

定义 7.1.1 设F为一个域，K为F的一个非空子集，如果相对于F中的加法和乘法，K也构成一个域，则称K为F的一个子域，F为K的一个扩域（也称F为K的一个扩张）。

例 1 复数域为实数域的扩域，实数域为有理数域的扩域，反过来，有理数域是实数域的一个子域，实数域是复数域的一个子域。

定义 7.1.2 没有真子域的域称为素域。

例 2 p 为素数，设 K 为有限域 F_p 的一个子域，则 $0,1 \in K$，

从而

$$1, 2\cdot 1, 3\cdot 1, \cdots, (p-1)\cdot 1 \in K,$$

故而

$$K = F_p。$$

有理数域 Q 亦为素域。

定理 7.1.1 设 p 为素数，F 为域，则

(1) 当 $char(F)=p$ 时，存在 F 的一个子域与 F_p 同构；

(2) 当 $char(F)=0$ 时，存在 F 的一个子域与 Q 同构。

证明：考虑映射 $\varphi: Z \to F$

$$\varphi(n)=n\cdot 1,$$

其中 **1** 为域 F 的单位元，则 φ 为一环同态。

定义 7.1.3 设F为域，K为F的一个子域，M为F的一个子集合，则包含K及M的所有F的子域的交构成包含K及M的F的最小子域，记为$K(M)$，是添加M而得到的K的扩域。

当M为有限集时，令$M=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$，则

$$K(M)=K(\alpha_1,\alpha_2,\cdots,\alpha_n)。$$

特别当$M=\{\alpha\}$时，$K(M)=K(\alpha)$，称为K的单扩域（或单扩张）。

定义 7.1.4 设K是F的一个子域，$\alpha \in F$。若存在$f(x) \in K[x]$，$f(x) \neq 0$，使得$f(\alpha)=0$，则称α为K上的代数元，否则称为超越元。若扩域F中的元都为K上的代数元，则称F为K的代数扩域（或代数扩张）。

假设$\alpha \in F$是K上的代数元，考虑集合

$$N_\alpha = \{ f(x) \in K[x] \mid f(\alpha)=0 \},$$

它是$K[x]$的一个理想，称为代数元α在$K[x]$中的零化理想。

对任意$f, g \in N_\alpha$，有

即$f-g, fg \in N_\alpha$。

又$\forall f \in N_\alpha, g \in K[x]$，

即 $fg \in N_\alpha$。

由$K[x]$为主理想整环知，存在$m_\alpha(x)\in K[x]$，$m_\alpha(x)\neq 0$，使得

$$N_\alpha=(m_\alpha(x))。$$

若限定$m_\alpha(x)$为首一多项式，则$m_\alpha(x)$由α唯一确定。

定义 **7.1.5** 以上由代数元α唯一确定的首一多项式$m_\alpha(x)\in K[x]$，称为α在K上的极小多项式。α在K上的次数指$m_\alpha(x)$的次数。

在提及代数元的极小多项式及其次数时一定要指明是在哪个域上！

定理 7.1.2 设$\alpha \in F$为K上的代数元，则其在K上的极小多项式$m_\alpha(x)$满足：

(1) $m_\alpha(x)$为$K[x]$中的不可约多项式；

(2) $\forall f \in K[x]$， $f(\alpha)=0 \Leftrightarrow m_\alpha(x) \mid f(x)$。

定义 7.1.6 F 为域 K 的一个扩张，将 F 看成 K 上的向量空间，若是有限维的，则称 F 为 K 的有限扩张，K 上向量空间 F 的维数称为扩张次数，记为 $(F:K)$。

例 **4** 复数域 C 是实数域 R 的一个扩张。

任意 $z \in C$，有

$$z = a + bi，\ a,b \in R，$$

且该表达式唯一确定，故 C 可看成 R 上的 **2** 维向量空间，所以有

$$(C:R) = 2，\text{基为} 1,\ i。$$

定理 7.1.3 域F为域E的有限扩张，域E为域K的有限扩张，则F为K的有限扩张，且

$$(F:K)=(F:E)(E:K)。$$

定理 **7.1.3** 中的E通常称为K和F间的中间域。

$$K \text{——} E \text{——} F$$

定理 7.1.4 域K的每一个有限扩张都是代数扩张。

定理 7.1.5 设$\alpha \in F$为K上的n次代数元，$m_\alpha(x)$为α在K上的极小多项式，则

(1) $K(\alpha) \cong K[x]/(m_\alpha(x))$；

(2) $(K(\alpha):K)=n$，且$\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$为$K(\alpha)$在$K$上的一组基。

注：**1.** $K(\alpha)=\{c_0+c_1\alpha+c_2\alpha^2+\cdots+c_{n-1}\alpha^{n-1}\mid c_i\in K,0\le i\le n-1\}$

$\cong K[x]/(m_\alpha(x))$

2. $K(\alpha)\cong K[x]/(m_\alpha(x))$，令$\varphi$为它们之间的同构，即

$$\varphi(f(\alpha))=f(x),$$

则对任意$k\in K$，有$\varphi(k)=k$。

定义 **7.1.7**（域的 **K-**同构）设F_1,F_2为域K的扩张，σ为F_1到F_2的同构映射，且对任意$k\in K$，有$\sigma(k)=k$，则称σ为F_1与F_2的 **K-**同构。

定义 7.1.8 F 为域 K 的一个扩张，F 称为 $f(x)\in K[x]$ 在 K 上的分裂域，是指它满足：

(1) $f(x)$ 在 $F[x]$ 内可分解成一次因式的乘积，即 $f(x)=a(x-\alpha_1)\cdots(x-\alpha_n)$，其中 a 为 $f(x)$ 的首系数，$\alpha_i\in F, 1\le i\le n$；

(2) $F=K(\alpha_1,\alpha_2,\cdots,\alpha_n)$。

定理 7.1.6 设K为一个域，$f(x)\in K[x]$为一不可约多项式，则存在K的一个扩域F使得$f(x)$在F中有根。设α,β都是$f(x)$的根，则K的两个单代数扩张$K(\alpha)$和$K(\beta)$有一个K-同构σ使得$\sigma(\alpha)=\beta$。

定理 7.1.7 设F为一个域，则每一非零多项式$f(x)\in F[x]$在F上都有一个分裂域。

例 5 我们来看分裂域的一个例子。

设 $f(x)=x^4-5x^2+6\in Q[x]$，易知在有理数域Q上有

$$f(x)=(x^2-2)(x^2-3)。$$

取不可约因式 $f_1(x)=x^2-2$，我们先作$E_1=Q(\alpha_1)$，在E_1中我们有

$$f_1(x)=x^2-2=(x-\alpha_1)(x+\alpha_1)，$$

此时

$$f(x)=(x-\alpha_1)(x+\alpha_1)(x^2-3)。$$

又 $f_2(x)=x^2-3$在E_1中不可约：

若存在$\xi\in E_1$使得$\xi^2=3$，可设$\xi=a+b\alpha_1$，$a,b\in Q$，我们有

$$\xi^2=(a^2+2b^2)+2ab\alpha_1=3，$$

则 $$a^2+2b^2=3且ab=0，$$

若$a=0$，则$b^2=\frac{3}{2}$；若$b=0$，则$a^2=3$。

这两种情况在有理数域Q中都是不可能的。

我们再作$E=E_1(\alpha_2)$，在E中我们有

$$f_2(x)=x^2-3=(x-\alpha_2)(x+\alpha_2)，$$

此时

$$f(x)=(x^2-2)(x^2-3)=(x-\alpha_1)(x+\alpha_1)(x-\alpha_2)(x+\alpha_2)，$$

故$E=E_1(\alpha_2)=Q(\alpha_1)(\alpha_2)=Q(\alpha_1,\alpha_2)$是$f(x)$在有理数域$Q$上的一个分裂域。

由定理 **7.1.5** 知

$$[E_1:Q]=2，[E:E_1]=2，$$

再由定理 **7.1.3** 知

$$[E:Q]=[E:E_1][E_1:Q]=4。$$

定理 7.1.8 设F为一个域，则每一非零多项式$f(x)\in F[x]$在F上的任意两个分裂域都是同构的。

7.2 有限域（Galois域）的性质

有限域根据它的发现者 **Evariste Galois**（**1811－1832**）的名字又被称为 **Galois** 域。它就是具有有限多个元的域，例如我们前面见到的F_p，其中p为素数，及$F[x]/(f(x))$，其中$f(x)$为$F[x]$上的首一不可约多项式。

定理 7.2.1 设F为一个有限域，则$|F| = p^n$，其中p为F的特征，n为F在其素域上的扩张次数。

定理 7.2.2 F 为 q 阶有限域，则任意 $a \in F$，有 $a^q = a$。

注：q 阶有限域 F 中的 q 个元均满足方程

$$x^q - x = 0,$$

即 F 的 q 个元是多项式

$$G(x) = x^q - x$$

的 q 个零点。

定理 7.2.3 设$q = p^n$，p为素数，则必存在一个q阶有限域，
并且在同构的意义下，这个域是唯一的。

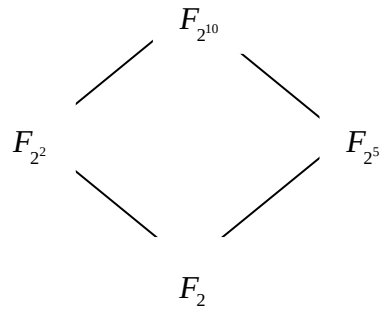
证明：（存在性）考虑$G(x) = x^q - x \in F_p[x]$在素域$F_p$上的一个分裂域。

（唯一性）利用分裂域的唯一性。

定理 7.2.4 设F_q为一$q=p^n$阶有限域，则F_q的每一子域的阶形如p^m，其中m为n的正因子。反之，若m为n的正因子，则F_q恰有一个p^m阶子域，且F_q中的元素a属于F_{p^m}当且仅当$a^{p^m}=a$。

例 **1** 确定$F_{2^{10}}$的所有子域。

解：**10** 的所有正因子为 **1, 2, 5, 10**，所以由定理 **7.2.3**，$F_{2^{10}}$的所有子域为$F_2, F_{2^2}, F_{2^5}, F_{2^{10}}$，它们之间的关系可用如下的哈斯图表示：



即F_2是$F_{2^2}, F_{2^5}, F_{2^{10}}$的子域，$F_{2^2}, F_{2^5}$是$F_{2^{10}}$的子域。

定理 7.2.5 有限域F_q的乘法群F_q^*是一个循环群。

证明：构造一个$|F_q^*|=q-1$阶元。

定义 7.2.1 循环群F_q^*的生成元称为有限域F_q的本原元。

利用循环群的知识易知：

有限域F_q共有$\varphi(q-1)$个本原元，

若a是一个本原元，则所有的本原元为

$$\{a^k \mid (k, q-1)=1\}。$$

由定理 **7.2.5** 知，有限域F_q中的所有非零元可以表示为其本原元a的整数次幂，若给定整数k，要求F_q中的非零元a^k是比较容易做到的。

而反过来，若给定F_q中的非零元b，要求正整数$n<q$使得$b=a^n$则是一个很困难的问题，这就是密码学中常用到的有限域上的离散对数问题。

定理 7.2.6 设F_q为一有限域，F_r为其有限扩张，则F_r为F_q的单扩域，即$F_r = F_q(\xi)$，其中ξ为F_r的任一本原元。

7.3 有限域的表示

给出有限域F_q中元素的不同表示方式，$q = p^n$， p为F_q的特征。

F_q是F_p的一个单扩张。若$f(x)$为F_p上的一个n次不可约多项式，则$f(x)$在F_q上必有根α，且$F_q = F_p(\alpha)$，而$F_p(\alpha) \cong F_p[x]/(f(x))$。

由此，我们可以用$F_p[x]$中次数小于n的多项式来表示F_q中的元，即将F_q看成是剩余类环$F_p[x]/(f(x))$，即

$$F_q = \{f(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F_p[x]\}; \qquad \textbf{(1)}$$

我们也可以用关于α的F_p上的次数小于n的多项式来表示F_q中的元，即

$$F_q = \{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \mid a_i \in F_p, i = 0,1,\cdots,n-1\}. \qquad \textbf{(2)}$$

域元素简记为其系数构成的n元组$(a_{n-1},\cdots,a_1,a_0)$

不同的是在表示“**(1)**”中的运算为模多项式$f(x)$的加法和模多项式$f(x)$的乘法。

由定理 **7.2.5** 知，我们还可以用F_q的一个本原元ξ来表示它的元，即

$$F_q=\{0,1,\xi^2,\cdots,\xi^{q-2}\}。 \qquad \textbf{(3)}$$

有限域的不同表示方式会影响其中运算的复杂程度。

在多项式表示法**(1),(2)**中加法容易计算，如

$$\beta=(b_{n-1},\cdots,b_0)，\ \gamma=(c_{n-1},\cdots,c_0)，$$

则
$$\beta+\gamma=(b_{n-1}+c_{n-1},\cdots,b_0+c_0)，$$

其中b_i+c_i为F_p中的加法运算。

本原元表示法**(3)**中乘法容易计算，但加法较为复杂。如

$$\beta=\xi^t，\ \gamma=\xi^s，$$

则
$$\beta\gamma=\xi^t\xi^s=\xi^{t+s}，$$

其中$t+s$为模$q-1$加法。

例 **1** 表示F_{16}

令$f(x)=x^4+x+1\in F_2[x]$，易验证$f(x)$为F_2上一个 **4** 次不可约多项式，故可构造有限域$F_{16}=F_{2^4}$，令α为$f(x)$在F_{16}中的一个根，则

$$F_{16}=\{f(x)=a_3x^3+a_2x^2+a_1x+a_0\in F_2[x]\},$$

或

$$F_{16}=\{b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0\,|\,b_i\in F_2,0\le i\le 3\},$$

简记为

$$F_{16}=\{0000,0001,0010,0011,0100,0101,0110,0111,$$
$$1000,1001,1010,1011,1100,1101,1110,1111\},$$

为方便，还可将上式中F_{16}的元素用适当进制的对应数来表示。例如，若用十进制数表示，则

$$F_{16}=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}。$$

由α为$f(x)$在F_{16}中的一个根知$\alpha^4+\alpha+1=0$，则有

$$\alpha^4=\alpha+1,$$

反复利用此式，可以得出

$$\alpha^5=\alpha(\alpha+1)=\alpha^2+\alpha$$
$$\alpha^6=\alpha(\alpha^2+\alpha)=\alpha^3+\alpha^2$$
$$\alpha^7=\alpha(\alpha^3+\alpha^2)=\alpha^4+\alpha^3=\alpha^3+\alpha+1$$
$$\alpha^8=\alpha(\alpha^3+\alpha+1)=\alpha^4+\alpha^2+\alpha=\alpha^2+1$$
$$\alpha^9=\alpha(\alpha^2+1)=\alpha^3+\alpha$$
$$\alpha^{10}=\alpha(\alpha^3+\alpha)=\alpha^4+\alpha^2=\alpha^2+\alpha+1$$
$$\alpha^{11}=\alpha(\alpha^2+\alpha+1)=\alpha^3+\alpha^2+\alpha$$
$$\alpha^{12}=\alpha(\alpha^3+\alpha^2+\alpha)=\alpha^4+\alpha^3+\alpha^2=\alpha^3+\alpha^2+\alpha+1$$
$$\alpha^{13}=\alpha(\alpha^3+\alpha^2+\alpha+1)=\alpha^4+\alpha^3+\alpha^2+\alpha=\alpha^3+\alpha^2+1$$
$$\alpha^{14}=\alpha(\alpha^3+\alpha^2+1)=\alpha^4+\alpha^3+\alpha=\alpha^3+1$$
$$\alpha^{15}=\alpha(\alpha^3+1)=\alpha^4+\alpha=1$$

说明α是一个 **15** 阶元，即为F_{16}的一个本原元，从而利用本原元表示法有

$$F_{16}=\{0,1,\alpha,\alpha^2,\cdots,\alpha^{14}\}。$$

而且F_{16}中每个元素的不同表示可列表如下：

$0=(0\,0\,0\,0)$，	$\alpha^4=(0\,0\,1\,1)$，	$\alpha^8=(0\,1\,0\,1)$，	$\alpha^{12}=(1\,1\,1\,1)$，
$\alpha=(0\,0\,1\,0)$，	$\alpha^5=(0\,1\,1\,0)$，	$\alpha^9=(1\,0\,1\,0)$，	$\alpha^{13}=(1\,1\,0\,1)$，
$\alpha^2=(0\,1\,0\,0)$，	$\alpha^6=(1\,1\,0\,0)$，	$\alpha^{10}=(0\,1\,1\,1)$，	$\alpha^{14}=(1\,0\,0\,1)$，
$\alpha^3=(1\,0\,0\,0)$，	$\alpha^7=(1\,0\,1\,1)$，	$\alpha^{11}=(1\,1\,1\,0)$，	$\alpha^{15}=(0\,0\,0\,1)$。

求乘法可用左边的表达式，如

求加法可用右边的表达式，如

现在就有一个问题，那就是如何寻找有限域F_q的一个本原元。

试算　　利用群元素的阶的性质

Gauss 算法

Guass 算法是一个用于求任一有限域F_q的本原元的算法。由 **Gauss** 算法可以获得一系列域元素$a_1, a_2, \cdots, a_k$，它们满足

$$ord(a_1) < ord(a_2) < \cdots < ord(a_k) = q-1,$$

$$ord(a_i) \mid ord(a_{i+1}),\ i = 1, 2, \cdots, k-1。$$

Gauss算法

1. 令$i=1$，取F_q中任一非零元a_i，计算其阶，记$ord(a_i)=k_i$。

2. 若$k_i=q-1$，则a_i为一本原元，停止循环；否则，转至“**3**”。

3. 取F_q中另一非零元b，满足b不是a_i的整数次幂，计算其阶，记$ord(b)=h$，若$h=q-1$，则令$a_{i+1}=b$即为一本原元，停止循环；否则，转至“**4**”。

4. 取整数t,s使得$t\mid k_i, s\mid h, (t,s)=1, ts=[k_i,h]$，令$a_{i+1}=a_i^{\frac{k_i}{t}}b^{\frac{h}{s}}$，则$ord(a_{i+1})=k_{i+1}=ts$，$i$增加 **1**，转至“**2**”。

注：a_i的阶随着i的增加在严格的递增

因为“**3**”中非零元b不是a_i的整数次幂意味着b的阶h一定不是k_i的因子

所以$ord(a_{i+1})=[k_i,h]$必严格大于k_i。

“4”中$ord(a_{i+1}) = ord(a_i^{\frac{k_i}{t}} b^{\frac{h}{s}}) = ts = k_{i+1}$

“4”中的“整数t,s”一定存在：

设m,n为任意两个整数，设它们的唯一分解式为

$$m = p_1^{e_1} \cdots p_r^{e_r} q_1^{c_1} \cdots q_l^{c_l}，\ n = p_1^{e_1'} \cdots p_r^{e_r'} g_1^{d_1} \cdots g_k^{d_k}，$$

其中 $p_i(i=1,2,\cdots,r)$ 为 m,n 共有的素因子，$q_i(i=1,2,\cdots,l)$ 和 $g_i(i=1,2,\cdots,k)$ 为互不相同的素数，$e_i(i=1,\cdots,r)$，$c_i(i=1,\cdots,l)$，$e_i'(i=1,\cdots,r)$，$d_i(i=1,\cdots,k)$ 均为正整数，取t,s如下：

$$t = p_1^{t_1} \cdots p_r^{t_r} q_1^{c_1} \cdots q_l^{c_l}，\ s = p_1^{s_1} \cdots p_r^{s_r} g_1^{d_1} \cdots g_k^{d_k}，$$

其中，对于任意$1 \le i \le r$

$$t_i = \begin{cases} e_i & 若 e_i \ge e_i' \\ 0 & 若 e_i < e_i' \end{cases}，\quad s_i = \begin{cases} 0 & 若 e_i \ge e_i' \\ e_i' & 若 e_i < e_i' \end{cases}，$$

则$t \mid m, s \mid n, (t,s) = 1, ts = [m,n]$。

例 **2** $f(x)=x^2-2\in F_5[x]$为F_5上一不可约多项式，由此我们可以构造F_{5^2}，

设α为$f(x)$在F_{5^2}中的一个根，则

$$F_{5^2}=\{c_1\alpha+c_0\,|\,c_0,c_1\in F_5\},$$

下面我们利用 **Gauss** 算法来求这个域的一个本原元。

取$a_1=\alpha$，计算$ord(a_1)$，为此我们利用$\alpha^2-2=0$，即$\alpha^2=2$，依次计算其整数次幂：

$$a_1^{\,0}=1,$$
$$a_1^{\,1}=\alpha,$$
$$a_1^{\,2}=2,$$
$$a_1^{\,3}=2\cdot a_1=2\alpha,$$
$$a_1^{\,4}=2\alpha\cdot a_1=2\alpha^2=4,$$
$$a_1^{\,5}=4\cdot a_1=4\alpha,$$
$$a_1^{\,6}=4\alpha\cdot a_1=4\alpha^2=3,$$
$$a_1^{\,7}=3\cdot a_1=3\alpha,$$
$$a_1^{\,8}=3\alpha\cdot a_1=3\alpha^2=1。$$

由此可得$ord(a_1)=8$，即 **Guass** 算法中$k_1=8$。

因为$k_1 \neq q-1=24$，所以a_1不是本原元。

转至“**3**”，选取$b=\alpha+1$，不是a_1的整数次幂，同样利用$\alpha^2-2=0$，即$\alpha^2=2$，依次计算其整数次幂：

$$b^0=1,\quad b^1=\alpha+1,\quad b^2=(\alpha+1)^2=\alpha^2+2\alpha+1=2\alpha+3,$$
$$b^3=(2\alpha+3)\cdot b=2\alpha^2+3=2,\quad b^4=2\cdot b=2\alpha+2,$$
$$b^5=(2\alpha+2)\cdot b=2\alpha^2+4\alpha+2=4\alpha+1,$$
$$b^6=(4\alpha+1)\cdot b=4\alpha^2+1=4,\quad b^7=4\cdot b=4\alpha+4,$$
$$b^8=(4\alpha+4)\cdot b=4\alpha^2+3\alpha+4=3\alpha+2,$$
$$b^9=(3\alpha+2)\cdot b=3\alpha^2+2=3,\quad b^{10}=3\cdot b=3\alpha+3,$$
$$b^{11}=(3\alpha+3)\cdot b=3\alpha^2+\alpha+3=\alpha+4,$$
$$b^{12}=(\alpha+4)\cdot b=\alpha^2+4=1。$$

由此可得$ord(b)=12$，即 **Gauss** 算法中$h=12$。

因为$h \neq q-1=24$，所以b不是本原元。

注意此时有

$$a_1=\alpha，\ k_1=8=2^3，$$
$$b=\alpha+1，\ h=12=2^2\cdot 3。$$

转至“**4**”，取$t=2^3=8$，$s=3$，则$ts=24=[8,12]$，因此

$$a_2=a_1^{\frac{k_1}{t}}b^{\frac{h}{s}}=a_1\cdot b^4=a_1(2a_1+2)=2a_1^{\ 2}+2a_1=2\alpha+4，$$

具有阶 **24**。

转至“**2**”，$k_2=24$，停止循环，$a_2=2\alpha+4$即为F_{5^2}的一个本原元。

7.4 有限域上的多项式

定义 7.4.1 设 $f(x)$为有限域F_q上的一个n次不可约首一多项式，若 $f(x)$的根α为F_{q^n}的本原元，则称 $f(x)$为$F_q[x]$中的本原多项式。

定义 7.4.2 设 $f(x)\in F_q[x]$， $f(0)\neq 0$，称使得

$$f(x)\,|\,x^d-1$$

成立的最小正整数d为多项式 $f(x)$的周期或阶，记为$\Pi(f(x))=\Pi(f)=d$。

定理 7.4.1 设 $f(x)$为有限域F_q上的一个n次不可约多项式，α 为 $f(x)$ 的一个根，则 $f(x)$ 的全部根为 $\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{n-1}}$，并且这$n$个根是互异的。

定理 **7.4.1** 中的$\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$称为$\alpha$关于$F_q$的共轭元。

由循环群的性质易知，α关于F_q的共轭元具有相同的阶。

由定理 **7.4.1** 的证明可以看出，α 的次数 n 即其极小多项式的次数 n 是使得

$$\alpha^{q^n} = \alpha$$

成立的最小正整数，也就是使得

$$q^n \equiv 1 (\mathrm{mod}\, ord(\alpha)) \qquad (*)$$

成立的最小正整数。

定理 7.4.2 设 $f(x)\in F_q[x]$为一n次不可约多项式，则$\Pi(f)$等于 $f(x)$在F_{q^n}中任一根的阶，特别地，$f(x)\in F_q[x]$为本原多项式当且仅当$\Pi(f)=q^n-1$。

定理 7.4.3 $F_q[x]$中的n次本原多项式共有$\dfrac{\varphi(q^n-1)}{n}$。

定理 7.4.4 设α是F_q的扩域F_{q^n}中的元素，则α在$F_q[x]$中的极小多项式为

$$f(x)=(x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{d-1}}),$$

其中d为α的次数，它由(*)式决定，并且$d \mid n$。

例 **1** 由 **7.3** 例 **1**，设α为本原多项式$f(x)=x^4+x+1\in F_2[x]$的一个根，则由$f(x)$构造的F_{16}^{*}可表示如下：

i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
α^i	0001	0010	0100	1000	0011	0110	1100	1011

i	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
α^i	0101	1010	0111	1110	1111	1101	1001	0001

$i=0$时，**1** 的极小多项式为$x-1\in F_2[x]$，也就是$x+1$。

$i=1$时，α的极小多项式就是定义该域的多项式，这里即为x^4+x+1。我们套用定理 **7.4.4**，有

$d=4$，因为$ord(\alpha)=15$，**4** 是使$2^4\equiv 1(\mathrm{mod}15)$成立的最小正整数，

于是α的极小多项式为

$$(x-\alpha)(x-\alpha^2)(x-\alpha^{2^2})(x-\alpha^{2^3})，$$

利用$\alpha^4=\alpha+1$可以验证，

$$(x-\alpha)(x-\alpha^2)(x-\alpha^{2^2})(x-\alpha^{2^3})=x^4+x+1。$$

$i=2$时，由上知$\alpha,\alpha^2,\alpha^4,\alpha^8$互为共轭元，它们具有相同的极小多项式，由上知即为$x^4+x+1$。

$i=3$时，$ord(\alpha^3)=\dfrac{15}{(3,15)}=5$，从而$d=4$，于是$\alpha^3$

的极小多项式为

$$\begin{aligned}&(x-\alpha^3)(x-(\alpha^3)^2)(x-(\alpha^3)^{2^2})(x-(\alpha^3)^{2^3})\\=&(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)\\=&x^4+x^3+x^2+x+1\end{aligned}$$

。

我们也可以通过寻找α^3的前 **5** 个整数次幂的线性相关性来获得它的极小多项式，例如

$$\begin{aligned}(\alpha^3)^0&=(0001),\\(\alpha^3)^1&=(1000),\\(\alpha^3)^2&=(1100),\\(\alpha^3)^3&=(1010),\\(\alpha^3)^4&=(1111),\end{aligned}$$

对于此例来说易知$(\alpha^3)^4+(\alpha^3)^3+(\alpha^3)^2+(\alpha^3)^1+1=0$，从而$\alpha^3$的极小多项式为

$$x^4+x^3+x^2+x+1。$$

一般情况下，我们可将不同整数次幂的向量表示构成一个矩阵，然后通过初等列变换来寻找它们之间的相关性。

例 **2** 由 **7.3** 例 **2**，$f(x)=x^2-2\in F_5[x]$，α 为 $f(x)$ 的一个根，则由 $f(x)$ 构造的 F_{5^2} 中 $\beta=2\alpha+4$ 为一本原元，从而所有 $\varphi(5^2-1)=8$ 个本原元为

$$\beta,\beta^5,\beta^7,\beta^{11},\beta^{13},\beta^{17},\beta^{19},\beta^{23}。$$

利用前面的方法可求得它们的极小多项式。

例如，β 的极小多项式为

$$(x-\beta)(x-\beta^5)=x^2-3x-2,$$

也就是 x^2+2x+3。

我们也可以利用β的前 **3** 个整数次幂

$$\beta^0=(0,1)，\ \beta=(2,4)，\ \beta^2=(1,4)，$$

得到如下F_5上的矩阵

$$\begin{pmatrix}0&1\\2&4\\1&4\end{pmatrix},$$

对该矩阵进行初等列变换，将它的第一列加到第二列上可得

$$\begin{pmatrix}0&1\\2&1\\1&0\end{pmatrix},$$

由此容易看到矩阵的第三行加上第二行的 **2** 倍再加上第一行的 **3** 倍等于零向量，即有 $\beta^2+2\beta+3=0$，

因此，亦可知β的极小多项式为 x^2+2x+3。

其它本原元的极小多项式也可同样求得。