Chapter 2 Structure of Finite Fields

2.1 Characterization of Finite Fields

Lemma 2.1

设 F 是一个有限域，K 是一个子域，其中有 q 个元素. 那么 F 有 q^m 个元素，其中 $m = [F : K]$.

证明： F 是 K 上的一个线性空间，因为 F 是有限的，所以线性空间也是有限维的.

记 $[F : K] = m$, 那么 F 有一组 K 上的基，由 m 个元素组成，分别为 $b_1, b_2, \ldots, b_m$.

因此每个元素都可以表示成 $a_1b_1 + a_2b_2 + \ldots + a_mb_m$ 的形式，其中 $a_1, a_2, \ldots, a_m \in K$

由于每个 a_i 都有 q 种取值，所以 F 中的元素数量就是 q^m.

Theorem 2.2

设 F 是一个有限域，那么 F 有 p^n 个元素，其中 p 是一个质数，是域 F 的特征，n 是 F 在其素子域上的次数.

证明： 根据 **Corollary 1.45** 可以知道有限域 F 的特征是素数.

因此根据 **Theorem 1.78** 可知 F 的素子域 K 和 $\mathbb{F}_p$ 同构，所以其含有 p 个元素，根据 **Lemma 2.1** 结论成立.

Lemma 2.3

如果一个有限域 F 含有 q 个元素，那么对于每个 $a \in F$ 都有 $a^q = a$.

证明： 对于 $a = 0$ 显然成立.

对于 $a \neq 0$, 所有 F 的非零元对于乘法形成了一个阶为 $q - 1$ 的群，因此 $a^{q-1} = 1, a \in F, a \neq 0$.

两边同时乘以 a 可知原命题成立.

Lemma 2.4

如果 F 是一个有限域，含有 q 个元素，K 是 F 的子域，那么多项式 $x^q - x \in K[x]$ 在 $F[x]$ 中可以分解成

$$x^q - x = \prod_{a \in F} (x - a)$$

F 是 $x^q - x$ 在 K 上的分裂域.

证明： 多项式 $x^q - x$ 的次数是 q, 在 F 上最多有 q 个根. 根据 **Lemma 2.3** 可知有 q 个这样的根，即 F 的所有元素.

因此这个多项式可以在 F 上分裂，且不能再更小的域上分裂.

Theorem 2.5 Existence and Uniqueness of Finite Fields

对于任意素数 p 和任意正整数 n 存在一个包含 p^n 个元素的有限域.

每个含有 $q=p^n$ 个元素的有限域都同构于 x^q-x 在 F_p 上的分裂域.

证明：

(1) 存在性

对于每一个 $q=p^n$, 考虑 $\mathbb{F}_p[x]$ 上的多项式 x^q-x, 设 F 为它在 $\mathbb{F}_p$ 上的分裂域.

这个多项式有 q 个不相同的根，因为导数 $qx^{q-1}-1=-1$ 所以根据 **Theorem 1.68** 可以得到这个结论.

设 $S=\{a\in F:a^q-a=0\}$. 因为：

(i) S 含有 $0,1$.

(ii) 根据 **Theorem 1.46** 可知 $(a-b)^q=a^q-b^q=a-b$, 所以 $a-b\in S$.

(iii) 对于 $a,b\in S,b\neq 0$ 有 $(ab^{-1})^q=a^qb^{-q}=ab^{-1}$, 所以 $ab^{-1}\in S$.

因此可以知道 S 是 F 的子域.

但是又因为 x^q-x 在 S 上分裂，因为 S 包含了它所有的根，因此 $F=S$.

又因为 S 中含有 q 个元素，所以 F 中也含有 q 个元素.

(2) 唯一性

设 F 是一个有 $q=p^n$ 个元素的有限域，那么根据 **Theorem 2.2** 可知 F 的特征是 p, $\mathbb{F}_p$ 是它的子域.

那么根据 **Lemma 2.4** 可知 F 是 x^q-x 在 $\mathbb{F}_p$ 上的分裂域. 所以根据分裂域的唯一性 **(Theorem 1.91)** 可知命题成立.

Theorem 2.6 Subfield Criterion

设 $\mathbb{F}_q$ 是一个有 $q=p^n$ 个元素的有限域. 那么每一个 $\mathbb{F}_q$ 的子域的阶都是 p^m, 其中 m 是 n 的正因子.

相反的，如果 m 是 n 的正因子，那么存在恰好一个 $\mathbb{F}_q$ 的子域，其有 p^m 个元素.

证明： 显然存在正数 $m\leq n$ 使得 $\mathbb{F}_q$ 的子域 K 的阶为 p^m. 那么根据 **Lemma 2.1** 可知 $q=p^n$ 一定是 p^m 的倍数，所以 $m\mid n$.

反过来，如果 m 是 n 的正因子，那么 $p^m-1|p^n-1$, 那么 $x^{p^m-1}\mid x^{p^n-1}$.

所以 $x^{p^m}-x|x^{p^n}-x$. 所以每个 $x^{p^m}-x$ 的根都是 $x^{p^n}-x$ 的根，根都是在 $\mathbb{F}_q$ 里的.

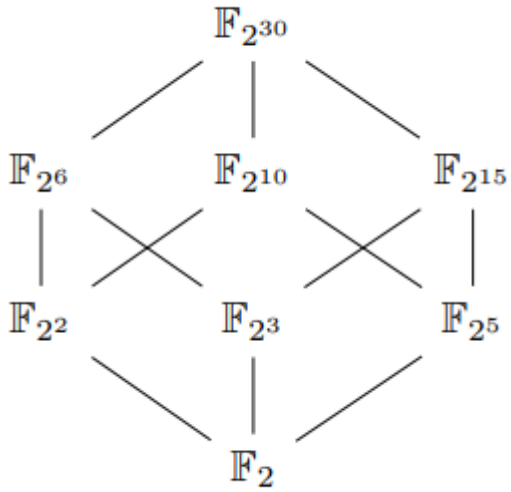
所以 $\mathbb{F}_q$ 一定含有一个 $x^{p^m}-x$ 在 $\mathbb{F}_p$ 上的分裂域作为子域，根据 **Theorem 2.5** 的推导可以知道这个分裂域的阶是 p^m.

如果有两个这样的子域存在，那么 $x^{p^m}-x$ 就会有超过 p^m 个在 $\mathbb{F}_q$ 上的根，这是不可能的，所以这样的子域唯一.

这也说明了域 $\mathbb{F}_{p^n}$ 的阶为 p^m 的子域包括了多项式 $x^{p^m}-x\in\mathbb{F}_p[x]$ 在 $\mathbb{F}_{p^n}$ 上的所有根，其中 $m\mid n$.

Example 2.7

考虑有限域 $\mathbb{F}_{2^{30}}$. 通过枚举 30 的因子可以找到所有它的子域. 不同的子域关系由下图所示.



Theorem 2.8

对于每个有限域 $\mathbb{F}_q$, 由域中非零元素构成的乘法群 $\mathbb{F}_q^*$ 是循环群.

证明： $q=2$ 的时候显然成立.

设 $q \geq 3, h=q-1$. 设 h 的因子分解形式为 $h=p_1^{r_1}p_2^{r_2}\dots p_m^{r_m}$. 群 $\mathbb{F}_q^*$ 的阶是 h.

对于每个 $i, 1 \leq i \leq m$, 多项式 $x^{h/p_i}-1$ 在 $\mathbb{F}_q^*$ 上最多只有 h/p_i 个根. 由于 $h/p_i < h$, 可以知道存在 $\mathbb{F}_q$ 上的非零元不是该多项式的根. 设 a_i 是其中的一个元素，令 $b_i = a_i^{h/p_i^{r_i}}$. 那么就有 $b_i^{p_i^{r_i}}=1$. 因此，b_i 的阶是 $p_i^{r_i}$ 的因子，可以写成 $p_i^{s_i}$ 的形式，其中 $0 \leq s_i \leq r_i$.

另一方面，由于

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$$

所以 b_i 的阶是 $p_i^{r_i}$.

下面要证 $b=b_1b_2\dots b_m$ 的阶是 h.

假设不是 h, 那么 b 的阶是一个 h 的真因子，因此是某个 h/p_i 的因子，$1 \leq i \leq m$. 不妨设是 h/p_1 的因子，那么就有

$$1 = b^{h/p_1} = b_1^{h/p_1}b_2^{h/p_1}\dots b_m^{h/p_1}$$

那么对于 $2 \leq i \leq m$ 就有 $p_i^{r_i}$ 整除 h/p_1, 因此就有 $b_i^{h/p_1}=1$. 因此 $b_1^{h/p_1}=1$

这说明 b_1 的阶一定整除 h/p_1. 但是因为 b_1 的阶是 $p_1^{r_1}$, 所以这个是不可能的.

因此 $\mathbb{F}_q^*$ 是由 b 所生成的循环群.

Definition 2.9 Primitive element

循环群 $\mathbb{F}_q^*$ 的生成元被称为 $\mathbb{F}_q$ 的本原元.

$\mathbb{F}_q$ 中的本原元个数是 $\phi(q-1)$.

本原元的存在可以说明每个有限域都可以被看做一个素子域的代数单扩张.

Theorem 2.10

设 $\mathbb{F}_q$ 是一个有限域，$\mathbb{F}_r$ 是其的一个有限域扩张. 那么 $\mathbb{F}_r$ 是 $\mathbb{F}_q$ 的一个代数单扩张，且每个 $\mathbb{F}_r$ 中的本原元都是 $\mathbb{F}_r$ 在 $\mathbb{F}_q$ 上的定义元.

证明： 设 $\mathbb{F}_r$ 的一个本原元是 ζ. 那么就有 $\mathbb{F}_q(\zeta) \subseteq \mathbb{F}_r$.

另一方面 $\mathbb{F}_q(\zeta)$ 包含了 0 和所有 ζ 的幂次，也就包含了所有 $\mathbb{F}_r$ 中的元素.

因此 $\mathbb{F}_r = \mathbb{F}_q(\zeta)$.

Corollary 2.11

对于每个有限域 $\mathbb{F}_q$ 和任意正整数 n, 存在一个 $\mathbb{F}_q[x]$ 上的 n 次不可约多项式.

证明： 设 $\mathbb{F}_r$ 是阶为 q^n 的域 $\mathbb{F}_q$ 的域扩张，那么就有 $[\mathbb{F}_r : \mathbb{F}_q] = n$. 根据 **Theorem 2.10** 可以知道存在 $\zeta \in \mathbb{F}_r$ 使得 $\mathbb{F}_r = \mathbb{F}_q(\zeta)$ 成立.

那么根据 **Theorem 1.82(i)** 和 **Theorem 1.86(ii)** 可以知道 $\mathbb{F}_q$ 上关于 ζ 的极小多项式在 $\mathbb{F}_q[x]$ 上次数为 n 且不可约.

2.2 Roots of Irreducible Polynomials

Lemma 2.12

设 $f \in \mathbb{F}_q[x]$ 是一个有限域 $\mathbb{F}_q$ 上的不可约多项式， α 是 f 在 $\mathbb{F}_q$ 的某个域扩张上的根

那对于 $h \in \mathbb{F}_q[x]$，当且仅当 $h(\alpha) = 0$ 的时候，有 $f|h$.

证明： 设 $f(x)$ 的首项系数是 a, 令 $g(x) = a^{-1}f(x)$.

那么 g 就是 $\mathbb{F}_q[x]$ 上的首一不可约多项式，且满足 $g(a) = 0$.

那么根据 **Definition 1.81** 关于极小多项式的定义， g 就是 a 在 $\mathbb{F}_q$ 上的极小多项式.

根据 **Theorem 1.82(ii)** 就可以得到 $g \mid h$. 因此就有 $f \mid h$.

Lemma 2.13

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.

那么 $f(x)|x^{q^n} - x$ 当且仅当 $m|n$.

证明：

(1) 充分性

设 a 是 f 在 f 在 $\mathbb{F}_{q^n}$ 上的分裂域中的一个根，那么就有 $a^{q^n} = a$, 所以 $a \in \mathbb{F}_{q^n}$.

所以 $\mathbb{F}_q(a)$ 是 $\mathbb{F}_{q^n}$ 的一个子域. 但是因为 $[\mathbb{F}_q(a) : \mathbb{F}_q] = m, [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, 根据 **Theorem 1.84** 可得 $m \mid n$.

(2) 必要性

如果 $m \mid n$ 就可以根据 **Theorem 2.6** 得到 $\mathbb{F}_{q^m}$ 是 $\mathbb{F}_{q^n}$ 的子域.

设 a 是 f 在 f 在 $\mathbb{F}_{q^n}$ 上的分裂域中的一个根，那么 $[\mathbb{F}_q(a) : \mathbb{F}_q] = m$, 因此 $\mathbb{F}_q(a) = \mathbb{F}_{q^m}$. 因此就有 $a \in \mathbb{F}_{q^n}$.

因此 $a^{q^n} = a$, 所以 a 就是多项式 $x^{q^n} - x \in \mathbb{F}_q[x]$ 的根. 那么根据 **Lemma 2.12** 就可以得到必要性成立.

Theorem 2.14

设 f 是 $\mathbb{F}_q[x]$ 上的一个次数为 m 的不可约多项式，若 f 在 $\mathbb{F}_{q^m}$ 上有根 a.

那所有 f 的根都是单根，分别是 $a, a^q, a^{q^2}, \ldots, a^{q^{m-1}}$.

证明： 设 a 是 f 在 f 在 $\mathbb{F}_{q^n}$ 上的分裂域中的一个根，那么 $[\mathbb{F}_q(a) : \mathbb{F}_q] = m$, 因此 $\mathbb{F}_q(a) = \mathbb{F}_{q^m}$. 因此就有 $a \in \mathbb{F}_{q^m}$.

下面要证明，如果 $b \in \mathbb{F}_{q^m}$ 是 f 的根，那么 b^q 也是 f 的根.

$f(x) = a_m x^m + \ldots + a_1 x + a_0, a_i \in \mathbb{F}_q, 0 \le i \le m$. 那么根据 **Lemma 2.3** 和 **Theorem 1.46** 可以得到

$$\begin{aligned} f(b^q) &= a_m b^{qm} + \ldots + a_1 b^q + a_0 = a_m^q b^{qm} + \ldots + a_1^q b^q + a_0^q \\ &= (a_m b^m + \ldots + a_1 b + a_0)^q = f(b)^q = 0 \end{aligned}$$

所以所有的元素 $a, a^q, a^{q^2}, \ldots, a^{q^{m-1}}$ 都是 f 的根了. 下面还需要证明这些根互不相等.

假设存在 $j, k, 0 \leq j < k \leq m-1$ 使得 $a^{q^j} = a^{q^k}$, 那么可以得到

$$a^{q^{m-k+j}} = a^{q^m} = a$$

那么根据 **Lemma 2.12** 可以得到 $f(x)$ 整除 $x^{q^{m-k+j}} - x$. 根据 **Lemma 2.13** 这只在 $m \mid m-k+j$ 的时候成立.

但是 $0 < m-k+j < m$, 这是不可能的，所以假设不成立，所以所有的根互不相等.

Corollary 2.15

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. 那么 f 在 $\mathbb{F}_q$ 上的分裂域是 $\mathbb{F}_{q^m}$.

证明： 根据 **Theorem 2.14** 可知 f 在 $\mathbb{F}_{q^m}$ 上分裂.

$\mathbb{F}_q(a, a^q, a^{q^2}, \ldots, a^{q^m}) = \mathbb{F}_q(a) = \mathbb{F}_{q^m}$ 对于 f 在 $\mathbb{F}_{q^m}$ 上的根 a 成立

那么 $[\mathbb{F}_q(a) : \mathbb{F}_q] = m$, 因此 $\mathbb{F}_q(a) = \mathbb{F}_{q^m}$. 因此就有 $a \in \mathbb{F}_{q^m}$.

那么分裂域就是 $\mathbb{F}_{q^m}$.

Corollary 2.16

任意两个 $\mathbb{F}_q[x]$ 上的相同次数的不可约多项式的分裂域同构.

Definition 2.17 Conjugates

设 F_{q^m} 是域 F_q 的扩张，且 $\alpha \in F_{q^m}$. 则在 F_q 上，元素 $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{q^{m-1}}$ 被称为 α 关于 $\mathbb{F}_q$ 的共轭元。

Theorem 2.18

元素 $\alpha \in \mathbb{F}_{q^m}$ 关于 $\mathbb{F}_q$ 的任何子域的共轭在群 $\mathbb{F}_{q^m}^*$ 上具有相同的阶.

证明： 根据 **Theorem 2.8** 可以知道群 $\mathbb{F}_{q^m}^*$ 是循环群。

那么根据 **Theorem 1.15(ii)** 可以知道 α^{q^k} 的阶是 $(q-1)/gcd(q^k, q-1) = q-1$. 这对于任意的 k 都是成立的.

所以原命题得证.

Corollary 2.19

设 a 是 $\mathbb{F}_q$ 上的本原元，那么 a 关于 $\mathbb{F}_q$ 的任何子域的共轭，也都是本原元.

Example 2.20

设 $a \in \mathbb{F}_{16}$ 是 $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ 上的根. 那么 $a, a^2, a^4 = a + 1, a^8 = a^2 + 1$ 都是 $\mathbb{F}_{16}$ 的本原元.

a 关于 $\mathbb{F}_4$ 的共轭元有 $a, a^4 = a + 1$.

共轭元和有限域的自同构之间有着紧密的关系.

设 $\mathbb{F}_{q^m}$ 是 $\mathbb{F}_q$ 的扩张，那么 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的自同构 σ 是指保持 $\mathbb{F}_q$ 中元素不变的自同构.

因此，需要 σ 是一个从 $\mathbb{F}_{q^m}$ 映射到自身的一一映射，且满足

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

对于所有的 $a, b \in \mathbb{F}_{q^m}$ 恒成立，且 $\sigma(a) = a$ 对于任意 $a \in \mathbb{F}_q$ 恒成立.

Theorem 2.21

$\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的自同构恰有 m 个，分别是 $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, 其中 $\sigma_j(a) = a^{q^j}, 0 \le j \le m - 1$.

证明： 首先对于每个 σ_j 和 $a, b \in \mathbb{F}_{q^m}$ 显然有 $\sigma_j(ab) = \sigma_j(a)\sigma_j(b)$, 根据 Theorem 1.46 就有 $\sigma(a + b) = \sigma(a) + \sigma(b)$, 因此证明了 σ_j 是 $\mathbb{F}_{q^m}$ 上的一个同态. 而因为 $\sigma_j(a) = 0$ 当且仅当 $a = 0$ 时成立，所以 σ_j 是一个单射. 又因为有限集上的单射也是满射，所以这样的映射是一个 $\mathbb{F}_{q^m}$ 上的自同构.

根据 Lemma 2.3 可以知道，$\sigma_j(a) = a$ 对于所有的 $a \in \mathbb{F}_q$ 都成立，所以每一个 σ_j 都是 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的自同构.

而由于这些映射是通过不同的 $\mathbb{F}_{q^m}$ 上的本原元所得到的，所以这些映射就互不相同.

现在设 σ 是任意的一个 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的映射，设 β 是一个 $\mathbb{F}_{q^m}$ 上的本原元，令 $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 \in F_q[x]$ 是 $\mathbb{F}_q$ 上的极小多项式，那么：

$$\begin{aligned} 0 &= \sigma(\beta^m + a_{m-1}\beta^{m-1} + \ldots + a_0) \\ &= \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \ldots + a_0 \end{aligned}$$

所以 $\sigma(\beta)$ 是 f 在 $\mathbb{F}_{q^m}$ 上的根. 那么根据 **Theorem 2.14** 就可以知道存在 $0 \le j \le m - 1$ 使得 $\sigma(\beta) = \beta^{q^j}$.

又因为 σ 是同态，所以对于每个 $\alpha \in \mathbb{F}_{q^m}$ 都有 $\sigma(\alpha) = \alpha^{q^j}$ 成立.

根据这个定理，可以发现所有 $\alpha \in \mathbb{F}_{q^m}$ 关于 $\mathbb{F}_q$ 的共轭元都是通过 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的全部自同构作用到 α 上得到的

这些自同构关于通常的映射复合形成一个群.

上面的定理表明这些所有的自同构都是 σ_1 所生成的阶为 m 的循环群.

2.3 Traces, Norms and Bases

下面要引入一个重要的从 F 到 K 的线性映射，其中 $K=\mathbb{F}_q, F=\mathbb{F}_{q^m}$ 是 K 的域扩张.

Definition 2.22 Trace and Characteristic Polynomial

对于 $a\in F=\mathbb{F}_{q^m}$ 和 $K=\mathbb{F}_q$, K 上的迹 $Tr_{F/K}(a)$ 被定义为

$$Tr_{F/K}(a)=a+a^q+\ldots+a^{q^{m-1}}$$

如果 K 是 F 的素子域，那么这个迹被称为 a 的绝对迹，记作 $Tr_F(a)$.

换句话说，a 在 K 上的迹就是 a 在 K 上的所有共轭元之和.

设 $f\in K[x]$ 是 a 在 K 上的极小多项式，次数为 d, $d\mid m$.

那么多项式 $g(x)=f(x)^{m/d}\in K[x]$ 被称为 a 在 K 上的特征多项式

根据 Theorem 2.14 和 Definition 2.17 可以知道 g 在 F 上的根就是 a 在 K 上的共轭，因此

$$g(x)=x^m+a_{m-1}x^{m-1}+\ldots+a_0=(x-a)(x-a^q)\ldots(x-a^{q^{m-1}})$$

根据韦达定理，可以发现

$$Tr_{F/K}(a)=-a_{m-1}$$

这一定是 K 中的元素.

Theorem 2.23 Properties of Trace

设 $K=\mathbb{F}_q, F=\mathbb{F}_{q^m}$. 那么迹 $Tr_{F/K}$ 满足：

(i) $Tr_{F/K}(\alpha+\beta)=Tr_{F/K}(\alpha)+Tr_{F/K}(\beta)$ 对于所有 $\alpha,\beta\in F$ 成立

(ii) $Tr_{F/K}(c\alpha)=cTr_{F/K}(\alpha)$ 对于所有 $c\in K,\alpha\in F$ 成立

(iii) $Tr_{F/K}$ 是 F 到 K 上的一个线性变换，其中 F 和 K 都看作 K 上的线性空间.

(iv) $Tr_{F/K}(a)=ma$ 对于所有 $a\in K$ 成立

(v) $Tr_{F/K}(\alpha^q)=Tr_{F/K}(\alpha)$ 对所有 $\alpha\in F$ 成立

证明：

(i) 对于所有的 $\alpha,\beta\in F$ 有

$$\begin{aligned}Tr_{F/K}(\alpha+\beta)&=\alpha+\beta+(\alpha+\beta)^q+\ldots+(\alpha+\beta)^{q^{m-1}}\\&=\alpha+\beta+\alpha^q+\beta^q+\ldots+\alpha^{q^{m-1}}+\beta^{q^{m-1}}\\&=Tr_{F/K}(\alpha)+Tr_{F/K}(\beta)\end{aligned}$$

(ii) 对于 $c\in K$ 根据 **Lemma 2.3** 可以知道对于所有的 $j\geq 0$ 都有 $c^{q^j}=c$. 那么对于 $\alpha\in F$ 就有：

$$\begin{aligned} Tr_{F/K}(c\alpha) &= c\alpha + c^q\alpha^q + \ldots + c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha + c\alpha^q + \ldots + c\alpha^{q^{m-1}} = c^T r_{F/K}(\alpha) \end{aligned}$$

(iii) 根据 (i) (ii) 可以知道 $Tr_{F/K}$ 是一个线性变换。为了证明这是一个满射，只需要证明存在 $\alpha \in F$ 满足 $Tr_{F/K}(\alpha) = 0$.

而根据定义 $Tr_{F/K}(\alpha) = 0$ 当且仅当 α 是多项式 $x^{q^{m-1}} + \ldots + x^q + x \in K[x]$ 在 F 上的一个根.

但是由于多项式最多有 q^{m-1} 个根，而 F 中含有 q^m 个元素，所以这是一个满射.

(iv) 根据迹的定义和 (iii) 可知成立

(v) 对于 $\alpha \in F$ 根据 Lemma 2.3 就有 $\alpha^{q^m} = \alpha$. 那么 $Tr_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^m} = Tr_{F/K}(\alpha)$.

迹不仅本身是一个 F 到 K 上的线性变换，它也可以用来表示其他 F 到 K 的线性变换，且与所选择的基无关。

Theorem 2.24

设 F 是有限域 K 的有限扩张，都看做 K 上的线性空间，那么从 F 到 K 的线性变换就是映射 $L_\beta, \beta \in F$, 其中 $L_\beta = Tr_{F/K}(\beta\alpha), \forall \alpha \in F$. 同时，对于 F 上的两个不同元素 β 和 γ 有 $L_\beta \neq L_\gamma$.

证明： 根据 **Theorem 2.23(iii)** 可以知道每一个映射 L_β 都是一个 F 到 K 的映射.

由于 $Tr_{F/K}$ 是 F 到 K 上的满射，那么对于 $\beta, \gamma \in F, \beta \neq \gamma$ 存在 $\alpha \in F$ 使得

$$L_\beta(\alpha) - L_\gamma(\alpha) = Tr_{F/K}(\beta\alpha) - Tr_{F/K}(\gamma\alpha) = Tr_{F/K}((\beta - \gamma)\alpha) \neq 0$$

成立，因此 L_β 和 L_γ 不同.

如果 $K = \mathbb{F}_q, F = \mathbb{F}_{q^m}$, 那么映射 L_β 产生了 q^m 个不同的 F 到 K 的映射.

从另一方面来说，每个 F 到 K 的映射都可以通过分配 K 中的 q 种任意元素，给由 m 个元素的构成的 F 在 K 上的基. 这种分配方式有 q^m 种，所以映射 L_β 就已经穷尽了所有的 F 到 K 的线性映射.

Theorem 2.25

设 F 是域 $K = \mathbb{F}_q$ 的有限扩张，那么对于 $\alpha \in F, Tr_{F/K}(\alpha) = 0$ 当且仅当存在 $\beta \in F$ 使得 $\alpha = \beta^q - \beta$.

证明： 当 $\alpha = \beta^q - \beta$ 时，$Tr_{F/K}(\alpha) = Tr_{F/K}(\beta^q - \beta) = Tr_{F/K}(\beta^q) - Tr_{F/K}(\beta) = 0$.

反过来，设 $\alpha \in F = \mathbb{F}_{q^m}$ 且 $Tr_{F/K}(\alpha) = 0$, 令 β 是 $x^q - x - \alpha$ 在 F 的某个域扩张上的根，那么 $\beta^q - \beta = \alpha$ 且

$$\begin{aligned} 0 = Tr_{F/K}(\alpha) &= \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + \ldots + (\beta^q - \beta)^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \ldots + (\beta^{q^m} - \beta^{q^{m-1}}) \\ &= \beta^{q^m} - \beta \end{aligned}$$

所以 $\beta \in F$.

Theorem 2.26 Transitivity of Trace

设 K 是有限域，F 是 K 的有限扩张，E 是 F 的有限扩张，那么

$$Tr_{E/K(\alpha)} = Tr_{F/K}(Tr_{E/F}(\alpha))$$

对于所有 $\alpha \in E$ 成立.

证明： 设 $K = \mathbb{F}_q$, 令 $[F : K] = m, [E : F] = n$, 那么根据 **Theorem 1.84** 就有 $[E : K] = mn$. 那么对于任意 $\alpha \in E$ 就有：

$$\begin{aligned} Tr_{F/K}(Tr_{E/F}(\alpha)) &= \sum_{i=0}^{m-1} Tr_{E/F}(\alpha)^{q^i} = \sum_{i=0}^{m-1}(\sum_{j=1}^{n-1} \alpha^{q^{jm}})^{q^i} \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1} \alpha^{q^k} \\ &= Tr_{E/K}(\alpha) \end{aligned}$$

Definition 2.27 Norm

对于 $\alpha \in F = \mathbb{F}_{q^m}$ 和 $K = \mathbb{F}_q$, α 在 K 上的范数 $N_{F/K}(\alpha)$ 定义为：

$$N_{F/K}(\alpha) = \alpha \cdot \alpha^q \cdot \ldots \cdot \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}$$

显然这也是 K 中的元素之一.

Theorem 2.28 Properties of Norm

设 $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$. 那么范数 $N_{F/K}$ 满足：

(i) $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$ 对于任意 $\alpha, \beta \in F$ 成立.

(ii) $N_{F/K}$ 是 F 到 K 的满射，也是 F^* 到 K^* 的满射

(iii) $N_{F/K}(a) = a^m$ 对于所有 $a \in K$ 成立

(iv) $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$ 对于所有 $\alpha \in F$ 成立.

证明：

(i) 根据定义，显然

(ii) 首先已经知道 $N_{F/K}$ 是 F 到 K 的映射，由于 $N_{F/K}(\alpha) = 0$ 当且仅当 $\alpha = 0$, 所以 $N_{F/K}$ 也是 F^* 到 K^* 的映射.

根据性质 (i) 可以知道 $N_{F/K}$ 是这些乘法群的同态，由于 $N_{F/K}$ 的核的元素就是多项式 $x^{(q^m-1)/q-1} - 1 \in K[x]$ 在 f 上的根，核的阶数 d 满足 $d \leq (q^m - 1)/(q - 1)$. 这个值 $\geq q - 1$.

因此 $N_{F/K}$ 是 F 到 K 的满射，也是 F^* 到 K^* 的满射.

(iii) 根据范数的定义，且对于 $a \in K$, 所有 a 关于 K 的共轭元都等于 a, 所以 (iii) 成立.

(iv) 根据 (i) 可知 $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)^q = N_{F/K}(\alpha)$. 又因为 $N_{F/K}(\alpha) \in K$ 所以 (iv) 成立.

Theorem 2.29 Transitivity of Norm

设 K 是一个有限域，F 是 K 的域扩张，E 是 F 的域扩张，那么

$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha))$$

对所有 $\alpha \in E$ 成立.

证明： 设 $K = \mathbb{F}_q$, 令 $[F:K] = m, [E:F] = n$, 那么根据 **Theorem 1.84** 就有 $[E:K] = mn$. 那么对于任意 $\alpha \in E$ 就有：

$$\begin{aligned} N_{F/K}(N_{E/F}(\alpha)) &= N_{F/K}(\alpha^{(q^{mn}-1)/(q^m-1)}) \\ &= (\alpha^{(q^{mn}-1)/(q^m-1)})^{(q^m-1)/(q-1)} \\ &= \alpha^{(q^mn-1)/(q-1)} \\ &= N_{E/K}(\alpha) \end{aligned}$$

Discussion 2.30

设 $\{a_1, \ldots, a_m\}$ 是有限域 F 在子域 K 上的一组基，那对于一个元素 $\alpha \in F$, 需要计算系数 $c_j(\alpha) \in K, 1 \leq j \leq m$ 使得

$$\alpha = c_1(\alpha)\alpha_1 + \ldots + c_m(\alpha)\alpha_m$$

注意到 $c_j : \alpha \to c_j(\alpha)$ 是 F 到 K 的线性变换，那么根据 **Theorem 2.24** 就可以知道存在 $\beta_j \in F$ 使得 $c_j(\alpha) = Tr_{F/K}(\beta_j\alpha)$ 对于所有的 $\alpha \in F$ 都成立. 令 $\alpha = \alpha_1$, 那么就有 $Tr_{F/K}(\beta_j\alpha_i) = 0$ 对于 $i \neq j$ 成立，$= 1$ 对于 $i = j$ 成立.

那么 $\{\beta_1, \ldots, \beta_m\}$ 也是一组 F 在 K 上的基，因为对于 $d_i \in K, 1 \leq i \leq m$ 如果有

$$d_1\beta_1 + \ldots + d_m\beta_m = 0$$

那么乘以一个确定值 α_i 并使用 $Tr_{F/K}$ 函数求值，可以得到 $d_i = 0$.

Definition 2.30 Duel Base

设 K 是一个有限域，F 是 K 的一个有限扩张，考虑两组 F 在 K 上的基 $\{\alpha_1, \ldots \alpha_m\}$,$\{\beta_1, \ldots, \beta_m\}$.

如果对于 $1 \leq i, j \leq m$ 有：

$$Tr_{F/K}(\alpha_i\beta_j) = \begin{cases} 0 & \text{for i} \neq \text{j} \\ 1 & \text{for i=j} \end{cases}$$

那么称这两组基为对偶基.

对于任意一组 F 在 K 上的基，都存在一组对偶基，且对偶基是唯一确定的

这是因为根据定义，系数 $c_j(\alpha) = Tr_{F/K}(\beta_j\alpha)$ 根据 **Theorem 2.24** 可知 $\beta_j \in F$ 由线性变换 c_j 唯一确定.

Example 2.31

设 $\alpha \in \mathbb{F}_8$ 是不可约多项式 $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ 的根. 那么 $\{\alpha, \alpha^2, \alpha^4 = \alpha^2 + \alpha + 1\}$ 是 $\mathbb{F}_8$ 在 $\mathbb{F}_2$ 上的一组基.

不难发现它的一组对偶基就是 $\{\alpha, \alpha^2, \alpha^2 + \alpha + 1\}$. 这样的对偶基我们称之为自对偶基.

考虑元素 $\alpha^5 \in \mathbb{F}_8$ 可以由 $\alpha^5 = c_1\alpha + c_2\alpha^2 + c_3(1 + \alpha + \alpha^2)$ 来表示，$c_1, c_2, c_3 \in \mathbb{F}_2$, 那么

$$c_1 = Tr_{\mathbb{F}_8}(\alpha \cdot \alpha^5) = 0$$
$$c_2 = Tr_{\mathbb{F}_8}(\alpha^2 \cdot \alpha^5) = 1$$
$$c_3 = Tr_{\mathbb{F}_8}((1+\alpha+\alpha^2)\alpha^5) = 1$$

所以 $\alpha^5 = \alpha^2 + 1 + \alpha + \alpha^2 = 1 + \alpha$

Definition 2.32 Normal Base

设 $K = \mathbb{F}_q, F = \mathbb{F}_{q^m}$. F 在 K 上有一组形如 $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ 的基.

如果 $\alpha \in F$ 且所有的 K 上的共轭互不相同，那么这组基叫做 F 在 K 上的正规基.

在上例中， $\{\alpha, \alpha^2, \alpha^4 = \alpha^2 + \alpha + 1\}$ 是 $\mathbb{F}_8$ 在 $\mathbb{F}_2$ 上的一组正规基.

Lemma 2.33 Artin Lemma

设 $\phi_1, \ldots, \phi_m$ 是不同的从群 G 到域 F 的乘法群 F^* 的同态，设 $a_1, \ldots, a_m$ 是 F 中的元素，不全为 0.

那么存在 $g \in G$ 使得

$$a_1\phi_1(g) + \ldots + a_m\phi_m(g) \neq 0$$

证明： 对 m 使用归纳法.

当 $m = 1$ 的时候，显然成立.

当 $m > 1$ 的时候，设对于 $m-1$ 以下的情况都成立. 如果 $a_1 = 0$ 根据归纳假设结论成立. 那么设 $a_1 \neq 0$.

假设对于任意 $g \in G$ 都有

$$a_1\phi_1(g) + \ldots + a_m\phi_m(g) = 0 \tag{2.1}$$

因为 $\phi_1 \neq \phi_m$ 所以存在 $h \in G$ 使得 $\phi_1(h) \neq \phi_m(h)$, 那么用 hg 替换 g 代入到式 (2.1) 中，根据同态定义则有

$$a_1\phi_1(h)\phi_1(g) + \ldots + a_m\phi_m(h)\phi_m(g) = 0$$

两边同乘 $\phi_m(h)^{-1}$

$$b_1\phi_1(g) + \ldots + b_{m-1}\phi_{m-1}(g) + a_m\phi_m(g) = 0$$

其中 $b_i = a_i\phi_i(h)\phi_m(h)^{-1}, 1 \leq i \leq m-1$.

与 (2.1) 式子作差得到

$$c_1\phi_1(g) + \ldots + c_{m-1}\phi_{m-1}(g) = 0$$

其中 $c_i = a_i - b_i, 1 \leq i \leq m-1$.

但是 $c_1 = a_1 - a_1\phi_1(h)\phi_m(h)^{-1} \neq 0$, 这和归纳假设矛盾，所以假设不成立.

所以对于 m 个同态的情况也成立，所以结论成立.

Discussion 2.34 Some Concepts of Linear Algebra

设 T 是域 K 上的有限维线性空间 V 上的线性算子，那么称多项式 $f(x)=a_nx^n+\ldots+a_1x+a_0\in K[x]$ 零化**(Annihilate)** T 如果 $a_nT^n+\ldots+a_1T+a_0I=0$ 成立. 其中 I 是单位算子，0 是 V 上的零元.

满足这样性质的最低正次数首一多项式被称为 T 的极小多项式. 这个多项式整除所有的 $K[x]$ 上的零化 T 的多项式.

例如，T 的极小多项式整除 T 的特征多项式 $g(x)=det(xI-T)$, 这个多项式的次数等于 V 的维数.

向量 $\alpha\in V$ 被称为 T 的循环向量，如果向量 $T^k\alpha, k=0,1,\ldots$ 生成 V.

Lemma 2.34

设 T 是有限维线性空间 V 上的一个线性算子，那么 T 拥有循环向量，当且仅当 T 的特征多项式等于其极小多项式.

Theorem 2.35 Normal Basis Theorem

对于任意的有限域 K 与其任意的域扩张 F, 都存在一组 F 在 K 上的正规基.

证明： 设 $K=\mathbb{F}_q, F=\mathbb{F}_{q^m}, m\geq 2$.

根据 **Theorem 2.21** 可知所有的 F 到 K 上的不同的自同构可以表示为 $\epsilon,\sigma,\sigma^2,\ldots,\sigma^{m-1}$, 其中 ϵ 是恒等变换，$\sigma(\alpha)=\alpha^q, \alpha\in F$, σ^j 表示连续进行 j 次 σ 变换.

对于 $\alpha,\beta\in F, c\in K$, 显然有

$$\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$$
$$\sigma(c\alpha)=\sigma(c)\sigma(\alpha)=c\sigma(\alpha)$$

所以 σ 是 F 到 K 上的线性算子.

由于 $\sigma^m=\epsilon$, 所以多项式 $x^m-1\in K[x]$ 零化 ϵ.

根据 **Lemma 2.33**, 把 $\epsilon,\sigma,\sigma^2,\ldots,\sigma^{m-1}$ 看成 F^* 上的满射，可以发现没有 $K[x]$ 上次数小于 m 的非零多项式可以零化 σ.

因此 x^m-1 就是 σ 的极小多项式.

由于其特征多项式可以被极小多项式整除，且特征多项式的次数是 m. 因此特征多项式也是 x^m-1.

Lemma 2.34 意味着存在元素 $\alpha\in F$ 使得 $\alpha,\sigma(\alpha),\sigma^2(\alpha),\ldots,\sigma^{m-1}(\alpha)$ 组成 F 因此也是 F 在 K 上的一组基.

因为它包含了所有 α 关于 K 的共轭，因此这组基是一组正规基.

下面给出一个判别式，用来判断一组给定的元素是否可以构成一个域扩张的基.

Definition 2.36 Discriminant

设 K 是有限域，F 是 K 的域扩张，次数是 m. 那么判别式 $\triangle_{F/K}(\alpha_1,\ldots,\alpha_m)$ 为阶为 m 的行列式，定义如下：

$$\triangle_{F/K}(\alpha_1,\ldots,\alpha_m)=\begin{vmatrix} Tr_{F/K}(\alpha_1\alpha_1) & Tr_{F/K}(\alpha_1\alpha_2) & \cdots & Tr_{F/K}(\alpha_1\alpha_m) \\ Tr_{F/K}(\alpha_2\alpha_1) & Tr_{F/K}(\alpha_2\alpha_2) & \cdots & Tr_{F/K}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ Tr_{F/K}(\alpha_m\alpha_1) & Tr_{F/K}(\alpha_m\alpha_2) & \cdots & Tr_{F/K}(\alpha_m\alpha_m) \end{vmatrix}$$

其中 $\alpha_1,\ldots,\alpha_m\in F$. 这个判别式一定是 K 中的一个元素.

Theorem 2.37

设 K 是有限域，F 是 K 的域扩张，次数是 m. $\alpha_1,\ldots,\alpha_m\in F$.

那么 $\{\alpha_1,\ldots,\alpha_m\}$ 是 F 在 K 上的一组基，当且仅当判别式 $\triangle_{F/K}(\alpha_1,\ldots,\alpha_m)\neq 0$.

证明： 设 $\{\alpha_1,\ldots,\alpha_m\}$ 是 F 在 K 上的一组基. 下面通过证明判别式 $\triangle_{F/K}(\alpha_1,\ldots,\alpha_m)$ 的行向量线性无关，从而证明判别式 $\triangle_{F/K}(\alpha_1,\ldots,\alpha_m)\neq 0$. 假设：

$$c_1Tr_{F/K}(\alpha_1\alpha_j)+\ldots+c_mTr_{F/K}(\alpha_m\alpha_j)=0,$$

其中 $c_1,\ldots,c_m\in K, 1\leq j\leq m$. 那么对于 $\beta=c_1\alpha_1+\ldots+c_m\alpha_m$ 有对于任意的 $1\leq j\leq m$ 有 $Tr_{F/K}(\beta\alpha_j)=0$.

又因为 $\alpha_1,\ldots,\alpha_m$ 形成 F, 所以对于任意的 $\alpha\in F$ 都有 $Tr_{F/K}(\beta\alpha)=0$. 这仅当 $\beta=0$ 时成立，即 $c_1\alpha_1+\ldots+c_m\alpha_m=0$, 即 $c_1=\ldots=c_m=0$. 因此向量组线性无关.

反过来，设判别式 $\triangle_{F/K}(\alpha_1,\ldots,\alpha_m)\neq 0$. 对于 $c_1,\ldots,c_m\in K$ 有 $c_1\alpha_1+\ldots+c_m\alpha_m=0$. 那么

$$c_1\alpha_1\alpha_j+\ldots+c_m\alpha_m\alpha_j=0$$

取迹函数

$$c_1Tr_{F/K}(\alpha_1\alpha_j)+\ldots+c_mTr_{F/K}(\alpha_m\alpha_j)=0$$

但由于判别式的行向量按照定义线性无关，所以 $c_1=\ldots=c_m=0$, 所以 $\alpha_1,\ldots,\alpha_m$ 在 K 上线性无关，所以是一组基.

Corollary 2.38

设 $\alpha_1,\ldots,\alpha_m\in\mathbb{F}_{q^m}$. 那么 $\{\alpha_1,\ldots,\alpha_m\}$ 是 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的一组基，当且仅当

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix}\neq 0$$

Theorem 2.39

对于 $\alpha\in\mathbb{F}_{q^m}$, $\{\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{m-1}}\}$ 是一组 $\mathbb{F}_{q^m}$ 到 $\mathbb{F}_q$ 的正规基，当且仅当：

多项式 x^m-1 和 $\alpha x^{m-1}+\alpha^q x^{m-2}+\ldots+\alpha^{q^{m-2}}x+\alpha^{q^{m-1}}$ 互素.

Theorem 2.40

任意有限域在其素子域上有一组由本原元组成的正规基.

2.4 Roots of Unity and Cyclotomic Polynomials

Definition 2.41 Cyclotomic Field and Root of Unity

设 n 是一个正整数, x^n-1 在 K 上的分裂域被称作 K 上的 n 次分圆域，记作 $K^{(n)}$

x^n-1 在 $K^{(n)}$ 上的根被称为 K 上的 n 次单位根，这些根的集合被记作 $E^{(n)}$.

$$x_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$$

Theorem 2.42

设 K 是特征为 p 的一个域，n 是正整数, 则：

(i) 如果 $p\nmid n$，那么 $E^{(n)}$ 是一个阶为 n 的循环群.

(ii) 如果 $p\mid n$, 令 $n=mp^e$, 其中 m,e 是正整数且 $p\nmid m$. 那么就有 $K^{(n)}=K^{(m)}$, $E^{(n)}=E^{(m)}$, x^n-1 在 $K^{(n)}$ 上的所有根就是 $E^{(m)}$ 中的 m 个元素，这些重根的重数为 p^e.

证明：

(i) $n=1$ 显然成立.

对于 $n\geq 2$. $f(x)=x^n-1$ 和 $f'(x)=nx^{n-1}$ 没有相同的根，所以根据 **Theorem 1.68**, x^n-1 没有重根。

从而 $E^{(n)}$ 中有 n 个元素.

设 $\zeta,\eta\in E^{(n)}$, 那么 $(\zeta\eta^{-1})^n=\zeta^n(\eta^n)^{-1}=1$, 因此 $\zeta\eta^{-1}\in E^{(n)}$. 所以 $E^{(n)}$ 是一个乘法群.

设 n 的因子分解结果为 $n=p_1^{e_1}p_2^{e_2}\dots p_t^{e^t}$, 可以证明一定存在一个元素 $\alpha_i\in E^{(n)}$ 使得这个元素不是多项式 $x^{n/p_i}-1$ 的根.

所以 $\beta_i=\alpha_i^{n/p_i^{e_i}}$ 的阶是 $p_i^{e_i}$, 所以 $E^{(n)}$ 是一个以 $\beta=\beta_1\beta_2\dots\beta_t$ 为生成元的循环群.

上述构造过程和 **Theorem 2.8** 相同

(ii) $x^n-1=x^{mp^e}-1=(x^m-1)^{p^e}$, 然后根据 (i) 结论显然成立.

Definition 2.43 Primitive n-th Root of Unity

设 K 是特征为 p 的一个域，n 是一个不整除 p 的正整数. 那循环群 $E^{(n)}$ 的生成元被称为 K 上的 n 次本原单位根.

K 上的 n 次本原单位根有 $\phi(n)$ 个. 如果其中一个是 ζ, 那其他的原根可以表示成 ζ^s, 其中$1\leq s\leq n$, 且 $gcd(s,n)=1$.

Definition 2.44 Cyclotomic Polynomial

设 K 是特征为 p 的一个域，n 是一个不整除 p 的正整数，ζ 是一个 K 上的 n 次本原单位根，那么多项式

$$Q_n(x)=\prod_{s=1,gcd(s,n)=1}^{n}(x-\zeta^s)$$

被称为 K 上的 n 次分圆多项式.

这个多项式的次数是 $\phi(n)$ 且系数都在 K 的 n 次分圆域上.

Theorem 2.45

设 K 是一个特征为 p 的域，n 是不被 p 整除的正整数，那么：

(i) $x^n-1=\prod_{d|n}Q_d(x)$

(ii) $Q_n(x)$ 的系数都在 K 的素子域上；特别地，如果 $K=\mathbb{Q}$, 那么所有的系数都在 $\mathbb{Z}$ 上.

证明：

(i) 如果 ζ 是 K 上的 n 次本原单位根，ζ^s 是 K 上任意的 n 次单位根，那么 $d=n/\gcd(s,n)$. 即 d 是 ζ^s 在 $E^{(n)}$ 上的阶. 由于

$$x^n-1=\prod_{s=1}^{n}(x-\zeta^s)$$

把 ζ^s 是 K 上的 d 次本原单位根的 $x-\zeta^s$ 求积就可以得到 $x^n-1=\prod_{d|n}Q_d(x)$

(ii) 对 n 使用归纳法. 首先可以发现 $Q_n(x)$ 是一个首一多项式.

$n=1$ 时 $Q_1(x)=x-1$ 结论显然成立.

$n\geq 2$ 时设对于 $1\leq d<n$ 结论都成立，那么根据 (i) 就有 $Q_n(x)=(x^n-1)/f(x), f(x)=\prod_{d|n,d<n}Q_d(x)$.

所以 $f(x)$ 的所有系数也都在 K 的素子域上（或者在 $\mathbb{Z}$ 上）.

那么通过对 x^n-1 和 $f(x)$ 做除法，可以发现 $Q_n(x)$ 的系数也在 K 的素子域上（或者在 $\mathbb{Z}$ 上）.

Example 2.46

设 r 是素数，$k\in\mathbb{N}$. 那么根据 **Theorem 2.45(i)** 可以知道

$$Q_{r^k}(x)=\frac{x^{r^k}-1}{Q_1(x)Q_r(x)\dots Q_{r^{k-1}}(x)}=\frac{x^{r^k}-1}{x^{r^{k-1}}-1}$$

所以

$$Q_r(x)=1+x^{r^{k-1}}+x^{2r^{k-1}}+\dots+x^{(r-1)r^{k-1}}$$

特别地，对于 $k=1$ 有 $Q_r(x)=1+x+x^2+\dots+x^{r-1}$.

Theorem 2.47

分圆域 $K^{(n)}$ 是域 K 的单代数扩张，且：

(i) 若 $K=\mathbb{Q}$, 那么分圆多项式 $Q_n(x)$ 在 K 上不可约，且 $[K^{(n)}:K]=\phi(n)$

(ii) 若 $K=\mathbb{F}_q$ 且 $gcd(q,n)=1$, 则 $Q_n(x)$ 可以分解成 $K[x]$ 上的 $\frac{\phi(n)}{d}$ 个不同的首一多项式，它们的次数都是 d. $K^{(n)}$ 是 K 上的一个分裂域，且 $[K^{(n)}:K]=d$, 其中 d 是满足 $q^d\equiv 1 \mod n$ 的最小正整数.

Example 2.48

设 $K=\mathbb{F}_{11}, Q_{12}(x)=x^4-x^2+1\in\mathbb{F}_{11}$.

那么根据 **Theorem 2.47(ii)** 可以得到次数为满足 $11^d\equiv 1 \mod 12$ 的最小正整数，解得 $d=2$.

分解可以得到 $Q_{12}(x)=(x^2+5x+1)(x^2-5x+1)$, 这两个多项式都是不可约的.

分圆域 $K^{(12)}$ 和 $\mathbb{F}_{121}$ 相等. （由 **Lemma 2.1** 可知）

Theorem 2.49

有限域 $\mathbb{F}_q$ 是其任意一个子域上的 $(q-1)$ 次分圆域.

证明： 多项式 $x^{q-1}-1$ 在 $\mathbb{F}_q$ 上分裂，因为它的根在 $\mathbb{F}_q$ 上都是非零元.

显然这个多项式不能在 $\mathbb{F}_q$ 的任意子域上分裂，所以 $\mathbb{F}_q$ 就是 $x^{q-1}-1$ 在其任意子域上的分裂域. 所以命题成立.

因为 $\mathbb{F}_q^*$ 是一个阶为 $q-1$ 的循环群，那么对于每一个 $q-1$ 的正因子 n 都存在阶为 n 的一个循环子群 $\{1,\alpha,\dots,\alpha^{n-1}\}$

这个循环子群上的所有元素就是 $\mathbb{F}_q$ 的任一子域的 n 次单位根，生成元 α 是 $\mathbb{F}_q$ 的任一子域的 n 次本原单位根.

Lemma 2.50

如果 d 是正整数 n 的因子，$1\le d<n$, 那么只要 $Q_n(x)$ 有定义，就有 $Q_n(x)$ 整除 $(x^n-1)/(x^d-1)$.

证明： 根据 **Theorem 2.45** 可以知道 $Q_n(x)$ 整除

$$x^n-1=(x^d-1)\frac{x^n-1}{x^d-1}$$

因为 d 是 n 的真因子，多项式 $Q_n(x)$ 和 x^d-1 没有公共根，因此 $\gcd(Q_n(x),x^d-1)=1$. 所以命题得证.

2.5 Representation of Elements of Finite Fields

这一节要介绍三种方法，去表示一个有限域 $\mathbb{F}_q$ 中的元素，元素个数 $q=p^n$, 其中 p 是 $\mathbb{F}_q$ 的特征.

Discussion 2.51 Method One

根据 **Theorem 2.10** 可以知道 $\mathbb{F}_q$ 是 $\mathbb{F}_p$ 的代数单扩张.

根据 **Theorem 2.14** 可以知道，如果 f 是一个 $\mathbb{F}_p[x]$ 上的一个 n 次多项式，那么 f 在 $\mathbb{F}_q$ 上存在根 α. 所以就有 $\mathbb{F}_q=\mathbb{F}_p(\alpha)$.

那么根据 **Theorem 1.86**, 每个 $\mathbb{F}_q$ 上的元素可以被唯一表示为 α 在 $\mathbb{F}_p$ 上的次数不超过 n 的多项式.

我们可以把 $\mathbb{F}_q$ 看作剩余类环 $\mathbb{F}_p[x]/(f)$.

Example 2.51 Method One

尝试表示 $\mathbb{F}_9$.

把 $\mathbb{F}_9$ 看成 $\mathbb{F}_3$ 的代数单扩张，次数为 2. 通过向 $\mathbb{F}_3$ 中添加一个 $\mathbb{F}_3$ 上不可约二次多项式的根 α 得到，比如 $f(x)=x^2+1\in\mathbb{F}_3[x]$.

那么 $f(\alpha)=\alpha^2+1=0\in\mathbb{F}_9$. $\mathbb{F}_9$ 中的九个元素可以用 $a_0+a_1\alpha$ 来表示，其中 $a_0,a_1\in\mathbb{F}_3$.

具体来说，$\mathbb{F}_9=\{0,1,2,\alpha,1+\alpha,2+\alpha,2\alpha,1+2\alpha,2+2\alpha\}$.

Discussion 2.52 Method Two

结合 **Theorem 2.47** 和 **Theorem 2.49** 可以得到另一个表示 $\mathbb{F}_q$ 的办法.

因为 $\mathbb{F}_q$ 是 $\mathbb{F}_p$ 上的 $q-1$ 次分圆域，所以可以通过分解分圆多项式 $Q_{q-1}\in\mathbb{F}_p[x]$ 来得到一系列 $\mathbb{F}_p[x]$ 上的不可约多项式，从而构造 $\mathbb{F}_q$. 这些不可约多项式的次数是相同的.

任意一个因子的根都是 $\mathbb{F}_p$ 的 $q-1$ 次本原单位根，从而也是 $\mathbb{F}_q$ 上的本原根. 所以 $\mathbb{F}_q$ 包含了 0 和这个本原根的所有幂次.

Example 2.52 Method Two

还是考虑 $\mathbb{F}_9$ 的构造.

可以发现 $\mathbb{F}_9=\mathbb{F}_3^{(8)}$, 即 $\mathbb{F}_3$ 的八次分圆域. 根据 **Example 2.46** 可以知道 $Q_8(x)=x^4+1\in\mathbb{F}_3[x]$, 分解得

$$Q_8(x)=(x^2+x+2)(x^2+2x+2)$$

设 ζ 是 x^2+x+2 的一个根，那么它就是 $\mathbb{F}_3$ 上的一个八次本原根. 因此所有 $\mathbb{F}_9$ 上的元素都可以用 ζ 的幂次表示，所以

$$\mathbb{F}_9=\{0,\zeta,\zeta^2,\dots,\zeta^8\}$$

考虑这个例子和方法一中的表示法的联系，可以发现 $\zeta=1+\alpha$, 其中 $\alpha^2+1=0$. 这样方法二得到的根就和方法一相同了.

Discussion 2.53 Method Three

第三种表示法需要通过矩阵来表示.

首先给定伴随矩阵的定义. 设首一多项式 $f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}+x^n$, 次数为正，那么伴随矩阵被定义为：

$$A=\begin{pmatrix}0&0&0&\ldots&0&-a_0\\1&0&0&\ldots&0&-a_1\\0&1&0&\ldots&0&-a_2\\\vdots&\vdots&\vdots&&\vdots&\vdots\\0&0&0&\ldots&1&-a_{n-1}\end{pmatrix}$$

这样的矩阵 A 满足 $f(A)=0$. 设 I 是一个 n 阶单位阵，那么 $a_0I+a_1A+\ldots+a_{n-1}A^{n-1}+A^n=0$.

因此，如果 A 是一个 $\mathbb{F}_p$ 上的 n 次不可约首一多项式的伴随矩阵，那么 $f(A)=0$. 因此 A 是 f 的一个根.

F_p 上由 A 表示的次数小于 n 的多项式产生了 $\mathbb{F}_q$ 上元素的表达方式.

Example 2.53 Method Three

仍然考虑 **Example 2.51** 中 $\mathbb{F}_9$ 的表示方法.

设 $f(x)=x^2+1\in\mathbb{F}_3[x]$. 根据定义，伴随矩阵为

$$A=\begin{pmatrix}0&2\\1&0\end{pmatrix}$$

那么域 $\mathbb{F}_9=\{0,I,2I,A,I+A,2I+A,2A,I+2A,2I+2A\}$

通过这种表示方法，有限域内的运算就是正常的矩阵运算，例如：

$$(2I+A)(I+2A)=\begin{pmatrix}2&2\\1&2\end{pmatrix}\begin{pmatrix}1&1\\2&1\end{pmatrix}=\begin{pmatrix}0&1\\2&0\end{pmatrix}=2A$$

用相同的方法，基于分解分圆多项式来表示有限域中元素的方法可以被用来进行矩阵形式的元素表示.

Example 2.54

设 $h(x)=x^2+x+2\in\mathbb{F}_3[x]$ 是分圆多项式 $Q_8\in\mathbb{F}_3[x]$ 上的不可约因子，那么 h 的伴随矩阵是

$$C=\begin{pmatrix}0&1\\1&2\end{pmatrix}$$

那么 $\mathbb{F}_9$ 就可以表示成

$$\mathbb{F}_9=\{0,C,C^2,\ldots,C^9\}$$

运算也是常规的矩阵运算，例如

$$C^6+C=\begin{pmatrix}2&1\\1&1\end{pmatrix}+\begin{pmatrix}0&1\\1&2\end{pmatrix}=\begin{pmatrix}2&2\\2&0\end{pmatrix}=C^3$$

2.6 Wedderburn's Theorem*

Theorem 2.55 Wedderburn's Theorem

每个有限除环都是域

Theorem 2.56-2.58

略过