第3章 有 限 域

3.1 定 义

F 是至少含有两个元素的集合，对于 F 的元素定义有“+”和“·”两种运算，并满足以下三个条件：

(1) 关于“+”运算 F 构成交换群，设其单位元为 0。

(2) $F\backslash\{0\}$ 关于运算“·”构成交换群。$F\backslash\{0\}$ 表示排除 0 元素以外的 F 元素全体。

(3) $a(b+c)=ab+ac$

$(b+c)a=ba+ca$

复数全体 C 关于复数的“+”和“·”构成复数域 C。

实数全体 R 关于数的“+”和“·”构成实数域 R。

有理数的全体 Q 关于数的“+”和“·”构成有理数域 Q。

若 p 是素数，$F=\{0,1,2,\cdots,p-1\}$ 关于 mod p 的“+”和“·”构成有限域 $F(p)$，这个域用 GF(p)表示它，称之为 Galois 域。在群论已讨论 F 关于 mod p 的“+”构成有限交换群，而 $F\backslash\{0\}=\{1,2,\cdots,p-1\}$ 关于 mod p 的“·”构成交换群，而且分配律成立。C,R,Q 不是有限域，域的元素无限多，GF(p)则是有限域。还可以将 GF(p)推广到 GF(p^n)，令

$$p(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1},\quad a_i\in \mathrm{GF}(p),\quad i=0,1,2,\cdots,n-1$$

$\{p(x)\}$ 的元素个数为 p^n 个。

例 GF(2)=$\{0,1\}$，$n=2$，次方小于 2 的系数在 GF(2)的多项式有 $2^3=8$ 个。

$$\begin{aligned}
&0\text{ 次：}p_{000}=0, && p_{001}=1\\
&1\text{ 次：}p_{010}=x, && p_{011}=x+1\\
&2\text{ 次：}p_{100}=x^2, && p_{101}=x^2+1\\
& && p_{110}=x^2+x, \quad p_{111}=x+x+1
\end{aligned}$$

系数在 GF(p)的多项式集合记为 GF[p,x]。

对应于整数中素数概念，GF[p,x]中有不可化约多项式，GF[2,x]次方等于 2 的多项式 x^2，$x^2+1=(x+1)^2$，$x^2+x=x(x+1)$。而 x^2+x+1，x^2+x+1 便是不可化约多项式，即不能表为两个次方为 1 的多项式之积。

三次方多项式有 8 个：

$$x^3,\quad x^3+1=(x+1)(x^2+x+1),\quad x^3+x=x(x+1)^2,\quad x^3+x+1$$

$$x^3+x^2=x^2(x+1),\quad x^3+x^2+1,\quad x^3+x^2+x=x(x^2+x+1)$$

$$x^3+x^2+x+1=(x+1)(x^2+x+1)+x(x+1)=(x+1)(x^2+1)$$

其中，只有 x^3+x+1 和 x^3+x^2+1 是不可化约的。

类似可证在 GF(2)四次方多项式不可化约的有：

$$x^4+x+1,\quad x^4+x^3+x^2+x+1,\quad x^4+x^3+1$$

其讨论留作练习。

若 $p(x)$和 $s(x)$是 GF$[p,x]$中两个多项式，但 $p(x)$的次方高于 $s(x)$的次方，则存在 $q(x)$和 $r(x)$，使

$$p(x) = q(x)s(x) + r(x)$$

$q(x)$是 $p(x)$除以 $s(x)$的商，$r(x)$是余项，$\deg(r(x)) < \deg(s(x))$，若 $p(x)$和 $s(x)$有次方最高的公因式 $d(x)$，则 $d(x)$也是 $q(x)$和 $r(x)$的次方最高的公因式，若 $d(x)=1$，则称 $p(x)$和 $s(x)$互素；若 $d(x)$是 $p(x)$和 $s(x)$的次方最高的公因式，则存在 $l(x)$和 $m(x) \in \mathrm{GF}[p,x]$，使

$$d(x) = l(x)p(x) + m(x)s(x)$$

3.2 有限域的特征与元素的阶

GF(p)和 GF(p^n)都是有限域，GF(p)是 GF(p^n)的最小子域，称 p 是 GF(p^n)域的特征。

定理 3.2.1 有限域 F 的元素个数是素数 p 的方幂。

证 令 1 表示 F 关于乘法的单位元素。$F=\{f_0, f_1, \cdots\}$满足递推关系

$$f_n = f_{n-1} + 1, \quad f_0 = 0$$

从递推关系可得

$$f_{m+n} = f_m + f_n, \quad f_{mn} = f_m f_n$$

但 F 有限，不可能所有 f_k 都是不同，“$f_0, f_1, \cdots$”第一次出现重复

$$f_k = f_{k+c}$$

$$f_{k+c} - f_k = f_c$$

故 $f_c=0$ 是$\{f_a\}$中第一个出现重复的元素，于是得

$$f_0, f_1, \cdots, f_{c-1}$$

全部不相同，c 便称为 F 的特征，整数 c 必然是素数。

如若不然，$c=ab$，$1 \leqslant a \leqslant c$，$1 \leqslant b \leqslant c$，$f_c = f_a f_b$。$f_c=0$，而 $f_a \neq 0$，$f_b \neq 0$ 这是不可能的。

阶的定义：α 是域 F 的一个元素，下列序列

$$1, \alpha, \alpha^2, \cdots, \alpha^n, \cdots$$

的所有元素都属于 F，故存在正整数 $O(\alpha)$，使 $\alpha^k = \alpha^{k+O(\alpha)}$ 对所有的 k 成立，即

$$\alpha^{O(\alpha)} = 1$$

称 $O(\alpha)$为元素 α 的阶。

定理 3.2.2 F 是有 q 个元素的有限域，$\forall \alpha \in F$，恒有

$$O(\alpha) \mid q-1$$

证 令 $F^* = F \backslash \{0\}$，F^* 为 F 中排除 0 元素以外的全体。其中 O 是 F 关于加法成 Abel 群的零元素，即加法的单位元。

由 α 构成的序列：

$$1, \alpha, \alpha^2, \cdots, \alpha^{o(x)-1}$$

为 $O(\alpha)$个 F^* 关于乘法的子群，根据 Lagrange 定理

$$O(\alpha) \mid q-1$$

例 3.2.1 $GF(11)=\{0,1,2,\cdots,10\}$，$3\in GF(11)$

$$3^2=9,\quad 3^3=27\equiv 5,\quad 3^4=81\equiv 4,\quad 3^5=243\equiv 1,\quad \bmod 11$$

$$O(3)=5,\quad 5\mid 10$$

例 3.2.2 $GF(2^3)=\{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\}$

$\alpha=x+1$，mod (x^3+x+1)有

$$x+1,\quad (x+1)^2=x^2+1,\quad (x+1)^3=x^3+x^2+x+1\equiv x^2$$

$$(x+1)^4\equiv x^2(x+1)=x^3+x^2\equiv x^2+x+1$$

$$(x+1)^5=x^5+5x^4+10x^3+10x^2+5x+1\equiv x^5+x^4+x+1\equiv x$$

$$\begin{array}{r|l} x^5+x^4 \qquad +x+1 & x^2+x\ \ +1 \\ \hline x^5 \quad +x^3+x^2 & \\ \hline x^4+x^3+x^2+x+1 & \\ x^4 \quad +x^2+x & \\ \hline x^3 \qquad +1 & \\ x^3 \quad +x+1 & \\ \hline x & \end{array}$$

$$(x+1)^6=x(x+1)=x^2+x$$

$$(x+1)^7=(x^2+x)(x+1)=x^3x\equiv 1$$

故 $x+1$ 的阶为 7。

引理 $p(x)$是系数在 F 的 m 次方首一多项式，则方程式

$$p(x)=0$$

最多有 m 个属于 F 的不同的根。

证 对 m 进行数学归纳法证明，$m=1$ 时引理显然为真，假定 $p(x)$的次方小于 m 时定理为真。

若存在 $\alpha\in F$，使$p(\alpha)=0$，$p(x)$除以$(x-\alpha)$，得

$$p(x)=q(x)(x-\alpha),$$

若 $p(x)$有根 $\beta\neq\alpha$，则由 $p(\beta)=0$ 导致 $q(\beta)=0$，$q(x)$的次方小于 m，根据假定 $q(x)=0$ 的根属于 F 的不超过 $m-1$，故 $p(x)=0$ 的根属于 F 的不超过 m。若 $m\geqslant 2$，但不存在 $\alpha\in F$，使 $p(\alpha)=0$，即 $p(x)=0$ 在 F 无解。

3.3 α^n 的阶

引理 若 $O(\alpha)=l$，则 $O(\alpha^h)=l/(h,l)$。

证 我们将利用这样的事实：$\alpha\neq 0$，$\alpha^s=1$，当而仅当 $O(\alpha)\mid s$。

令 $d=(h,l)$，故

$$\alpha^{h(l/d)}=\alpha^{l(h/d)}=(\alpha^l)^{h/d}=1$$

故

$$O(\alpha^h)\mid (l/d) \qquad (A)$$

令 $O(\alpha^h)=k$，则 $\alpha^{hk}=1$，l/hk。

又因 $d=(h,l)$，故存在整数 a 和 b，使

$$d = ah + bl$$

$$dk = ahk + blk$$

因 $l \mid hk$，故 $l \mid dk$ 而 $\left(\frac{l}{d}\right) \Big| k$，即 $\left(\frac{l}{d}\right) \Big| O(\alpha^h)$。因 $O(\alpha^h) \mid (l \mid d)$ 和 $\left(\frac{l}{d}\right) \Big| O(\alpha^h)$，所以 $O(\alpha^h)=l/d$。

例 3.3.1 $F=\{0,1,2,\cdots,12\}$，mod 13 有

$\beta = 2$，$\beta^2 = 4$，$\beta^3 = 8$，$\beta^4 = 16 \equiv 3$，$\beta^5 = 32 \equiv 6$，$\beta^6 = 64 \equiv 12$

$\beta^7 \equiv 24 \equiv 11$，$\beta^8 \equiv 22 \equiv 9$，$\beta^9 \equiv 18 \equiv 5$

$\beta^{10} \equiv 10$，$\beta^{11} \equiv 20 \equiv 7$，$\beta^{12} \equiv 14 \equiv 1$

$O(2) = 12$

$O(2^2) = 12/(12,2) = 12/2 = 6$，$O(2^8) = 12/(12,8) = 12/4 = 3$

$O(2^3) = 12/(12,3) = 12/3 = 4$，$O(2^9) = 12/(12,9) = 12/3 = 4$

$O(2^4) = 12/(12,4) = 12/4 = 3$，$O(2^{10}) = 12/(12,10) = 12/2 = 6$

$O(2^5) = 12/(12,5) = 12/1 = 12$，$O(2^{11}) = 12/(12,11) = 12/1 = 12$

$O(2^6) = 12/(12,6) = 12/6 = 2$，$O(2^{12}) = 12/(12,12) = 1$

$O(2^7) = 12/(12,7) = 12/1 = 12$

$\alpha=2$ 不存在阶为 5,8,9,10,11 的元素，阶为 12 的元素 4 个，即 $\alpha=2$，$\alpha=2^5$，$\alpha=2^7$，$\alpha=\alpha^{11}$。

定理 l 是一整数，F 是一有限域，F 或不存在阶为 l 的元素，或正好有 $\phi(l)$ 个阶为 l 的元素。

证明留作思考。

还是以 $F=\{0,1,2,\cdots,12\}$ 为例，mod 13 有

$O(1) = 1$

$O(2) = 12$

$O(3) = 3$：$3^2 = 9$，$3^3 \equiv 1$

$O(4) = 6$：$4^2 = 16 \equiv 3$，$4^3 \equiv 12$，$4^4 \equiv 48 \equiv 9$，$4^5 \equiv 36 \equiv 10$

$4^6 \equiv 40 \equiv 1$

$O(5) = 4$：$5^2 = 25 \equiv 12$，$5^3 \equiv 60 \equiv 8$，$5^4 \equiv 40 \equiv 1$

$O(6) = 12$：$6^2 \equiv 36 \equiv 10$，$6^3 \equiv 60 \equiv 8$，$6^4 \equiv 48 \equiv 9$，$6^5 \equiv 54 \equiv 2$

$6^6 \equiv 12$，$6^7 \equiv 72 \equiv 7$，$6^8 \equiv 42 \equiv 3$，$6^9 \equiv 18 \equiv 5$，$6^{10} \equiv 30 \equiv 4$

$6^{11} \equiv 24 \equiv 11$，$6^{12} = 66 = 1$

$O(7) = 12$：$7^2 = 49 \equiv 10$，$7^3 \equiv 70 \equiv 5$，$7^4 \equiv 35 \equiv 9$，$7^5 \equiv 63 \equiv 11$

$7^6 \equiv 77 \equiv 12$，$7^7 \equiv 84 \equiv 6$，$7^8 \equiv 42 \equiv 3$，$7^9 \equiv 21 \equiv 8$，$7^{10} \equiv 56 \equiv 4$

$7^{11} \equiv 28 \equiv 2$，$7^{12} \equiv 14 \equiv 1$

$O(8) = 4$：$8^2 = 64 \equiv 12$，$8^3 \equiv 96 \equiv 5$，$8^4 \equiv 40 \equiv 1$

$O(9) = 3$：$9^2 = 81 \equiv 3$，$9^3 \equiv 27 \equiv 1$

$O(10)=6$：$10^2=100\equiv 9$，　$10^3\equiv 90\equiv 12$，　$10^4\equiv 120\equiv 3$，　$10^5\equiv 30\equiv 4$

$10^6\equiv 40\equiv 1$

$O(11)=12$：$11^2\equiv 121\equiv 4$，　$11^3\equiv 44\equiv 5$，　$11^4\equiv 55\equiv 3$，　$11^5\equiv 33\equiv 7$

$11^6\equiv 77\equiv 12$，　$11^7\equiv 132\equiv 2$，　$11^8\equiv 22\equiv 9$，　$11^9\equiv 99\equiv 8$

$11^{10}\equiv 88\equiv 10$，　$11^{11}\equiv 110\equiv 6$，　$11^{12}\equiv 66\equiv 1$

$O(12)=2$，　$12^2=144\equiv 1$

总之 $O(\beta)=1$ 的一个，$O(\beta)=2$ 的一个，$O(\beta)=3$ 的两个，$O(\beta)=4$ 的两个，$O(\beta)=5$，7，8，9，10，11 的 0 个，$O(\beta)=6$ 的两个，$O(\beta)=12$ 的四个。

例 3.3.2　$p(x)=x^4+x^3+x^2+x+1$，mod $p(x)$的 GF(2^4)的 16 个元素：

$0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1,x^3,x^3+1,x^3+x,x^3+x+1,x^3+x^2,x^3+x^2+1,x^3+x^2+x,x^3+x^2+x+1$。　mod $p(x)$有

$O(1)=1$：$1^1\equiv 1$

$O(x)=5$：x^1,x^2,x^3，　$x^4\equiv x^3+x^2+x+1$，　$x^5\equiv x^4+x^3+x^2+x\equiv 1$

$O(x+1)=15$：$(x+1)^2\equiv x^2+1$

$(x+1)^3\equiv (x^2+1)(x+1)\equiv x^3+x^2+x+1$

$(x+1)^4\equiv (x^2+1)^2=x^4+1\equiv x^3+x^2+x$

$(x+1)^5=(x+1)(x^3+x^2+x)\equiv x^4+x\equiv x^3+x^2+1$

$(x+1)^6\equiv (x^3+x^2+1)(x+1)\equiv x^4+x^2+x+1\equiv x^3$

$(x+1)^7\equiv x^3(x+1)\equiv x^4+x^3\equiv x^2+x+1$

$(x+1)^8\equiv (x^2+x+1)(x+1)=x^3+1$

$(x+1)^9\equiv (x^3+1)(x+1)\equiv x^4+x^3+x+1\equiv x^2$

$(x+1)^{10}\equiv x^2(x+1)\equiv x^3+x^2$

$(x+1)^{11}\equiv (x^3+x^2)(x+1)\equiv x^4+x^2+x^3+x+1$

$(x+1)^{12}\equiv (x^3+x+1)(x+1)\equiv x^4+x^3+x^2+1=x$

$(x+1)^{13}\equiv x(x+1)=x^2+x$

$(x+1)^{14}\equiv (x^2+x)(x+1)\equiv x^3+x$

$(x+1)^{15}\equiv (x^3+x)(x+1)=x^4+x^3+x^2+x\equiv 1$

总之 $(x+1)^3=x^3+x^2+x+1$

$(x+1)^6=x^3$

$(x+1)^9=x^2$

$(x+1)^{12}=x$

这四个元素的阶为 15/(15,3)=15/(15,6)=15/(15,9)=15/(15,12)=15/3=5。以 x^2 为例

$$x^2,x^4=x^3+x^2+x+1$$

$$(x^2)^3=(x^3+x^2+x+1)x^2=x^5+x^4+x^3+x^2=x$$

$$\begin{array}{r} x \\ x^4+x^3+x^2+x+1\overline{)\,x^5+x^4+x^3+x^2} \\ \underline{x^5+x^4+x^3+x^2+x} \\ x \end{array}$$

$$(x^2)^4 \equiv x \cdot x^2 \equiv x^3$$
$$(2^5)^5 \equiv x^5 \equiv 1。$$

$$\begin{array}{r|l} x^4+x^3+x^2+x+1 & x+1 \\ \hline x^5 & \\ x^5+x^4+x^3+x^2+x & \\ \hline x^4+x^3+x^2+x & \\ x^4+x^3+x^2+x+1 & \\ \hline 1 & \end{array}$$

1 $O(x+1)=15$

$(x+1)^2=x^2+1$

$O((x+1)^2)=O(x^2+1)=15/(15,2)=15$

2 $(x+1)^{13}\equiv x^2+x$

$O((x+1)^{13})=O(x^2+x)=15/(15,13)=15$

3 $(x+1)^8\equiv x^3+1$

$O((x+1)^8)=O(x^3+1)=15/(15,8)=15$

4 $(x+1)^{14}\equiv x^3+x$,

$O(x^3+x)=O((x+1)^{14})=15/(15,14)=15$

5 $(x+1)^{11}=x^3+x+1$

$O(x^3+x+1)=O((x+1)^{11})=15/(15,11)=15$

6 $(x+1)^4=x^3+x^2+x$

$O(x^3+x^2+x)=O((x+1)^4)=15/(15,4)=15$

7 $(x+1)^7=x^2+x+1$

$O(x^2+x+1)=O((x+1)^7)=15/(15,7)=15$

阶为 15 的元素个数 8 个。

同理可证

$$O(x^3+x^2)=O((x+1)^{10})=15/(15,10)=3$$
$$O(x^3+x^2+1)=O((x+1)^5)=15/(15,5)=3$$

阶为 3 的元素个数有两个。

3.4 本原元素

$F^*=F\backslash\{0\}$是关于运算“·”的 Abel 群，也是循环群：

$$\{g,g^2,\cdots,g^{q-1}=e\}$$

它的生成元素 g 便称之为域 F 的本原元素，如前节 GF(2^4)域有阶为 15 的元素 8 个，8 个元素：

$$x+1,\quad x^2+1,\quad x^2+x,\quad x^2+x+1,\quad x^3+1$$
$$x^3+x,\quad x^3+x+1,\quad x^3+x^2+x$$

都是 GF(2^4)的本原元素。

下面给出求本原元素的算法。

设 F 的元素个数为 q，

(S1)：$i\leftarrow 1$，取 F 中非零元素 α，计算 α_1 的阶 $O(\alpha_1)=l_1$。

(S2)：若 $l_i=q-1$，则 α_i 便是 F 的本原元素，停止。否则转 S3。

(S3)：另选 F 的非零元素 β，要求 β 不是 α_i 的幂，计算 β 的阶 l，若 $l=q-1$，则 β 是本原元素，停止，否则转 S4。

(S4)：求 $d|l_i, e|l$，使 $(d,e)=1, de=\mathrm{lcm}(l_i,l)$

令

$$\alpha_{i+1}=\alpha_i^{l_i/d}\beta^{l/e},\quad l_{i+1}\leftarrow \mathrm{lcm}(l_i,l)$$

$i\leftarrow i+1$，转 S2。

以 $p(x)=x^4+x^3+x^2+x+1$，mod $p(x)$的 GF(2^4)为例，

$$\alpha=x^3+x^2+1,\quad O(\alpha)=3$$

$\beta=x^3$，$O(\beta)=5$，$O(\alpha)=3$，$O(\beta)=5$ 由读者自己来验证，取 $d=3, e=5$

$$de=\mathrm{lcm}(3,5)=15$$

$$\alpha_{i+1}=\alpha\beta=(x^3+x^2+1)x^3=x^6+x^5+x^3$$

$$x^4=x^3+x^2+x+1,\quad x^5=x^4+x^3+x^2+x=1$$

$$x^6=x$$

故

$$\alpha_{i+1}\equiv x^3+x+1 \bmod p(x)$$

$$O(x^3+x+1)=15$$

注意：在 S3 中 β 的阶 l 不可能是 l_i 的因数，因所有 $x^{l_i}=1$ 的解必是 α_i 的幂，l 不是，所以 $\mathrm{lcm}(l_i,l)$ 是 l_i 的倍数，严格地大于 l_i。

例 mod (x^2-2)的 GF(5^2)的元素 $ax+b, a,b\in$GF(5)。

$$\alpha_1=a_1x+b_1,\quad \alpha_2=a_2x+b_2$$

$$\alpha_1+\alpha_2=(a_1+\alpha_2)x+(b_1+b_2)$$

$$\alpha_1\alpha_2=(a_1x+b_1)(a_2x+b_2)=a_1a_2x^2+(a_1b_2+a_2b_1)x+b_1b_2$$

$$=2a_1a_2+(a_1b_2+a_2b_1)x+b_1b_2=(a_1b_1+a_2b_2)x+2a_1a_2+b_1b_2$$

取

$$\alpha_1=x,\quad \alpha_1^2=x^2\equiv 2,\quad \alpha_1^3\equiv 2x,\quad \alpha_1^4\equiv 2x^2=4$$

$$\alpha_1^5\equiv 4x,\quad \alpha_1^6\equiv 4x^2\equiv 8\equiv 3,\quad \alpha_1^7\equiv 3x,\quad \alpha_1^8\equiv 3x^2\equiv 6\equiv 1$$

故，$O(\alpha_1)=8$，α_1 不是 GF(2^2)的本原元素。取 $\beta=x+1$，β 不属 α_1 的幂，mod (x^2-2)有

$$\beta^2=(x+1)^2=x^2+2x+1=2x+2+1=2x+3$$

$$\beta^3=(2x+3)(x+1)=2x^2+(2+3)x+3=5x+4+3\equiv 52+2\equiv 2$$

$$\beta^4=2(x+1)=2x+2$$

$$\beta^5=(2x+2)(x+1)=2x^2+4x+2\equiv 4x+6\equiv 4x+1$$

$$\beta^6\equiv(4x+1)(x+1)=4x^2+5x+1\equiv 8+1\equiv 4$$

$$\beta^7\equiv 4(x+1)=4x+4$$

$$\beta^8 \equiv (4x+4)(x+1) = 4x^2+8x+4 \equiv 3x+8+4 \equiv 3x+2$$
$$\beta^9 = (3x+2)(x+1) \equiv 3x^2+5x+2 \equiv 6+2 \equiv 3$$
$$\beta^{10} \equiv 3(x+1) = 3x+3$$
$$\beta^{11} \equiv (3x+3)(x+1) = 3x^2+6x+3 \equiv x+6+3 \equiv x+4$$
$$\beta^{12} \equiv (x+4)(x+1) = x^2+5x+4 \equiv 6 \equiv 1$$
$$O(\beta) = O(x+1) = 12$$
$$\alpha = x, \quad \beta = x+1, \quad l_1 = 8, \quad l = 12, \quad \mathrm{lcm}(8,12) = 24$$
$$d = 8, \quad e = 3$$
$$\alpha_2 = x(x+1)^4 = x(x^4+4x^3+6x^2+4x+1)$$
$$\equiv x(x^4+4x^3+x^2+4x+1)$$
$$\equiv x^5+4x^3+x^3+4x^2+x \equiv 2x+2 \bmod (x^2-2)$$
$$x^2 \equiv 2, \quad x^3 \equiv 2x, \quad x^4 \equiv 2x^2 \equiv 4, \quad x^5 \equiv 4x$$

代入

$$x^5+4x^4+x^3+4x^2+x \equiv 4x+16+2x+8+x = 7x+24 \equiv 2x+4$$

可以验证 $O(2x+4)=24$，验证过程留作练习。

3.5 极小多项式

定义 $\beta \in \mathrm{GF}(p^n)$ 使 $f(\beta)=0$ 的次方最小的首一多项式 $f(x)$，称之为 β 的极小多项式。

$f(x)$ 是 β 的极小多项式，则 $f(x)$ 必定是不可化约的，如若不然，存在 $p(x)$ 和 $q(x)$，使 $f(x)=p(x)q(x)$，则

$$f(\beta) = p(\beta)q(\beta) = 0$$

导致 $p(\beta)=0$ 或 $q(\beta)=0$，不论是 $p(\beta)=0$ 还是 $q(\beta)=0$，它们的次方都低于 $f(x)$，跟极小多项式的假定相矛盾。

若另有多项式 $F(x)$，使 $F(\beta)=0$，而且 $f(x) \nmid F(x)$，则存在 $q(x)$ 和 $r(x)$ 得

$$F(x) = q(x)f(x) + r(x)$$

$r(x)$ 的次方小于 $f(x)$ 的次方，由 $F(\beta)=0$，$f(\beta)=0$，导致 $r(\beta)=0$，这跟 $f(x)$ 作为 β 的极小多项式的定义相矛盾。这说明 $f(x)$ 是 β 的极小多项式，若另有 $F(x)$，$F(\beta)=0$，则 $f(x) \mid F(x)$。

例 $\bmod (x^4+x^3+1)$，构成的 $\mathrm{GF}(2^4)$，α^3 的极小多项式是

$$f(x) = x^4+x^3+x^2+x+1$$

即证

$$(\alpha^3)^4+(\alpha^3)^3+(\alpha^3)^2+(\alpha^3)+1 = 0$$

即

$$\alpha^{12}+\alpha^9+\alpha^6+\alpha^3+1 = 0, \quad \alpha^4 = \alpha^3+1, \quad \alpha^5 = \alpha^4+\alpha = \alpha^3+\alpha+1$$
$$\alpha^6 = \alpha^4+\alpha^2+\alpha = \alpha^3+\alpha^2+\alpha+1, \quad \alpha^7 = \alpha^4+\alpha^3+\alpha^2+\alpha = \alpha^2+\alpha+1$$
$$\alpha^8 = \alpha^3+\alpha^2+\alpha, \quad \alpha^9 = \alpha^4+\alpha^3+\alpha^2 = \alpha^2+1, \quad \alpha^{10} = \alpha^3+\alpha$$

$$\alpha^{11}=\alpha^4+\alpha^2=\alpha^3+\alpha^2+1,\quad \alpha^{12}=\alpha^4+\alpha^3+\alpha=\alpha+1$$

故

$$\alpha^{12}+\alpha^9+\alpha^6+\alpha^3+1=(\alpha+1)+(\alpha^2+1)+(\alpha^3+\alpha^2+\alpha+1)+\alpha^3+1=0$$

即 $x^4+x^3+x^2+x+1$ 是 x^3 的极小多项式。

下面将 mod(x^4+x+1)的 GF(2^4)的 15 个非零元素和它对应的极小多项式罗列于后。

(1) $\alpha,\alpha^2,\alpha^4,\alpha^8$ 的极小多项式：x^4+x+1

(2) $\alpha^3,\alpha^6,\alpha^9,\alpha^{12}$的极小多项式：$x^4+x^3+x^2+x+1$

(3) α^5,α^{10}的极小多项式：x^2+x+1

(4) $\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}$的极小多项式：$x^4+x^3+1$

总之，$\forall\alpha\in$GF(p^m)总存在$-f(x)\in$GF$[p,x]$,便有如下性质

(1) $f(x)=0$;

(2) $f(x)$的次方小于 m;

(3) 若$\exists g(x)\in$GF$[p,x]$使 $g(x)=0$,则 $f(x)|g(x)$。

3.6 不可化约多项式

主要讨论在 GF(2)上不可化约多项式，一个多项式是否可化约要考虑所在的域，最简单的一个例子 x^2+1 在实数域它是不化约的，但在复数域可化约成$(x+i)(x-i)$，在 GF(2)域也是可化约的，$(x+1)^2=x^2+1$。

现将 GF(2)的不可化约多项式按次方的顺序讨论如下所示。

(1) 一次方：x, $x+1$

(2) 二次方的多项式共有四个：x^2, x^2+1, x^2+x, x^2+x+1,其中由两个一次方项相乘而得的有

$$x^2=x\cdot x,\quad x^2+x=x(x+1),\quad (x+1)^2=x^2+1$$

故二次方不可化约的多项式：x^2+x+1

(3) 三次方的多项式有 2^3 项：

$$x^3,\quad x^3+1,\quad x^3+x,\quad x^3+x+1,\quad x^3+x^2$$
$$x^3+x^2+1,\quad x^3+x^2+x,\quad x^3+x^2+x+1$$

其中由三个一次方项相乘的有

$$x^3=x\cdot x\cdot x,\quad (x+1)^3=x^3+x^2+x+1$$
$$x^2(x+1)=x^3+x^2,\quad x(x+1)^2=x^3+x$$

由一个一次方和一个二次方不可化约多项式之积有：

$$x(x^2+x+1)=x^3+x^2+x,\quad (x+1)(x^2+x+1)=x^3+1$$

剩下的为不可化约多项式有：

$$x^3+x^2+1,\quad x^3+x+1$$

(4) 四次方不可化约多项式分析如下：

四次多项式有 $2^4=16$ 项，即

x^4，x^4+1，x^4+x，x^4+x+1，x^4+x^2，x^4+x^2+1

x^4+x^2+x，x^4+x^2+x+1，x^4+x^3，x^4+x^3+1

x^4+x^3+x，x^4+x^3+x+1

$x^4+x^3+x^2$，$x^4+x^3+x^2+1$，$x^4+x^3+x^2+x$，$x^4+x^3+x^2+x+1$

由四个一次方项相乘有：

x^4，$(x+1)^4=x^4+1$，$x(x+1)^3=x(x^3+x^2+x+1)=x^4+x^3+x^2+x$

$x^2(x+1)^2=x^2(x^2+1)=x^4+x^2$，$x^3(x+1)=x^4+x^3$

由两个二次方不可化约多项式的乘积：

$$(x^2+x+1)^2=x^4+x^2+1,\quad (2^2+1)^2=x^4+1$$

由两个一次方项和一个二次方不可化约多项式之积：

$x^2(x^2+x+1)=x^4+x^3+x^2$，$(x+1)^2(x^2+x+1)=x^4+x^3+x+1$

$x(x+1)(x^2+x+1)=(x^2+x)(x^2+x+1)=x^4+x$

由一个一次方项和一个三次方不可化约多项式之积：

$x(x^3+x+1)=x^4+x^2+x$

$(x+1)(x^3+x+1)=x^4+x^2+x+x^3+x+1=x^4+x^3+x^2+1$

$x(x^3+x^2+1)=x^4+x^3+x$

$(x+1)(x^3+x^2+1)=x^4+x^2+x+1$

故得四次方不可化约多项式有

$$x^4+x+1,\quad x^4+x^3+1,\quad x^4+x^3+x^2+x+1$$

类似的步骤可得五次方不可化约多项式，乃至五次以上不可化约多项式。

令 I_n 表 n 次方不可化约多项式的数目。

$\overline{C}(n,r)$表从 n 个中取 r 个作允许重复的组合的组合数，而且

$$\overline{C}(n,r)=C(n+r-1,r)$$

$I_1=2$，显然，即 x，$x+1$ 两个：

$$I_2=2^2-\overline{C}(2,2)=2^2-C(3,2)=4-3=1$$

即二次方不可化约多项式个数为 1。

$$\begin{aligned}I_3&=2^3-\overline{C}(2,3)-2\cdot 1\\&=8-C(4,3)-2=8-4-2=2\end{aligned}$$

其中 $\overline{C}(2,3)$表由两个一次方项取 3 个作允许重复组合的组合，$2*1$ 项表由两个一次方项和一个二次方项不可化约多项式之积。

$$\begin{aligned}I_4&=2^4-I_1I_3-\overline{C}(I_1,4)-I_2^2-\overline{C}(I_1,2)I_2\\&=16-2\cdot 2-C(5,4)-1-3=16-4-5-4=3\end{aligned}$$

I_1I_3 项的意义容易理解，$\overline{C}(I_1,4)$表从 I_1 个一次方项取四个作允许重复组合的组合数，$\overline{C}(I_2,2)$的意义也不难理解，

$$\begin{aligned}I_5&=2^5-I_1I_4-I_2I_3-\overline{C}(I_1,2)I_3-\overline{C}(I_1,3)I_2-\overline{C}(I_2,2)I_1-\overline{C}(I_1,5)\\&=32-6-2-3\cdot 2-4-2-6=6\\I_6&=2^6-I_1I_5-I_2I_4-\overline{C}(I_3,2)-\overline{C}(I_2,3)-C(I_1,3)I_3-\overline{C}_1(I_1,6)\\&\quad-\overline{C}(I_1,4)I_2-\overline{C}(I_1,2)\overline{C}(I_2,2)-I_1I_2I_3\\&=9\end{aligned}$$