Chapter 3 Polynomials over Finite Fields

3.1 Order of Polynomials and Primitive Polynomials

Lemma 3.1

设 $f \in \mathbb{F}_q[x]$, $f(0) \neq 0$ 且次数 $m \geq 1$. 则存在一个正整数 $e \leq q^m - 1$ 使得 $f(x)|x^e - 1$.

证明：

考虑剩余类环 $\mathbb{F}_q[x]/(f)$, 它有 $q^m - 1$个非零剩余类，不妨设这 q^m 个剩余类为 $x^j + (f)$, $j = 0, 1, \ldots, q^m - 1$, 这些都是非零剩余类，所以存在满足$0 \leq r < s \leq q^m - 1$ 的整数 r, s 满足 $x^s \equiv x^r \mod f(x)$

又因为 x 和 $f(x)$ 互素，所以有 $x^{s-r} \equiv 1 \mod f(x)$, 即 $f(x)$ 整除 $x^{s-r} - 1$. 显然 $s - r < q^m - 1$,

Definition 3.2 Order

设 $f \in \mathbb{F}_q[x]$ 是一个非零多项式。

若 $f(0) \neq 0$, 定义满足 $f(x)|x^e - 1$ 的最小正整数 e 为 f 的阶，记做 $ord(f) = ord(f(x))$.

若 $f(0) = 0$, 则有 $f(x) = x^h g(x)$, 其中 $h \in \mathbb{N}$ 且 $g \in \mathbb{F}_q[x]$, $g(0) \neq 0$. 则定义 $ord(f) = ord(g)$.

Theorem 3.3 Order of Irreducible Polynomial

设 $f \in \mathbb{F}_q[x]$ 是一个 $\mathbb{F}_q$ 上的不可约多项式，次数为 m 且有 $f(0) \neq 0$. 那么 $ord(f)$ 等于 f 在乘法群 $\mathbb{F}_{q^m}^*$ 上的任一个根的阶。

证明：

由 **Corollary 2.15** 可知 $\mathbb{F}_{q^m}$ 是 f 在 $\mathbb{F}_q$ 上的一个分裂域.

由 **Theorem 2.18** 可知在群 $\mathbb{F}_{q^m}^*$ 上 f 的每个根都具有相同的阶

设 $\alpha \in \mathbb{F}_{q^m}$ 是 f 的任意一个根.

由 **Lemma 2.12** 可知当且仅当 $\alpha^e = 1$ 的时候， $f(x)|x^e - 1$.

根据 $ord(f)$ 的定义，**Theorem 3.3** 成立. 证毕.

Corollary 3.4

设 $f \in \mathbb{F}_q[x]$ 是一个 $\mathbb{F}_q$ 上的不可约多项式，次数为 m. 则 $ord(f)|q^m - 1$.

这个定理对于可约多项式不一定成立。

证明：

设 $f(x)=cx,\ c\in\mathbb{F}_q^*$. 这种情况下 $ord(f)=1$ 结论显然。

否则, 由于 $\mathbb{F}_{q^m}^*$ 是一个阶数为 q^m-1 的群，由 **Theorem 3.3** 可知 **Corollary 3.4** 成立.

Theorem 3.5 Number of Monic Irreducible Polynomials

在 $\mathbb{F}_q[x]$ 中，次数为 m 且阶为 e 的首一不可约多项式个数为：

(1) $e\geq 2$ 且 m 是 q 模 e 的阶(设$gcd(q,e)=1$，m 是满足$q^m\equiv 1 \mod e$ 的最小正整数)，则个数为 $\frac{\phi(e)}{m}$.

(2) 当 $m=e=1$ 时，个数为 2.

(3) 其他情况时，个数为 0.

特别的， $\mathbb{F}_q[x]$ 上阶为 e 的不可约多项式的次数等于模 e 意义下的 q 的乘法阶.

证明：

设 $f(x)$ 是 $\mathbb{F}_q[x]$ 上的不可约多项式，且 $f(0)\neq 0$.

根据 **Theorem 3.3** 可以知道，当且仅当 f 的所有根都是 $\mathbb{F}_q$ 上的 e 次本原单位根，即 f 整除分圆多项式 Q_e时，有 $ord(f)=e$.

根据 **Theorem 2.47(ii)** 可知， Q_e 所有的首一多项式因子都有相同的次数，设其为 d, 其中 d 是满足 $q^d\equiv 1 \mod e$ 的最小正整数，这样的因子有 $\frac{\phi(e)}{m}$ 个.

对于 $m=e=1$, 考虑首一不可约多项式 $f(x)=x$ 即可.

Lemma 3.6

设 c 是一个正整数, $f\in\mathbb{F}_q[x],\ f(0)\neq 0$.

当且仅当 $f|x^c-1$ 的时， $ord(f)|c$.

证明：

(1) 若 $e=ord(f)|c$, 则有$f(x)|x^e-1$, 而$x^e-1|x^c-1$, 所以$f(x)|x^c-1$.

(2) 若 $f(x)|x^c-1$, 有 $c\geq e$, 即 $c=me+r$, 其中 $m\in\mathbb{N}$ 且 $0\leq r<e$.

因此， $x^c-1=(x^{me}-1)x^r+(x^r-1)$, 只有当 $r=0$ 的时候该式成立. 因此 $e|c$.

Corollary 3.7

设 e_1 和 e_2 是两个正整数，那么在 $\mathbb{F}_q[x]$ 上，$gcd(x^{e_1}-1,x^{e_2}-1)=x^d-1,$ 其中 $d=gcd(e_1,e_2)$.

证明：

设首一多项式 $f(x)=gcd(x^{e_1}-1,x^{e_2}-1)$. 由于 $gcd(x^{e_1}-1,x^{e_2}-1)=x^d-1$, 所以有 $x^d-1|f(x)$.

同时，由于 $f(x)=gcd(x^{e_1}-1,x^{e_2}-1)$, 由 **Lemma 3.6** 可知 $ord(f)|e_1$ 且 $ord(f)|e_2$.

因此，$ord(f)=d$, 由 **Lemma 3.6** 可知 $f(x)|x^d-1$.

综上有 $f(x) = x^d - 1$.

Theorem 3.8 calculate the order

设 $g \in \mathbb{F}_q[x]$ 是一个 $\mathbb{F}_q$ 上的不可约多项式，$g(0) \neq 0$ 且 $ord(g) = e$. 给定正整数 b, 设 $f = g^b$.

设 t 为满足 $p^t \geq b$ 的最小正整数，其中 p 是域 $\mathbb{F}_q$ 的特征。则有 $ord(f) = ep^t$.

证明：

令 $c = ord(f)$，$f(x)|x^c - 1$ 和 $g(x)|x^c - 1$ 有着相同的真假。由 **Lemma 3.6** 可知 $e|c$.

因此 $g(x)|x^e - 1$, 因此$f(x)|(x^e - 1)^b$, 而这个东西是整除 $(x^e - 1)^{p^t} = x^{ep^t} - 1$ 的.

由 **Lemma 3.6**, $c|ep^t$. 而 c 可以写成 ep^u 的形式，其中 $0 \leq u \leq t$.

注意到 $x^e - 1$ 只含有单根，这是因为 e 不是 p 的倍数。所以所有 $x^{ep^u} - 1 = x^{ep^t} - 1$ 的根都有幂数 p^u.

而 $g(x)^b|x^{ep^u} - 1$, 比较根的幂次可以发现 $p^u \geq b$, 从而得到 $u \geq t$.

因此， $u = t$, $c = ep^t$.

Theorem 3.9 calculate the order

设 $g_1, g_2, \ldots, g_k$ 是域 $\mathbb{F}_q$ 上两两互素的非零多项式，令 $f = g_1 g_2 \ldots g_k$.

则 $ord(f) = lcm(ord(g_1), ord(g_2), \ldots, ord(g_k))$.

证明:

只需要考虑 $g_i(0) \neq 0$ 的多项式. 以下所有 i 都有约束条件 $1 \leq i \leq k$.

令 $e = ord(f), e_i = ord(g_i), c = lcm(e_1, e_2, \ldots, e_k)$. 则对于每一个 $g_i(x)$, 都有 $g_i(x)|x^{e_i} - 1$, 所以$g_i(x)|x^c - 1$.

由于这些多项式两两互素，所以有 $f(x)|x^c - 1$. 由 **Lemma 3.6** 可知 $e|c$.

另一方面，由于 $f(x)|x^e - 1$, 且对于每一个 $g_i(x)$, 都有 $g_i(x)|x^e - 1$. 由 **Lemma 3.6** 可知对每一个 e_i 都有 $e_i|e$, 因此 $c|e$.

因此 $e = c$.

Example 3.10 calculate the order

尝试求 $f(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ 的阶.

分解上式可得 $f(x) = (x^2 + x + 1)^3 (x^4 + x + 1)$.

而 $ord(x^2 + x + 1) = 3$, 由 **Theorem 3.8** 可得 $ord(x^2 + x + 1)^3 = 12$.

同时，$ord(x^4 + x + 1) = 15$, 所以由 **Theorem 3.9** 可得 $ord(f) = lcm(12, 15) = 60$.

Theorem 3.11

设有限域 $\mathbb{F}_q$ 的特征是 p, 令 $f \in \mathbb{F}_q[x]$ 是一个正次数多项式，且 $f(0) \neq 0$.

令 $f = af_1^{b_1}f_2^{b_2}\dots f_k^{b_k}$, 其中 $a \in \mathbb{F}_q, b_1, \dots, b_k \in \mathbb{N}, f_1, \dots, f_k$ 是 $\mathbb{F}_q[x]$ 上不同的首一不可约多项式，是 f 在$\mathbb{F}_q[x]$ 上的标准分解.

那么， $ord(f) = ep^t$, 其中 $e = lcm(ord(f_1), ord(f_2), \dots, ord(f_k))$, t 是满足 $p^t \geq max(b_1, \dots, b_k)$ 的最小正整数.

Definition 3.12 Reciprocal polynomial

设 $f(x) = a_nx^n + a_{n-1}^{n-1} + \dots + a_1x + a_0 \in \mathbb{F}_q[x], a_n \neq 0$.

那 $f(x)$ 的互反多项式 f^* 定义为 $f^*(x) = x^nf(\frac{1}{x}) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$.

Theorem 3.13

设 f 是 $\mathbb{F}_q[x]$ 上的一个非零多项式， f^* 是其互反多项式. 那么有 $ord(f) = ord(f^*)$.

证明：

考虑 $f(0) \neq 0$ 的情况.

由于当且仅当 $f(x) | x^e - 1$ 的时候 $f^*(x) | x^e - 1$, 所以结论成立.

如果 $f(0) = 0$. 则 $f(x) = x^hg(x), h \in \mathbb{N}, g \in \mathbb{F}_q[x], g(0) \neq 0$. 而 $g^* = f^*$.

所以 $ord(f) = ord(g) = ord(g^*) = ord(f^*)$.

Theorem 3.14

对于奇数 q, 令 $f \in \mathbb{F}_q[x]$ 是一个正次数多项式，且 $f(0) \neq 0$. 令 $e = ord(f(x)), E = ord(f(-x))$.

若 e 是 4 的倍数，则 $E = e$; 若 e 是奇数，那么 $E = 2e$.

如果 e 是 2 的倍数但不是 4 的倍数，那么如果所有 f 的不可约因子的阶都是偶数，就有 $E = e/2$, 否则 $E = e$.

证明： 因为 $ord(f(x)) = e$, 所以 $f(x) \mid x^{2e} - 1$, 所以 $f(-x) | (-x)^{2e} - 1 = x^{2e} - 1$. 所以根据 **Lemma 3.6**, $E | 2e$.

同理 $e | 2E$. 所以 E 的所有合法取值只能为 $2e, e$ 或 $e/2$.

如果 $4 \mid e$ 就有 e 和 E 都是偶数. 由于 $f(x) \mid x^e - 1, f(-x) \mid (-x)^e - 1 = x^e - 1$. 所以 $e | E$. 同理有 $E | e$.

所以就有 $E = e$.

如果 e 是奇数，那么 $f(-x) \mid -x^e - 1$, 即 $f(-x) | x^e + 1$. 但是 $f(-x) \nmid x^e - 1$, 所以只能有 $E = 2e$.

否则不妨设 $e = 2h$, 其中 h 是奇数. 设 f 是一个 $\mathbb{F}_q[x]$ 上不可约多项式的幂，那么因为 $ord(f) = 2h$, 可以得到 $f(x) | (x^h - 1)(x^h + 1)$ 且 $f(x) \nmid x^h - 1$. 但是 $x^h - 1$ 和 $x^h + 1$ 是互质的，那么就有 $f(x) | x^h + 1$.

所以 $f(-x) | (-x)^h + 1 = -x^h + 1$, 所以 $f(-x) | x^h - 1$. 所以 $E = e/2$.

注意到根据 **Theorem 3.8** 可以知道一个不可约多项式的幂的阶是偶数，当且仅当不可约多项式本身的阶是偶数.

设 f 的分解式为

$$f = g_1 \dots g_k$$

其中 g_i 是一个不可约多项式的幂次且不同的 g 两两互质，那么根据 **Theorem 3.9** 可以得到

$$ord(f) = 2h = lcm(ord(g_1), \dots, ord(g_k))$$

设对于 $1 \le i \le m, ord(g_i) = 2h_i$, 对于 $m+1 \le i \le k$ 有 $ord(g_i) = h_i$, 其中 h_i 是奇数且满足 $lcm(h_1, \dots, h_k) = h$.

那么可以知道 $ord(g_i(-x)) = h, 1 \le i \le m$ 且 $ord(g_i(-x)) = 2h_i, m+1 \le i \le k$, 从而

$$E = lcm(h_1, \dots, h_m, 2h_{m+1}, \dots, 2h_k)$$

所以当 $m = k$ 的时候 $E = h = e/2$.

当 $m < k$ 的时候 $E = 2h = e$.

Definition 3.15 Primitive Polynomial

$\mathbb{F}_{q^m}$ 的本原元在 $\mathbb{F}_q$ 上的极小多项式 f 被称作 $\mathbb{F}_q$ 上的本原多项式.

Theorem 3.16

设 $f \in \mathbb{F}_q[x]$, 次数为 m, f 是 $\mathbb{F}_q$ 上的本原多项式，当且仅当 f 是首一多项式, $f(0) \ne 0$, 且 $ord(f) = q^m - 1$.

证明：

如果 f 是 $\mathbb{F}_q$ 上的本原多项式，那么 f 首一且 $f(0) = 0$. 因为 f 在 $\mathbb{F}_q$ 上不可约，所以根据 **Theorem 3.3** 可知，$ord(f) = q^m - 1$, 且有 $\mathbb{F}_{q^m}$ 上的本原元作根.

反过来，由于 $ord(f) = q^m - 1$, 所以 $m \ge 1$, 下面证明 f 在 $\mathbb{F}_q$ 上不可约.

假设 f 在 $\mathbb{F}_q$ 上可约，那么它要么是一个不可约多项式的幂，要么是两个互素的多项式的乘积.

对于第一种情况，设 $f = g^b$, 其中 $g \in \mathbb{F}_q[x], g(0) \ne 0, b = 2$, g 是 $\mathbb{F}_q$ 上的不可约多项式。那么根据 **Theorem 3.8** 可以得到 $ord(f)$ 可以被 $\mathbb{F}_q$ 的特征整除，然而 $q^m - 1$ 不可以，得到矛盾；

对于第二种情况，设 $f = g_1 g_2$, 设它们的阶是 m_1, m_2, 如果 $e_i = ord(g_i), i = 1, 2$ 那么根据 **Theorem 3.9** 就有 $ord(f) \le e_1 e_2$, 所以根据 **Lemma 3.1** 可以得到 $e_i \le q^{m_i} - 1$, 又因为：

$$ord(f) \le (q^{m_1} - 1)(q^{m_2} - 1) < q^{m_1 + m_2} - 1 = q^m - 1$$

得到矛盾。综上 f 在 $\mathbb{F}_q$ 上不可约，根据 **Theorem 3.3** 可以知道 f 是 $\mathbb{F}_q$ 上的本原多项式.

Lemma 3.17

设 $f \in \mathbb{F}_q[x]$ 是一个正次数多项式， $f(0) \ne 0$. 设 r 是能让 x^r 和 $\mathbb{F}_q$ 中某些元素模 $f(x)$ 同余的最小正整数，即对于一个 $a \in \mathbb{F}_q^*$ 满足 $x^r \equiv a \mod f(x)$ 的最小正整数.

那么就有 $ord(f) = hr$, 其中 h 是 a 在乘法群 $\mathbb{F}_q^*$ 上的阶.

证明：

设 $e = ord(f)$. 因为 $x^e \equiv 1 \mod f(x)$, 那么一定有 $e \geq r$, 所以 $e = sr + t$, $s \in \mathbb{N}, 0 \leq t < r$. 所以有

$$1 \equiv x^e \equiv x^{sr+t} \equiv a^s x^t \mod f(x)$$

因此 $x^t \equiv a^{-s} \mod f(x)$. 根据 r 的定义，只能有 $t = 0$. 所以 $a^s \equiv 1 \mod f(x)$, 因此 $a^s = 1$, 得到 $s \geq h, e \geq hr$.

反过来 $x^{hr} \equiv a^h \equiv 1 \mod f(x)$, 所以 $e = hr$.

Theorem 3.18

设 $f \in \mathbb{F}_q[x]$ 是一个次数为 $m \geq 1$ 的多项式，它是 $\mathbb{F}_q$ 上的本原多项式，当且仅当 $(-1)^m f(0)$ 是 $\mathbb{F}_q$ 上的本原元，且存在最小正整数 $r = \frac{q^m - 1}{q-1}$ 使得 $\mathbb{F}_q$ 中某些元素与 x^r 模 $f(x)$ 同余. 如果 f 是 $\mathbb{F}_q$ 上的本原多项式时，就有 $x^r \equiv (-1)^m f(0) \mod f(x)$.

证明：

如果 f 是 $\mathbb{F}_q$ 上的本原多项式，那么 f 有一个根 $\alpha \in \mathbb{F}_{q^m}$, 其中 α 是 $\mathbb{F}_{q^m}$ 上的本原元. 通过计算 $N_{F_{q^m}/F^q}(\alpha)$, 可以发现 f 是 $\mathbb{F}_q$ 上关于 α 的特征多项式，所以就有

$$(-1)^m f(0) = \alpha^{(q^m-1)/(q-1)} \tag{3.2}$$

可以发现 $(-1)^m f(0)$ 在 $\mathbb{F}_q^*$ 上的阶是 $q-1$, 也就是说 $(-1)^m f(0)$ 是一个 $\mathbb{F}_q$ 上的本原元. 又因为 f 是 $\mathbb{F}_q$ 上关于 α 的极小多项式，上式说明：

$$x^{(q^m-1)/(q-1)} \equiv (-1)^m f(0) \mod f(x)$$

所以就有 $r \leq (q^m - 1)/(q-1)$. 但是根据 **Theorem 3.16** 和 **Lemma 3.17** 可知 $q^m - 1 = ord(f) = (q-1)r$, 所以 $r = (q^m - 1)/(q-1)$.

反过来，假设后面的条件都成立，即 $r = (q^m - 1)/(q-1)$, 根据 Lemma 3.17 可以知道 $ord(f)$ 和 q 互素. 所以根据 Theorem 3.11 可以知道 f 可以分解成 $f = f_1 \dots f_k$ 这样的若干个 $\mathbb{F}_q$ 上首一不可约多项式的乘积. 设次数 $m_i = deg(f_i)$, 那么 $ord(f_i)$ 整除 $q^{m_i} - 1$ 根据 **Corollary 3.4** 对于 $1 \leq i \leq k$ 恒成立. 所以 $q^{m_i} - 1$ 整除 d, 其中

$$d = (q^{m_1} - 1) \dots (q^{m_k} - 1)/(q-1)^{k-1}$$

因此 $ord(f_i)$ 整除 d. 那么根据 **Lemma 3.6** 可以得到 $f_i(x)$ 整除 $x^d - 1$. 所以 $f(x)$ 整除 $x^d - 1$. 如果 $k \geq 2$, 则有：

$$d < (q^{m_1 + \dots + m_k} - 1)/(q-1) = (q^m - 1)/(q-1) = r$$

这和 r 的定义矛盾，所以 $k = 1$ 且 f 是 $\mathbb{F}_q$ 上的不可约多项式.

如果 $\beta \in \mathbb{F}_{q^m}$ 是 f 的一个根，那么根据式 (3.2) 就有 $\beta^r = (-1)^m f(0)$, 所以就有 $x^r \equiv (-1)^m f(0) \mod f(x)$.

因为$(-1)^m f(0)$ 在 $\mathbb{F}_q^*$ 上的阶是 $q-1$， 那么根据 **Lemma 3.17** 可以知道 $ord(f) = q^m - 1$, 根据 Theorem 3.16 可知 f 是 $\mathbb{F}_q$ 上的本原多项式.

Example 3.19

考虑多项式 $f(x) = x^4 + x^3 + x^2 + 2x + 2 \in \mathbb{F}_3[x]$. 因为 f 在 $\mathbb{F}_3$ 上不可约，可以得到 $ord(f) = 80 = 3^4 - 1$.

因此，根据 **Theorem 3.16** 可以知道 f 是 $\mathbb{F}_3$ 上的本原多项式；根据 **Theorem 3.18** 代入 $q = 3, m = 4$ 可知 $x^{40} \equiv 2 \mod f(x)$.

3.2 Irreducible Polynomials

Theorem 3.20

对任意有限域 $\mathbb{F}_q$ 和任意整数 $n \in \mathbb{N}$, 则所有 $\mathbb{F}_q$ 上的次数可以整除 n 的首一不可约多项式的乘积为 $x^{q^n} - x$.

证明：

由 **Lemma 2.13** 可知，出现在 $g(x) = x^{q^n} - x$ 的分解形式中的首一不可约多项式是次数可以整除 n 的多项式. 由于 $g'(x) = -1$, 所以由 **Theorem 1.68** 可知 g 在其 $\mathbb{F}_q$ 上的分裂域没有重根，所以每个次数整除 n 的首一不可约多项式都在分解式中出现恰好一次。原命题得证。

Corollary 3.21 Number of Monic Irreducible Polynomials

设 $N_q(d)$ 是 $\mathbb{F}_q[x]$ 上次数为 d 的首一不可约多项式个数，则有 $q^n = \sum_{d|n} dN_q(d)$

这个式子对于 $n \in \mathbb{N}$ 都成立.

证明：

由 **Theorem 3.20**, 对比结论式和分解形式的次数可以得到这个结论。

Definition 3.22 Moebius function

莫比乌斯函数 μ 是定义在 $\mathbb{N}$ 上的函数。

$$\mu(n) = \begin{cases} 1 & \text{n=1} \\ (-1)^k & \text{n是k个不同素数的乘积} \\ 0 & \text{n被某个素数的平方整除} \end{cases}$$

Lemma 3.23 Moebius Function Sum

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{n=1} \\ 0 & \text{n>1} \end{cases}$$

证明：

只需要考虑所有 $\mu(d) \neq 0$ 的 d, 即只需要考虑 n 的不同素因子 $p_1, p_2, \ldots, p_k$.

$n = 1$ 是显然的，考虑 $n > 1$ 的情况：

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \le i_1 < i_2 \le k} \mu(p_{i_1}, p_{i_2}) + \ldots + \mu(p_1 p_2 \ldots p_k) \\ &= 1 + C_k^1(-1) + C_k^2(-1)^2 + \ldots + C_k^k(-1)^k \\ &= (1 + (-1))^k \\ &= 0 \end{aligned}$$

Theorem 3.24 Moebius Inversion Formula

莫比乌斯反演公式：

对于所有 $n \in \mathbb{N}$:

$H(n) = \sum_{d|n} h(d)$ 当且仅当 $h(n) = \sum_{d|n} \mu(\frac{n}{d})H(d) = \sum_{d|n} \mu(d)H(\frac{n}{d})$

$H(n) = \prod_{d|n} h(d)$ 当且仅当 $h(n) = \prod_{d|n} H(d)^{\mu(n/d)} = \prod_{d|n} H(\frac{n}{d})^{\mu(d)}$

证明：

上面两个式子本质相同，只证明第一个.

$$\begin{aligned}\sum_{d|n} \mu(\frac{n}{d})H(d) &= \sum_{d|n} \mu(d)H(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{c|n/d} h(c) \\ &= \sum_{c|n} \sum_{d|n/c} \mu(d)h(c) = \sum_{c|n} h(c) \sum_{d|n/c} \mu(d) \\ &= h(n)\end{aligned}$$

Theorem 3.25 Reduction of Corollary 3.21

设 $N_q(n)$ 是 $\mathbb{F}_q[x]$ 上次数为 n 的首一不可约多项式个数，则

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$$

证明：

令 $h(n) = nN_q(n)$, $H(n) = q^n$, 由莫比乌斯反演上式显然成立。

Example 3.26

求 $\mathbb{F}_q[x]$ 上次数为 20 的首一不可约多项式个数.

解：

$$\begin{aligned}N_q(20) &= \frac{1}{20}(\mu(1)q^{20} + \mu(2)q^{10} + \mu(4)q^5 + \ldots + \mu(20)q) \\ &= \frac{1}{20}(q^{20} - q^{10} - q^4 + q^2)\end{aligned}$$

Theorem 3.27

考虑域 K, 其特征为 p, 考虑正整数 $n \in \mathbb{N}$ 且 $n \nmid p$, 那么 K 上的 n 次分圆多项式 Q_n 满足

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}$$

证明：

令 $h(n) = Q_n(x)$, $H(n) = x^n - 1$, 由莫比乌斯反演上式显然成立。

Example 3.28

设域 K 上定义的分圆多项式 Q_{12}.

则有

$$\begin{aligned} Q_{12}(x) &= \prod_{d|12}(x^{12/d}-1)^{\mu(d)} \\ &= (x^{12}-1)^{\mu(1)}(x^6-1)^{\mu(2)}(x^4-1)^{\mu(3)}(x^3-1)^{\mu(4)}(x^2-1)^{\mu(6)}(x-1)^{\mu(12)} \\ &= \frac{(x^{12}-1)(x^2-1)}{(x^6-1)(x^4-1)} \\ &= x^4-x^2+1 \end{aligned}$$

Theorem 3.29

记所有 $\mathbb{F}_q[x]$ 上次数为 n 的**所有首一不可约多项式的乘积**为 $I(q,n;x)$. 则:

$$I(q,n;x)=\prod_{d|n}(x^{q^d}-x)^{\mu(n/d)}=\prod_{d|n}(x^{q^{n/d}}-x)^{\mu(d)}$$

证明: 由 **Theorem 3.20** 可以知道 $x^{q^n}-x=\prod_{d|n}I(q,d;x)$

令 $h(n)=I(q,n;x)$, $H(n)=x^{q^n}-x$, 由莫比乌斯反演上式得证。

Example 3.30

计算 $I(2,4;x)$.

解:

$$\begin{aligned} I(2,4;x) &= (x^{16}-x)^{\mu(1)}(x^4-x)^{\mu(2)}(x^2-x)^{\mu(4)} \\ &= \frac{x^{16}-x}{x^4-x} \\ &= \frac{x^{15}-1}{x^3-1} \\ &= x^{12}+x^9+x^6+x^3+1 \end{aligned}$$

Theorem 3.31 Product of Monic Irreducible Polynomials

设 $Q_m(x)$ 是 $\mathbb{F}_q$ 上的 m 次分圆多项式，则有

$$I(q,n;x)=\prod_m Q_m(x)$$

其中 m 是 q^n-1 的所有正因子， $n>1$ 是 q 模 m 的阶.

证明:

对于 $n>1$, 令集合 S 表示所有 $\mathbb{F}_{q^n}$ 上的元素. 那对于每个 $\alpha\in S$ 都有在 $\mathbb{F}_q$ 上的次数为 n 的极小多项式，它也是 $I(q,n;x)$ 的一个根. 同时，如果 β 也是 $I(q,n;x)$ 的一个根，那 β 也是一个在 $\mathbb{F}_q[x]$ 上的次数为 n 的首一不可约多项式的根，也就是说 $\beta\in S$.

所以可以得到

$$I(q,n;x)=\prod_{\alpha\in S}(x-\alpha) \tag{1}$$

如果 $\alpha \in S$, 则有 $\alpha \in \mathbb{F}_{q^n}^*$. 所以在这个乘法群里， α 的阶是 q^n-1 的因子。而 $\gamma \in \mathbb{F}_{q^n}^*$ 是 $\mathbb{F}_{q^n}$ 的真子域 $\mathbb{F}_{q^d}$ 中的元素，当且仅当 $\gamma^{q^d}=\gamma$, 即当且仅当 γ 的阶整除 q^d-1. 因此，对于 $\alpha \in S$, 设其阶是 m, 则一定满足 $q^n \equiv 1 \mod m$. 对于满足这个条件的某个 q^n-1 的因子 m, 令 S_m 表示 S 中阶为 m 的元素，那 S 可以表示成若干个 S_m 的交，所以 (1) 式可以写成

$$I(q,n;x)=\prod_m \prod_{\alpha \in S_m}(x-\alpha) \tag{2}$$

可以发现 S_m 包括了所有 $\mathbb{F}_{q^n}^*$ 中阶为 m 的元素. 也就是说， S_m 是 F_q 的 m 次本原根的集合. 由分圆多项式的定义 (**Definition 2.44**) 可以知道，

$$\prod_{\alpha \in S_m}(x-\alpha)=Q_m(x) \tag{3}$$

所以结论得证。

Example 3.32

尝试确定 $\mathbb{F}_2[x]$ 上所有次数为 4 的首一不可约多项式.

解： 由 **Theorem 3.31** 可以知道 $I(2,4;x)=Q_5(x)Q_{15}(x)$, 由 **Theorem 2.47(ii)** 可以得到 $Q_5(x)=x^4+x^3+x^2+x+1$ 是 $\mathbb{F}_2[x]$ 上的不可约多项式；同理， $Q_{15}(x)$ 可以分解成 $\mathbb{F}_2[x]$ 上两个次数为 4 的不可约多项式（因为 $\frac{\phi(15)}{4}=2$）.

考虑 $Q_5(x+1)=x^4+x^3+1$, 它在 $\mathbb{F}_2[x]$ 上不可约，它整除 $Q_{15}(x)$, 所以有

$$Q_{15}(x)=(x^4+x^3+1)(x^4+x+1)$$

所以所有的 $\mathbb{F}_2[x]$ 上所有次数为 4 的首一不可约多项式为 $x^4+x^3+x^2+x+1$, x^4+x^3+1 和 x^4+x+1.

Theorem 3.33

设 α 是一个 $\mathbb{F}_{q^m}$ 上的元素， $\mathbb{F}_{q^m}$ 是 $\mathbb{F}_q$ 的一个域扩张. 设 α 在 $\mathbb{F}_q$ 上的次数是 d, $g \in \mathbb{F}_q[x]$ 是 α 在 $\mathbb{F}_q$ 上的极小多项式，则：

(i) g 在 $\mathbb{F}_q$ 上不可约，设它的次数是 d, 则有 $d|m$.

(ii) 设多项式 $f \in \mathbb{F}_q[x]$, 则 $f(\alpha)=0$ 当且仅当 $g|f$.

(iii) 设 f 是一个 $\mathbb{F}_q[x]$ 上的首一不可约多项式，$f(\alpha)=0$, 则 $f=g$.

(iv) $g(x)|x^{q^d}-x$ 且 $g(x)|x^{q^m}-x$

(v) g 的根是 $\alpha, \alpha^2, \ldots, \alpha^{q^{d-1}}$, g 是 $\mathbb{F}_q$ 上这些元素的极小多项式.

(vi) 如果 $\alpha \neq 0$, 那么 $ord(g)$ 等于 α 在乘法群 $\mathbb{F}_{q^m}^*$ 中的阶.

(vii) g 是 F_q 上的本原多项式，当且仅当 α 在 $\mathbb{F}_{q^m}^*$ 中的阶是 q^d-1.

证明：

(i) 不可约可以由 **Theorem 1.82(i)** 得到，整除性可以由 **Theorem 1.86** 得到.

(ii) 由 **Theorem 1.82(ii)** 可得.

(iii) 由 (ii) 可得.

(iv) 由 (i) 和 **Lemma 2.13** 可得.

(v) 前半部分由 (i) 和 **Theorem 2.14** 可得，后半部分由 (ii) 可得.

(vi) 由于 $\alpha \in F_{q^d}^*$, $F_{q^d}^*$ 又是 $F_{q^m}^*$ 的一个子群，由 **Theorem 3.3** 可得结论.

(vii) 如果 g 是 $\mathbb{F}_q$ 上的本原多项式，那么 $ord(g) = q^d - 1$, 由 (vi) 可知 α 在 $F_{q^m}^*$ 上的阶是 $q^d - 1$.

反过来，如果 α 在 $F_{q^m}^*$ (和 $F_{q^m}^*$)上的阶是 $q^d - 1$，那么 α 就是 $\mathbb{F}_{q^d}$ 上的一个本原元，所以由 **Definition 3.15** 可以知道 g 是 F_q 上的本原多项式.

3.3 Construction of Irreducible Polynomials

Lemma 3.34

设 $s \geq 2,\ e \geq 2,\ gcd(e,q)=1,\ m$ 是 s 模 e 的阶. 设 $t \geq 2$，它的素因子可以整除 e 但不整除 $(s^m-1)/e$, 如果 $t \equiv 0 \mod 4$ 则附加 $s^m \equiv 1 \mod 4$

那么 mt 是 s 模 et 的阶.

证明：

尝试对 t 的素因子个数进行归纳法证明.

首先，设 t 是一个素数，令 $d=(s^m-1)/e$, 那么 $s^m=de+1$, 所以：

$$\begin{aligned} s^{mt} &= (1+de)^t \\ &= 1+C_t^1 de + C_t^2 d^2 e^2 + \ldots + C_t^{t-1} d^{t-1} e^{t-1} + d^t e^t \end{aligned}$$

显然，这个式子除了第一项和最后一项可以整除 et.

对于最后一项，由于 $t|e$, 所以这一项可以整除 et. 所以可以得到 $s^{mt} \equiv 1 \mod et$.

设 s 模 et 的阶是 k, 那么就有 $k|mt$. 由定义 $s^k \equiv 1 \mod et$, 那么就有 $s^k \equiv 1 \mod e$, 那么就有 $m|k$.

由于 t 是一个素数，那么 $k=m$ 或者 $k=mt$.

如果 $k=m$ 则有 $s^m \equiv 1 \mod et$, 因此 $de \equiv 0 \mod et$, $t|d$, 导出矛盾.

所以 $k=mt$.

下面考虑 t 有至少两个素因子的情况，即 $t=rt_0$, 其中 r 是 t 的一个素因子.

现在已经知道 s 模 er 的阶是 mr 了，如果可以证明每个 t_0 的素因子都整除 er, 但不整除 $d_0=(s^{mr}-1)/er$, 那么对于 t_0 的归纳假设就可以得到 s 模 $ert_0=et$ 的阶等于 $mrt_0=mt$.

令 r_0 是 t_0 的一个素因子，由于每个 t 的素因子都整除 e, 所以 r_0 整除 er.

令 $d=(s^m-1)/e$, 则有 $s^{mr}-1=c(s^m-1)$, 其中 $c=s^{m(r-1)}+\ldots+s^m+1$, 因此 $d_0=c(s^m-1)/er=cd/r$.

同时，因为 $s^m \equiv 1 \mod e$ 且 $r|e$, 所以 $s^m \equiv 1 \mod r$, 所以 $c \equiv r \equiv 0 \mod r$. 因此 c/r 是一个整数.

又因为 $r_0 \nmid d$, 所以只需要证明 $r_0 \nmid c/r$ 就可以证明 $r_0 \nmid cd/r$ 了.

注意到 $s^m \equiv 1 \mod r_0$, 所以 $c \equiv r \mod r_0$. 如果 $r_0 \neq r$, 就有 $c/r \equiv 1 \mod r_0$, 所以 $r_0 \nmid c/r$.

如果 $r_0=r$, 那么存在 $b \in \mathbb{Z}$ 使得 $s^m \equiv 1+br \mod r^2$

因此 $s^{mj} \equiv (1+br)^j \equiv 1+jbr \mod r^2$ 对于 $j \geq 0$ 都成立，因此

$$c \equiv r + br\sum_{j=0}^{r-1} j \equiv r + br\frac{r(r-1)}{2} \mod r^2$$

所以

$$\frac{c}{r} \equiv 1 + b\frac{r(r-1)}{2} \mod r$$

如果 r 是奇数，那么 $c/r \equiv 1 \mod r$, 所以 $r_0 = r \nmid c/r$.

剩下的只有 $r_0 = r = 2$ 的情况，由假设，t 是 4 的倍数，$s^m \equiv 1 \mod 4$.

因为 $c = s^m + 1$, 所以 $c \equiv 2 \mod 4$, 因此 $c/r = c/2 \equiv 1 \mod 2$. 所以$r_0 = r \nmid c/r$.

Theorem 3.35

设 $f_1(x), f_2(x), \ldots, f_N(x)$ 是 $\mathbb{F}_q[x]$ 上两两不同的首一不可约多项式，次数都是 m, 阶都是 e.

设 $t \geq 2$, 它的素因子可以整除 e 但不整除 $(q^m - 1)/e$, 如果 $t \equiv 0 \mod 4$, 则附加 $q^m \equiv 1 \mod 4$.

那么 $f_1(x^t), f_2(x^t), \ldots, f_N(x^t)$ 都是 $\mathbb{F}_q[x]$ 上两两不同的首一不可约多项式，次数都是 mt, 阶都是 et.

证明：

引理：（有待证明）对于素数 p 和可以被 p 整除的正整数 $m \in \mathbb{N}$, 有 $Q_{mp}(x) = Q_m(x^p)$

条件蕴含 $e \geq 2$. 根据 **Theorem 3.5** 可知，当且仅当 m 是 q 模 e 的阶的时候， $\mathbb{F}_q[x]$ 上两两不同的，次数都是 m, 阶都是 e 的首一不可约多项式才存在，其中个数 $N = \frac{\phi(e)}{m}$.

由 **Lemma 3.34** 可知，mt 是 q 模 et 的阶，而 $\phi(et)/mt = \phi(e)/m$, 所以 $\mathbb{F}_q[x]$ 上两两不同的，次数都是 mt, 阶都是 et 的首一不可约多项式个数也是 N. 因此，只需要证明每个多项式 $f_j(x^t), 1 \leq j \leq N$ 在 $\mathbb{F}_q[x]$ 上都不可约，而且阶是 et 即可.

根据 **Theorem 3.3** 可知每个 $f_j(x^t)$ 的根都是 $\mathbb{F}_q$ 上的 n 次本原单位根，所以 $f_j(x)$ 整除 $\mathbb{F}_q$ 上的分圆多项式 $Q_e(x)$.

所以 $f_j(x^t) \mid Q_e(x^t)$. 由引理， $f_j(x^t) \mid Q_{et}(x)$.

根据 **Theorem 2.47(ii)** 可知，$Q_{et}(x)$ 在 $\mathbb{F}_q[x]$ 上不可约因子的次数等于 q 模 et 的阶，这个阶等于 mt. 因为 $f_j(x^t)$ 的次数是 mt, 所以它在 $\mathbb{F}_q[x]$ 上不可约. 从而由于 $f_j(x^t) \mid Q_{et}(x)$, $f_j(x^t)$ 的阶则是 et.

Example 3.36

已知 $\mathbb{F}_2[x]$ 上次数为 4, 阶为 15 的不可约多项式，它们有 $x^4 + x^3 + 1$ 和 $x^4 + x + 1$. 那么：

$\mathbb{F}_2[x]$ 上次数为 12, 阶为 45 的不可约多项式有 $x^{12} + x^9 + 1$ 和 $x^{12} + x^3 + 1$.

$\mathbb{F}_2[x]$ 上次数为 60, 阶为 225 的不可约多项式有 $x^{60} + x^{45} + 1$ 和 $x^{60} + x^{15} + 1$.

$\mathbb{F}_2[x]$ 上次数为 100, 阶为 375 的不可约多项式有 $x^{100} + x^{75} + 1$ 和 $x^{100} + x^{25} + 1$.

Theorem 3.37

设 $f_1(x), f_2(x), \ldots, f_N(x)$ 是 $\mathbb{F}_q[x]$ 上两两不同的首一不可约多项式，次数都是奇数 m, 阶都是 e.

令 $q = 2^a u - 1, t = 2^b v$, 其中 $a, b \geq 2, u, v$ 是奇数， t 的素因子可以整除 e 但不整除 $(q^m - 1)/e$.

令 $k = min(a, b)$. 那么：

每个多项式 $f_j(x^t)$ 可以分解成 2^{k-1} 个 $\mathbb{F}_q[x]$ 上次数为 $mt2^{1-k}$ 首一不可约多项式 $g_{ij}(x)$ 的乘积.

这些 $2^{k-1}N$ 个多项式 $g_{ij}(x)$ 都是 $\mathbb{F}_q[x]$ 上次数为 $mt2^{1-k}$, 阶数为 et 的首一不可约多项式.

证明:

第一部分:

若 $v \geq 3$, 由 **Theorem 3.35** 可知， $f_1(x^v), f_2(x^v), \ldots, f_N(x^v)$ 都是 $\mathbb{F}_q[x]$ 上次数为奇数 mv, 阶都是 ev 的互不相等的首一不可约多项式. 只需要处理 $v = 1$ 的情况, 此时 $t = 2^b$.

当 $t = 2^b$ 时，由 **Theorem 3.35** 的证明过程可知 m 是 q 模 e 的阶， $N = \frac{\phi(e)}{m}$, 且 $f_j(x^t) \mid Q_{et}(x)$.

由 **Theorem 2.47(ii),** $Q_{et}(x)$ 可以分解成 $\mathbb{F}_q[x]$ 上的若干个不同的次数为 d 的首一不可约多项式，其中 d 是 q 模 et 的阶.

因为 $q^d \equiv 1 \mod et$, 所以有 $q^d \equiv 1 \mod e$, 所以有 $m \mid d$. 下面根据 a, b 的大小关系来讨论.

(1) 设 $a \geq b$, 那么 $q^{2m} - 1 = (q^m - 1)(q^m + 1)$, 第一项可以被 e 整除；而由于 $q \equiv -1 \mod 2^a$, 所以 $q \equiv -1 \mod t$, 因此 $q^m \equiv (-1)^m \equiv -1 \mod t$, 所以第二项可以被 t 整除.

综上，可以得到 $q^{2m} \equiv et$, 所以有 $d = m$ 或 $d = 2m$.

如果 $d = m$, 就有 $q^m \equiv 1 \mod et$, 因此 $q^m \equiv 1 \mod t$, 这和 $q \equiv -1 \mod t$ 矛盾.

所以 $d = 2m = m2^{b-k+1} = m$.

(2) 若 $a < b$, 对 h 进行归纳法：设 w 是奇数，对任意 $h \in \mathbb{N}$ 有:

$$q^{m2^h} \equiv 1 + w2^{a+h} \mod 2^{a+h+1} \tag{4}$$

考虑 $h = 1$, 那么就有:

$$\begin{aligned} q^{2m} &= (2^a u - 1)^{2m} \\ &= 1 - 2^{a+1}um + \sum_{n=2}^{2m} C_{2m}^n (-1)^{2m-n} 2^{na} u^n \\ &\equiv 1 + w2^{a+1} \mod 2^{a+2} \end{aligned}$$

其中 $w = -um$, 假设存在 $h \in \mathbb{N}$ 使公式 (4) 成立，那就存在 $c \in \mathbb{Z}$ 使下式成立:

$$q^{m2^h} = 1 + w2^{a+h} + c2^{a+h+1}$$

所以就有

$$q^{m2^{h+1}} = (1 + w2^{a+h} + c2^{a+h+1})^2 \equiv 1 + w2^{a+h+1} \mod 2^{a+h+2}$$

所以对于 $h + 1$ 也成立，因此由归纳法，公式 (4) 成立.

首先，令 $h = b - a + 1$ 代入 (4), 则有

$$q^{m2^{b-a+1}} \equiv 1 \mod 2^{b+1}$$

此外，由 $q^m \equiv 1 \mod e$ 可以得到

$$q^{m2^{b-a+1}} \equiv 1 \mod e$$

所以有

$$q^{m2^{b-a+1}} \equiv 1 \mod L, L = lcm(2^{b+1}, e)$$

因为所有 t 的素因子都整除 e, 所以 e 是偶数，但是 $4 \nmid e$. 这是因为 $q^m \equiv 1 \mod e$ 且 $q^m \equiv -1 \mod 4$.

因此 $L = e2^b = et$, 因此 $q^{m2^{b-a+1}} \equiv 1 \mod et$.

另一方面，令 $h = b - a$, 可以得到

$$q^{m2^{b-a}} \equiv 1 + w2^b \not\equiv 1 \mod 2^{b+1}$$

所以

$$q^{m2^{b-a}} \not\equiv 1 \mod et$$

所以必有 $d = m2^{b-a+1} = m2^{b-k+1}$. 因此 $d = m2^{b-k+1} = mt2^{1-k}$ 成立.

第二部分：

因为 $Q_{et}(x)$ 可以分解成 $\mathbb{F}_q[x]$ 上的不同的次数为 $mt2^{1-k}$ 的首一不可约多项式. 对比系数可以得到这些因子的个数是 2^{k-1}.

由于每个$f_j(x^t)$ 的不可约因子 $g_{ij}(x)$ 都整除 $Q_et(x)$, 每个 $g_{ij}(x)$ 的阶都是 et.

下面证明每个 $g_{ij}(x), 1 \le i \le 2^{k-1}, 1 \le j \le N$ 都是不同的.

假设存在一个与之相同的 $g(x)$, 那么对于 $j_1 \ne j_2$, 有 $g(x) \mid f_{j_1}(x^t)$, $g(x) \mid f_{j_2}(x^t)$.

那么每个 $g(x)$ 的根 β 都会是 $f_{j_1}(x)$ 和 $f_{j_2}(x)$ 的公共根，这和 $f_{j_1}(x)$ 与 $f_{j_2}(x)$ 是不同的首一不可约多项式相矛盾.

所以每个 $g_{ij}(x)$ 都是不同的.

那么由 **Theorem 3.5** 可以得到 $\mathbb{F}_q[x]$ 上次数为 $mt2^{1-k}$, 阶为 et 的首一不可约多项式个数是：

$$\frac{\phi(et)}{mt2^{1-k}} = \frac{2^{k-1}\phi(et)}{mt} = \frac{2^{k-1}\phi(e)}{m} = 2^{k-1}N$$

所以 $g_{ij}(x)$ 就是这些多项式.

Theorem 3.38 Find all Irreducible Polynomials whose Orders Divide a Specific Number

多项式 $g_{t_1}, g_{t_2}, \dots, g_{t_n}$ 是 $\mathbb{F}_q[x]$ 上全部的阶可以整除 e 的且常数项不为零的首一不可约多项式.

其中，$t_1 = 1, t_j$ 是满足 $t_j \equiv t_i q^b \mod e, 1 \le i < j$ 的最小正整数，其中 b 是非负正整数.

$T = (t_1, t_2, \dots, t_n)$

证明：

根据定义，每个 g_{t_i} 都是 $\mathbb{F}_q[x]$ 上的首一不可约多项式，且有 $g_{t_i}(0) \ne 0$.

因为 g_{t_i} 有根 a^{t_i}, 它在 $\mathbb{F}_{q^m}^*$ 上的阶可以整除 a 的阶，所以由 **Theorem 3.3** 可知 $ord(g_{t_i}) \mid e$.

设 g 是 $\mathbb{F}_q[x]$ 上的任意一个首一不可约多项式，阶为 d, $d \mid e$, $g(0) \ne 0$.

设 β 是 g 的一个根，那么就有 $b^d = 1$, 所以 $b^e = 1$, 所以 β 是 $\mathbb{F}_q$ 上的一个 e 次单位根.

而 a 是 $\mathbb{F}_q$ 上的一个 e 次本原单位根，由 **Theorem 2.42(i)** 存在 $t \in \mathbb{N}$ 使得 $\beta = a^t$.

根据 T 的定义，存在 i 和 $b \geq 0$ 满足 $t \equiv t_i q^b \mod e$. 因此 $\beta = a^t = (a^{t_i})^{q^b}$, 根据 **Theorem 2.14**, β 是 g_{t_i} 的根.

由于 g 是 β 在 $\mathbb{F}_q$ 上的极小多项式，根据 **Theorem 3.33(iii)** 可知 $g = g_{t_i}$.

下面只需要证明这 t_n 个 g_i 互不相同. 假设 $g_{t_i} = g_{t_j}, i \neq j$. 那么 a^{t_i} 和 a^{t_j} 是 g_{t_i} 的根，所以存在 $b \geq 0$ 使得 $a^{t_j} = (a^{t_i})^{q^b}$.

所以 $t_j \equiv t_i q^b \mod e$. 但是 $t_j \equiv t_i q^0 \mod e$, 根据集合 T 的定义，矛盾. 所以这些 g_i 互不相同.

Theorem 3.39 Calculate the Characteristic Polynomial

设 f 是 $\mathbb{F}_q[x]$ 上次数为 m 的首一不可约多项式. 令 $\alpha \in \mathbb{F}_{q^m}$ 是 f 的一个根，那么对于 $t \in \mathbb{N}$, 记 f_t 为 $\alpha^t \in \mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的特征多项式，那么：

$$f_t(x^t) = (-1)^{m(t+1)} \prod_{j=1}^{t} f(\omega_j x)$$

其中 $\omega_1, \ldots, \omega_t$ 是 $\mathbb{F}_q$ 上的 t 次单位根.

证明：

令 $\alpha = \alpha_1, \ldots, \alpha_m$ 是 f 的所有根，那么 $\alpha_1^t, \ldots, \alpha_m^t$ 就是 f_t 的所有根.

那么就有：

$$\begin{aligned} f_t(x^t) &= \prod_{i=1}^{m} (x^t - \alpha_i^t) \\ &= \prod_{i=1}^{m} \prod_{j=1}^{t} (x - \alpha_i \omega_j) \\ &= \prod_{i=1}^{m} \prod_{j=1}^{t} \omega_j (\omega_j^{-1} x - \alpha_i) \end{aligned}$$

比较该恒等式中的系数

$$x^t - 1 = \prod_{j=1}^{t} (x - \omega_j)$$

得到

$$\prod_{j=1}^{t} \omega_j = (-1)^{t+1}$$

由于 $\omega_1^{-1}, \ldots, \omega_t^{-1}$ 遍历$\mathbb{F}_q$ 上的所有 t 次单位根 , 所以有

$$\begin{aligned} f_t(x^t) &= (-1)^{m(t+1)} \prod_{j=1}^{t} \prod_{i=1}^{m} (\omega_j^{-1} x - \alpha_i) \\ &= (-1)^{m(t+1)} \prod_{j=1}^{t} f(\omega^{-1} x) \\ &= (-1)^{m(t+1)} \prod_{j=1}^{t} f(\omega_j x) \end{aligned}$$

Example 3.40

考虑 $\mathbb{F}_2[x]$ 上的不可约多项式 $f(x)=x^4+x+1$. 计算 f_3.

解： 要计算 f_3, 可以发现 F_2 上的三次单位根是 $1,\omega,\omega^2$, 其中 ω 是 x^2+x+1 在 $\mathbb{F}_4$ 上的根. 那么就有：

$$\begin{aligned} f_3(x^3) &= (-1)^{16} f(x) f(\omega x) f(\omega^2 x) \\ &= (x^4+x+1)(\omega x^4+\omega x+1)(\omega^2 x^4+\omega^2 x+1) \\ &= x^{12}+x^9+x^6+x^3+1 \end{aligned}$$

所以 $f_3(x)=x^4+x^3+x^2+x+1$.

也可以用矩阵的方法去求 f_t. 令 $f(x)=x^m-a_{m-1}x^{m-1}-\ldots-a_1x-a_0$, 令 A 是 $f(x)$ 的伴随矩阵，定义为：

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{m-1} \end{pmatrix}$$

那么 $f(x)$ 就是 A 的特征多项式，$f(x)=det(xI-A)$. 那么对于每个 $t\in\mathbb{N}$ 只需要计算 A^t 就可以得到特征多项式 $f_t(x)$ 的值了.

Example 3.41

当且仅当 $k=m$ 的时候， f_t 在 $\mathbb{F}_q[x]$ 上不可约，即当且仅当 m 是 q 模 $d=e/gcd(t,e)$ 的阶的时候.

考虑 $q=2,m=6,e=63$ 的情况.

由于 q 模某个 e 的因子的阶一定是 m 的一个因子，所以只能有 $k=1,2,3$. 那么 $q^k-1=1,3,7$.

那么 $q^k\equiv 1 \mod d$ 成立只在 $d=1,3,7$ 的时候成立。因此 f_t 在 $F_2[x]$ 上可约当且仅当 $gcd(t,63)=9,21,63$.

所以当 $t\neq 9,18,21,27,36,42,45,54,63$ 的时候， f_t 在 $F_2[x]$ 上不可约.

Method 3.42 Determining Minimal Polynomials(i)

下面给出一个求极小多项式的方法.

设 θ 是 F_{q^m} 在 F_q 上的定义元, 那么 $\{1,\theta,\ldots,\theta^{m-1}\}$ 就是 F_{q^m} 在 F_q 上的一组基.

为了找到 F_{q^m} 在 F_q 上以 β 作为一组基的极小多项式，设基为 $\{1,\beta,\ldots,\beta^m\}$

其中

$$\beta^{i-1}=\sum_{j=1}^{m} b_{ij}\theta^{j-1}$$

对 $1\le i\le m+1$ 都成立.

那么 g 可以表示为 $g(x)=c_mx^m+\ldots+c_1x+c_0$. 现在需要让 g 为次数最小的满足 $g(\beta)=0$ 的首一多项式（即以 β 为根），那么就可以得到线性方程的一个齐次系统：

$$\sum_{i=1}^{m+1} c_{i-1} b_{ij} = 0 \tag{5}$$

对 $1 \leq j \leq m$ 都成立, c_i 都是未知数. 令 B 为这个齐次系统的系数矩阵，设其秩为 r. 那么解空间的维数就是 $s = m + 1 - r$.

因为 $1 \leq r \leq m$, 所以有 $1 \leq s \leq m$. 所以就可以给 s 规定相应的值.

如果 $s = 1$, 就令 $c_m = 1$; 如果 $s > 1$, 就令 $c_m = c_{m-1} = \ldots = c_{m-s+2} = 0, c_{m-s+1} = 1$. 剩下的系数由 (5) 式解出.

Example 3.42

设 $\theta \in \mathbb{F}_{64}$ 是 $\mathbb{F}_2[x]$ 上不可约多项式 $x^6 + x + 1$ 的根. 对于 $\beta = \theta^3 + \theta^4$, 有:

$$\begin{aligned}
\beta^0 &= 1 \\
\beta^1 &= \theta^3 + \theta^4 \\
\beta^2 &= 1 + \theta + \theta^2 + \theta^3 \\
\beta^3 &= \theta + \theta^2 + \theta^3 \\
\beta^4 &= \theta + \theta^2 + \theta^4 \\
\beta^5 &= 1 + \theta^3 + \theta^4 \\
\beta^6 &= 1 + \theta + \theta^2 + \theta^4
\end{aligned}$$

所以

$$B = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0
\end{pmatrix}$$

可以发现 $rank(B) = 3$. 所以 $s = m + 1 - r = 4$, 所以 $c_6 = c_5 = c_4 = 0, c_3 = 1$. 剩下的系数由式 (5) 产生，可以计算得到 $c_2 = 1, c_1 = 0, c_0 = 1$. 所以最后可以得到以 β 为根的在 $\mathbb{F}_2$ 上的极小多项式为 $g(x) = x^3 + x^2 + 1$.

Method 3.43 Determining Minimal Polynomials(ii)

另一个求极小多项式的方法由 **Theorem 3.33(v)** 确定.

计算 $\beta, \beta^q, \beta^{q^2}, \ldots$ 直到寻找到最小的正整数 d 使得 $\beta^{q^d} = \beta$. 这个 d 就是 g 的次数，所以就有:

$$g(x) = (x - \beta)(x - \beta^q) \ldots (x - \beta^{q^{d-1}})$$

$\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{d-1}}$ 都是 β 在 $\mathbb{F}_q$ 上的共轭元， g 是 $\mathbb{F}_q$ 上的以这些元素为根的极小多项式.

Example 3.43

计算 $\mathbb{F}_2$ 上以 $\mathbb{F}_{16}$ 每个元素为根的极小多项式.

解：设 $\theta \in \mathbb{F}_{16}$ 是 $\mathbb{F}_2$ 上本原多项式 $x^4 + x + 1$ 的根，那么每个元素都可以被写成 θ 的幂次.

i	θ^i	i	θ^i
0	1	8	$1 + \theta^2$
1	θ	9	$\theta + \theta^3$
2	θ^2	10	$1 + \theta + \theta^2$
3	θ^3	11	$\theta + \theta^2 + \theta^3$
4	$1 + \theta$	12	$1 + \theta + \theta^2 + \theta^3$
5	$\theta + \theta^2$	13	$1 + \theta^2 + \theta^3$
6	$\theta^2 + \theta^3$	14	$1 + \theta^3$
7	$1 + \theta + \theta^3$		

以 β 为根的 $\mathbb{F}_2$ 上的极小多项式为：

$\beta = 0$: $g_1(x) = x$

$\beta = 1$: $g_2(x) = x + 1$

$\beta = \theta$: θ 不同的共轭元有 $\theta, \theta^2, \theta^4, \theta^8$, 极小多项式为 $g_3(x) = (x - \theta)(x - \theta^2)(x - \theta^4)(x - \theta^8) = x^4 + x + 1$

$\beta = \theta^3$: θ^3 不同的共轭元由 $\theta^3, \theta^6, \theta^{12}, \theta^{24} = \theta^9$, 所以极小多项式为 $g_4(x) = x^4 + x^3 + x^2 + x + 1$

$\beta = \theta^5$ 和 $\beta = \theta^7$ 的情况同上，极小多项式分别为 $g_5(x) = x^2 + x + 1$ 和 $g_6(x) = x^4 + x^3 + 1$.

所有这些 $\mathbb{F}_2$ 上的元素及其共轭元遍历了 F_{16}.

Method 3.44 Determining Primitive Polynomials

方法一：

根据 **Theorem 2.47(ii)** 可以知道所有 $\mathbb{F}_q$ 上次数为 m 的本原多项式的乘积等于分圆多项式 Q_e, 其中 $e = q^m - 1$.

那么，所有 $\mathbb{F}_q$ 上次数为 m 的本原多项式可以通过分解 Q_e 得到。

方法二：

先构造一个 $\mathbb{F}_{q^m}$ 上的本原元，然后构造以这个本原元为根的 $\mathbb{F}_q$ 上的极小多项式.

要寻找一个本原元，需要寻找一个 $\mathbb{F}_{q^m}^*$ 上阶为 $q^m - 1$ 的一个元素，分解为 $q^m - 1 = h_1 \dots h_k$, 其中 h_i 两两互素.

如果对于每个 $1 \leq i \leq k$, 可以找到一个阶为 h_i 的元素 $\alpha_i \in \mathbb{F}_{q^m}^*$, 那么乘积 $\alpha_1 \dots \alpha_k$ 的阶就是 $q^m - 1$, 这个乘积就是一个本原元.

Example 3.44

寻找一个 $\mathbb{F}_3$ 上次数为 4 的本原多项式.

解： $e = 3^4 - 1 = 80 = 16 \cdot 5$.

首先构造两个 $\mathbb{F}_{81}^*$ 中的元素，阶分别为 16 和 5. 阶为 16 的元素是分圆多项式 $Q_{16}(x) = x^8 + 1 \in \mathbb{F}_3[x]$ 的根.

因为 3 模 16 的阶是 4, 所以 $Q_{16}(x)$ 可以分解成 2 个 $\mathbb{F}_3[x]$ 上次数为 4 的首一不可约多项式.

$$Q_{16}(x) = (x^4 - 1 + x^2)(x^4 - 1 - x^2)$$

$f(x) = x^4 - x^2 - 1$ 在 $\mathbb{F}_3$ 上不可约，设 f 的一个根为 θ, 那么 $\mathbb{F}_{81} = \mathbb{F}_3(\theta)$. 此外， θ 在 $\mathbb{F}_{81}^*$ 中的阶是 16.

如果要找到一个阶为 5 的元素 α, 记 $\alpha = a + b\theta + c\theta^2 + d\theta^3$, 其中 $a, b, c, d \in \mathbb{F}_3$.

因为 $\alpha^{10} = 1$, 所以

$$\begin{aligned}
1 = \alpha^9\alpha &= (a + b\theta^9 + c\theta^{18} + d\theta^{27})(a + b\theta + c\theta^2 + d\theta^3) \\
&= (a - b\theta + c\theta^2 - d\theta^3)(a + b\theta + c\theta^2 + d\theta^3) \\
&= (a + c\theta^2)^2 - (b\theta + d\theta^3)^2 = a^2 + (2ac - b^2)\theta^2 + (c^2 - 2bd)\theta^4 - d^2\theta^6 \\
&= a^2 + c^2 - d^2 + bd + (c^2 + d^2 - b^2 - ac + bd)\theta^2
\end{aligned}$$

进行系数比较可以得到

$$\begin{aligned}
a^2 + c^2 - d^2 + bd &= 1 \\
c^2 + d^2 - b^2 - ac + bd &= 0
\end{aligned}$$

令 $a = d = 0$, 则有 $b^2 + c^2 = 1$. 令 $b = c = 1$, 那么 $\alpha = \theta + \theta^2$ 的阶为 5.

那么 $\zeta = \theta\alpha = \theta^2 + \theta^3$ 的阶是 80, 是 $\mathbb{F}_{81}$ 的一个本原元. 所以以 ζ 为根的 $\mathbb{F}_3$ 上的极小多项式是：

$$\begin{aligned}
g(x) &= (x - \zeta)(x - \zeta^3)(x - \zeta^9)(x - \zeta^{27}) \\
&= (x - \theta^2 - \theta^3)(x - 1 + \theta + \theta^2)(x - \theta^2 + \theta^3)(x - 1 - \theta + \theta^2) \\
&= x^4 + x^3 + x^2 - x - 1
\end{aligned}$$

这就是 $\mathbb{F}_3$ 上次数为 4 的本原多项式.

Example 3.45

寻找一个 $\mathbb{F}_2$ 上次数为 6 的本原多项式.

解： $e = 2^6 - 1 = 63 = 9 \cdot 7$

首先构造两个 $\mathbb{F}_{64}^*$ 中的元素，阶分别为 9 和 7.

由于 2 模 9 的阶是 6, 所以分圆多项式 $Q_9(x) = x^6 + x^3 + 1$ 在 $\mathbb{F}_2$ 上不可约. 设 $Q_9(x)$ 的一个根为 θ, 那么其阶数为 9, 且 $\mathbb{F}_{64} = \mathbb{F}_2(\theta)$.

一个阶为 7 的元素 $\alpha \in \mathbb{F}_{64}^*$ 满足 $\alpha^8 = \alpha$, 所以 $\alpha = \sum_{i=0}^5 a_i\theta^i$, 其中 $a_i \in F_2, 0 \leq i \leq 5$, 那么：

$$\begin{aligned}\sum_{i=0}^{5} a_i\theta^i &= (\sum_{i=0}^{5} a_i\theta^i)^8 = \sum_{i=0}^{5} a_i\theta^{8i} \\ &= a_0 + a_1\theta^8 + a_2\theta^7 + a_3\theta^6 + a_4\theta^5 + a_5\theta^4 \\ &= a_0 + a_3 + a_2\theta + a_1\theta^2 + a_3\theta^3 + (a_2 + a_5)\theta^4 + (a_1 + a_4)\theta^5\end{aligned}$$

对比系数可以得到

$$\begin{aligned}a_3 &= 0 \\ a_1 &= a_2 \\ a_4 &= a_2 + a_5\end{aligned}$$

令 $a_0 = a_3 = a_4 = 0, a_1 = a_2 = a_5 = 1$, 那么 $\alpha = \theta + \theta^2 + \theta^5$ 是一个阶数为 7 的元素. 那么 $\zeta = \alpha\theta = 1 + \theta^2$ 是 $\mathbb{F}_{64}$ 的本原元.

使用前面的方法，得到 $g(x) = x^6 + x^4 + x^3 + x + 1$

这就是 $\mathbb{F}_2$ 上次数为 6 的本原多项式.

Theorem 3.46 Factorize Irreducible Polynomials on Extension Field

设 f 是 $\mathbb{F}_q$ 上次数为 n 的不可约多项式，设 $k \in \mathbb{N}$. 那么：

f 可以分解成 $\mathbb{F}_{q^k}[x]$ 上的 d 个不可约多项式，它们的次数都是 n/d, 其中 $d = gcd(k, n)$.

证明：

如果 $f(0) = 0$, 结果显然.

设 $f(0) \neq 0$. 设 g 是 f 在 $\mathbb{F}_{q^k}[x]$ 上的一个不可约因子. 若 $ord(f) = e$, 那么因为 g 的根都是 f 的根，由 **Theorem 3.3** 可知 $ord(g) = e$.

由 **Theorem 3.5** 可知 q 模 e 的阶是 n 且 g 的次数等于 q^k 模 e 的阶. 而 $q^j, j = 0, 1, \ldots$ 模 e 构成了一个阶为 n 的循环群.

因此由 **Theorem 1.15(ii)** 可知 q^k 模 e 的阶是 n/d, 即 g 的次数是 n/d.

Corollary 3.47

一个 $\mathbb{F}_q$ 上的不可约多项式在 $\mathbb{F}_{q^k}$ 上仍然不可约，当且仅当 $gcd(k, n) = 1$.

这个结论根据 **Theorem 3.46** 是显然的.

Example 3.48

考虑 **Example 3.45** 中 $\mathbb{F}_2$ 上次数为 6 的本原多项式 $g(x) = x^6 + x^4 + x^3 + x + 1$. 这个多项式在 $\mathbb{F}_{16}$ 上.

根据 **Theorem 3.46** 得到 $n = 6, k = 4$, 所以 $d = gcd(k, n) = 2$. 因此 g 在 $\mathbb{F}_{16}[x]$ 上可以分解成两个不可约三次多项式.

令 g_1 是一个因子，它有根 $\zeta = 1 + \theta^2$. g_1 的其它根是 $\mathbb{F}_{16}$ 共轭根 $\zeta^{16}, \zeta^{256} = \zeta^4$.

因为这些根在 $\mathbb{F}_4$ 上也是共轭的，所以 $g_1 \in \mathbb{F}_4[x]$. 那么有 $\beta = \zeta^{21}$ 是 $\mathbb{F}_2$ 上的三次单位根，那么 $\mathbb{F}_4 = \{0, 1, \beta, \beta^2\}$

所以

$$\begin{aligned} g_1(x) &= (x-\zeta)(x-\zeta^4)(x-\zeta^{16}) \\ &= x^3 + (\zeta+\zeta^4+\zeta^{16})x^2 + (\zeta^5+\zeta^{17}+\zeta^{20})x + \zeta^{21} \end{aligned}$$

而 $\zeta^4 = 1+\theta^2+\theta^5, \zeta^{16} = 1+\theta^5$, 所以 $\zeta+\zeta^4+\zeta^{16} = 1$. 同理 $\zeta^5+\zeta^{17}+\zeta^{20} = 1$, 所以 $g_1(x) = x^3+x^2+x+\beta$. 用它去除 $g(x)$

得到

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

这个多项式是在 $\mathbb{F}_4[x]$ 上的，所以也在 $\mathbb{F}_{16}[x]$ 上. 上面的分解结果，这两个因子是 $\mathbb{F}_4$ 上的本原多项式，但不是 $\mathbb{F}_{16}$ 上的.

根据 **Corollary 3.47** , 多项式 g 在 $\mathbb{F}_2$ 的部分域扩张上仍然不可约，例如 $\mathbb{F}_{32}$ 和 $\mathbb{F}_{128}$.

3.4 Linearized Polynomials

Definition 3.49 Q-Polynomial

多项式

$$L(x)=\sum_{i=0}^{n}\alpha_i x^{q^i}$$

它的系数在 $\mathbb{F}_q$ 的域扩张 $\mathbb{F}_{q^m}$ 上，那么这个多项式就被称为 $\mathbb{F}_{q^m}$ 上的 $q-$多项式.

这样的多项式满足下面两个性质，设 F 是 $\mathbb{F}_{q^m}$ 的任意一个域扩张，$L(x)$ 是 $\mathbb{F}_{q^m}$ 上的线性化多项式，那么

$$L(\beta+\gamma)=L(\beta)+L(\gamma) \tag{6}$$

$$L(c\beta)=cL(\beta) \tag{7}$$

这两条性质的第一条是由 Theorem 1.46 决定的，第二条是因为对于 $c\geq 0, c\in\mathbb{F}_q$ 有 $c^{q^i}=c$.

因此，如果把 F 看成 $\mathbb{F}_q$ 上的一个线性空间，那么线性化多项式 $L(x)$ 就是 F 上的一个线性算子.

Theorem 3.50

设 $L(x)$ 是 $\mathbb{F}_{q^m}$ 上的非零 $q-$多项式，$\mathbb{F}_{q^m}$ 的一个域扩张 $\mathbb{F}_{q^s}$ 包括了所有 $L(x)$ 的根.

那么每个 $L(x)$ 的根有相同的重数，重数为 1 或者 q 的幂次，同时这些根形成了 $\mathbb{F}_{q^s}$ 的一个子空间，其中 $\mathbb{F}_{q^s}$ 可以看做 $\mathbb{F}_q$ 上的线性空间.

证明： 根据式 (6)(7) 可以知道对于每个根的线性组合，如果系数在 $\mathbb{F}_q$ 上，那么这个组合仍然是一个根，那么 $L(x)$ 上的根就组成了一个 $\mathbb{F}_{q^s}$ 的子空间，如果

$$L(x)=\sum_{i=0}^{n}\alpha_i x^{q^i}$$

那么就有 $L'(x)=\alpha_0$. 因此 $L(x)$ 在 $\alpha_0\neq 0$ 的时候只有单根.

否则，就有 $\alpha_0=\alpha_1=\ldots=\alpha_{k-1}=0$, 但是 $\alpha_k\neq 0, k\geq 1$, 那么

$$L(x)=\sum_{i=k}^{n}\alpha_i x^{q^i}=\sum_{i=k}^{n}\alpha_i^{q^{mk}}x^{q^i}=(\sum_{i=k}^{n}\alpha_i^{q^{(m-1)k}})^{q^k}$$

这是一个只有单根的线性化多项式的 q^k 次方，所以每个 $L(x)$ 的根的重数都是 q^k.

Lemma 3.51

设 $\beta_1,\beta_2,\ldots,\beta_n$ 都是 $\mathbb{F}_{q^m}$ 里的元素，那么

$$\begin{vmatrix}\beta_1 & \beta_1^q & \beta_1^{q^2} & \cdots & \beta_1^{q^{n-1}}\\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \cdots & \beta_2^{q^{n-1}}\\ \vdots & \vdots & & \vdots & \\ \beta_n & \beta_n^q & \beta_n^{q^2} & \cdots & \beta_n^{q^{n-1}}\end{vmatrix}=\beta_1\prod_{j=1}^{n-1}\prod_{c_1,\ldots,c_j\in\mathbb{F}_q}(\beta_{j+1}-\sum_{k=1}^{j}c_k\beta_k) \tag{8}$$

且这个行列式值不为 0 当且仅当 $\beta_1,\beta_2,\ldots,\beta_n$ 在 $\mathbb{F}_q$ 上线性无关.

证明： 记 (8) 式左侧的行列式为 D_n. 下面通过数学归纳法证明这个式子.

当 $n=1$ 时显然成立. 考虑 $n \geq 1$ 的情况. 考虑如下的多项式

$$D(x)=\begin{vmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} & \beta_1^{q^n} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} & \beta_2^{q^n} \\ \vdots & \vdots & & \vdots & \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} & \beta_n^{q^n} \\ x & x^q & \cdots & x^{q^{n-1}} & x^{q^n} \end{vmatrix}$$

按最后一行展开得到

$$D(x)=D_n x^{q^n}+\sum_{i=0}^{n-1}\alpha_i x^{q^i}$$

其中 $\alpha_i \in \mathbb{F}_{q^m}, 0 \leq i \leq n-1$.

首先假设 $\beta_1, \beta_2, \ldots, \beta_n$ 在 $\mathbb{F}_q$ 上线性无关. 由于对于 $1 \leq k \leq n$ 都有 $D(\beta_k)=0$

又因为 $D(x)$ 是 $\mathbb{F}_{q^m}$ 上的 $q-$多项式，所以所有的线性组合 $c_1\beta_1+\ldots+c_n\beta_n, c_k \in \mathbb{F}_q, 1 \leq k \leq n$ 都是 $D(x)$ 的根.

因此 $D(x)$ 有 q^n 个不一样的根，所以可以得到下面的分解式

$$D(x)=D_n \prod_{c_1,\ldots,c_n \in \mathbb{F}_q}(x-\sum_{k=1}^{n}c_k\beta_k) \tag{9}$$

如果 $\beta_1, \beta_2, \ldots, \beta_n$ 在 $\mathbb{F}_q$ 上线性相关，那么就有 $D_n=0$ 且存在不全为零的 $b_1, \ldots, b_n \in \mathbb{F}_q$ 使得 $\sum_{k=1}^{n}b_k\beta_k=0$. 所以

$$\sum_{k=1}^{n}b_k\beta_k^{q^j}=(\sum_{k=1}^{n}b_k\beta_k)^{q^j}=0$$

对于 $j=0,1,\ldots,n$ 成立.

因此 $D(x)$ 前 n 个行向量在 $\mathbb{F}_q$ 上线性无关，因此 $D(x)=0$. 因此 (9) 式在所有情况下都成立. 因此

$$D_{n+1}=D(\beta_{n+1})=D_n \prod_{c_1,\ldots,c_n \in \mathbb{F}_q}(\beta_{n+1}-\sum_{k=1}^{n}c_k\beta_k)$$

因此根据归纳法 (8) 式成立，结论得证.

Theorem 3.52

设 U 是 $\mathbb{F}_{q^m}$ 的线性子空间，看作 $\mathbb{F}_q$ 上的线性空间. 那么对于任意非负的正整数 k, 多项式

$$L(x)=\prod_{\beta \in U}(x-\beta)^{q^k}$$

都是 $\mathbb{F}_{q^m}$ 上的 $q-$多项式.

证明： 因为 q^k 次的 $\mathbb{F}_{q^m}$ 上的 $q-$多项式仍然是 $q-$多项式，所以只需要考虑 $k=0$ 的情况.

设 $\{\beta_1, \ldots, \beta_n\}$ 是 U 在 $\mathbb{F}_q$ 上的一组基，那么 (8) 式中的 D_n 不等于 0, 所以根据式 (9) 就有

$$\begin{aligned} L(x) &= \prod_{\beta \in U}(x-\beta) \\ &= \prod_{c_1,\ldots,c_n \in \mathbb{F}_q}(x-\sum_{k=1}^{n} c_k\beta_k) \\ &= D_n^{-1}D(x) \end{aligned}$$

这样就证明了 $L(x)$ 是 $\mathbb{F}_{q^m}$ 上的 $q-$多项式.

Method 3.53 Find the Roots of Linearized Polynomials

线性化多项式的性质给出了一个求根的方法. 设

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

是 $\mathbb{F}_{q^m}$ 上的 $q-$多项式，我们现在需要去找到 $L(x)$ 在 $\mathbb{F}_{q^m}$ 的某个域扩张 F 上的所有根.

考虑映射 $L:\beta \in F \to L(\beta) \in F$, 这是一个 $\mathbb{F}_q$ 上线性空间 F 上的一个线性变换. 因此 L 可以用一个 $\mathbb{F}_q$ 上的矩阵表示.

令 $\{\beta_1,\ldots,\beta_s\}$ 是一组 F 在 $\mathbb{F}_q$ 上的基，那么每个 $\beta \in F$ 都可以写成

$$\beta = \sum_{j=1}^{s} c_j\beta_j, c_j \in \mathbb{F}_q, 1 \le j \le s$$

所以

$$L(\beta) = \sum_{j=1}^{s} c_j L(\beta_j)$$

现在令

$$L(\beta_j) = \sum_{k=1}^{s} b_{jk}\beta_k$$

其中 $b_{jk} \in \mathbb{F}_q, 1 \le j,k \le s$.

再令 B 是一个 $\mathbb{F}_q$ 上的 $s \times s$ 矩阵，元素 (j,k) 为 b_{jk}. 那么就有

$$(c_1,\ldots,c_s)B = (d_1,\ldots,d_s)$$

那么就有

$$L(\beta) = \sum_{k=1}^{s} d_k\beta_k$$

那么 $L(\beta)=0$ 等价于

$$(c_1,\ldots c_s)B = (0,\ldots,0) \tag{10}$$

这是一个关于 $c_1,\ldots,c_s$ 的齐次线性方程组. 设矩阵 B 的秩为 r, 那么 (10) 式有 q^{s-r} 个解.

每个解都产生了一个 $L(x)$ 在 F 上的根 $\beta = \sum_{j=1}^{s} c_j\beta_j$

因此寻找多项式在域上的根的问题就被转化成了求解齐次线性方程组的问题.

Example 3.53

考虑线性化多项式 $L(x)=x^9-x^3-\alpha x\in\mathbb{F}_9[x]$, 其中 α 是 $\mathbb{F}_3$ 上的本原多项式 x^2+x-1 的根.

下面要找多项式 $L(x)$ 在 $\mathbb{F}_{81}$ 上的根，首先找到一组 $\mathbb{F}_{81}$ 在 $\mathbb{F}_3$ 上的基 $\{1,\zeta,\zeta^2,\zeta^3\}$, 其中 ζ 是 $\mathbb{F}_3$ 上本原多项式 $x^4+x^3+x^2-x-1$ 的根.

考虑阶数，$\alpha^{3^2-1}=1=\zeta^{3^4-1}$, 那么就有 $\alpha=\zeta^{10j}, j=1,3,5,7$. (j 的取值需要互素)

又因为 $\zeta^{20}+\zeta^{10}-1=0$, 所以可以取 $\alpha=\zeta^{10}=-1+\zeta+\zeta^2-\zeta^3$. 下面计算

$$
\begin{aligned}
L(1)&=-\alpha=1-\zeta-\zeta^2+\zeta^3\\
L(\zeta)&=\zeta^9-\zeta^3-a\zeta=-\zeta-\zeta^2-\zeta^3\\
L(\zeta^2)&=-1+\zeta^3\\
L(\zeta^3)&=1-\zeta^3
\end{aligned}
$$

那么得到矩阵

$$
B=\begin{pmatrix}
1 & -1 & -1 & 1\\
0 & -1 & -1 & -1\\
-1 & 0 & 0 & 1\\
1 & 0 & 0 & -1
\end{pmatrix}
$$

式 (10) 有两个线性无关的解，分别是 $(0,0,1,1)$ 和 $(-1,1,0,1)$. 所以所有的解都可以用这两个解的线性组合表示.

所以根有 $\theta_1=0,\theta_2=\zeta^2+\zeta^3,\theta_3=-\zeta^2-\zeta^3,\theta^4=-1+\zeta+\zeta^3$

$\theta_5=1-\zeta-\zeta^3,\theta_6=-1+\zeta+\zeta^2-\zeta^3,\theta_7=1-\zeta-\zeta^2+\zeta^3,\theta_8=1-\zeta+\zeta^2,\theta_9=-1+\zeta-\zeta^2$

这种找根的方法可以被用于一类更普通的多项式——仿射多项式

Definition 3.54 Affine Q-polynomial

形如 $A(x)=L(x)-\alpha$ 的多项式被称为仿射 $q-$多项式，其中 $L(x)$ 是 $\mathbb{F}_{q^m}$ 上的 $q-$多项式，$\alpha\in\mathbb{F}_{q^m}$.

元素 $\beta\in F$ 是 $A(x)$ 的根，当且仅当 $L(\beta)=\alpha$. 类似 (10) 式，可以得到

$$
(c_1,\dots,c_s)B=(d_1,\dots,d_s)\tag{11}
$$

其中 $\alpha=\sum_{k=1}^s d_k\beta_k$.

这是一个关于 $c_1,\dots,c_s$ 的齐次线性方程组，每个解向量都可以贡献一个 $A(x)$ 的解 $\beta=\sum_{j=1}^s c_j\beta_j$

Method 3.54 Find Roots of Positive Degree Polynomial on Extension Field

下面介绍一个寻找 $\mathbb{F}_{q^m}$ 上的任意正次数多项式 $f(x)$ 在 $\mathbb{F}_{q^m}$ 的域扩张 F 上的根的方法.

首先，找到一个 $\mathbb{F}_{q^m}$ 上可以被整除 $f(x)$ 的非零的仿射多项式 $A(x)$.

第二步用上面的求仿射多项式的根的方法（式 (11)）来求 $A(x)$ 的根. 因为 $f(x)$ 在 F 上的根一定在 $A(x)$ 在 F 上的根里面，所以只需要对于每个 $A(x)$ 在 F 上的根 β 计算 $f(\beta)$ 的值，来确定这个根到底是不是 $f(x)$ 的根.

那么问题变成了如何寻找这样的仿射多项式 $A(x)$. 步骤如下

设 $f(x)$ 的次数 $n \geq 1$. 对于所有 $i = 0, 1, \ldots, n-1$, 计算余式 $r_i(x)$, 其中 $x^{q^i} \equiv r_i(x) \mod f(x)$.

接着去确定不全为零的元素 $\alpha_i \in \mathbb{F}_{q^m}$. 使得 $\sum_{i=0}^{n-1} \alpha_i r_i(x)$ 是一个常数多项式，这包括了 $n-1$ 个消去 x^j 系数的条件, $1 \leq j \leq n-1$.

因此这形成了一个有 $n-1$ 个线性方程，n 个未知变量($\alpha_0, \ldots, \alpha_{n-1}$) 的一个齐次方程系统，这样的系统存在非平凡解. 每当一个非平凡解被确定的时候，就可以得到 $\sum_{i=0}^{n-1} \alpha_i r_i(x) = \alpha$, 其中 $\alpha \in \mathbb{F}_{q^m}$. 那么就有

$$\sum_{i=0}^{n-1} \alpha_i x^{q^i} \equiv \sum_{i=0}^{n-1} \alpha_i r_i(x) \equiv \alpha \mod f(x)$$

因此

$$A(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} - \alpha$$

是一个 $\mathbb{F}_{q^m}$ 上可以被整除 $f(x)$ 的非零的仿射多项式.

Example 3.55

设多项式 $f(x) = x^4 + \theta^2 x^3 + \theta x^2 + x + \theta \in \mathbb{F}_4[x]$, 其中 θ 是多项式 $x^2 + x + 1 \in \mathbb{F}_2[x]$ 的一个解.

试寻找 $f(x)$ 在 $\mathbb{F}_{64}$ 上的根.

解：尝试使用 **Method 3.54** 的方法，首先找到一个可以被 $f(x)$ 的整除的仿射多项式 $f(x)$. 显然在本例中 $q = 2$.

进行对 $f(x)$ 的模运算，得到 $x \equiv x = r_0(x)$, $x^2 \equiv x^2 = r_1(x)$, $x^4 \equiv \theta^2 x^3 + \theta x^2 + x + \theta = r_2(x)$, $x^8 \equiv \theta^3 + \theta^2 + x + \theta = r_3(x)$.

$\alpha_0 r_0(x) + \ldots + \alpha_3 r_3(x)$ 应该是常数多项式，对比系数可以得到

$$\begin{gathered}
\alpha_0 + \alpha_2 + \alpha_3 = 0 \\
\alpha_1 + \theta\alpha_2 + \theta\alpha_3 = 0 \\
\theta^2\alpha_2 + \theta\alpha_3 = 0
\end{gathered}$$

令 $\alpha_3 = 1$, 解得 $\alpha_2 = \theta^2, \alpha_1 = \theta^2, \alpha_0 = \theta$. 因此

$$\alpha = \alpha_0 r_0(x) + \ldots + \alpha_3 r_3(x) = \theta^2$$

所以

$$\begin{aligned}
A(x) &= \alpha_3 x^8 + \alpha_2 x^4 + \alpha_1 x^2 + \alpha_0 x - \alpha \\
&= x^8 + \theta^2 x^4 + \theta^2 x^2 + \theta x + \theta^2
\end{aligned}$$

下面开始求根. 设 ζ 是本原多项式 $x^6 + x + 1$ 在 $\mathbb{F}_2$ 上的根，那么 $\{1, \zeta, \zeta^2, \ldots, \zeta^5\}$ 就是一组 $\mathbb{F}_{64}$ 在 $\mathbb{F}_2$ 上的基. 因为 θ 是 $\mathbb{F}_2$ 的三次本原单位根，取 $\theta = \zeta^{21} = 1 + \zeta + \zeta^3 + \zeta^4 + \zeta^5$. 通过 $\theta^2 = \theta + 1 = \zeta + \zeta^3 + \zeta^4 + \zeta^5$, 可以得到

$$\begin{array}{lcccccccccc}
L(1) & = & \zeta & & & + & \zeta^3 & + & \zeta^4 & + & \zeta^5 \\
L(\zeta) & = & \zeta & + & \zeta^2 & & & & & + & \zeta^5 \\
L(\zeta^2) & = & & & \zeta^2 & + & \zeta^3 & + & \zeta^4 & + & \zeta^5 \\
L(\zeta^3) & = & \zeta & & & + & \zeta^3 & + & \zeta^4 & & \\
L(\zeta^4) & = & & & & & & & & + & \zeta^5 \\
L(\zeta^5) & = & & & \zeta^2 & + & \zeta^3 & + & \zeta^4 & &
\end{array}$$

对应的矩阵是

$$B=\begin{pmatrix}0&1&0&1&1&1\\0&1&1&0&0&1\\0&0&1&1&1&1\\0&1&0&1&1&0\\0&0&0&0&0&1\\0&0&1&1&1&0\end{pmatrix}$$

同时

$$(d_1,\ldots,d_s)=(0,1,0,1,1,1)$$

求解式 (11) 得到通解向量

$$(1,0,0,0,0,0)+a_1(0,1,1,1,0,0)+a_2(1,1,1,0,1,0)+a_3(1,1,0,0,0,1)$$

其中 $a_1,a_2,a_3\in\mathbb{F}_2$

全部代入得到八个解 $\eta_1,\ldots,\eta_8$. 依次计算 $f(\eta_i)$ 进行验证，得到有四个根，分别是

$$x_1=\zeta+\zeta^2+\zeta^4, x_2=1+\zeta+\zeta^2+\zeta^3, x_3=\zeta^3+\zeta^4, x_4=1+\zeta+\zeta^3+\zeta^4+\zeta^5$$

仿射空间: 没有起点只有方向与大小的向量所构成的线性空间。

Theorem 3.56

设 $A(x)$ 是一个 $\mathbb{F}_{q^m}$ 上的正次数仿射 $q-$多项式，$\mathbb{F}_{q^s}$ 是 $\mathbb{F}_{q^m}$ 的域扩张，包括了所有 $A(x)$ 的根.

那么每个 $A(x)$ 的根有相同的重数，是 1 或是 q 的幂次，所有的根形成 $\mathbb{F}_{q^s}$ 的仿射空间（线性空间），其中 $\mathbb{F}_{q^s}$ 可以看成 $\mathbb{F}_q$ 上的线性空间.

证明： 关于根的重数问题和 **Theorem 3.50** 中证法相同.

现在令 $A(x)=L(x)-\alpha$, 其中 $L(x)$ 是 $\mathbb{F}_{q^m}$ 上的 $q-$多项式，设 β 是 $A(x)$ 的一个根.

那么 $\gamma\in\mathbb{F}_q$ 是 $A(x)$ 的一个根，当且仅当 $L(\gamma)=\alpha=L(\beta)$, 当且仅当 $L(\gamma-\beta)=0$, 当且仅当 $\gamma\in\beta+U$ 的时候成立.

其中 U 是 $\mathbb{F}_{q^s}$ 的一个线性子空间，包括了所有 $L(x)$ 的根. 因此所有 $A(x)$ 的根形成了 $\mathbb{F}_{q^s}$ 的仿射空间.

Theorem 3.57

设 T 是 $\mathbb{F}_{q^m}$ 上的仿射子空间，那么对于所有非负整数 k, 多项式

$$A(x)=\prod_{\gamma\in T}(x-\gamma)^{q^k}$$

是 $\mathbb{F}_{q^m}$ 上的仿射 $q-$多项式.

证明： 令 $T=\eta+U$, 其中 U 是 $\mathbb{F}_{q^m}$ 的线性子空间，那么根据 **Theorem 3.52**

$$L(x)=\prod_{\beta\in U}(x-\beta)^{q^k}$$

是 $\mathbb{F}_{q^m}$ 上的 $q-$多项式. 因此

$$A(x)=\prod_{\gamma\in T}(x-\gamma)^{q^k}=\prod_{\beta\in U}(x-\eta-\beta)^{q^k}=L(x-\eta)$$

显然是一个 $\mathbb{F}_{q^m}$ 上的仿射 $q-$多项式.

定义符号乘法 $\otimes$ 来表示运算的复合

$$L_1(x)\otimes L_2(x)=L_1(L_2(x))$$

显然复合得到的多项式也是 $q-$多项式.

这个符号满足交换律、结合律、分配律.

$\mathbb{F}_q$ 上所有的 $q-$多项式**对于符号乘法和常规加法构成一个整环**.

Definition 3.58 Q-Associate

$\mathbb{F}_{q^m}$ 上的多项式

$$l(x)=\sum_{i=0}^{n}\alpha_i x^i$$

和

$$L(x)=\sum_{i=0}^{n}\alpha_i x^{q^i}$$

那么称这两个多项式 $q-$相伴.

具体的，$l(x)$ 是 $L(x)$ 的传统 $q-$相伴，$L(x)$ 是 $l(x)$ 的线性 $q-$相伴.

Lemma 3.59

设 $L_1(x)$ 和 $L_2(x)$ 是 $\mathbb{F}_q$ 上的 $q-$多项式，$l_1(x)$ 和 $l_2(x)$ 是他们的传统 $q-$相伴，那么 $l(x)=l_1(x)l_2(x)$ 和 $L(x)=L_1(x)L_2(x)$ 互为 $q-$相伴.

证明：

$$l(x)=\sum_i a_i x^i=\sum_j b_j x^j\sum_k c_k x^k=l_1(x)l_2(x)$$

$$L(x)=\sum_i a_i x^{q^i}=\sum_j b_j(\sum_k c_k x^{q^k})^{q^j}=\sum_j b_j\sum_k c_k x^{q^{j+k}}=L_1(x)\otimes L_2(x)$$

这两个式子成立当且仅当

$$a_i=\sum_{j+k=i}b_j c_k$$

对每一个 i 都成立.

Corollary 3.60

设 $L_1(x)$ 和 $L(x)$ 是 $\mathbb{F}_q$ 上的 $q-$多项式，$l_1(x)$ 和 $l(x)$ 是他们的传统 $q-$相伴.

那么 $L_1(x)$ 符号整除 $L(x)$ 当且仅当 $l_1(x)$ 整除 $l(x)$.

Example 3.61

设 $L(x)$ 是 $\mathbb{F}_q$ 上的 $q-$多项式, 存在整数 $m \in \mathbb{N}$ 使得这个多项式符号整除 $x^{q^m} - x$.

那么存在一个 $\mathbb{F}_q$ 上的 $q-$多项式 $L_1(x)$ 使得

$$x^{q^m} - x = L(x) \otimes L_1(x) = L_1(x) \otimes L(x) = L_1(L(x)) \tag{12}$$

设 α 是 $\mathbb{F}_{q^m}$ 里的元素，仿射多项式 $L(x) - \alpha$ 在 $\mathbb{F}_{q^m}$ 上至少有一个根的充要条件是 $L_1(\alpha) = 0$.

如果 $L_1(\alpha) = 0$, 那么所有 $L(x) - \alpha$ 的根都在 $\mathbb{F}_{q^m}$ 上. 设其中一个根为 β. 即 $L(\beta) = \alpha$.

那么就有 $L_1(\alpha) = \beta^{q^m} - \beta = 0$. 反过来，设 $L_1(\alpha) = 0$, 设 γ 是 $L(x) - \alpha$ 在 $\mathbb{F}_{q^m}$ 的某扩域上的根，那么 $L(\gamma) = \alpha$.

那么 $\gamma^{q^m} - \gamma = L_1(\alpha) = 0$, 所以 $\gamma \in \mathbb{F}_{q^m}$.

多项式 $L_1(x)$ 可以通过如下方法计算: 设 $l(x)$ 是 $L(x)$ 的传统 $q-$相伴，$l_1(x) = (x^m - 1)/l(x)$, 然后令 $L_1(x)$ 是 $l_1(x)$ 的线性 $q-$相伴. 可以发现，如果令 $L(x) = x^q - x$, 这就是 **Theorem 2.25** 的一个特殊形式.

Theorem 3.62

设 $L_1(x)$ 和 $L(x)$ 是 $\mathbb{F}_q$ 上的 $q-$多项式，$l_1(x)$ 和 $l(x)$ 是他们的传统 $q-$相伴. 那么下面三个条件等价：

(i) $L_1(x)$ 符号整除 $L(x)$

(ii) $L_1(x)$ 常规除法下整除 $L(x)$

(iii) $l_1(x)$ 整除 $l(x)$

证明： 根据 **Theorem 3.60** 可知 (i) 和 (iii) 等价，所以只需要证明 (i) 和 (ii) 等价.

设 $L_1(x)$ 符号整除 $L(x)$, 那么就存在 $\mathbb{F}_q$ 上的 $q-$多项式 $L_2(x)$ 使得

$$L(x) = L_1(x) \otimes L_2(x) = L_2(x) \otimes L_1(x) = L_2(L_1(x))$$

设

$$L_2(x) = \sum_{i=0}^{n} a_i x^{q^i}$$

那么就有

$$L(x) = a_0 L_1(x) + a_1 L_1(x)^q + \ldots + a_n L_1(x)^{q^n}$$

显然在常规除法下 $L_1(x)$ 整除 $L(x)$.

反过来，假设在常规除法下 $L_1(x)$ 整除 $L(x)$.

那么 $L_1(x)$ 非零，由带余除法则有 $l(x) = k(x) l_1(x) + r(x)$, 其中 $deg(r(x)) < deg(l_1(x))$.

考虑线性化 $q-$多项式就有 $L(x)=K(x)\otimes L_1(x)+R(x)$.

前面已经证明了 $L_1(x)$ 在常规除法下整除 $K(x)\otimes L_1(x)$, 因此就有 $L_1(x)$ 在常规除法下整除 $R(x)$.

但是由于 $R(x)$ 的次数比 $L_1(x)$ 低，所以只能有 $R(x)=0$. 因此就证明了 $L_1(x)$ 符号整除 $L(x)$.

Theorem 3.63

设 $f(x)$ 在 $\mathbb{F}_q[x]$ 上不可约，设其线性化 $q-$相伴为 $F(x)$. 那么 $F(x)/x$ 的每个不可约因子的次数在 $\mathbb{F}_q[x]$ 上都等于 $ord(f(x))$.

证明： 如果 $f(0)=0$ 情况显然，考虑 $f(0)\neq 0$. 设 $e=ord(f(x))$, 令 $h(x)\in\mathbb{F}_q[x]$ 是 $F(x)/x$ 的一个次数为 d 的不可约因子.

那么 $f(x)\mid x^e-1$. 根据 **Theorem 3.62** 可以得到 $F(x)\mid x^{q^e}-x$. 所以有 $h(x)\mid x^{q^e}-x$. 故根据 **Theorem 3.20** 有 $d\mid e$.

由带余除法，$x^d-1=g(x)f(x)+r(x), g(x), r(x)\in\mathbb{F}_q[x], deg(r(x))<deg(f(x))$. 所以

$$x^{q^d}-x=G(x)\otimes F(x)+R(x)$$

因为 $h(x)\mid x^{q^d}-x$ 且 $h(x)\mid G(x)\otimes F(x)$. 所以就有 $h(x)\mid R(x)$.

如果 $r(x)$ 不是零多项式，那么 $r(x)$ 和 $f(x)$ 互素，所以就存在多项式 $s(x),k(x)\in\mathbb{F}_q[x]$ 使得

$$s(x)r(x)+k(x)f(x)=\gcd(r(x),f(x))=1$$

所以

$$S(x)\otimes R(x)+K(x)\otimes F(x)=x$$

因为 $h(x)\mid R(x), h(x)\mid F(x)$, 所以 $h(x)\mid x$. 这是不可能的. 所以 $r(x)$ 是零多项式，因此就有 $f(x)\mid x^d-1$.

所以根据 **Lemma 3.6** 可知 $e\mid d$.

综上有 $d=e$.

类似的，可以对符号乘法定义符号不可约、符号分解、最大符号公因子等概念.

两个多项式的最大公因子和最大符号公因子是相同的.

根据 Theorem 3.50 可以知道 $\mathbb{F}_q$ 上非零 $q-$多项式的根形成一个 $\mathbb{F}_q$ 上的线性空间. 这些根有着一个性质：他们的 q 次幂也是根.

因此定义集合 $q-$模 (***q-modulus***) 来包括这样的性质.

设 M 是 $\mathbb{F}_q$ 上的有限维线性空间，包含于 $\mathbb{F}_q$ 的某个域扩张里，M 中所有元素的 q 次幂仍然在 M 内，那称集合 M 为 $q-$模.

$$M=\{\beta^q,\beta\in M\}$$

Example 3.64

考虑 $\mathbb{F}_2$ 上的 $2-$多项式 $L(x)=x^{16}+x^8+x^2+x$. 它的传统 $2-$相伴 $l(x)=x^4+x^3+x+1$ 在 $\mathbb{F}_2[x]$ 上有标准分解

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

所以

$$L(x)=(x^4+x^2+x)\otimes(x^2+x)\otimes(x^2+x)$$

是 $L(x)$ 的符号分解，分解为 $\mathbb{F}_2$ 上的符号不可约多项式的乘积.

Theorem 3.65

首一多项式 $L(x)$ 是 $\mathbb{F}_q$ 上的 $q-$多项式，当且仅当 $L(x)$ 的每个根有相同的重数，重数为 1 或 q 的幂次，这些根形成了 $q-$模.

证明：必要性根据 **Theorem 3.50** 显然. 反过来，根据 **Theorem 3.52** 和题设条件说明 $L(x)$ 是 $\mathbb{F}_q$ 的某个扩域上的 $q-$多项式，设 M 是 $q-$模，包括了所有 $L(x)$ 的根，那么存在非负整数 k 使得

$$L(x)=\prod_{\beta\in M}(x-\beta)^{q^k}$$

由于 $M=\{\beta^q:\beta\in M\}$, 所以

$$L(x)^q=\prod_{\beta\in M}(x^q-\beta^q)^{q^k}=\prod_{\beta\in M}(x^q-\beta)^{q^k}=L(x^q)$$

如果

$$L(x)=\sum_{i=0}^{n}\alpha_i x^{q^i}$$

就有

$$\sum_{i=0}^{n}\alpha_i^q x^{q^{i+1}}=L(x)^q=L(x^q)=\sum_{i=0}^{n}\alpha_i x^{q^{i+1}}$$

所以对于任意 $0\le i\le n$ 都有 $\alpha_i^q=\alpha_i$. 因此 $\alpha_i\in\mathbb{F}_q$.

因此 $L(x)$ 是 $\mathbb{F}_q$ 上的 $q-$多项式.

任意 $\mathbb{F}_q$ 上次数为 q 的 $q-$多项式都在 $\mathbb{F}_q$ 上符号不可约.

对于次数大于 q 的 $q-$多项式，可以用 $q-$模去描述符号不可约多项式的特征.

Theorem 3.66

$\mathbb{F}_q$ 上次数大于 q 的 $q-$多项式 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约，当且仅当 $L(x)$ 有单根，且包括所有 $L(x)$ 的根的 $q-$模集合 M 中没有 它本身和 $\{0\}$ 以外的 $q-$模.

证明：

(1) 必要性

首先设 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约. 如果 $L(x)$ 有重根，那么根据 **Theorem 3.65** 可知有 $L(x)=L_1(x)^q$, 其中 $L_1(x)$ 是 $\mathbb{F}_q$ 上的一个次数大于 1 的 $q-$多项式. 但这样就有 $L(x)=x^q\otimes L_1(x)$, 这和 $L(x)$ 符号不可约矛盾，因此 $L(x)$ 只有单根.

下一步，如果 N 是一个包含于 M 的 $q-$模，那么根据 **Theorem 3.65** 可以知道 $L_2(x)=\prod_{\beta\in N}(x-\beta)$ 是 $\mathbb{F}_q$ 上的 $q-$多项式. 由于在常规除法下 $L_2(x)\mid L(x)$, 所以根据 **Theorem 3.62** $L_2(x)$ 符号整除 $L(x)$. 但是 $L(x)$ 在 $\mathbb{F}_q$ 上是符号不可约的，所以 $deg(L_2(x))=1$ 或者 $deg(L_2(x))=deg(L(x))$. 那么 N 就是 $\{0\}$ 或者 M.

(2) 充分性

设 $L(x)=L_1(x)\otimes L_2(x)$ 是 $L(x)$ 在 $\mathbb{F}_q$ 上的符号分解，其中 $L_1(x),L_2(x)$ 都是 $q-$多项式.

那么 $L_1(x)$ 符号整除 $L(x)$, 那么根据 **Theorem 3.62** 就有 $L_1(x)\mid L(x)$ 在一般除法下成立. 那么 $L_1(x)$ 有单根，且包含所有 $L_1(x)$ 的根的 $q-$模 N 被 M 包含. 因此 N 就是 $\{0\}$ 或者 M, 所以 $deg(L_1(x))=1$ 或者 $deg(L_1(x))=deg(L(x))$. 因此 $L_1(x)$ 和 $L_2(x)$ 必有一个次数为 1, 因此 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约.

Definition 3.67 Q-Primitive Root

设 $L(x)$ 是 $\mathbb{F}_{q^m}$ 上的非零 $q-$多项式. ζ 是 $L(x)$ 在 $\mathbb{F}_{q^m}$ 上的根.

如果 ζ 不是 $\mathbb{F}_{q^m}$ 上任意的更低次数非零 $q-$多项式的根，那么 ζ 称为 $L(x)$ 的 $\mathbb{F}_{q^m}$ 上的 $q-$本原根.

可以这样理解这个概念。假设 $g(x)$ 是 ζ 在 $\mathbb{F}_{q^m}$ 上的极小多项式，那么 ζ 是 $L(x)$ 的 $\mathbb{F}_{q^m}$ 上的 $q-$本原根，当且仅当 $g(x)\mid L(x)$ 且 $g(x)$ 不整除 $\mathbb{F}_{q^m}$ 上任意的更低次数非零 $q-$多项式.

给定一个 $\mathbb{F}_{q^m}$ 的某个域扩张上的元素 ζ， 总能够找到一个 $\mathbb{F}_{q^m}$ 上的非零 $q-$多项式使得 ζ 是它的 $\mathbb{F}_{q^m}$ 上的 $q-$本原根.

设 $g(x)$ 是 $\mathbb{F}_{q^m}$ 上 ζ 的极小多项式，次数为 n. 容易验证 $\mathbb{F}_{q^m}$ 上可以整除 $g(x)$ 的最低次首一 $q-$多项式 $L(x)$ 是可以被唯一确定的，这个多项式被称为 $\mathbb{F}_{q^m}$ 上的**极小 $q-$多项式**.

Theorem 3.68

设 ζ 是 $\mathbb{F}_{q^m}$ 的某个域扩张上的元素，$M(x)$ 是其 $\mathbb{F}_{q^m}$ 上的极小 $q-$多项式.

那么 $\mathbb{F}_{q^m}$ 上的 $q-$多项式 $K(x)$ 有根 ζ 当且仅当存在 $\mathbb{F}_{q^m}$ 上的 $q-$多项式 $L(x)$ 使得 $K(x)=L(x)\otimes M(x)$.

特殊的，若 $m=1$, 说明 $K(x)$ 有根 ζ 当且仅当 $K(x)$ 符号整除 $M(x)$.

证明： 设 $K(x)=L(x)\otimes M(x)=L(M(x))$. 那么就有 $K(\zeta)=0$.

反过来，令

$$M(x)=\sum_{j=0}^{t}\gamma_j x^{q_j},\gamma_t=1$$

设

$$K(x)=\sum_{h=0}^{r}\alpha_h x^{q^h},r\geq t$$

有 ζ 为一个根. 令 $s=r-t$ 且当 $j<0$ 的时候有 $\gamma_j=0$. 考虑下面的 $s+1$ 个线性方程，其中 $\beta_0,\ldots,\beta_s$ 是未知量：

$$\begin{gathered}\beta_0+\gamma_{t-1}^{q}\beta_1+\gamma_{t-2}^{q^2}\beta_2+\ldots+\gamma_{t-s}^{q^s}\beta_s=\alpha_t\\ \beta_1+\gamma_{t-1}^{q^2}\beta_2+\ldots+\gamma_{t-s+1}^{q^s}\beta_s=\alpha_{t+1}\\ \cdots\\ \beta_{s-1}+\gamma_{t-1}^{q^s}\beta_s=\alpha_{r-1}\\ \beta_s=\alpha_r\end{gathered}$$

显然这个方程组有唯一解，若

$$L(x)=\sum_{i=0}^{s}\beta_i x^{q^i},R(x)=K(x)-L(M(x))$$

就有

$$\begin{aligned}R(x)&=\sum_{h=0}^{r}\alpha_h x^{q^h}-\sum_{i=0}^{s}\beta_i(\sum_{j=0}^{t}\gamma_j x^{q^j})^{q^i}\\&=\sum_{h=0}^{r}\alpha_h x^{q^h}-\sum_{i=0}^{s}\beta_i\sum_{j=0}^{t}\gamma_j^{q^i}x^{q^{i+j}}\\&=\sum_{h=0}^{r}\alpha_h x^{q^h}-\sum_{h=0}^{r}(\sum_{i=0}^{s}\gamma_{h-i}^{q^i}\beta_i)x^{q^h}\\&=\sum_{h=0}^{s}(\alpha_h-\sum_{i=0}^{s}\gamma_{h-i}^{q^i}\beta_i)x^{q^h}\end{aligned}$$

所以 $R(x)$ 的次数小于 q^t. 但是因为 $R(\zeta)=K(\zeta)-L(M(\zeta))=0$, 根据 $M(x)$ 的定义可以知道 $R(x)$ 只能是零多项式.

因此就有 $K(x)=L(M(x))=L(x)\otimes M(x)$.

Lemma 3.69 Euler's Function

定义欧拉函数 $\phi_q(f)$ 表示 $\mathbb{F}_q[x]$ 中比 f 次数低，且和 f 互素的多项式的个数. 那么这个函数有下面的几条性质：

(i) 如果 $deg(f)=0$, 那么 $\phi_q(f)=1$

(ii) 如果 f 和 g 互素，那么 $\phi_q(fg)=\phi_q(f)\phi_q(g)$.

(iii) 如果 $deg(f)=n\geq 1$, 那么

$$\phi_q(f)=q^n(1-q^{-n_1})\ldots(1-q^{-n_r})$$

其中 n_i 表示 f 在 $\mathbb{F}_q[x]$ 上标准分解为若干首一不可约多项式后，每个不同的不可约多项式的次数.

证明： (i) 显然

(ii) 设 $\phi_q(f)=s,\phi_q(g)=t$. 和 f,g 互素的多项式分别记为 $f_1,\ldots,f_s$ 与 $g_1,\ldots,g_t$.

设多项式 $h\in\mathbb{F}_q[x]$ 满足 $deg(h)<deg(fg)$ 且 $\gcd(fg,h)=1$. 那么 $\gcd(f,h)=\gcd(g,h)=1$.

那么存在有序对 (i,j) 使得 $h\equiv f_i \mod f, h\equiv g_j \mod g$ 成立，其中 $1\leq i\leq s,1\leq j\leq t$.

反过来，给定有序对 (i,j), 根据中国剩余定理一定存在一个多项式 $h \in \mathbb{F}_q[x]$ 满足 $h \equiv f_i \mod f, h \equiv g_j \mod g$, 且 $\deg(h) < \deg(fg)$. 这个 h 满足 $\gcd(f,h) = \gcd(g,h) = 1$. 那么就有 $\gcd(fg,h) = 1$.

因此这 st 个有序对 (i,j) 和满足 $\deg(h) < \deg(fg)$ 与 $\gcd(fg,h) = 1$ 的多项式 $h \in \mathbb{F}_q[x]$ 一一对应.

因此 $\phi_q(fg) = st = \phi_q(f)\phi_q(g)$. ϕ_q 也是积性函数.

(iii) 只需要考虑 $\phi_q(b^e)$ 的值，其中 b 是 $\mathbb{F}_q[x]$ 上的不可约多项式，次数为 m，e 是正整数.

对于 $h \in \mathbb{F}_q[x]$，若 $\deg(h) < \deg(b^e) = em$，和 b^e 互素的多项式即可以被 b 整除的多项式，记作 $h = gb, \deg(g) < em - m$.

显然这样的 g 的个数为 q^{em-m}. 所以 $\phi_q(b^e) = q^{em} - q^{em-m} = q^{em}(1 - q^{-m})$. 根据积性函数的性质 (iii) 成立.

Theorem 3.70 Number of Q-Primitive Roots

设 $L(x)$ 是 $\mathbb{F}_q$ 上的非零 $q-$多项式，$l(x)$ 是它的传统 $q-$相伴. 设 N_L 表示 $L(x)$ 在 $\mathbb{F}_q$ 上的 $q-$本原根的个数，当 $L(x)$ 有重根的时候，$N_L = 0$; 当 $L(x)$ 的根都是单根时，$N_L = \phi_q(l(x))$.

Corollary 3.71

每个 $\mathbb{F}_q$ 上的非零 $q-$多项式，如果只有单根，那么它在 $\mathbb{F}_q$ 上至少有一个 $q-$本原根.

Theorem 3.72

设 M 是 $\mathbb{F}_q$ 上的 $q-$模，维数 $m \geq 1$. 那么存在一个元素 $\zeta \in M$ 使得 $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ 是一组 M 在 $\mathbb{F}_q$ 上的基.

证明： 根据 **Theorem 3.65** 可以知道 $L(x) = \prod_{\beta \in M}(x - \beta)$ 是 $\mathbb{F}_q$ 上的 $q-$多项式，根据 **Corollary 3.71** 可以知道 $L(x)$ 必然有一个 $\mathbb{F}_q$ 上的 $q-$本原根 ζ. 因此 $\zeta, \zeta^q, \ldots, \zeta^{q^{m-1}}$ 都是 M 中的元素. 如果这些元素在 $\mathbb{F}_q$ 上线性相关，那么 ζ 就是一个 $\mathbb{F}_q$ 上次数小于 $q^m = \deg(L(x))$ 的非零 $q-$多项式的根，这和 $L(x)$ 的定义矛盾. 所以这些元素在 $\mathbb{F}_q$ 上线性无关，所以 $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ 是一组 M 在 $\mathbb{F}_q$ 上的基.

Theorem 3.73

在 $\mathbb{F}_{q^m}$ 中，恰有 $\phi_q(x^m - 1)$ 个元素 ζ, 使得 $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ 是一组 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的基.

证明： 首先根据 **Lemma 2.4** 有

$$L(x) = \prod_{\beta \in \mathbb{F}_{q^m}} (x - \beta) = x^{q^m} - x$$

且每个 $L(x)$ 在 $\mathbb{F}_q$ 上的 $q-$本原根都可以产生一组题设的基.

从另一方面来说，如果 $\zeta \in \mathbb{F}_{q^m}$ 不是 $L(x)$ 在 $\mathbb{F}_q$ 上的 $q-$本原根，也就是说 $\zeta, \zeta^q, \ldots, \zeta^{q^{m-1}}$ 在 $\mathbb{F}_q$ 上是线性相关的，也就是说这些元素不构成一组 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的基.

从而满足条件的 $\zeta \in \mathbb{F}_{q^m}$ 的个数也就是 $L(x)$ 在 $\mathbb{F}_q$ 上的 $q-$本原根的个数，根据 **Theorem 3.70** 可以知道个数为 $\phi_q(x^m - 1)$ 个.

由于 $\zeta, \zeta^q, \ldots, \zeta^{q^{m-1}}$ 里的每个元素生成的 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的正规基都是相同的，所以 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的不同正规基的组数为

$$\frac{\phi_q(x^m-1)}{m}$$

Example 3.74

试计算 $\mathbb{F}_{64}$ 在 $\mathbb{F}_2$ 上的不同的正规基的数量.

解： 由上面的公式，正规基的数量为

$$\frac{\phi_2(x^6-1)}{6}$$

而

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

所以根据 **Lemma 3.69(iii)** 有

$$\phi_2(x^6-1)=2^6(1-\frac{1}{2})(1-\frac{1}{4})=24$$

所以不同的正规基数量为 4 个.

3.5 Binomials and Trinomials

二项式**(Binomials)** 是一个只有两个非零项组成的多项式，其中一个为常数项. 不可约二项式可以被专门讨论，对此，我们需要讨论非线性的首一二项式.

Theorem 3.75 Binomials' Irreducibility

设 $t \geq 2$ 是一个整数，$a \in \mathbb{F}_q^*$. 那么二项式 $x^t - a$ 在 $\mathbb{F}_q[x]$ 上不可约，当且仅当下面两个条件成立：

(i) 每个 t 的素因子整除 a 在 $\mathbb{F}_q^*$ 中的阶 e, 但不整除 $(q-1)/e$.

(ii) 如果 $4 \mid t$, 那么 $q \equiv 1 \mod 4$.

证明： 设这两个条件都满足.

那么 $f(x) = x - a$ 是一个 $\mathbb{F}_q[x]$ 上阶为 e 的不可约多项式，那么根据 **Theorem 3.35** 可知 $f(x^t) = x^t - a$ 也是不可约多项式.

设 (i) 不满足，那么就存在一个 t 的素因子 r 使得其整除 $(q-1)/e$ 或不整除 e. 考虑第一种情况, 设 $rs = (q-1)/e, s \in \mathbb{N}$.

那么 $\mathbb{F}_q^*$ 的由 r 次幂元素形成的子群的阶为 $(q-1)/r = es$，因此包含一个由 a 生成的阶为 e 的 $\mathbb{F}_q^*$ 的子群.

具体的说，存在 $b \in \mathbb{F}_q^*$ 使得 $a = b^r$, 因此 $x^t - a = x^{t_1 r} - b^r$ 有因子 $x^{t_1} - b$.

剩余情况，假设 r 不整除 $(q-1)/e$ 和 e. 那么 r 不整除 $q-1$. 那么存在 $r_1 \in \mathbb{N}$ 使得 $r_1 r \equiv 1 \mod (q-1)$.

因此 $x^t - a = x^{t_1 r} - a^{r_1 r}$ 有因子 $x^{t_1} - a^{t_1}$. 不满足题设的不可约.

设 (i) 满足但是 (ii) 不满足，那么存在 $t_2 \in \mathbb{N}$ 使得 $t = 4t_2$ 且 $q \not\equiv 1 \mod 4$.

但是 (i) 可以得到 e 是一个偶数，而因为 $e \mid q-1$ 所以 q 是一个奇数，因此 $q \equiv 3 \mod 4$.

那么根据 **Theorem 3.37** 多项式 $x^t - a$ 可约.

也可通过直接证明的方法来证明. 首先可以知道 $e \equiv 2 \mod 4$. 此外 $a^{e/2} = -1$. 所以就有 $x^t - a = x^t + a^{(e/2)+1} = x^t + a^d$, 其中 $d = (e/2) + 1$ 是一个偶数，那么

$$\begin{aligned} a^d &= 4(2^{-1}a^{d/2})^2 \\ &= 4(2^{-1}a^{d/2})^{q+1} = 4c^4 \end{aligned}$$

其中 $c = (2^{-1}a^{d/2})^{(q+1)/4}$.

所以就可以得到分解式

$$\begin{aligned} x^t - a &= x^{4t_2} + 4c^4 \\ &= (x^{2t_2} + 2cx^{t_2} + 2c^2)(x^{2t_2} - 2cx^{t_2} + 2c^2) \end{aligned}$$

因此也不满足题设的不可约，综上原命题得证.

Pre-Theorem 3.76

考虑上面的 $q \equiv 3 \mod 4$ 的情况，可以把 q 写成 $2^A u - 1$ 的形式，其中 $A \geq 2$ 且 u 是奇数.

设上面的条件 (i) 满足，且 t 可以被 2^A 整除. 那么设 $t = Bv, B = 2^{A-1}, v$ 是偶数. 那么在 **Theorem 3.37** 里 $k = A$.

那么对于 $f(x) = x - a$ 可以把 $f(x^t) = x^t - a$ 分解成 B 个 $\mathbb{F}_q[x]$ 上次数为 $t/B = v$ 的首一不可约多项式的乘积，这些不可约因子是可以被唯一确定的.

由上面的证明可以知道 $d = (e/2) + 1$ 是一个偶数. 那么 $\gcd(2B, q-1) = 2$, 存在 $r \in \mathbb{N}$ 使得 $2Br \equiv d \mod (q-1)$.

令 $b = a^r \in \mathbb{F}_q$, 就可以得到下面的分解.

Theorem 3.76 Factorization of Binomials

在上面给出的条件和表示法下，设

$$F(x) = \sum_{i=0}^{B/2} \frac{(B-i-1)!B}{i!(B-2i)!} x^{B-2i} \in \mathbb{F}_q[x]$$

那么它所有的根 $c_1, \ldots, c_B$ 都在 $\mathbb{F}_q$ 里，且在 $\mathbb{F}_q[x]$ 上可以有标准分解

$$x^t - a = \prod_{j=1}^{B} (x^v - bc_j x^{v/2} - b^2)$$

证明： 对于一个 $\mathbb{F}_q$ 的域扩张上的非零元 γ, 有

$$(x - \gamma)(x + \gamma^{-1}) = x^2 - \beta x - 1$$

其中 $\beta = \gamma - \gamma^{-1}$.

根据 **Theorem 1.76** 有

$$\begin{aligned} s_B(x_1, x_2) &= x_1^B + x_2^B \\ &= \sum_{i_1 + 2i_2 = B, i_1, i_2 \geq 0} (-1)^{i_2} \frac{(i_1 + i_2 - 1)B}{i_1! i_2!} \sigma_1(x_1, x_2)^{i_1} \sigma_2(x_1, x_2)^{i_2} \\ &= \sum_{i_2=0}^{B/2} (-1)^{i_2} \frac{(B - i_2 - 1)!B}{(B-2i_2)! i_2!} (x_1 + x_2)^{B-2i_2} (x_1 x_2)^{i_2} \end{aligned}$$

令 $x_1 = \gamma, x_2 = -\gamma^{-1}$, 有

$$\gamma^B + \gamma^{-B} = \sum_{i=0}^{B/2} (-1)^i \frac{(B-i-1)!B}{(B-2i_2)! i_2!} \beta^{B-2i} (-1)^i = F(\beta)$$

如果 c_j 是 $F(x)$ 在 $\mathbb{F}_q$ 的某个域扩张上的根，γ_j 满足 $\gamma_j - \gamma_j^{-1} = c_j$. 那么 $\gamma_j^B + \gamma_j^{-B} = F(c_j) = 0$.

那么 $\gamma_j^{2B} = -1$. 又因为 $q + 1 = 2Bu$, u 是奇数，那么就有 $\gamma_j^{q+1} = -1$, 因此 $\gamma_j^q = -\gamma_j^{-1}$, 那么

$$c_j^q = (\gamma_j - \gamma_j^{-1})^q = \gamma_j^q - \gamma_j^{-q} = -\gamma_j^{-1} + \gamma_j = c_j$$

因此 $c_j \in \mathbb{F}_q$. 又因为 $F(x)$ 首一，所以

$$F(x) = \prod_{j=1}^{B} (x - c_j)$$

因此

$$\gamma^B+\gamma^{-B}=F(\beta)=\prod_{j=1}^{B}(\beta-c_j)=\prod_{j=1}^{B}(\gamma-\gamma^{-1}-c_j)$$

因此

$$\gamma^{2B}+1=\prod_{j=1}^{B}(\gamma^2-c_j\gamma-1)$$

因为这个式子对于所有 $\mathbb{F}_q$ 的任意域扩张上的任意元素 γ 都成立，那么就得到

$$x^{2B+1}=\prod_{j=1}^{B}(x^2-c_jx-1)$$

通过把 x 替换为 $b^{-1}x^{v/2}$ 然后再乘上 b^{2B}. 就得到

$$x^{Bv}+b^{2B}=x^t+a^{2Br}=x^t+a^d=x^t-a$$

的分解式. 这个分解式的因子都在 $\mathbb{F}_q[x]$ 上不可约，因为 x^t-a 的标准分解里是 B 个次数为 v 的 $\mathbb{F}_q[x]$ 上的不可约多项式.

Example 3.77 Factorization of Binomials

在 $\mathbb{F}_7[x]$ 上分解二项式 $x^{24}-3$.

解： 由题 $q=2^3-1$. 所以就有 $t=24,A=3,B=2^{A-1}=4,v=t/B=6,a=3$.

在 $\mathbb{F}_7^*$ 上可以知道元素 $a=3$ 的阶是 $e=6$. 而 $t=24=2^3\times 3$. 满足 **Theorem 3.75(i)**, 所以 **Theorem 3.76** 可以使用.

因为 $e=6$, 所以 $d=(e/2)+1=4$.

考虑同余方程 $2Br\equiv d \mod (q-1)$ 即 $8r\equiv 4 \mod 6$. 解得 $r=2$. 因此 $b=a^2=2$.

因此

$$\begin{aligned}F(x)&=\sum_{i=0}^{B/2}\frac{(B-i-1)!B}{i!(B-2i)!}x^{B-2i}\\&=\sum_{i=0}^{2}\frac{(3-i)!\times 4}{i!(4-2i)!}x^{4-2i}\\&=\frac{24}{24}x^4+\frac{8}{2}x^2+\frac{4}{2}\\&=x^4+4x^2+2\end{aligned}$$

$F(x)=x^4+4x^2+2$ 在 $\mathbb{F}_7$ 上有根 $1,3,-1,-3$. 所以 $x^{24}-3$ 在 $\mathbb{F}_7[x]$ 上的标准分解为

$$\begin{aligned}x^{24}-3&=\prod_{j=1}^{B}(x^v-bc_jx^{v/2}-b^2)\\&=\prod_{j=1}^{4}(x^6-2c_jx^3-4)\\&=(x^6-2x^3-4)(x^6+2x^3-4)(x^6+x^3-4)(x^6-x^3-4)\end{aligned}$$

三项式(Trinomial) 是一个有三个非零项组成的多项式，其中一个是常数项. 首先考虑仿射三项式.

Theorem 3.78 Trinomials' Irreducibility

设 $a \in \mathbb{F}_q$, p 是域 $\mathbb{F}_q$ 的特征. 那么三项式 $x^p - x - a$ 在 $\mathbb{F}_q[x]$ 上不可约当且仅当多项式 $\mathbb{F}_q$ 上没有根.

证明： 设 β 是 $x^p - x - a$ 在 $\mathbb{F}_q$ 的某个域扩张上的根，那么根据 **Theorem 3.56** 可以知道 $x^p - x - a$ 的根是 $\beta + U$，

其中 U 是线性化多项式 $x^p - x$ 的根. 但是 $U = \mathbb{F}_p$, 因此

$$x^p - x - a = \prod_{b \in \mathbb{F}_p} (x - \beta - b)$$

假设 $x^p - x - a$ 有一个首一因子 $g \in \mathbb{F}_q[x]$ 满足 $1 \leq r = \deg(g) < p$. 那么

$$g(x) = \prod_{i=1}^{r} (x - \beta - b_i)$$

将其与 x^{r-1} 对比系数可以知道 $r\beta + b_1 + \ldots + b_r$ 是 $\mathbb{F}_q$ 的一个元素. 又因为 r 在 $\mathbb{F}_q$ 上存在乘法逆元，所以 $\beta \in \mathbb{F}_q$.

所以就有 $x^p - x - a$ 在 $\mathbb{F}_q[x]$ 上可非平凡分解，所以它在 $\mathbb{F}_q$ 上有根. 证毕.

另一侧是显然的.

Corollary 3.79

设 $a \in \mathbb{F}_q$, p 是域 $\mathbb{F}_q$ 的特征. 那么三项式 $x^p - x - a$ 在 $\mathbb{F}_q[x]$ 上不可约当且仅当 $Tr_{\mathbb{F}_q}(a) \neq 0$.

证明： 根据 **Theorem 2.25** 可知 $x^p - x - a$ 在 $\mathbb{F}_q[x]$ 上有根当且仅当绝对迹 $Tr_{\mathbb{F}_q}(a) \neq 0$.

所以根据 **Theorem 3.78** 命题成立.

注意到对于 $b \in \mathbb{F}_q^*$ **多项式** $f(x)$ **在** $\mathbb{F}_q$ **上不可约当且仅当** $f(bx)$ **在** $\mathbb{F}_q$ **上不可约**，所以上面的结论对于形如 $b^p x^p - bx - a$ 的三项式也适用.

Theorem 3.80 Factorization of Trinomials

对于多项式 $x^q - x - a$, 其中 a 是 $F = \mathbb{F}_q$ 的子域 $K = \mathbb{F}_r$ 中的元素，那么在 $\mathbb{F}_q[x]$上有如下分解：

$$x^q - x - a = \prod_{j=1}^{q/r} (x^r - x - \beta_j) \tag{13}$$

其中 β_j 是 $\mathbb{F}_q$ 上满足 $Tr_{F/k}(\beta_j) = a$ 的不同元素.

证明： 对一个给定的 β_j, 设 γ 是 $x^r - x - \beta_j$ 在 $\mathbb{F}_q$ 的某个域扩张上的根，那么 $\gamma^r - \gamma = \beta_j$, 且

$$\begin{aligned} a &= Tr_{F/K}(\beta_j) \\ &= Tr_{F/K}(\gamma^r - \gamma) \\ &= (\gamma^r - \gamma) + (\gamma^r - \gamma)^r + (\gamma^r - \gamma)^{r^2} + \ldots + (\gamma^r - \gamma)^{q/r} = \gamma^q - \gamma \end{aligned}$$

所以 γ 是 $x^q - x - a$ 的根. 又因为 $x^r - x - \beta_j$ 只有单根，所以 $x^r - x - \beta_j$ 整除 $x^q - x - a$.

那么对于多项式 $x^r - x - \beta_j, 1 \leq j \leq q/r$, 这些多项式两两互素，所以式 (13) 的右侧整除 $x^q - x - a$.

通过对比次数和首项系数就可以知道式 (13) 左右是相等的.

Example 3.81 Factorization of Trinomials

考虑 $\mathbb{F}_9[x]$ 上的 x^9-x-1.

将 $\mathbb{F}_9$ 看成 $\mathbb{F}_3(\alpha)$, 其中 α 是 $\mathbb{F}_3[x]$ 上不可约多项式 x^2-x-1 的根，可以去求 $\mathbb{F}_9$ 上绝对迹等于 1 的元素有 $-1,\alpha,1-\alpha$.

所以根据 (13) 式可以得到分解形式

$$\begin{aligned} x^9-x-1 &= \prod_{j=1}^{3}(x^3-x-\beta_j) \\ &= (x^3-x+1)(x^3-x-\alpha)(x^3-x-1+\alpha) \end{aligned}$$

这三个多项式在 $\mathbb{F}_9[x]$ 上都是不可约的，所以这就是原式在 $\mathbb{F}_9[x]$ 上的标准分解.

不可约三项式的有关信息可以被用来通过给定的多项式来构造新的不可约多项式.

Theorem 3.82

设 $f(x)=x^m+a_{m-1}x^{m-1}+\ldots+a_0$ 是特征为 p 的有限域 $\mathbb{F}_q$ 上的不可约多项式，设 $b\in\mathbb{F}_q$.

那么多项式 $f(x^p-x-b)$ 在 $\mathbb{F}_q$ 上不可约，当且仅当绝对迹 $Tr_{\mathbb{F}_q}(mb-a_{m-1})\neq 0$.

证明：设绝对迹 $Tr_{\mathbb{F}_q}(mb-a_{m-1})\neq 0$. 令 $K=\mathbb{F}_q$, 设 F 是 f 在 K 上的分裂域.

如果 $\alpha\in F$ 是 f 的一个根，那么根据 **Theorem 2.14**, 所有的 f 的根为 $\alpha,\alpha^q,\ldots,\alpha^{q^{m-1}}$, 且 $F=K(\alpha)$.

此外 $Tr_{F/K}(\alpha)=-a_{m-1}$, 然后根据 **Theorem 2.26** 就有

$$Tr_F(\alpha+b)=Tr_K(Tr_{F/K}(\alpha+b))=Tr_K(-a_{m-1}+mb)\neq 0$$

根据 **Corollary 3.79** 三项式 $x^p-x-(\alpha+b)$ 在 F 上不可约. 因此 $[F(\beta):F]=p$, 其中 β 是 $x^p-x-(\alpha+b)$ 的一个根. 那么根据 **Theorem 1.84** 就有

$$[F(\beta):K]=[F(\beta):F][F:K]=pm$$

所以 $\alpha=\beta^p-\beta-b$. 所以 $\alpha\in K(\beta), K(\beta)=K(\alpha,\beta)=F(\beta)$.

因此 $[K(\beta):K]=pm$, 所以 β 在 K 上的极小多项式的次数为 pm. 但是 $f(\beta^p-\beta-b)=f(\alpha)=0$, 因此 β 是次数为 pm 的首一多项式 $f(x^p-x-b)$ 的一个根.

根据 **Theorem 3.33(ii)** 可以知道 $f(x^p-x-b)$ 是 β 在 K 上的极小多项式，那么根据 **Theorem 3.33(i)** 可知 $f(x^p-x-b)$ 在 $K=\mathbb{F}_q$ 上是不可约的.

反过来，如果绝对迹 $Tr_{\mathbb{F}_q}(mb-a_{m-1})=0$. 那么 $x^p-x-(\alpha+b)$ 在 F 上可约，所以对于任意 $x^p-x-(\alpha+b)$ 的根 β 都有

$$[F(\beta):F]<p$$

那么根据前面的证明同理可以知道 β 是 $f(x^p-x-b)$ 的根，且 $[F(\beta):K]<pm$, 因此 $f(x^p-x-b)$ 在 $K=\mathbb{F}_q$ 上可约.

Theorem 3.83

设 $f(x)=x^r-ax-b\in\mathbb{F}_q[x]$, 其中 $r>2$, 是域 $\mathbb{F}_q$ 的特征的幂次，且二项式 $x^{r-1}-1$ 在 $\mathbb{F}_q$ 上不可约.

那么 $f(x)$ 是一个线性多项式和一个 $\mathbb{F}_q$ 上次数为 $r-1$ 的不可约多项式的乘积.

证明： 首先，$f'(x)=-a\neq 0$. 所以 $f(x)$ 只有单根. 设 p 为域 $\mathbb{F}_q$ 的特征，那么根据定义 $f(x)$ 是 $\mathbb{F}_q$ 上的 $p-$仿射多项式.

因此根据 **Theorem 3.56** 两个 $f(x)$ 的不同根的差 γ 是 $p-$多项式 x^r-ax 的根，也是 $x^{r-1}-a$ 的根.

由于 $r-1>1$ 且二项式 $x^{r-1}-1$ 在 $\mathbb{F}_q$ 上不可约，所以就有 $\gamma\notin\mathbb{F}_q$. 从而证明了存在 $f(x)$ 的根 α 满足 $\alpha\notin\mathbb{F}_q$.

那么 $\alpha^q\neq\alpha$ 也是 $f(x)$ 的一个根，且现在已知 $\alpha^q-\alpha$ 是不可约多项式 $x^{r-1}-a$ 在 $\mathbb{F}_q$ 上的根，所以 $[\mathbb{F}_q(\alpha^q-\alpha):\mathbb{F}_q]=r-1$.

又因为 $\mathbb{F}_q[\alpha^q-\alpha]\subseteq\mathbb{F}_q(\alpha)$, 所以就有 $m=[\mathbb{F}_q(\alpha):\mathbb{F}_q]$ 是 $r-1$ 的倍数.

另一方面， α 是次数为 r 的多项式 $f(x)$ 的根，所以 $m\leq r$. 又因为 $r>2$, 所以只能有 $m=r-1$.

因此 α 在 $\mathbb{F}_q$ 上的极小多项式是一个次数为 $r-1$ 且整除 $f(x)$ 的在 $\mathbb{F}_q$ 上不可约的多项式. 所以原命题成立.

Theorem 3.84

设 p 是素数，三项式 $f(x)=x^p-x-a\in\mathbb{F}_p[x]$ 是 $\mathbb{F}_p$ 上的本原多项式，

当且仅当 a 是 $\mathbb{F}_p$ 上的本原元，且 $ord(x^p-x-1)=(p^p-1)/(p-1)$.

证明： 设 $f(x)=x^p-x-a$ 是 $\mathbb{F}_p$ 上的本原多项式，那么根据 **Theorem 3.18** 可知 a 必然是 $\mathbb{F}_p$ 的本原元.

设 β 是 $g(x)=x^p-x-1$ 在 $\mathbb{F}_p$ 的域扩张上的根，那么

$$0=ag(\beta)=a(\beta^p-\beta-1)=a^p\beta^p-a\beta-a=f(a\beta)$$

所以 $\alpha=a\beta$ 也是 $f(x)$ 的根. 因此对于 $0<r<(p^p-1)/(p-1)$ 有 $\beta^r\neq 1$, 否则对于 $0<r(p-1)<p^p-1$ 有 $\alpha^{r(p-1)}=1$, 这和 α 是 $\mathbb{F}_{p^p}$ 的本原元相矛盾. 同时 $g(x)$ 根据 **Corollary 3.79** 在 $\mathbb{F}_p$ 上不可约，所以

$$g(x)=x^p-x-1=(x-\beta)(x-\beta^p)\dots(x-\beta^{p^{(p-1)}})$$

通过对比常数项系数可以得到 $\beta^{(p^p-1)/(p-1)}=1$. 因此根据 **Theorem 3.3** 可以得到 $ord(x^p-x-1)=(p^p-1)/(p-1)$.

反过来，如果 a 是 $\mathbb{F}_p$ 上的本原元且 $ord(x^p-x-1)=(p^p-1)/(p-1)$.

那么 a 和 β 在乘法群 $\mathbb{F}_{p^p}^*$ 上的阶就是 $p-1$ 和 $(p^p-1)/(p-1)$. 那么

$$\begin{aligned}(p^p-1)/(p-1)&=1+p+p^2+\dots+p^{p-1}\equiv 1+1+1+\dots+1\\&\equiv p\equiv 1 \mod(p-1)\end{aligned}$$

所以 $p-1$ 和 $(p^p-1)/(p-1)$ 互素. 因此 $\alpha=a\beta$ 在乘法群 $\mathbb{F}_{p^p}^*$ 上的阶就是 $(p-1)(p^p-1)/(p-1)=p^p-1$.

因此 α 是 $\mathbb{F}_{p^p}^*$ 上的本原元，所以 $f(x)$ 是 $\mathbb{F}_q$ 上的本原多项式.

Example 3.85

考虑 $p=5$. 那么 $(p^p-1)/(p-1)=781=11\cdot 71$.

通过 **Theorem 3.84** 的证明过程可以知道 $x^{781}\equiv 1 \mod (x^5-x-1)$.

而因为 $x^{11}\not\equiv 1 \mod (x^5-x-1)$ 且 $x^{71}\not\equiv 1 \mod (x^5-x-1)$, 所以 $ord(x^5-x-1)=781$.

可以发现 2 和 3 是 $\mathbb{F}_5$ 上的本原元，因此根据 **Theorem 3.84** 就可以知道 x^5-x-2 和 x^5-x-3 是 $\mathbb{F}_5$ 上的本原多项式.

考虑特征为奇数的域 $\mathbb{F}_q$ 上的三项式 x^2+x+a, 显然这个三项式在 $\mathbb{F}_q$ 上不可约当且仅当 a 不能表示成 $a=4^{-1}-b^2, b\in\mathbb{F}_q$ 的形式. 因此恰有 $(q-1)/2$ 种方法来选择 $a\in\mathbb{F}_q$ 的值使得 x^2+x+a 在 $\mathbb{F}_q$ 上不可约.

更一般的，使得 x^2+x+a 在 $\mathbb{F}_q$ 上不可约的 $a\in\mathbb{F}_q$ 的值可以渐近为 q/n. 如下面的定理所示.

Theorem 3.86

设 $\mathbb{F}_q$ 是一个有限域，特征为 p. 对于满足 $2n(n-1)$ 不被整数 p 整除的整数 $n\geq 2$, 设 $T_n(q)$ 表示使得 x^2+x+a 在 $\mathbb{F}_q$ 上不可约的 $a\in\mathbb{F}_q$ 的个数，那么就有

$$|T_n(q)-\frac{q}{n}|\leq B_n q^{1/2}$$

其中 B_n 是只与 n 有关的常数.

Theorem 3.87

三项式 $x^n+ax^k+b\in\mathbb{F}_q[x]$ 的判别式为

$$\begin{aligned}D(x^n+ax^k+b)=&(-1)^{n(n-1)/2}b^{k-1}\\&\cdot(n^Nb^{N-K}-(-1)^N(n-k)^{N-K}k^Ka^N)^d\end{aligned}$$

其中 $n>k\geq 1, d=\gcd(n,k), N=n/d, K=k/d$.

判别式 $D(f)=0$ 意味着多项式 f 有重根.