有限域基础

冯荣权编著

北京大学数学学院

前言

域是一种重要的代数运算系统，可以在其中做加、减、乘、除运算，法国天才数学家 Galois 利用群与域解决了代数方程是否有根式解问题。有限域是含有有限个元素的域，它除了具有一些与我们熟知的有理数域、实数域和复数域同样的性质外，还有很多这些域所不具备的特殊而奇妙的特性。著名数学家 Fermat、Euler、Lagrange、Gauss、Galois 等开启了这些特性的研究，由有限域的这些特性的研究所形成的有限域理论就成为现代代数学的一个重要分支。近几十年来，有限域理论发展迅速，在信息安全、计算机、通信等诸多实际领域有着广泛的应用，已成为这些领域的工程技术人员不可或缺的数学工具。

本书是为北京大学研究生《有限域》课程所编写的讲义，目的是使学生掌握有限域理论的基本知识和方法。全书共分八章，第一章为代数基础，介绍了学习本书所必需的预备知识。第二、三章介绍了有限域的基本性质，包括有限域的群结构、有限域的存在唯一性、迹、范数、基等内容。第四、五、六章介绍了有限域上的多项式，包括分圆多项式、线性化多项式、不可约多项式和置换多项式等，还给出了有限域上多项式的分解算法。第七章介绍了有限域上代数方程的求解方法以及解的个数的估计等。第八章介绍了有限域上的指数和，包括 Gauss 和、Jacobi 和以及它们的一些应用等。

本书力求叙述简洁、推理详细，内容尽可能封闭。可作为数学、计算机、信息安全、通信等专业研究生的教材或教学参考书，也可供信息安全、计算机、通信等实际领域的工程技术人员参考。

在本书的编写过程中, 作者参考了国内外许多有关的书, 讲义和论文, 我们将它们一一列在本书最后的参考文献中。本书中很多章节的内容、例题和习题都并非作者原创, 而是取材于这些参考文献, 在此一并致谢。由于水平所限, 本书难免有错漏与不足, 欢迎读者批评指正。

编者

2022. 2.

目录

前言 **ii**

第一章 代数基础 **1**

1.1 环与域 1
1.2 多项式 4
1.3 域的扩张 10
1.4 Euler ϕ-函数 12
1.5 习题 16

第二章 有限域的性质 **20**

2.1 有限域的群结构 20
2.2 有限域的存在唯一性 24
2.3 极小多项式 28
2.4 有限域中元素的表示 32
2.5 习题 35

第三章 迹, 范数和基 **37**

3.1 迹与范数 37
3.2 基 44
3.3 对偶基 47
3.4 正规基 52
3.5 习题 56

第四章 有限域上的多项式 **59**

4.1 分圆多项式 59
4.2 分解多项式的 Berlekamp 算法 63

4.3 多项式的阶 69
4.4 线性化多项式 75
4.5 习题 84

第五章 有限域上的不可约多项式 87
5.1 有限域上不可约多项式的判定 87
5.2 多项式的复合 96
5.3 多项式的复合乘积 102
5.4 不可约多项式的构作 108
5.5 习题 113

第六章 置换多项式 117
6.1 置换多项式的判定 117
6.2 Dickson 多项式与线性化多项式的置换性质 124
6.3 AGW 准则 133
6.4 习题 140

第七章 有限域上多项式的根 144
7.1 多项式在扩域中的根 144
7.2 解的个数 147
7.3 求根算法 159
7.4 有限域上多项式的分解 168
7.5 二次型 172
7.6 习题 179

第八章 指数和 183
8.1 有限交换群的特征 183
8.2 有限交换群上的离散 Fourier 变换 189
8.3 Gauss 和 196
8.4 Jacobi 和 205
8.5 特征和 213
8.6 两个应用 223
8.7 习题 231

第一章　代数基础

本章给出本书需要的一些基础知识, 这些知识可在大学的《初等数论》、《高等代数》和《抽象代数》课程中学到. 下面用符号 $\mathbb{N}$ 表示自然数 (非负整数) 集合, $\mathbb{Z}$ 表示整数集合, $\mathbb{Q}$ 为有理数集合, $\mathbb{R}$ 为实数集合, $\mathbb{C}$ 为复数集合. 用 $\gcd(s,t)$ 表示整数 (或多项式) s 和 t 的最大公因数 (式), 用 $\mathrm{lcm}(s,t)$ 表示整数 (或多项式) s 和 t 的最小公倍数 (式).

1.1　环与域

设 R 是一非空集合, R 上有两种代数运算, 分别称为加法和乘法, 记为 "$+$" 和 "$\cdot$", 且满足

(1) R 对加法做成交换群, 即 $(R,+)$ 为交换群.

(2) R 对乘法做成幺半群, 即 $(R,\cdot)$ 为幺半群.

(3) 乘法对加法的左右分配律成立, 即对任意 $a,b,c\in R$, 有

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca.$$

则称 R 为一个环.

注意环中乘法不一定满足交换律, 满足乘法交换律的环称为交换环. 另外如上定义规定环中有乘法单位元, 但很多文献 (书籍) 中定义的环不要求这一点. 环中的乘法单位元称为环的单位元, 常记为 1, 而环中加法的零元也称为环的零元素, 记为 0.

设 $R=\{0\}$, 定义 $0+0=0$, $0\cdot 0=0$, 在这两种运算下 R 是一个环, 称这个环为零环, 它有单位元 0. 显然它是交换环.

设 R 是环, 则对任意 $a\in R$, 有 $0a=a0=0$. 这表明, 若环中单位元 $1=0$, 则 $R=\{0\}$. 设 $R\neq\{0\}$, 则 $1\neq 0$, 故环 R 中的 0 是不可逆的. 环中有单位元, 但也并不是环中每个非零元都有逆, 乘法可逆元素称为可逆元 (或单位). 环 R 中所有可逆元在乘法下构成一个群, 称为环 R 的乘法群, 记为 $U(R)$. 若环 R 至少含有 2 个元素且其中每个非零元都可逆, 则称 R 为除环 (或体).

注意环中乘法没有消去律, 即对于 $a,b,c\in R$, $a\neq 0$, $ab=ac$ (或 $ba=ca$), 则不一定有 $b=c$. (群中有消去律是因为群中每个元素都可逆, 但环中并不是每个非零元都可逆) 自然若 a 有逆, 且 $ab=ac$ (或 $ba=ca$), 则 $b=c$. 所以, 除环中的乘法有消去律. 设 H 为除环, $a,b\in H$ 且 $a\neq 0$, 则方程 $ax=b$ 和 $xa=b$ 在 H 中有解, 分别为 $a^{-1}b$ 和 ba^{-1}. (形式上说, 除环中可以做除法)

设 R 为环, $a\neq 0$, $b\neq 0$, 但是 $ab=0$, 则称 a 是 R 的一个左零因子, b 是 R 的一个右零因子. 既为左零因子又为右零因子的元素称为 R 的零因子. 至少含有 2 个元素且没有零因子的交换环称为整环. 整环中有消去律, 事实上, 若 $a\neq 0$ 且 $ab=ac$, 则 $a(b-c)=0$, 由于该环中没有零因子, 所以 $b-c=0$, 即 $b=c$. 容易验证除环中两个非零元素之积一定非零, 即除环没有零因子, 由此也可以得到除环中有消去律.

交换除环称为域. 即域 F 是一个集合, 至少含有 2 个元素, 在 F 中有两个代数运算, 加法 "$+$" 和乘法 "$\cdot$", 且满足 $(F,+)$ 为交换群, $(F^*,\cdot)$ 为交换群, 其中 $F^*=F\setminus\{0\}$, 且乘法对加法的分配律成立. 有限域即元素个数有限的域.

显然 $\mathbb{Q}$, $\mathbb{R}$ 和 $\mathbb{C}$ 在通常数的加法和乘法下构成域, 分别称为有理数域, 实数域和复数域, 它们都是无限域. 但是整数集 $\mathbb{Z}$ 在通常数的加法和乘法下不是域, 而是一个整环.

设 $\mathbb{F}_2=\{0,1\}$, 定义 $0+0=1+1=0$, $0+1=1+0=1$, $0\cdot 0=0\cdot 1=1\cdot 0=0$, $1\cdot 1=1$, 则在这两个运算下, $\mathbb{F}_2$ 成为一个域, 这是一个有限域.

设环 $R\neq\{0\}$, R 的特征为最小正整数 k 使得 $k\cdot 1=0$, 并记为 $k=\mathrm{char}R$, 如果这样的正整数 k 不存在, 则令 $\mathrm{char}R=0$. 显然, $\mathrm{char}R$ 为 R 的单位元 1 在 R 的加法群 $(R,+)$ 中的阶 (当阶有限时), 若 1 在 R 的加法群中的阶无限, 则 $\mathrm{char}R=0$. 设环 R 的特征为正整数 k, 则对任意 $a\in R$ 有

$$k\cdot a=\underbrace{a+a+\cdots+a}_{k\text{ 个}}=a(\underbrace{1+1+\cdots+1}_{k\text{ 个}})=a(k\cdot 1)=a0=0,$$

所以当环的特征为正整数时, 此特征就是环的加法群的方次数 (群中所有元素阶的最小公倍数). 进一步地, 若 $\mathrm{char}R=k>0$, 则对任意 $a\in R$ 和任意正整数 m 满足 $k\mid m$, 我们有 $ma=0$.

例 1.1:

(i) 设正整数 $n>1$, 令 $n\mathbb{Z}:=\{na\mid a\in\mathbb{Z}\}$. 注意到 $n\mathbb{Z}$ 中没有单位元, 故不为环.

(ii) *全矩阵环* $M_n(R)$. 令 $M_n(R)$ 为环 R 上的所有 $n\times n$ 矩阵构成的集合, 它在通常矩阵的加法和乘法下构成环. 其零元素为零矩阵, 单位元为单位矩阵 I, 其特征 $\mathrm{char}M_n(R)=\mathrm{char}R$. 若 $n>1$, 则 $M_n(R)$ 非交换且有零因子.

(iii) *全函数环* R^X. 设 R 为环, X 为一非空集合. 从 X 到 R 的所有映射的集合 R^X 在按点加法和乘法下构成一个环 (对任意 $f,g\in R^X$ 和任意 $x\in X$, $(f+g)(x)=f(x)+g(x)$,

$(fg)(x) = f(x)g(x)$), 容易验证 R^X 交换当且仅当 R 交换且 $\mathrm{char}R^X = \mathrm{char}R$. 一般说来, R^X 有零因子.

(iv) 设 $Q := (\mathbb{R}^4, +, \cdot)$, 加法为分量相加, 乘法定义为

$$(a,b,c,d)\cdot(a',b',c',d') := (aa'-bb'-cc'-dd', ab'+ba'+cd'-dc',$$
$$ac'-bd'+ca'+db', ad'+bc'-cb'+da').$$

记 $1 := (1,0,0,0)$, $i := (0,1,0,0)$, $j := (0,0,1,0)$, $k := (0,0,0,1)$, 则有 $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, 且

$$Q = \{a1 + bi + cj + dk \mid a,b,c,d \in \mathbb{R}\}.$$

所以 Q 可以看成是实数域 $\mathbb{R}$ 上的 4-维向量空间, 其元素称为四元数. $(Q,+,\cdot)$ 是一个除环, 称为*四元数除环*, 它不是域. $(\{\pm 1, \pm i, \pm j, \pm k\}, \cdot)$ 是一个 8 阶群, 称为*四元数群*.

□

定理 1.1: 我们有如下结论:

(i) 有限整环是域.

(ii) 有限除环是域 (Wedderburn 定理).

(iii) 整环的特征为 0 或为素数.

(iv) 域是整环.

(v) 有限域的特征为素数.

□

定理 1.2: 设 R 是交换环, 其特征为素数 p, 则对任意 $a_1, a_2, \ldots, a_k \in R$ 和任意 $n \in \mathbb{N}$, 有

$$(a_1 + a_2 + \cdots + a_k)^{p^n} = a_1^{p^n} + a_2^{p^n} + \cdots + a_k^{p^n}.$$

□

设 R 是环, 若 S 是 R 的加法子群 (即对任意 $x, y \in S$ 有 $x - y \in S$), 且对任意 $r \in R$ 有 $Sr = \{xr \mid x \in S\} \subseteq S$ 及 $rS = \{rx \mid x \in S\} \subseteq S$, 则称 S 是 R 的一个理想. 设 S 为环 R 的理想, 若 R 的单位元 $1 \in S$, 则有 $S = R$. 进一步地, 若理想 S 中含有可逆元, 则也必有 $S = R$. 所以环的非平凡理想一定不含有可逆元.

设 R 为交换环, 取定 $a \in R$, 容易验证 $aR = \{ar \mid r \in R\}$ 为 R 的理想. 称其为由元素 a 生成的主理想, 记为 (a).

设 S 为环 R 的理想, 自然是 R 的加法子群. 又 R 的加法群为交换群, 所以 S 为 R 的加法正规子群, 这样就有加法商群 R/S, 这是对 S 的加法陪集的加法群, 即 $R/S = \{a + S \mid a \in R\}$, 其加法为 $(a+S)+(b+S) = (a+b)+S$. 在 R/S 中定义乘法 $(a+S)(b+S) = ab+S$, 它确实为 R/S 中的运算. 事实上, 若有 $a + S = a' + S$, $b + S = b' + S$, 其中 $a, a', b, b' \in R$, 则有 $a - a' \in S$, $b - b' \in S$, 所以 $ab - a'b' = a(b-b') + (a-a')b' \in S$ (这里用到 S 为理想这个假

设), 故 $ab+S=a'b'+S$, 即前面定义的乘法与代表元选取无关. 这样, R/S 作为 R 的加法群的商群已有加法, 又有上面定义的乘法. 容易验证在这两种运算下, R/S 是一个环, 其中的单位元为 $1+S$, 称为 R 对 S 的商环.

整数环 $\mathbb{Z}$ 的每个理想都是它的加法子群, 必为循环群, 所以 $\mathbb{Z}$ 的每个理想都是主理想. 设 n 为正整数, 商环 $\mathbb{Z}/(n)$ 称为整数模 n 的剩余类环, 记为 $\mathbb{Z}_n$, 它的乘法群即整数模 n 的乘法群 $U(n)$, 此群的阶为 $\phi(n)$, 即 $<n$ 且与 n 互素的非负整数的个数.

设 R 是交换环, P 是 R 的理想, $P\neq R$, 如果对于任意 $a,b\in R$, 若 $ab\in P$, 则有 $a\in P$ 或者 $b\in P$, 则称 P 为 R 的素理想.

设 R 是环 (不一定交换), M 是 R 的理想且 $M\neq R$, 对任意 R 的理想 N, 若有 $M\subseteq N$, 必有 $N=M$ 或者 $N=R$, 则称 M 为 R 的极大理想. 所以极大理想即没有真包含它的非平凡理想.

定理 1.3: 设 R 是交换环, S 是 R 的理想, 则有

(i) S 为 R 的素理想当且仅当 R/S 是整环.

(ii) S 为 R 的极大理想当且仅当 R/S 是域.

(iii) R 的极大理想一定为素理想.

□

定理 1.4: 我们有如下结论:

(i) 整数环 $\mathbb{Z}$ 为主理想整环, 其理想 $M=(n)$ 为极大理想当且仅当 n 为素数.

(ii) 整数模 n 的剩余类环 $\mathbb{Z}_n$ 是域当且仅当 n 为素数.

(iii) 设 p 为素数, 则存在 p 元有限域.

□

注意到前面的有限域 $\mathbb{F}_2$ 就是 $\mathbb{Z}_2$.

环同态基本定理: 设 R,R' 是环, $\varphi:R\to R'$ 为环同态, 令 $K=\mathrm{Ker}\varphi$, 则 $R/K\cong\varphi(R)$. □

设 R 为特征为 n 的环 (n 为 0 或正整数), 则 $\varphi:\mathbb{Z}\to R$, $m\mapsto m\cdot 1$ 为环同态, 又显然有 $\mathrm{Ker}\varphi=(n)$, 由环同态基本定理有嵌入 $\mathbb{Z}_n\hookrightarrow R$, 所以特征为 0 的环包含整数环 $\mathbb{Z}$, 特征为正整数 n 的环包含整数模 n 的剩余类环 $\mathbb{Z}_n$. 特别地, 设 F 为域, 若 $\mathrm{char}F=0$, 则 F 包含 $\mathbb{Z}$, 从而也包含 $\mathbb{Z}$ 的分式域 $\mathbb{Q}$, 若 $\mathrm{char}F=p$, p 为素数, 则 F 包含 p 元域 $\mathbb{Z}_p$. 有理数域 $\mathbb{Q}$ 和素数 p 元域 $\mathbb{Z}_p$ 是素域, 即不含有其它真子域的域.

1.2 多项式

设 R 是一个环, x 是 R 上的一个不定元, 对任意 $a_0,a_1,\ldots,a_n\in R$, 称表达式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

为 R 上的一个多项式, a_ix^i 称为此多项式的 i 次项, a_i 为其系数, $0 \le i \le n$. 所有系数均为 0 的多项式称为零多项式, 也记为 0. 设 $f(x) \neq 0$, 定义 $f(x)$ 的次数为 $f(x)$ 中系数非零的最高项的次数, 记为 $\deg f(x)$, 此次数最高的项也称为多项式的首项, 首项系数为 1 的多项式称为首一多项式. 规定零多项式的次数为 $-\infty$. 对于多项式 $f(x) = \sum_{i=0}^{n} a_ix^i$ 和 $g(x) = \sum_{i=0}^{m} b_ix^i$, $f(x) = g(x)$ 当且仅当 $m = n$, 且对所有 $0 \le i \le n$ 都有 $a_i = b_i$. 用 $R[x]$ 表示环 R 上的所有多项式构成的集合, 对于 $f(x) = \sum_{i=0}^{n} a_ix^i$, $g(x) = \sum_{i=0}^{m} b_ix^i \in R[x]$, 不妨设 $n \ge m$, 定义

$$f(x) + g(x) = \sum_{i=0}^{n}(a_i + b_i)x^i, \quad f(x)g(x) = \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_ib_j\right)x^k,$$

其中在多项式加法定义时, 若 $i > m$, 则定义 $b_i = 0$. 在这样的加法、乘法运算下, $R[x]$ 为一个环, 称为环 R 上的一元多项式环.

容易验证 $R[x]$ 为交换环当且仅当 R 交换. 又显然有

$$\begin{aligned} \deg(f(x) + g(x)) &\le \max(\deg f(x), \deg g(x)), \\ \deg(f(x)g(x)) &\le \deg f(x) + \deg g(x). \end{aligned}$$

进一步地, 若环 R 为整环, 则 $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$, 从而 $R[x]$ 也是整环. 还可以证明若环 R 为唯一因式分解整环, 则 $R[x]$ 也是唯一因式分解整环 (证明并不平凡).

下面只考虑域上的多项式. 设 F 是一个域, $f(x), g(x) \in F[x]$, 如果存在 $h(x) \in F[x]$ 使得 $f(x) = g(x)h(x)$, 则称 $g(x)$ 整除 $f(x)$ (或者称 $f(x)$ 可被 $g(x)$ 整除), 记作 $g(x) \mid f(x)$. 这时也说 $g(x)$ 是 $f(x)$ 的因式 (或者说 $f(x)$ 是 $g(x)$ 的倍式). 若 $g(x)$ 不整除 $f(x)$ (或者 $f(x)$ 不能被 $g(x)$ 整除), 则记作 $g(x) \nmid f(x)$.

对于域上的一元多项式, 我们有下面的带余除法.

定理 1.5: 设 $g(x) \neq 0$ 是 $F[x]$ 中一个多项式, 则对任意 $f(x) \in F[x]$, 存在唯一多项式 $q(x), r(x) \in F[x]$, 使得

$$f(x) = q(x)g(x) + r(x), \quad \text{且} \quad \deg r(x) < \deg g(x).$$

□

例 1.2: 设 $f(x) = 2x^5 + x^4 + 4x + 3$, $g(x) = 3x^2 + 1 \in \mathbb{Z}_5[x]$, 利用长除容易得到 $q(x) = 4x^3 + 2x^2 + 2x + 1$, $r(x) = 2x + 2$. □

环 $F[x]$ 中存在带余除法可推出 $F[x]$ 为欧氏环, 从而为主理想整环.

定理 1.6: 设 J 为 $F[x]$ 的一个非零理想, 则存在唯一的首一多项式 $p(x) \in F[x]$, 使得 $J = (p(x))$. □

设 $f(x), g(x) \in F[x]$, 若 $h(x) \mid f(x)$ 且 $h(x) \mid g(x)$, 则称 $h(x)$ 是 $f(x)$ 和 $g(x)$ 的公因式. 若 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的公因式, 且 $f(x)$ 和 $g(x)$ 的每个公因式都整除 $d(x)$, 则称 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的最大公因式. 显然两个零多项式的最大公因式依然为 0, 而不全为 0 的两个多项式 $f(x)$ 和 $g(x)$ 的首一最大公因式唯一, 记作 $\gcd(f(x), g(x))$. 设 $f(x), g(x) \in F[x]$, 不全为 0, 则 $J = (f(x)) + (g(x))$ 依然为 $F[x]$ 的理想且 $J \neq 0$, 所以存在唯一的首一多项式 $d(x) \in F[x]$

使得 $(f(x))+(g(x))=(d(x))$. 显然 $d(x)=\gcd(f(x),g(x))$ 且存在 $u(x)$, $v(x)\in F[x]$ 使得 $d(x)=u(x)f(x)+v(x)g(x)$. 给定两个非零多项式 $f(x)$ 和 $g(x)$, 利用辗转相除 (或称为 Euclid 算法) 可以求出它们的最大公因式 $d(x)$ 和如上的多项式 $u(x)$, $v(x)$. 若 $\gcd(f(x),g(x))=1$, 则称多项式 $f(x)$ 和 $g(x)$ 互素. 类似地可以定义多个多项式的最大公因式, 也有类似的性质.

显然环 $F[x]$ 中的可逆元为所有次数为 0 的多项式, 即 $U(F[x])=F^*$. 设 $p(x)\in F[x]$, $\deg p(x)\geq 1$, 若 $p(x)$ 不能写成 $p(x)=a(x)b(x)$ 的形式, 其中 $a(x)$, $b(x)$ 都是 $F[x]$ 中的不可逆元, 则称 $p(x)$ 为不可约多项式, 或称 $p(x)$ 在域 F 上不可约, 否则称为可约多项式 (域 F 上的不可约多项式即整环 $F[x]$ 中的不可约元). 显然一个多项式是否可约与考虑的域有关, 例如 $p(x)=x^2-2$ 在有理数域 $\mathbb{Q}$ 上不可约, 但在实数域 $\mathbb{R}$ 上可约. 设 $p(x)$ 在域 F 上不可约, 则对任意 $f(x)\in F[x]$ 有 $p(x)\mid f(x)$ 或者 $p(x)$ 与 $f(x)$ 互素. 注意到不可约多项式也是整环 $F[x]$ 中的素元, 即若 $p(x)$ 不可约且对 $f(x),g(x)\in F[x]$ 有 $p(x)\mid f(x)g(x)$, 则 $p(x)\mid f(x)$ 或者 $p(x)\mid g(x)$.

定理 1.7: 设 $f(x)\in F[x]$, $\deg f(x)\geq 1$, 则 $f(x)$ 有如下分解

$$f(x)=ap_1(x)^{e_1}p_2(x)^{e_2}\cdots p_k(x)^{e_k}, \tag{1.1}$$

其中 $a\in F^*$, $p_1(x),p_2(x),\ldots,p_k(x)$ 是 $F[x]$ 中互不相同的首一不可约多项式, $e_1,e_2,\ldots,e_k$ 为正整数. 进一步地, 如上分解式除因式次序外是唯一的. □

定理 1.7 称为域上多项式的唯一因式分解定理, 其中的式 (1.1) 称为多项式 $f(x)$ 的标准分解式. 后面我们会给出有限域上多项式的分解方法.

设 $f(x),g(x)\in F[x]$, $f(x)\neq 0$, $\deg g(x)\geq 1$, 若 $g(x)^2\mid f(x)$, 则称 $g(x)$ 为 $f(x)$ 的重因式. 进一步地, 若 $g(x)^m\mid f(x)$ 但是 $g(x)^{m+1}\nmid f(x)$, 则称 $g(x)$ 为 $f(x)$ 的 m-重因式. 为判断多项式有无重因式, 我们需要多项式的形式微商.

设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, 称 $f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+2a_2x+a_1$ 为 $f(x)$ 的形式微商. 容易证明, 对任意 $f(x),g(x)\in F[x]$, $c\in F$, m 为正整数, 有 $(f(x)+g(x))'=f'(x)+g'(x)$, $(cf(x))'=cf'(x)$, $(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$, $(f(x)^m)'=mf(x)^{m-1}f'(x)$.

若域 F 的特征为 0 或者若 F 的特征为素数 p 且 $F^p:=\{a^p\mid a\in F\}=F$, 则称 F 为完全 (perfect) 域.

定理 1.8: 设 F 为完全域, $f(x)\in F[x]$, $\deg f(x)\geq 1$, 则 $f(x)$ 有重因式当且仅当 $f(x)$ 与 $f'(x)$ 不互素.

证明: 设 $f(x)$ 有重因式 $g(x)$, 则 $f(x)=g(x)^2h(x)$, 所以

$$f'(x)=2g(x)g'(x)h(x)+g(x)^2h'(x),$$

故 $g(x)\mid\gcd(f(x),f'(x))$. 由于 $\deg g(x)\geq 1$, $f(x)$ 与 $f'(x)$ 不互素.

反之, 设 $f(x)$ 与 $f'(x)$ 不互素, 令 $d(x)=\gcd(f(x),f'(x))$, 则 $\deg d(x)\geq 1$. 设 $p(x)$ 为 $d(x)$

的一个不可约因式并记 $f(x)=p(x)q(x)$, 则

$$f'(x)=p'(x)q(x)+p(x)q'(x),$$

所以 $p(x)\mid p'(x)q(x)$. 由于 F 为完全域, $p(x)$ 不可约, 所以 $p'(x)\neq 0$, 又 $\deg p'(x)<\deg p(x)$, 所以 $p(x)\nmid p'(x)$. 由 $p(x)\mid p'(x)q(x)$ 可得 $p(x)\mid q(x)$, 故 $p(x)^2\mid f(x)$, 即 $f(x)$ 有重因式. □

由证明容易看出定理 1.8 的必要性对任意域上的多项式都成立, 所以对任意域 F 上的多项式 $f(x)$, 若 $f(x)$ 与 $f'(x)$ 互素, 则 $f(x)$ 无重因式. 注意定理 1.8 的充分性对非完全域是不对的. 又容易验证任意有限域都是完全域.

设 E 为 F 的扩域, $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$, $b\in E$, 令 $f(b)=a_nb^n+a_{n-1}b^{n-1}+\cdots+a_1b+a_0$, 称其为 x 用 b 的代入. 显然 $f(b)\in E$, 故每个多项式 $f(x)\in F[x]$ 都给出 E 到自身的映射 $b\mapsto f(b)$, 这时也称 $f(x)$ 是域 E 上的一个多项式函数.

设 $f(x)\in F[x]$, $b\in E$, 若 $f(b)=0$, 则称 b 为 $f(x)$ (在 E 中) 的根或零点.

定理 1.9: 设 $f(x)\in F[x]$, 则 $b\in F$ 为 $f(x)$ 的根当且仅当 $x-b\mid f(x)$. □

显然, 设 $f(x)\in F[x]$, $\deg f(x)=2$ 或 3, 则 $f(x)$ 在 F 上不可约当且仅当 $f(x)$ 在 F 中无根. 设 $f(x)\in F[x]$, $b\in F$, m 为正整数, 若 $(x-b)^m\mid f(x)$ 但是 $(x-b)^{m+1}\nmid f(x)$, 称 m 为根 b 的重数, 若 $m=1$, 则称 b 为 $f(x)$ 的单根, 若 $m\geq 2$, 则称 b 为 $f(x)$ 的重根.

定理 1.10: 设 $f(x)\in F[x]$, $\deg f(x)\geq 1$, 则 $b\in F$ 为 $f(x)$ 的重根当且仅当 b 为 $\gcd(f(x),f'(x))$ 的根.

证明: 必要性显然, 下证充分性. 设 b 为 $\gcd(f(x),f'(x))$ 的根, 则有 $x-b\mid f(x)$, 记 $f(x)=(x-b)h(x)$, 则

$$f'(x)=h(x)+(x-b)h'(x),$$

由 $x-b\mid f'(x)$, 有 $x-b\mid h(x)$, 所以 $(x-b)^2\mid f(x)$, 即 b 为 $f(x)$ 的重根. □

定理 1.11: 设 $f(x)\in F[x]$, $\deg f(x)=n\geq 1$, 则 $f(x)$ 在 F 中有至多 n 个根, 其中根的个数包括重数.

证明: 对 n 作归纳. 若 $n=1$, 则 $f(x)=ax+b$, $a\neq 0$, 它在 F 中有 1 个根 $-b/a$. 设 $n\geq 2$, 若 $f(x)$ 在 F 中无根, 我们已证. 若 $f(x)$ 有根 $\alpha\in F$, 则有 $f(x)=(x-\alpha)g(x)$. 显然 $f(x)$ 的根或为 α 或为 $g(x)$ 的根. 由于 $g(x)$ 的次数为 $n-1$, 由归纳假设, $g(x)$ 在 F 中有至多 $n-1$ 个根, 从而 $f(x)$ 在 F 中有至多 n 个根. □

注意此定理对一般环上的多项式不成立, 例如 x^2-1 在环 $\mathbb{Z}_8$ 中有 4 个根 $\overline{1},\overline{3},\overline{5},\overline{7}$. 这是因为域上的一元多项式环 $F[x]$ 是唯一因式分解整环而 $\mathbb{Z}_8[x]$ 并不是. 设 E 是 F 的扩域, $f(x)\in F[x]$, 则 $f(x)$ 也可视为 E 上的多项式, 所以任一 n 次多项式在它扩域中的根的个数至多有 n 个. 对于域 F, 把 F 上的所有多项式的根放在一起组成集合 Ω, 则 Ω 做成一个域, 称其为 F 的代数闭包. 所以 F 上任一 n 次多项式在 F 的代数闭包中恰有 n 个根. 由定理 1.10, 得到对于 $f(x)\in F[x]$, $\deg f(x)\geq 1$, 则 $f(x)$ 在 F 的代数闭包中有重根当且仅当 $f(x)$ 与 $f'(x)$

不互素.

注意到多项式的因式与对应的域有关, 而多项式的根通常指在扩域中的根, 所以多项式有无重因式与其有无重根是有区别的. 显然有重因式的多项式一定有重根, 但反之不一定成立.

定理 1.12: 设 $n \geq 0$, $a_0, a_1, \ldots, a_n$ 是域 F 中 $n+1$ 个互异元素, 则对 F 中任意 $n+1$ 个元素 $b_0, b_1, \ldots, b_n$ (可以相同), 存在唯一的多项式 $f(x) \in F[x]$, 使得 $\deg f(x) \leq n$ 且 $f(a_i) = b_i$, $i = 0, 1, \ldots, n$. □

进一步地, 定理 1.12 中的多项式可以得出, 即为

$$f(x) = \sum_{i=0}^{n} b_i \frac{(x-a_0)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_0)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)},$$

这称为 Lagrange 插值公式. 由此定理可知, 若 F 为 q 元域, 则任一 F 到其自身的映射都可以用一个次数小于 q 的多项式来唯一表示.

设 $f(x) \in F[x]$ 非零, 考虑商环 $F[x]/(f(x))$, 首先 $a \mapsto a + (f(x))$ 是 F 到 $F[x]/(f(x))$ 的一个单同态, 即嵌入, 所以 F 为 $F[x]/(f(x))$ 的子环 (域). 另外, 环 $F[x]/(f(x))$ 中每一元素形如 $\overline{g(x)} = g(x) + (f(x))$. 由于对于 $g_1(x) \neq g_2(x)$, 可能有 $\overline{g_1(x)} = \overline{g_2(x)}$, 那么怎样选取每个陪集 $\overline{g(x)}$ 的代表元呢? 设多项式 $f(x)$ 的次数为 n, 对任意 $g(x) \in F[x]$, 做带余除法 $g(x) = q(x)f(x) + r(x)$, 其中 $r(x)$ 的次数小于 n, 则有 $\overline{g(x)} = \overline{r(x)}$, 这说明每个陪集都可用一个次数小于 n 的多项式作为代表元. 若 $r_1(x)$, $r_2(x)$ 的次数都小于 n, 且 $\overline{r_1(x)} = \overline{r_2(x)}$, 则有 $f(x)$ 整除 $r_1(x) - r_2(x)$, 又 $r_1(x) - r_2(x)$ 的次数小于 n, 所以 $r_1(x) = r_2(x)$. 这表明若要求陪集代表元的次数小于 n, 则代表元是唯一的. 所以, $F[x]/(f(x)) = \{\overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}} \mid a_i \in F\}$. 若 F 为无限域, 则商环 $F[x]/(f(x))$ 中有无限个元素. 若 F 为有限域, 设 $|F| = q$, 则 $|F[x]/(f(x))| = q^n$, 即 $F[x]/(f(x))$ 是一个有限环.

定理 1.13: 设 $f(x) \in F[x]$, 则 $(f(x))$ 为 $F[x]$ 的极大理想当且仅当 $f(x)$ 在 F 上不可约, 从而商环 $F[x]/(f(x))$ 是域当且仅当 $f(x)$ 在 F 上不可约. □

设 $f(x) \in F[x]$ 不可约, 则当 $\deg f(x) \geq 2$ 时, $f(x)$ 在 F 中无根, 但是 $f(x)$ 在 F 的扩域 $F[x]/(f(x))$ 中有根, 例如 $x + (f(x))$ 就是它的一个根. 由此我们有域论基本定理 (Kronecker 定理)：设 F 为域, $f(x) \in F[x]$, $\deg f(x) \geq 1$, 则存在 F 的扩域 E 使得 $f(x)$ 在 E 中有根. 进一步地, 由于整环包含在它的分式域中, 所以系数在一个整环中的非常数多项式也一定在此整环的某个扩域中有根. 但此结论对一般的交换环并不成立, 例如, $f(x) = 2x + 1 \in \mathbb{Z}_4[x]$ 在包含 $\mathbb{Z}_4$ 的任一环中无根.

例 1.3: 取 $F = \mathbb{R}$, $p(x) = x^2 + 1$, 则 $p(x)$ 在实数域上不可约, 故 $\mathbb{R}[x]/(p(x))$ 是域. 这时 $\mathbb{R}[x]/(p(x))$ 中元素形如 $\overline{a + bx}$, 其中 $a, b \in \mathbb{R}$. 加法为

$$\overline{a + bx} + \overline{a' + b'x} = \overline{(a + a') + (b + b')x}.$$

乘法为

$$\overline{a + bx} \cdot \overline{a' + b'x} = \overline{aa' + (ab' + a'b)x + bb'x^2}. \tag{1.2}$$

但是式 (1.2) 右边的多项式次数为 2 (除非 b 或 b' 为 0), 我们需要选择次数小于 2 的多项式作为它的代表元. 注意到 $\overline{x^2} = \overline{-1}$, 我们可以得到其乘法为

$$\overline{a+bx} \cdot \overline{a'+b'x} = \overline{(aa'-bb') + (ab'+a'b)x}.$$

容易验证 $\overline{a+bx} \mapsto a+bi$ 是 $\mathbb{R}[x]/(p(x))$ 到复数域 $\mathbb{C}$ 的一个同构, 所以 $\mathbb{R}[x]/(p(x))$ 就是复数域. □

下面我们取 F 为有限域 $\mathbb{Z}_p$. 这种类型的构造是理解有限域的关键, 后面我们会证明任一非素数个元素的有限域都可以这样得到.

例 1.4: 设 $F = \mathbb{Z}_2$, $p(x) = x^3 + x + 1$. 由于 $p(x)$ 次数为 3, $p(0) = p(1) \neq 0$, 即 $p(x)$ 在 $\mathbb{Z}_2$ 中无根, 所以 $p(x)$ 在 $\mathbb{Z}_2$ 上不可约.

因为 $p(x)$ 次数为 3, $\mathbb{Z}_2[x]/(p(x))$ 中元素形如 $a_2x^2 + a_1x + a_0$, $a_i \in \mathbb{Z}_2$ (为了简单起见, 我们去掉了陪集表示符号上面的横线), 它也可以表示为 $\mathbb{Z}_2$ 上的 3-维向量 (a_2, a_1, a_0). 其加法就是通常的分量相加, 其乘法如何? 首先我们做相应的多项式乘法如下:

$$\begin{aligned}&(a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0) = a_2b_2x^4 + (a_2b_1 + a_1b_2)x^3 \\ &+(a_2b_0 + a_1b_1 + a_0b_2)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0.\end{aligned} \tag{1.3}$$

注意到

$$x^3 \equiv x + 1 \pmod{x^3 + x + 1} \qquad \text{和} \qquad x^4 \equiv x^2 + x \pmod{x^3 + x + 1}.$$

所以 $a_2b_2x^4 \equiv a_2b_2x^2 + a_2b_2x$, $(a_2b_1 + a_1b_2)x^3 \equiv (a_2b_1 + a_1b_2)x + (a_2b_1 + a_1b_2)$. 记 $(a_2, a_1, a_0) \cdot (b_2, b_1, b_0) = (c_2, c_1, c_0)$, 则有

$$\begin{cases} c_2 &= a_2b_2 + a_2b_0 + a_1b_1 + a_0b_2, \\ c_1 &= a_2b_2 + a_2b_1 + a_1b_2 + a_1b_0 + a_0b_1 \\ c_0 &= a_2b_1 + a_1b_2 + a_0b_0. \end{cases} \tag{1.4}$$

这个乘法法则既不简单也不显然, 但由定理 1.7, 我们确实把 $\mathbb{Z}_2$ 上的 3-维向量空间做成一个域, 此域含 8 个元素, 是非素数个元素的有限域.

为简化乘法, 下面看此 8 元域中元素的另一种表示, 首先计算 x 的方幂模去多项式 $p(x) = x^3 + x + 1$: $x^0 \equiv 1$, $x^1 \equiv x$, $x^2 \equiv x^2$, $x^3 \equiv x + 1$, $x^4 \equiv x^2 + x$, $x^5 \equiv x^3 + x^2 \equiv x^2 + x + 1$, $x^6 \equiv x^3 + x^2 + x \equiv x^2 + 1$, $x^7 \equiv x^3 + x \equiv 1$. 这表明此域中的 7 个非零元素都是 $x \pmod{p(x)}$ 的方幂, 记陪集 $\overline{x}$ 为元素 α, 作为 3-维向量, $\alpha = (0, 1, 0)$. 所以我们有

$$\begin{aligned}&\alpha^0 \equiv 1, \qquad &&\alpha^1 \equiv \alpha, \qquad &&\alpha^2 \equiv \alpha^2, \qquad &&\alpha^3 \equiv \alpha + 1 \\ &\alpha^4 \equiv \alpha^2 + \alpha, \quad &&\alpha^5 \equiv \alpha^2 + \alpha + 1, \quad &&\alpha^6 \equiv \alpha^2 + 1, \quad &&\alpha^7 \equiv 1.\end{aligned}$$

我们利用以 α 为底的对数, $\log_\alpha \beta = k$ 意为 $\alpha^k = \beta$, 我们得到下面的对数表和指数表 (依然用

$\mathbb{Z}_2$ 上的 3-维向量表示此 8 元域中的元素):

β	$\log_\alpha \beta$
000	-
001	0
010	1
011	3
100	2
101	6
110	4
111	5

和

k	α^k
-	000
0	001
1	010
2	100
3	011
4	110
5	111
6	101

这样我们可以容易计算域中两个元素的乘积, 例如计算 $a \cdot b = (110) \cdot (111)$, 由于 $\log_\alpha a = 4$, $\log_\alpha b = 5$, 所以 $a \cdot b = \alpha^4 \cdot \alpha^5 = \alpha^9 = \alpha^2 = (100)$. □

1.3 域的扩张

设 E 是域, $F \subseteq E$, 若 F 在 E 的运算下也成为域, 则称 F 为 E 的子域, 而 E 称为 F 的扩域, 简记为 E/F. 显然, F 为 E 的子域当且仅当对任意 $x, y \in F$, $y \neq 0$, 有 $x - y, xy^{-1} \in F$. 不包含任何真子域的域称为素域. 若 $\mathrm{char}F = 0$, 则 F 的素子域为有理数域 $\mathbb{Q}$, 若 $\mathrm{char}F = p$, 则 F 的素子域为有限域 $\mathbb{Z}_p$.

设 E 是 F 的扩域, E 中有加法, 也有乘法, 把 F 对 E 的乘法看成 F 对 E 的数量乘法, 则 E 自然地成为 F 上的线性空间. 以 $[E : F]$ 表示 E 作为 F 上线性空间的维数, 称为 E 对 F 的扩张次数. 若 $[E : F] = \infty$, 则 E 称为 F 的无限次扩域, 若 $[E : F] = n$, 则称 E 为 F 的有限次 (n 次) 扩域.

定理 1.14: 设 $F \subset H \subset E$ 是域扩张, 则 $[E : F] = [E : H][H : F]$. 所以若 E/F 是有限次扩张, 则 H/F 和 E/H 也都是有限次扩张且 $[H : F]$ 和 $[E : H]$ 都整除 $[E : F]$. □

设 E 是 F 的扩域, 任取 $\alpha \in E$, 则 E 的包含 F 和 α 的最小子域是什么? 因为 E 本身就是一个包含 F 和 α 的子域, 所以这样的域是存在的. 显然, 它是 E 的所有包含 F 和 α 的子域的交, 故这个最小的域又是唯一的, 用 $F(\alpha)$ 来表示这个域. 显然 $F(\alpha)$ 对 F 中的元素和 α 的所有可能的有限次加、减、乘、除 (除数不为 0) 封闭, 所以形如 $\frac{f_1(\alpha)}{f_2(\alpha)}$ 的元素一定属于 $F(\alpha)$, 其中 $f_1(x), f_2(x) \in F[x]$, $f_2(\alpha) \neq 0$. 又容易验证

$$\left\{ \frac{f_1(\alpha)}{f_2(\alpha)} \mid f_1(x), f_2(x) \in F[x], f_2(\alpha) \neq 0 \right\}$$

是一个 E 的包含 F 和 α 的子域, 所以

$$F(\alpha) = \left\{ \frac{f_1(\alpha)}{f_2(\alpha)} \mid f_1(x), f_2(x) \in F[x], f_2(\alpha) \neq 0 \right\},$$

这表明 $F(\alpha)$ 中的元素就是由 F 中的元和 α 的所有可能的有限次加、减、乘、除 (除数不为 0) 运算所得到. $F(\alpha)$ 称为 F 的一个单扩张.

设 $F \subset E$ 是域扩张, $\alpha \in E$, 若 α 是 F 上某一个非零多项式的根, 则称 α 为 F 上的代数元, 否则称为 F 上的超越元. 例如 $\sqrt{2}, \sqrt[5]{3}$ 都是有理数域 $\mathbb{Q}$ 上的代数元, 而 π, e 是 $\mathbb{Q}$ 上的超越元. 若 E 中每个元素都是 F 上的代数元, 则称 E 是 F 的代数扩张. 容易证明有限次扩张都是代数扩张.

设 $\alpha \in E$ 为 F 上的代数元, 则存在 $f(x) \in F[x]$, $f(x) \neq 0$ 使得 $f(\alpha) = 0$. 取以 α 为根的次数最低的首一多项式 $p(x)$, 则 $p(x)$ 不可约, 称多项式 $p(x)$ 为 α 在域 F 上的极小多项式. 由带余除法容易证明, 对任意 $f(x) \in F[x]$, 若 α 为 $f(x)$ 的根, 则 $p(x) \mid f(x)$, 所以 α 在域 F 上的极小多项式唯一, 而极小多项式 $p(x)$ 的次数也称为 α 在域 F 上的次数, 也记为 $\deg\alpha$. 事实上域 F 上所有以 α 为根的多项式构成的集合 $S = \{f(x) \in F[x] \mid f(\alpha) = 0\}$ 是 $F[x]$ 的一个理想且 $S = (p(x))$.

设 α 为 F 上的代数元, $p(x)$ 为 α 在域 F 上的极小多项式且 $\deg p(x) = n$. 任取 $\frac{f_1(\alpha)}{f_2(\alpha)} \in F(\alpha)$, 其中 $f_2(\alpha) \neq 0$. 所以 $p(x) \nmid f_2(x)$, 故 $\gcd(p(x), f_2(x)) = 1$. 存在 $u(x), v(x) \in F[x]$ 使得 $u(x)p(x) + v(x)f_2(x) = 1$, 代入 α, 得 $v(\alpha)f_2(\alpha) = 1$, 即 $\frac{1}{f_2(\alpha)} = v(\alpha)$. 所以 $\frac{f_1(\alpha)}{f_2(\alpha)} = f_1(\alpha)v(\alpha) = g(\alpha)$, 其中 $g(x) = f_1(x)v(x) \in F[x]$. 这说明 $F(\alpha)$ 中每一元素一定形如 $g(\alpha)$, 对某个 $g(x) \in F[x]$. 进一步地, 做带余除法 $g(x) = h(x)p(x) + r(x)$, 其中 $\deg r(x) < n$, 则 $g(\alpha) = r(\alpha)$. 所以 $F(\alpha)$ 中每个元素又形如 $r(\alpha)$, 对某个次数小于 n 的多项式 $r(x) \in F[x]$, 故 $F(\alpha)$ 中每个元素都是 $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 的 F 上的线性组合, 又易知 $1, \alpha, \cdots, \alpha^{n-1}$ 在 F 上线性无关. 所以 $F(\alpha)$ 作为 F 上的线性空间, $1, \alpha, \cdots, \alpha^{n-1}$ 是它的一组基, 故 $[F(\alpha) : F] = n$, 即 $F(\alpha)$ 在 F 上的扩张次数为 α 在 F 上的次数.

设 α, β 为 F 上的代数元, 则 β 也是 $F(\alpha)$ 上的代数元, 故 $[F(\alpha)(\beta) : F] = [F(\alpha)(\beta) : F(\alpha)][F(\alpha) : F]$ 有限, 所以 $F(\alpha)(\beta)$ 是 F 上的代数扩张, 所以 $\alpha \pm \beta$, $\alpha\beta$, $\alpha\beta^{-1}$ $(\beta \neq 0)$ 仍为 F 上的代数元, 所以 F 上所有代数元构成域, 这就是 F 的代数闭包.

设 $F(\alpha)$ 为单扩张, 则 $\pi : F[x] \to F(\alpha)$, $f(x) \mapsto f(\alpha)$ 为环同态. 若 α 为 F 上的代数元, 且 $p(x)$ 是 α 在 F 上的极小多项式, 则 π 为满同态且 $\mathrm{Ker}\pi = (p(x))$, 由环同态基本定理得 $F[x]/(p(x)) \cong F(\alpha)$. 即这时的单扩张 $F(\alpha)$ 就是多项式环 $F[x]$ 模去一个不可约多项式所得到的剩余类环, 也就是把域 $F[x]/(p(x))$ 中的元素 $\overline{x}$ 记成 α 所得到. 若 α 为 F 上的超越元, 则 $\mathrm{Ker}\pi = (0)$, 这时 π 为单同态且 $F[x] \cong \pi(F[x])$ 为 $F(\alpha)$ 的一个真子环.

综合上面的讨论, 我们有如下定理.

定理 1.15: 设 α 是域 F 上的 n 次代数元, 它在 F 上的极小多项式为 $p(x)$, 则有

(i) 多项式 $p(x)$ 在 F 上不可约.

(ii) 单扩张 $F(\alpha)$ 同构于剩余类环 $F[x]/(p(x))$.

(iii) 扩张次数 $[F(\alpha) : F] = n$, 且 $1, \alpha, \ldots, \alpha^{n-1}$ 构成 $F(\alpha)$ 在 F 上的一组基.

□

设 $f(x) \in F[x]$ 不可约, 则存在域 F 的单代数扩张 $F(\alpha)$ $(= F[x]/(f(x)))$ 使得 α 在 F 上的极小多项式为 $f(x)$. 进一步地, 设 α 和 β 是 $f(x)$ 在 F 的扩域中的根, 则存在域同构 $\sigma : F(\alpha) \to F(\beta)$ 使得 $\sigma|_F = \mathrm{id}$ 且 $\sigma(\alpha) = \beta$.

设 E 是一个域, 则 E 的全体自同构的集合关于变换的合成构成一个群, 称其为 E 的自同构群, 记为 $\mathrm{Aut}(E)$. 若 E 是域 F 的一个扩张, E 的所有 F-自同构 (或称为 E 在 F 上的自同构, 即 E 的保持 F 中的每个元素都不动的自同构) 的集合

$$\mathrm{Gal}(E/F) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_F = \mathrm{id}\}$$

构成 $\mathrm{Aut}(E)$ 的一个子群, 称为 E 在 F 上的 Galois 群.

1.4 Euler ϕ-函数

设 R 为环, I_1, I_2 为环 R 的理想, 定义

$$\begin{aligned} I_1 + I_2 &= \{x_1 + x_2 \mid x_1 \in I_1, x_2 \in I_2\}, \\ I_1 \cap I_2 &= \{x \mid x \in I_1, x \in I_2\}, \\ I_1 I_2 &= \{\text{有限和 } \textstyle\sum_i x_{1i}x_{2i} \mid x_{1i} \in I_1, x_{2i} \in I_2\}. \end{aligned}$$

容易验证 $I_1 + I_2$, $I_1 \cap I_2$, $I_1 I_2$ 都是 R 的理想, 分别称之为 I_1 与 I_2 的和、交、乘积. 又显然有 $I_1 I_2 \subseteq I_1 \cap I_2$.

设 R 为环, I_1, I_2 为环 R 的理想, 若 $I_1 + I_2 = R$, 则称 I_1 与 I_2 互素. 显然, 在整数环 $\mathbb{Z}$ 中, 两个理想 (r) 和 (s) 互素当且仅当正整数 r 和 s 互素. 在域 F 的多项式环 $F[x]$ 中, 两个理想 $(r(x))$ 和 $(s(x))$ 互素当且仅当多项式 $r(x)$ 和 $s(x)$ 互素. 容易验证若环 R 的理想 I 与 I_1, I_2 都互素, 则 I 与 $I_1 I_2$ 互素, 从而 I 与 $I_1 \cap I_2$ 也互素.

设 $R_1, R_2, \ldots, R_r$ 都是环, 令 $R = R_1 \times R_2 \times \cdots \times R_r$ 是它们作为集合的 Cartesian 乘积, 即

$$R = R_1 \times R_2 \times \cdots \times R_r = \{(x_1, x_2, \cdots, x_r) \mid x_i \in R_i, 1 \le i \le r\}.$$

在 R 上按对应分量相加和相乘定义 R 上的运算, 即

$$\begin{aligned} (x_1, x_2, \cdots, x_r) + (y_1, y_2, \cdots, y_r) &= (x_1 + y_1, x_2 + y_2, \cdots, x_r + y_r), \\ (x_1, x_2, \cdots, x_r)(y_1, y_2, \cdots, y_r) &= (x_1 y_1, x_2 y_2, \cdots, x_r y_r), \end{aligned}$$

在这样的运算下, R 成为一个环, 称为环 $R_1, R_2, \ldots, R_r$ 的直和, 记作 $R = R_1 \oplus R_2 \oplus \cdots \oplus R_r$. 显然元素 $(x_1, x_2, \cdots, x_r) \in R$ 可逆当且仅当对每个 $1 \le i \le r$, x_i 在 R_i 中可逆, 所以 $R_1 \oplus R_2 \oplus \cdots \oplus R_r$ 的乘法群为这些环的乘法群的直积 $U(R_1) \times U(R_2) \times \cdots \times U(R_r)$.

定理 1.16: (中国剩余定理) 设 R 是环, $I_1, I_2, \ldots, I_r$ 是 R 的两两互素的理想, 则有环同构

$$R/I_1 \cap I_2 \cap \cdots \cap I_r \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_r.$$

□

设 $R=\mathbb{Z}$, $I_i=(m_i)$. 则 $I_1,I_2,\ldots,I_r$ 两两互素即整数 $m_1,m_2,\ldots,m_r$ 两两互素, 又容易算出 $I_1\cap I_2\cap\cdots\cap I_r=(m_1m_2\cdots m_r)$, 所以中国剩余定理给出 $\mathbb{Z}/(m_1m_2\cdots m_r)\cong\mathbb{Z}/(m_1)\oplus\mathbb{Z}/(m_2)\oplus\cdots\oplus\mathbb{Z}/(m_r)$. 或者说, 设 $m_1,m_2,\ldots,m_r$ 是两两互素的正整数, 则对任意整数 $a_1,a_2,\ldots,a_r$, 同余方程组

$$\begin{cases} x &\equiv a_1 \pmod{m_1},\\ x &\equiv a_2 \pmod{m_2},\\ &\vdots\\ x &\equiv a_r \pmod{m_r} \end{cases}$$

有解, 且解在模 $m=m_1m_2\cdots m_r$ 下唯一. 进一步地, 若对每个 $1\le i\le r$ 有 a_i 与 m_i 互素, 则上述同余方程组的解与 m 互素, 反之亦然. 在域 F 上的多项式环 $F[x]$ 中也有类似的结果, 这里我们省略叙述.

设 $\mathbb{Z}$ 为整数环, n 为正整数, 考虑商环 $\mathbb{Z}_n=\mathbb{Z}/(n)$ 的乘法群 $U(n)=U(\mathbb{Z}_n)$, 此群也称为整数模 n 的乘法群. 若 $n=1$, 则 $\mathbb{Z}_1=\{\overline{0}\}$, $U(1)=\{\overline{0}\}$ 是 1 阶群. 若 $n\ge 2$, 设 $\overline{k}\in\mathbb{Z}_n$, 则 $\overline{k}$ 可逆当且仅当存在 $\overline{l}\in\mathbb{Z}_n$ 使得 $\overline{kl}=\overline{1}$, 看成整数来说, 即 $n\mid 1-kl$, 或存在 $t\in\mathbb{Z}$ 使得 $kl+tn=1$, 这等价于 k 与 n 互素. 所以群 $U(n)$ 的阶为小于 n 的自然数 (包括整数 0) 中与 n 互素的数的个数, 记这个数为 $\phi(n)$, 而 ϕ 作为正整数集合上的函数也称为 Euler ϕ-函数.

设 $\overline{a}\in U(n)$, 称 $\overline{a}$ 在群 $U(n)$ 中的阶为整数 a 模 n 的乘法阶, 记为 $\mathrm{ord}_n(a)$. 特别地, 若 $U(n)$ 为循环群, $\overline{a}$ 为此群的生成元, 则称 a 为模 n 的原根, 所以 a 为模 n 的原根当且仅当 $\mathrm{ord}_n(a)=\phi(n)$. 由初等数论可知, $U(n)$ 为循环群当且仅当 $n=1$, 2, 4, p^e, $2p^e$, 其中 p 为奇素数, e 为正整数.

显然 $\phi(1)=1$. 若 p 为素数, e 为正整数, 则容易得到 $\phi(p^e)=p^e-p^{e-1}=p^{e-1}(p-1)$. 设 s 和 t 为互素的正整数, 由中国剩余定理有 $U(st)\cong U(s)\times U(t)$, 故有 $\phi(st)=\phi(s)\phi(t)$.

定理 1.17:

(i) 设正整数 s, t 互素, 则 $\phi(st)=\phi(s)\phi(t)$.

(ii) 设正整数 n 的标准分解式为 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, 其中 $p_1,p_2,\cdots,p_r$ 是互不相同的素数, $e_i\ge 1$, $1\le i\le r$, 则

$$\phi(n)=\prod_{i=1}^{r}p_i^{e_i-1}(p_i-1)=n\cdot\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

□

注意到一般说来, 如果不知道 n 的分解, 则很难求出 $\phi(n)$. 设 $G=\langle a\rangle$ 为 n 阶循环群, 对任意 $b\in G$, 显然有 $\mathrm{ord}(b)\mid n$. 问对于 $d\mid n$, G 中阶为 d 的元素个数是什么? G 中元素为 a^k 的形式, 其中 $0\le k\le n-1$, 而 $\mathrm{ord}(a^k)=\mathrm{ord}(a)/\gcd(\mathrm{ord}(a),k)=n/\gcd(n,k)$. 若 $\mathrm{ord}(a^k)=d$,

则有 $\gcd(n,k)=\frac{n}{d}$, 这等价于 $\gcd(d,k/\frac{n}{d})=1$. 故这样的 k 有 $\phi(d)$ 个, 即群 G 中阶为 d 的元素有 $\phi(d)$ 个 (注意到这个数仅与 d 有关). 把循环群 G 中的元素按它的阶来分类，我们得到

$$\sum_{d|n}\phi(d)=n. \tag{1.5}$$

设 G 是一交换群, 其运算写为"+". 设 $a(1),a(2),\dots$ 和 $b(1),b(2),\dots$ 是群中元素组成的两个序列, 满足对所有的 $n\geq 1$, 有

$$a(n)=\sum_{d|n}b(d). \tag{1.6}$$

下面我们要找到用这些 a 的值来表示 b 的表达式.

注意到由式 (1.6), $b(1)=a(1)$ 且对 $n\geq 2$,

$$b(n)=a(n)-\sum_{d|n,d\neq n}b(d),$$

$b(n)$ 可由这些 $a(d)$ 唯一表出, 例如

$$\begin{aligned}
b(1) &= a(1),\\
b(2) &= a(2)-a(1),\\
b(3) &= a(3)-a(1),\\
b(4) &= a(4)-a(2),\\
b(5) &= a(5)-a(1),\\
b(6) &= a(6)-a(3)-a(2)+a(1),\\
&\vdots
\end{aligned}$$

但是我们需要的是一般的公式. 为此, 我们在正整数集合上定义 Möbius 函数 μ 如下: 设 n 的标准分解式为 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, 其中 $p_1,p_2,\cdots,p_r$ 是互不相同的素数, $e_i\geq 1$, $1\leq i\leq r$, 定义 $\mu(n)$ 为

$$\mu(n)=\begin{cases}1, & \text{若 } n=1;\\ (-1)^r, & \text{若 } e_1=e_2=\cdots=e_r=1;\\ 0, & \text{其它.}\end{cases} \tag{1.7}$$

换句话说, 若 n 可被一个素数的平方整除, 则 $\mu(n)=0$, 若 n 是偶数个互不相同的素数乘积, 则 $\mu(n)=1$, 而若 n 是奇数个互不相同的素数乘积, 则 $\mu(n)=-1$. 由定义 $\mu(1)=1$. 若 $n\geq 2$, 则有

$$\sum_{d|n}\mu(d)=\sum_{d|p_1p_2\cdots p_r}\mu(d)=\sum_{i=0}^{r}\binom{r}{i}(-1)^i=(1+(-1))^r=0.$$

所以, 我们有

$$\sum_{d|n}\mu(d)=\begin{cases}1, & \text{若 } n=1;\\ 0, & \text{若 } n>1.\end{cases} \tag{1.8}$$

定理 1.18: 设 $a(n)$, $b(n)$ 是定义在正整数集上, 取值在一个交换群 (运算写为加法) 中的两个函数, 则

$$a(n)=\sum_{d|n}b(d) \tag{1.6}$$

当且仅当

$$b(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)a(d). \tag{1.9}$$

证明: 设 (1.6) 成立, 则

$$\sum_{d|n}\mu\left(\frac{n}{d}\right)a(d)=\sum_{d|n}\mu\left(\frac{n}{d}\right)\sum_{e|d}b(e)=\sum_{e|n}b(e)\sum_{d:\,e|d|n}\mu\left(\frac{n}{d}\right)=\sum_{e|n}b(e)\sum_{f|\frac{n}{e}}\mu(f)=b(n).$$

上式的最后一步用到式 (1.8). 类似可以由 (1.9) 推出 (1.6). □

注意到式 (1.9) 也可以写成

$$b(n)=\sum_{d|n}\mu(d)a\left(\frac{n}{d}\right).$$

定理 1.18 称为 Möbius 反演公式. 利用此反演公式, 我们可以求出 Euler 函数 $\phi(n)$. 因为 $n=\sum_{d|n}\phi(d)$, 在定理 1.18 中令 $a(n)=n$, $b(n)=\phi(n)$, 则得到

$$\phi(n)=\sum_{d|n}\mu(d)\cdot\frac{n}{d}=n\sum_{d|n}\frac{\mu(d)}{d}.$$

进一步地, 设 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ 是 n 的标准分解式, 则有

$$\sum_{d|n}\frac{\mu(d)}{d}=\sum_{d|p_1p_2\cdots p_r}\frac{\mu(d)}{d}=\sum_{i=0}^{r}(-1)^i\cdot\sum_{1\le j_1,\ldots,j_i\le r}\frac{1}{p_{j_1}\cdots p_{j_i}}=\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

故

$$\phi(n)=n\cdot\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)=\prod_{i=1}^{r}p_i^{e_i-1}(p_i-1).$$

若交换群 G 中的运算写为乘法, 则 Möbius 反演公式可表为下面的定理.

定理 1.19: 设 $a(n)$, $b(n)$ 是定义在正整数集上, 取值在一个交换群 (运算写为乘法) 中的两个函数, 则

$$a(n)=\prod_{d|n}b(d)$$

当且仅当

$$b(n)=\prod_{d|n}a(d)^{\mu(\frac{n}{d})}.$$

□

下面看 Euler ϕ-函数在有限域上多项式环的推广. 设 F 为 q 元域, $f(x)\in F[x]$, $\deg f(x)=n$, 则 $F[x]/(f(x))$ 为 q^n 阶有限环, 它的乘法群 $U(F[x]/(f(x)))$ 的阶记为 $\Phi_q(f(x))$. 容易证明,

对于 $\overline{g(x)} \in F[x]/(f(x))$, $\deg g(x) < n$, 则 $\overline{g(x)}$ 在 $F[x]/(f(x))$ 中可逆当且仅当多项式 $g(x)$ 与 $f(x)$ 互素. 所以 $\Phi_q(f(x))$ 即为次数小于 $\deg f(x)$ 且与 $f(x)$ 互素的 F 上的多项式的个数.

定理 1.20: 函数 Φ_q 有如下性质:

(i) 设 $f(x)$ 次数为 0, 则 $\Phi_q(f(x)) = 1$.

(ii) 设 $p(x)$ 是次数为 m 的不可约多项式, e 为正整数, 则

$$\Phi_q(p(x)^e) = q^{me} - q^{m(e-1)} = q^{me}(1 - q^{-m}).$$

(iii) 设 $s(x)$, $t(x)$ 互素, 则 $\Phi_q(s(x)t(x)) = \Phi_q(s(x))\Phi_q(t(x))$.

(iv) 设 $\deg f(x) = n \geq 1$, 则

$$\Phi_q(f(x)) = q^n(1 - q^{-n_1})(1 - q^{-n_2}) \cdots (1 - q^{-n_r}),$$

其中 $n_1, n_2, \cdots, n_r$ 是 $f(x)$ 的标准分解式中互不相同的首一不可约多项式的次数.

□

1.5 习题

1.1 给出本章中所有定理的证明.

1.2 设 $F = \mathbb{Z}_p(t)$, 其中 t 为 $\mathbb{Z}_p$ 上的超越元, $f(x) = x^p - t \in F[x]$, 证明多项式 $f(x)$ 与 $f'(x)$ 不互素但是 $f(x)$ 无重因式.

1.3 设 $f(x) = ax^2 + bx + c$ 为实数域 $\mathbb{R}$ 上的 2 次不可约多项式 (这等价于 $b^2 - 4ac < 0$), 证明域 $\mathbb{R}[x]/(f(x))$ 同构于复数域 $\mathbb{C}$.

1.4 给定 $\mathbb{Z}_2[x]$ 中的不可约多项式 $x^4 + x + 1$, 构造一个具有 16 个元素的域.

a. 给出此域中类似于 (1.4) 式的乘法法则.

b. 构造一个类似于例 1.4 中的"对数表".

1.5 设 R 为 Gauss 整数环, 令 $p = 1 + \sqrt{-1}$. 给出域 $R/(p)$ 的一个完全描述.

1.6 给定欧氏环 $\mathbb{Z}_3[x]$ 中的不可约多项式 $p(x) = x^2 - x - 1$, 通过给出加法和乘法表构作域 $\mathbb{Z}_3[x]/(p(x))$.

1.7 证明

$$\sum_{d^2|n} \mu(d) = |\mu(n)|.$$

1.8 计算和式 $\sum_{d|n} |\mu(d)|$.

1.9 a. 证明

$$\lim_{n\to\infty}\sup\frac{\phi(n)}{n}=1 \qquad \text{和} \qquad \lim_{n\to\infty}\inf\frac{\phi(n)}{n}=0.$$

b. 分别找出满足 $\phi(n)/n>0.99$ 和 $\phi(n)/n<0.1$ 的最小正整数 n.

1.10 设 p 为素数, 证明对任意整数 $0\le j\le p-1$ 有

$$\binom{p-1}{j}\equiv(-1)^j\,(\mathrm{mod}\ p),$$

并由此证明对特征为素数 p 的交换环 R 中的任意元素 a,b 有

$$(a-b)^{p-1}=\sum_{j=0}^{p-1}a^jb^{p-1-j}.$$

1.11 设 $f(x)$ 和 $g(x)$ 是域 F 上的两个不全为常数的互素多项式, 证明存在唯一的多项式 $u(x),v(x)\in F[x]$ 使得 $u(x)f(x)+v(x)g(x)=1$ 且 $\deg(u(x))<\deg(g(x))$ 和 $\deg(v(x))<\deg(f(x))$.

1.12 设 F 为域, $f(x)\in F[x]$, 证明 $\{g(f(x))\mid g(x)\in F[x]\}=F[x]$ 当且仅当 $\deg(f(x))=1$.

1.13 设 $p(x)$, $q(x)$ 和 $r(x)$ 是实数域 $\mathbb{R}$ 上的多项式且满足 $p^2(x)=xq^2(x)+xr^2(x)$, 证明 $p(x)=q(x)=r(x)=0$.

1.14 设 $f_i(x)$, $i=1,2,\dots,n$ 是域 F 上的 n 个非零多项式, 求 $m(x)\in F[x]$ 使得

$$\bigcap_{i=1}^{n}(f_i(x))=(m(x)).$$

1.15 设 p 为素数, F 为域, $c\in F$, 证明多项式 x^p-c 在 F 上不可约当且仅当 x^p-c 在 F 中无根.

1.16 设 p 为素数, $f(x)\in\mathbb{Z}[x]$, 证明对所有 $a\in\mathbb{Z}$ 均有 $f(a)\equiv 0\,(\mathrm{mod}\ p)$ 当且仅当存在 $g(x),h(x)\in\mathbb{Z}[x]$ 使得 $f(x)=(x^p-x)g(x)+ph(x)$.

1.17 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 和 $g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$ 为域 F 上的两个多项式, 次数分别为 n 和 m, 定义 $f(x)$ 和 $g(x)$ 的结式 $R(f,g)$ 为如下的 $m+n$ 阶行列式

$$R(f,g)=\begin{vmatrix}
a_n & a_{n-1} & * & \cdots & * & a_1 & a_0 & 0 & 0 & \cdots & 0 & 0\\
0 & a_n & a_{n-1} & \cdots & * & * & a_1 & a_0 & 0 & \cdots & 0 & 0\\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots\\
0 & 0 & 0 & \cdots & a_n & a_{n-1} & * & * & * & \cdots & a_1 & a_0\\
b_m & b_{m-1} & * & \cdots & b_1 & b_0 & 0 & 0 & 0 & \cdots & 0 & 0\\
0 & b_m & b_{m-1} & \cdots & * & b_1 & b_0 & 0 & 0 & \cdots & 0 & 0\\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots\\
0 & 0 & 0 & \cdots & 0 & b_m & b_{m-1} & * & * & \cdots & b_1 & b_0
\end{vmatrix},$$

其中多项式 $f(x)$ 的系数构成了行列式 $R(f,g)$ 的前 m 行, 而多项式 $g(x)$ 的系数构成了行列式 $R(f,g)$ 的后 n 行, 试完成下列问题.

a 设 $f(x)$ 在 F 的扩域中的 n 个根为 $\alpha_1,\alpha_2,\ldots,\alpha_n$, 即 $f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, 证明

$$R(f,g)=a_n^m\prod_{i=1}^{n}g(\alpha_i).$$

b 证明 $f(x)$ 与 $g(x)$ 互素当且仅当 $R(f,g)\neq 0$.

c 设多项式 $f(x)\in F[x]$ 在它的分裂域中有 $f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, 其中 $a_n\neq 0$, 定义 $f(x)$ 的判别式 $D(f)$ 为

$$D(f)=a_n^{2n-2}\prod_{1\leq i<j\leq n}(\alpha_j-\alpha_i)^2,$$

证明 $D(f)\in F$ 且 $D(f)=(-1)^{\frac{n(n-1)}{2}}a_n^{-1}R(f,f')$, 并具体求出 2 次和 3 次多项式的判别式.

d 判断 $\mathbb{Z}_3$ 上的多项式 $f(x)=x^3+x+1$ 和 $g(x)=2x^5+x^2+2$ 是否有公共根.

e 设 $f(x_1,x_2,\ldots,x_n)$ 和 $g(x_1,x_2,\ldots,x_n)$ 都是域 F 上的 n 元多项式且 x_n 在其中都出现, 把 f 和 g 看成是 x_n 的系数在环 $F[x_1,\ldots,x_{n-1}]$ 中的多项式 $\overline{f}[x_n]$ 和 $\overline{g}[x_n]$, 其结式 $R(\overline{f},\overline{g})$ 是 F 上的一个以 $x_1,\ldots,x_{n-1}$ 为未定元的多项式, 设 $\alpha_1,\alpha_2,\ldots,\alpha_{n-1},\alpha_n$ 在 F 的扩域 K 中, 证明 $(\alpha_1,\alpha_2,\ldots,\alpha_{n-1},\alpha_n)$ 是 $f(x_1,x_2,\ldots,x_n)$ 和 $g(x_1,x_2,\ldots,x_n)$ 的公共解当且仅当 $(\alpha_1,\alpha_2,\ldots,\alpha_{n-1})$ 是 $R(\overline{f},\overline{g})$ 的解, 并由此求出有理数域 $\mathbb{Q}$ 上的两个二元多项式 $f(x,y)=x(y^2-x)^2+y^5$ 和 $g(x,y)=y^4+y^3-x^2$ 的公共解.

1.18 设 $f(x)\in\mathbb{Q}[x]$, 可用下面方法来寻找 $f(x)$ 的次数 $\leq s$ 的因式:

(1) 用 $f(x)$ 系数分母的最小公倍数乘以 $f(x)$ 可使 $f(x)\in\mathbb{Z}[x]$;

(2) 取 $s+1$ 个整数 $a_0,a_1,\ldots,a_s\in\mathbb{Z}$ 使得 $a_0,a_1,\ldots,a_s$ 不是 $f(x)$ 的根并计算 $f(a_i)$, $0\leq i\leq s$;

(3) 对每个 $s+1$ 元组 $(b_0,b_1,\ldots,b_s)$, 其中 $b_i\mid f(a_i)$, $0\leq i\leq s$, 确定多项式 $g(x)\in\mathbb{Q}[x]$ 满足 $\deg(g(x))\leq s$ 且对 $0\leq i\leq s$ 有 $g(a_i)=b_i$ (例如利用 Lagrange 插值公式);

(4) 判断 (3) 中得到的多项式 $g(x)$ 是否为 $f(x)$ 的因式.

如上方法称为 Kronecker 方法, 试完成下列问题.

a. 设 $\deg(f(x))=n$, $s=\lfloor\frac{n}{2}\rfloor$, 证明若 Kronecker 方法得到的 $f(x)$ 的因式都是常数多项式, 则 $f(x)$ 在 $\mathbb{Q}$ 上不可约 (即若 $f(x)$ 在 $\mathbb{Q}$ 上可约, 则 Kronecker 方法一定可以给出 $f(x)$ 的非平凡因式).

b. 利用 Kronecker 方法给出多项式$f(x)=\frac{1}{3}x^6-\frac{5}{3}x^5+2x^4-x^3+5x^2-\frac{17}{3}x-1$ 在 $\mathbb{Q}$ 上的标准分解式.

1.19 设 p 为素数, e 为正整数, 整系数多项式 $f(x)$, $g_e(x)$, $h_e(x)$, $u(x)$, $v(x) \in \mathbb{Z}[x]$ 满足

$$f(x) \equiv g_e(x)h_e(x) \,(\mathrm{mod}\ p^e)$$

和

$$u(x)g_e(x) + v(x)h_e(x) \equiv 1 \,(\mathrm{mod}\ p),$$

设 $g_e(x)$ 为首一多项式, $\deg(u(x)) < \deg(h_e(x))$ 且 $\deg(v(x)) < \deg(g_e(x))$, 证明存在整系数多项式 $g_{e+1}(x)$, $h_{e+1}(x) \in \mathbb{Z}[x]$ 使得

$$\begin{aligned} g_{e+1}(x) &\equiv g_e(x) \,(\mathrm{mod}\ p^e) \\ h_{e+1}(x) &\equiv h_e(x) \,(\mathrm{mod}\ p^e) \\ f(x) &\equiv g_{e+1}(x)h_{e+1}(x) \,(\mathrm{mod}\ p^{e+1}) \end{aligned}$$

和

$$u(x)g_{e+1}(x) + v(x)h_{e+1}(x) \equiv 1 \,(\mathrm{mod}\ p),$$

且 $g_{e+1}(x)$, 和 $h_{e+1}(x)$ 在模 p^{e+1} 下是唯一的.

第二章　有限域的性质

本章我们讨论有限域的抽象性质, 上一章中我们知道对于一些正整数 q, q 元域是存在的, 比如 q 为素数, $q=8$ (例 1.4), $q=9$ (习题 1.6) 等.

2.1　有限域的群结构

定理 2.1: 有限域 F 的元素个数 q 为素数方幂, $q=p^n$, 其中 p 为 F 的特征, n 是 F 关于其素子域的次数.

证明: 有限域 F 的特征一定为某个素数 p, 故 F 的素子域为 $\mathbb{Z}_p$, 由 F 有限得知扩张次数 $[F:\mathbb{Z}_p]$ 有限, 设 $[F:\mathbb{Z}_p]=n$. 取 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 为 F 在 $\mathbb{Z}_p$ 上的一组基. 则 F 中每个元素都可以唯一地表成 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的线性组合, 而系数取自域 $\mathbb{Z}_p$, 所以 $|F|=p^n$. □

F 为 $\mathbb{Z}_p$ 上的 n 维线性空间, 所以 F 中每个元素可以看成分量取自 $\mathbb{Z}_p$ 的 n-维向量, 且 F 的加法就是向量的分量相加, $\mathbb{Z}_p$ 的加法群为 p 阶循环群, 所以 F 的加法群为 n 个 p 阶循环群的直积, 即初等交换 p-群.

定理 2.2: 设 F 为 q 元域, E 为 F 的扩域, 则元素 $\beta\in E$ 落在它的子域 F 中当且仅当 $\beta^q=\beta$, 特别地, F 中每个元素都是多项式 x^q-x 的根.

证明: 设 $\beta\in F$. 若 $\beta=0$, 显然有 $\beta^q=\beta$. 若 $\beta\neq 0$, 由于 F 的乘法群 F^* 为 $q-1$ 阶群, 故 $\beta^{q-1}=1$, 所以 $\beta^q=\beta$. 这样 F 中的 q 个元素已给出多项式 x^q-x 的 q 个根, 又此多项式次数为 q, 它在 E 中有至多 q 个根, 所以 E 中 F 外的元素不是 x^q-x 的根, 这表明对于 $\beta\in E$, 若 $\beta^q=\beta$, 则 $\beta\in F$. □

设 F 是一个 q 元域, 由定理 2.2 得到在 $F[x]$ 中有

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

设 F 为任意域, F 的乘法群为 F^*. 对于 $\alpha\in F^*$, 用 $\mathrm{ord}(\alpha)$ 表示 α 在群 F^* 中的阶.

若 F^* 中有 t 阶元 α. 设 $\beta\in F^*$ 满足 $\beta^t=1$, 则 β 一定为 α 的方幂. 事实上, t 个元素 $1,\alpha,\ldots,\alpha^{t-1}$ (一定互异) 均为多项式 x^t-1 的根, 而此多项式在域 F 中至多有 t 个根, 故 $1,\alpha,\ldots,\alpha^{t-1}$ 就是 x^t-1 的全部根, 所以存在某个 $0\le i\le t-1$ 使得 $\beta=\alpha^i$. 由于

$\mathrm{ord}(\alpha^i) = t/\gcd(i,t)$, 所以 $\mathrm{ord}(\alpha^i) = t$ 当且仅当 $\gcd(i,t) = 1$. 这表明若 F^* 中有 t 阶元, 则 t 阶元的个数为 $\phi(t)$.

例 2.1: 设 $\mathrm{ord}(\alpha) = 12$, 其中 α 是域 F 中某个元素. 我们可以计算 α^i 的阶如下表, $i = 0, 1, \ldots, 11$.

i	$\gcd(i,12)$	$\mathrm{ord}(\alpha^i)$
0	12	1
1	1	12
2	2	6
3	3	4
4	4	3
5	1	12
6	6	2
7	1	12
8	4	3
9	3	4
10	2	6
11	1	12

只需知道域 F 中有 12 阶元, 则 F 中恰有 4 个 12 阶元! 进一步地, 恰有 2 个 6 阶元, 2 个 4 阶元, 2 个 3 阶元, 1 个 2 阶元, 1 个 1 阶元. 这里我们只通过整数的运算, 并未用到域 F 的特性. □

下面设 F 为 q 元有限域, 这时 F^* 的阶为 $q-1$. 若 $t \nmid (q-1)$, 则 F^* 中无 t 阶元; 若 $t \mid (q-1)$, 则 F^* 中或者无 t 阶元, 或者有 $\phi(t)$ 个 t 阶元. 用 $\psi(t)$ 表示 F 中 t 阶元的个数, 则有

$$\sum_{t|(q-1)} \psi(t) = q-1,$$

又由式 (1.5) 知

$$\sum_{t|(q-1)} \phi(t) = q-1,$$

两式相减有

$$\sum_{t|(q-1)} (\phi(t) - \psi(t)) = 0.$$

但是对满足 $t \mid (q-1)$ 的所有正整数 t, 有 $\phi(t) - \psi(t) \geq 0$, 故由上式得到对 $q-1$ 的每个正因子 t, 均有 $\phi(t) - \psi(t) = 0$, 即 $\psi(t) = \phi(t)$.

定理 2.3: 设 F 为 q 元域, 则其乘法群 F^* 中有 $\phi(q-1)$ (≥ 1) 个 $q-1$ 阶元素, 所以 F 的乘法群 F^* 为循环群. □

循环群 F^* 的生成元, 即 F^* 中的 $q-1$ 阶元素, 称为域 F 的本原元素, 故 q 元域有 $\phi(q-1)$ 个本原元素. 又显然 q 元域中任意非零元 α 的逆 $\alpha^{-1}=\alpha^{q-2}$, 同时除二元域外, 任一有限域的所有元素之和为 0. 事实上, 设 F 为 q 元域, 其中 $q\geq 3$. 取 F 的一个本原元素 α, 则 F 中所有元素之和为

$$\sum_{\beta\in F}\beta=0+1+\alpha+\alpha^2+\cdots+\alpha^{q-2}=\frac{1-\alpha^{q-1}}{1-\alpha}=0.$$

例 2.2: 考虑有限域 $\mathbb{Z}_7=\{0,1,2,3,4,5,6\}$. 计算 2 的方幂得到 $2^0=1$, $2^1=2$, $2^2=4$, $2^3=1$. 所以元素 2 和它的方幂都不是 $\mathbb{Z}_7$ 的本原元素. 再试验元素 3, 3 的方幂为 $3^0=1$, $3^1=3$, $3^2=2$, $3^3=6$, $3^4=4$, $3^5=5$, $3^6=1$. 所以 $\mathrm{ord}(3)=6$, 即 3 是域 $\mathbb{Z}_7$ 的本原元. 由于方幂指数 5 与 6 互素, 所以 $3^5=5$ 的阶也是 6, 即 5 也是域 $\mathbb{Z}_7$ 的本原元. $\mathbb{Z}_7$ 有 $\phi(6)=2$ 个本原元素. □

在前面这个例子中, 我们用随机选取的办法来找出本原元素, 但当域中元素很多时, 这种办法并不适用. 事实上, 若 F 为 q 元域, 则任取 F^* 中的一个元素, 其为本原元素的概率为 $\frac{\phi(q-1)}{q-1}$, 由习题 1.9 知, 在有些情形下, 数 $\frac{\phi(q-1)}{q-1}$ 可以任意小. 一般说来, 没有一个确定性的有效算法来找到有限域的一个本原元素, 下面给出一个寻找有限域本原元素的随机算法, 它来源于 Gauss, 称为 Gauss 算法. Gauss 算法可以输出有限域中的一个元素序列 $\alpha_1,\alpha_2,\ldots,\alpha_k$ 使得 $\mathrm{ord}(\alpha_1)\mid\mathrm{ord}(\alpha_2)\mid\cdots\mid\mathrm{ord}(\alpha_k)=q-1$.

Gauss 算法:

G1. 令 $i=1$, 在域 F 中随机选取一个元素 α_1, 设 $\mathrm{ord}(\alpha_1)=t_1$.

G2. 设已找到 $\alpha_i\in F$ 且有 $t_i=\mathrm{ord}(\alpha_i)$, 若 $t_i=q-1$, 则停止: α_i 就是所求的本原元.

G3. 否则选取非零元素 $\beta\in F$ 使其不是 α_i 的方幂, 设 $\mathrm{ord}(\beta)=s$. 若 $s=q-1$, 则令 $\alpha_{i+1}=\beta$ 且停止.

G4. 否则选取整数 d 和 e 满足 $d\mid t_i$, $e\mid s$, $\gcd(d,e)=1$ 且 $de=\mathrm{lcm}(t_i,s)$. 令 $\alpha_{i+1}=\alpha_i^{\frac{t_i}{d}}\cdot\beta^{\frac{s}{e}}$, 则 $\mathrm{ord}(\alpha_{i+1})=t_{i+1}=de=\mathrm{lcm}(t_i,s)$. 把 i 增加 1 并回到步骤 G2.

注记:

- 在步骤 G3, 因为 β 不是 α_i 的方幂, 所以 β 的阶 s 不是 t_i 的因子, 从而 $\mathrm{lcm}(t_i,s)$ 为 t_i 的倍数且严格大于 t_i.
- 在步骤 G4, 对任意给定的两个正整数 m 和 n, 一定存在整数 d 和 e 满足 $d\mid m$, $e\mid n$, $\gcd(d,e)=1$ 且 $de=\mathrm{lcm}(m,n)$. (事实上, 设 m 或 n 的素因子为 $p_1,p_2,\ldots,p_r$ 且 m 和 n 的素因子分解式为

  $$m=p_1^{\mu_1}p_2^{\mu_2}\cdots p_r^{\mu_r}\qquad\text{和}\qquad n=p_1^{\nu_1}p_2^{\nu_2}\cdots p_r^{\nu_r},$$

  其中 $\mu_i,\nu_i\geq 0$, $1\leq i\leq r$. 令

  $$d=\prod_{j:\ \mu_j\geq\nu_j}p_j^{\mu_j}\qquad\text{和}\qquad e=\prod_{j:\ \mu_j<\nu_j}p_j^{\nu_j},$$

则 d, e 即为所求. 例如, 若 $m = 12 = 2^2 \cdot 3$, $n = 18 = 2 \cdot 3^2$, 则 $d = 2^2 = 4$, $e = 3^2 = 9$.)

- 在步骤 G4, 元素 $\alpha_i^{\frac{t_i}{d}}$ 的阶为 d 而元素 $\beta^{\frac{s}{e}}$ 的阶为 e, 由于 $\gcd(d, e) = 1$, 所以它们乘积的阶为 de. 这样元素 α_{i+1} 的阶 t_{i+1} 为 $\mathrm{ord}(\alpha_i)$ 的倍数且严格大于它, 有限步后这个过程一定可以终结到一个本原元素.

例 2.3: 设 $F = \mathbb{Z}_5[x]/(x^2-2)$, x^2-2 在 $\mathbb{Z}_5$ 上不可约, 这是一个 25 元域. 把 F 中的元素看成是 2-维向量 (a, b), 其中 $a, b \in \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. F 中的加法为 $(a_1, b_1)+(a_2, b_2) = (a_1+a_2, b_1+b_2)$. 为定义乘法, 把元素 (a, b) 看成多项式 $ax + b$, 由于 $x^2 \equiv 2 \pmod{x^2 - 2}$, 所以

$$(a_1x + b_1) \cdot (a_2x + b_2) = a_1a_2x^2 + (a_1b_2 + a_2b_1)x + b_1b_2 \equiv (a_1b_2 + a_2b_1)x + (2a_1a_2 + b_1b_2),$$

从而 F 中的乘法为

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1b_2 + a_2b_1, 2a_1a_2 + b_1b_2).$$

下面利用 Gauss 算法来找 F 的一个本原元素, 取 $\alpha_1 = (1, 0)$. 为计算 $\mathrm{ord}(\alpha_1)$, 我们计算下面这个方幂的表:

i	α_1^i
0	$(0, 1)$
1	$(1, 0)$
2	$(0, 2)$
3	$(2, 0)$
4	$(0, 4)$
5	$(4, 0)$
6	$(0, 3)$
7	$(3, 0)$
8	$(0, 1)$.

所以 $\mathrm{ord}(\alpha_1) = 8$, 即在 Gauss 算法中我们有 $t_1 = 8$. 因为 $t_1 \neq q - 1 = 24$, α_1 不是本原元, 我

们需要进入步骤 G3, 选取元素 β 使其不是 α_1 的方幂, 比如取 $\beta=(1,1)$, 计算下表

i	β^i
0	$(0,1)$
1	$(1,1)$
2	$(2,3)$
3	$(0,2)$
4	$(2,2)$
5	$(4,1)$
6	$(0,4)$
7	$(4,4)$
8	$(3,2)$
9	$(0,3)$
10	$(3,3)$
11	$(1,4)$
12	$(0,1)$.

得到 $\mathrm{ord}(\beta)=12$. 现在我们有 $\alpha_1=(1,0)$, $t_1=8=2^3$, $\beta=(1,1)$, $s=12=2^2\cdot 3$. 我们进入步骤 G4, 这里取 $d=2^3=8$, $e=3$, 则 $\gcd(d,e)=1$ 且 $de=24=\mathrm{lcm}(8,12)$. 这样 $\alpha_2=\alpha_1^{\frac{t_1}{d}}\cdot\beta^{\frac{s}{e}}=\alpha_1\beta^4=(1,0)\cdot(2,2)=(2,4)$ 的阶为 24, 即 $t_2=24$. 返回步骤 G2, 停止; 这样我们便求出 F 的一个本原元素 $(2,4)$. □

2.2 有限域的存在唯一性

我们已经证明有限域中的元素个数一定是素数方幂, 反之, 任给素数 p 和正整数 n, 是否一定存在 p^n 元有限域? $n=1$ 时问题已解决, $\mathbb{Z}_p$ 就是一个 p 元域, 当 $n\geq 2$ 时, 如果存在域 $\mathbb{Z}_p$ 上的 n 次不可约多项式 $p(x)$, 则 $\mathbb{Z}_p[x]/(p(x))$ 就是 p^n 元域. 这样自然有下面两个问题:

A. 对于哪些素数 p 和正整数 n, 存在域 $\mathbb{Z}_p$ 上的 n 次不可约多项式?

B. 是否有其它方式构造有限域? 即两个同阶有限域是否同构?

本节我们要回答这两个问题.

首先考虑更一般的情形, 设 F 是一个 q 元域, n 为任意正整数, 是否存在域 F 上的 n 次不可约多项式? 注意到多项式 $x^{q^n}-x\in F[x]$ 可以唯一地分解为 F 上的首一不可约多项式的乘积, 那么 $x^{q^n}-x$ 的这些首一不可约因式有什么特性?

定理 2.4: 设 $f(x)$ 是 F 上的首一不可约多项式且 $\deg f(x)=d$, 则 $f(x)\mid(x^{q^n}-x)$ 当且仅当 $d\mid n$.

证明: 充分性: 设 $d \mid n$. 构造域 $K = F[x]/(f(x))$, 则 K 中有 q^d 个元素. 记 $\alpha = \overline{x} \in K$, 则由定理 2.2 知 $\alpha^{q^d} = \alpha$, 即 α 为多项式 $x^{q^d} - x$ 的根, 由于 α 是 $f(x)$ 的根, 又 $f(x)$ 不可约, 所以 α 在 F 上的极小多项式为 $f(x)$, 故 $f(x) \mid (x^{q^d} - x)$. 因为 $d \mid n$, 所以 $(x^{q^d} - x) \mid (x^{q^n} - x)$, 从而 $f(x) \mid (x^{q^n} - x)$.

必要性: 设 $f(x) \mid (x^{q^n} - x)$. 由于 $f(x)$ 不可约且 $\deg f(x) = d$, 由上面的证明知 $f(x) \mid (x^{q^d} - x)$, 所以 $f(x) \mid \gcd(x^{q^n} - x, x^{q^d} - x) = x^{q^e} - x$, 其中 $e = \gcd(d, n)$. 在域 $K = F[x]/(f(x))$ 中, 记 $\alpha = \overline{x}$, 则 α 在 F 上的极小多项式为 $f(x)$, 从而 $\alpha^{q^e} = \alpha$. 任取 $\beta \in K$, 则 $\beta = A_0 + A_1\alpha + \cdots + A_{d-1}\alpha^{d-1}$, 其中 $A_i \in F$, 由定理 1.2 和 2.2 有

$$\beta^{q^e} = A_0^{q^e} + A_1^{q^e}\alpha^{q^e} + \cdots + A_{d-1}^{q^e}(\alpha^{q^e})^{d-1} = A_0 + A_1\alpha + \cdots + A_{d-1}\alpha^{d-1} = \beta,$$

即任意 $\beta \in K$ 都是多项式 $x^{q^e} - x$ 的根. 由于多项式 $x^{q^e} - x$ 在 K 中有至多 q^e 个根, 所以 $q^e \geq q^d$, 即 $e \geq d$. 又 $e = \gcd(d, n)$ 为 d 的因子, 从而 $e = d$, 这便得到 $d \mid n$. □

记 $I_{q,d}(x)$ 为 $F[x]$ 中所有 d 次首一不可约多项式的乘积 (若这样的多项式不存在, 则令 $I_{q,d}(x) = 1$). 注意到 $(x^{q^n} - x)' = -1$, $x^{q^n} - x$ 与它的形式微商互素, 所以 $x^{q^n} - x$ 无重因式, 再由定理 2.4 可以得到

$$x^{q^n} - x = \prod_{d \mid n} I_{q,d}(x), \tag{2.1}$$

例 2.4: 设 $q = 2$, $n = 4$. 则 $x^{16} + x$ 为 $\mathbb{Z}_2$ 上所有次数为 1, 2 和 4 的不可约多项式 (一定首一) 的乘积. 事实上, $x^{16} + x$ 在 $\mathbb{Z}_2[x]$ 中的分解为

$$x^{16} + x = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1)x,$$

乘之可得 $I_{2,1}(x) = x^2 + x$, $I_{2,2}(x) = x^2 + x + 1$, $I_{2,4}(x) = x^{12} + x^9 + x^6 + x^3 + 1$. □

比较等式 (2.1) 两边多项式的次数, 可得如下结论.

推论 2.5: 设 $I_q(n)$ 为 q 元域上的 n 次首一不可约多项式的个数, 则有

$$q^n = \sum_{d \mid n} dI_q(d). \tag{2.2}$$

□

在定理 1.18 中取 $a(n) = q^n$, $b(n) = nI_q(n)$, 由 Möbius 反演公式得

$$I_q(n) = \frac{1}{n} \cdot \sum_{d \mid n} \mu(d) q^{\frac{n}{d}}, \tag{2.3}$$

当 $d = 1$ 时, 可取到 (2.3) 式的主项, 对于给定的 q, 当 n 很大时, 我们有近似值 $I_q(n) \sim \frac{q^n}{n}$, 因为 q 元域上的 n 次首一多项式的个数为 q^n, 则随机选取一个 n 次首一多项式, 它不可约的概率大约为 $\frac{1}{n}$.

当 q 给定时, 我们可以计算出 $I_q(1) = q$, $I_q(2) = \frac{1}{2}(q^2 - q)$, $I_q(3) = \frac{1}{3}(q^3 - q)$, $I_q(4) = \frac{1}{4}(q^4 - q^2)$, $I_q(5) = \frac{1}{5}(q^5 - q)$, $I_q(6) = \frac{1}{6}(q^6 - q^3 - q^2 + q)$, 等等. 由此可得到 $I_q(n) \neq 0$. 例如,

因为 $\frac{6I_q(6)}{q} = q^5 - q^2 - q + 1 \equiv 1 \pmod{q}$, 不为 0, 所以 $I_q(6) \neq 0$. 一般说来,

$$I_q(n) = \frac{1}{n} \cdot \sum_{d|n} \mu(d) q^{\frac{n}{d}} \geq \frac{1}{n}(q^n - q^{n-1} - q^{n-2} - \cdots - q) = \frac{q^n(q-2)+q}{n(q-1)} > 0,$$

这样我们就证明了如下定理.

定理 2.6: 对任意有限域 F 和任意正整数 n, 一定存在 F 上的 n 次不可约多项式. □

设 p 为素数, $q = p^n$, 由于存在 $\mathbb{Z}_p$ 上的 n 次不可约多项式 $f(x)$, $\mathbb{Z}_p[x]/(f(x))$ 就是一个 q 元域.

推论 2.7: 对任意素数幂 q, 存在 q 元有限域. □

下面讨论有限域的唯一性问题, 我们可以证明, 任意两个同阶域是同构的.

设 p 为素数, $q = p^n$, 以下证明 q 元域在同构意义下唯一. 任意取定一个 $\mathbb{Z}_p[x]$ 中的 n 次首一不可约多项式 $f(x)$ (由定理 2.6, 这样的多项式 $f(x)$ 存在), 由定理 2.4 知 $f(x)$ 整除 $x^{p^n} - x$, 即存在某个 $J(x) \in \mathbb{Z}_p[x]$ 使得

$$x^{p^n} - x = f(x)J(x). \tag{2.4}$$

设 F 为一个 q 元域, 则 F 为它的素子域 $\mathbb{Z}_p$ 的 n 次扩域. 由于 F 为 p^n 元域, $x^{p^n} - x$ 在域 F 上可以分解为一次因式的乘积

$$x^{p^n} - x = \prod_{\beta \in F} (x - \beta). \tag{2.5}$$

比较 (2.4) 和 (2.5), 对任意 $\beta \in F$, $f(\beta)J(\beta) = 0$, 但是 $J(x)$ 在域 F 中有至多 $p^n - n$ 个根, 所以至少有 n 个 F 中元素 β 满足 $f(\beta) = 0$, 即 $f(x)$ 在 F 中有根.

设 $\alpha \in F$ 是多项式 $f(x)$ 的根, 由于 $f(x)$ 是 $\mathbb{Z}_p$ 上的首一不可约多项式, 故 α 在 $\mathbb{Z}_p$ 上的极小多项式为 $f(x)$, 这样 F 中的 n 个元素 $1, \alpha, \ldots, \alpha^{n-1}$ 在域 $\mathbb{Z}_p$ 上一定线性无关. 事实上, 若存在 $\lambda_k \in \mathbb{Z}_p$, $0 \leq k \leq n-1$, 使得 $\sum_{k=0}^{n-1} \lambda_k \alpha^k = 0$, 则 α 是多项式 $\lambda(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1} x^{n-1} \in \mathbb{Z}_p[x]$ 的根, 从而 $f(x) \mid \lambda(x)$, 又由于 $\deg \lambda(x) < n$, 所以 $\lambda(x) = 0$, 即 $\lambda_0 = \lambda_1 = \cdots = \lambda_{n-1} = 0$. 注意到 $[F : \mathbb{Z}_p] = n$, 所以 $1, \alpha, \ldots, \alpha^{n-1}$ 是 F 在 $\mathbb{Z}_p$ 上的一组基, 这表明任意 $\beta \in F$ 可以唯一表成 $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = g(\alpha)$ 的形式, 其中 $g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{Z}_p[x]$.

定义映射 $\pi : \mathbb{Z}_p[x] \to F$ 为 $\pi(g(x)) = g(\alpha)$, 对任意 $g(x) \in \mathbb{Z}_p[x]$. 容易验证 π 为环的满同态, 由环同态基本定理, 有 $\mathbb{Z}_p[x]/\mathrm{Ker}\,\pi \cong F$. 又 α 在 $\mathbb{Z}_p$ 上的极小多项式为 $f(x)$, 故 $\mathrm{Ker}\,\pi = (f(x))$, 即域 F 同构于 $\mathbb{Z}_p[x]/(f(x))$.

注意到 $f(x)$ 事先取定, 并不依赖于 F, 即对于 $\mathbb{Z}_p$ 上的两个 n 次不可约多项式 $f(x)$ 和 $g(x)$, $\mathbb{Z}_p[x]/(f(x))$ 和 $\mathbb{Z}_p[x]/(g(x))$ 都同构于任一个 p^n 元域. 我们有如下定理.

定理 2.8: 对任意素数幂 $q = p^n$, 在同构意义下存在唯一一个 q 元域, 它可以通过 $\mathbb{Z}_p[x]$ 模去一个 $\mathbb{Z}_p$ 上的 n 次不可约多项式得到. □

由唯一性, q 元域常记为 $\mathbb{F}_q$ 或者 $GF(q)$, 这里 GF 表示 Galois 域, 以纪念法国数学家 Galois, 历史上是 Galois 在 1830 年首先研究了一般有限域的性质. 注意到当 p 为素数时, $\mathbb{F}_p = \mathbb{Z}_p$, 而当 $n \geq 2$ 时, $\mathbb{F}_{p^n} \neq \mathbb{Z}_{p^n}$, 因这时 $\mathbb{Z}_{p^n}$ 不是域.

命题 2.9: 设 p 为素数, F 为 p^n 元域, 则 F 的子域的阶为 p^d, 其中 $d \mid n$. 反之, 对于任意 $d \mid n$, F 存在唯一一个 p^d 元子域.

证明: 设 K 为 F 的子域, 可设 $|K| = p_1^d$, 其中 p_1 为素数. 设 $[F : K] = t$, 则 $|F| = |K|^t$, 即 $p^n = (p_1^d)^t = p_1^{dt}$. 因为 p, p_1 都是素数, 所以 $p_1 = p$ 且 $n = dt$, 故 $|K| = p^d$ 且 $d \mid n$.

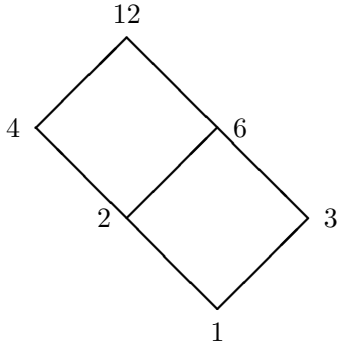
另一方面, 设 F 为 p^n 元域, 则

$$x^{p^n} - x = \prod_{\alpha \in F} (x - \alpha).$$

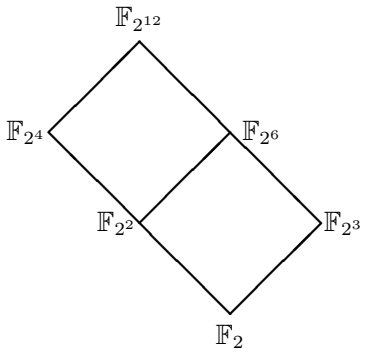
若 $d \mid n$, 则 $(x^{p^d} - x) \mid (x^{p^n} - x)$, 所以多项式 $x^{p^d} - x$ 可在 F 上分解为一次因式的乘积, 由 $x^{p^d} - x$ 无重根, 故 $K = \{\alpha \in F \mid \alpha^{p^d} = \alpha\}$ 中恰含有 p^d 个元素. 又容易验证, 对任意 α, $\beta \in K$, $\beta \neq 0$, 有 $\alpha - \beta$, $\alpha\beta^{-1} \in K$, 所以 K 为 F 的子域. 这表明对 n 的因子 d, F 存在 p^d 元子域. 进一步地, 若 $K_1 \neq K_2$ 都是 F 的 p^d 元子域, 则 $|K_1 \cup K_2| > p^d$, 又 $K_1 \cup K_2$ 中每个元素都是多项式 $x^{p^d} - x$ 的根, 与 $x^{p^d} - x$ 在 F 中的根至多有 p^d 个矛盾. □

由此命题的证明知有限域和它的子域有相同的特征.

例 2.5: 设 $n = 12$. 将 n 的所有因子不重复地排列出来, 连线表示对应的下面的数整除上面的数 (连续的连线有整除的连续性, 所以有连线的上面的数比下面的数只相差一个素因子), 没有整除关系的数之间没有连线, 这样的图称为 n 的因子构成的格. 易知 12 的因子构成的格为



所以域 $\mathbb{F}_{2^{12}}$ 的子域结构为



(从上图可以得到命题 2.9 的一个推论, 即 $\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^{\gcd(m,n)}}$.) □

2.3 极小多项式

设 F 是一个有限域, $K = \mathbb{F}_q$ 是 F 的一个 q 元子域, 设 F 关于 K 的扩张次数为 n, 即 $[F : K] = n$, 则 $F = \mathbb{F}_{q^n}$. 由于 F/K 为有限扩张, 故为代数扩张, 从而任取 $\alpha \in F$, α 是 K 上的代数元, 本节我们讨论 α 在 K 上的极小多项式. 显然元素 0 在 K 上的极小多项式为 x, 所以只需讨论 $\alpha \neq 0$ 的情形.

注意到 q 为素数 p 的方幂, 其中 $p = \mathrm{char}K = \mathrm{char}F$, 所以对任意 $\alpha_1, \alpha_2, \ldots, \alpha_t \in F$ 和任意 $k \geq 1$, 由定理 1.2 有

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_t)^{q^k} = \alpha_1^{q^k} + \alpha_2^{q^k} + \cdots + \alpha_t^{q^k}.$$

设多项式 $p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_s x^s \in K[x]$ 满足 $p(\alpha) = 0$, 则有 $p(\alpha^q) = 0$. 事实上,

$$p(\alpha^q) = \sum_{k=0}^{s} p_k (\alpha^q)^k = \sum_{k=0}^{s} p_k^q (\alpha^k)^q = \left(\sum_{k=0}^{s} p_k \alpha^k \right)^q = 0^q = 0.$$

(因为 $p_k \in K$, 我们有 $p_k^q = p_k$). 所以若 α 是 $p(x)$ 的根, 则 α^q 也是, 用 α^q 来代替 α, 有 $(\alpha^q)^q = \alpha^{q^2}$ 也是 $p(x)$ 的根, 重复这个过程, 我们有 $\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$ 都是 $p(x)$ 的根, 它们称为 α 的共轭元素 (关于子域 K). 显然 α 的共轭元素只有有限多个, 所以序列 $\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$ 中一定有重复. 设 $\alpha^{q^d} = \alpha^{q^j}$ 为第一个重复, 其中 $j < d$, 则 $1 = \alpha^{q^d - q^j} = \alpha^{q^j(q^{d-j}-1)}$, 所以 $\mathrm{ord}(\alpha) \mid q^j(q^{d-j} - 1)$. 由于 $\mathrm{ord}(\alpha) \mid (q^n - 1)$, 这便得到 $\gcd(\mathrm{ord}(\alpha), q^j) = 1$, 所以 $\mathrm{ord}(\alpha) \mid (q^{d-j} - 1)$, 由此可推出 $\alpha^{q^{d-j}} = \alpha$, 由于如上假设是第一个重复, 我们得到 $j = 0$. 再由 d 的最小性知 d 为满足 $q^d \equiv 1 \pmod{\mathrm{ord}(\alpha)}$ 的最小正整数, 即 q 模 $\mathrm{ord}(\alpha)$ 的乘法阶.

现在 α 在 K 上的极小多项式一定有 d 个根 $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$. 定义

$$f_\alpha(x) = (x - \alpha)(x - \alpha^q)(x - \alpha^{q^2}) \cdots (x - \alpha^{q^{d-1}}),$$

则 $f_\alpha(x)$ 为 α 的极小多项式的因子. 把多项式 $f_\alpha(x)$ 展开为

$$f_\alpha(x) = x^d + A_{d-1}x^{d-1} + \cdots + A_1 x + A_0,$$

其中系数 $A_i \in F$. 两边同时 q 次幂得到

$$(x-\alpha)^q(x-\alpha^q)^q\cdots(x-\alpha^{q^{d-1}})^q = x^{qd}+A_{d-1}^q x^{q(d-1)}+\cdots+A_1^q x^q+A_0^q, \tag{2.1}$$

由于 $(x-\beta)^q = x^q+(-1)^q\beta^q = x^q-\beta^q$, 所以 (2.1) 式的左边为 $f_\alpha(x^q)$. 再由 $f_\alpha(x)=\sum A_i x^i$ 得到

$$f_\alpha(x^q) = x^{qd}+A_{d-1}x^{q(d-1)}+\cdots+A_1x^q+A_0,$$

所以 $A_i^q = A_i$, $0\le i\le d-1$, 即对所有 i 有 $A_i\in K$. 因为 $f_\alpha(x)$ 是 α 在 K 上的极小多项式的因子, 又 $f_\alpha(x)\in K[x]$, 所以 $f_\alpha(x)$ 就是 α 在 K 上的极小多项式. 我们把此结论写成如下定理.

定理 2.10: 设 F 为 q^n 元域, K 是它的 q 元子域. 设 $\alpha\in F^*$, 则 α 在 K 上的极小多项式为

$$f_\alpha(x) = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\cdots(x-\alpha^{q^{d-1}}),$$

其中 d 为满足 $q^d\equiv 1 \pmod{\mathrm{ord}(\alpha)}$ 的最小正整数. □

进一步地, 显然 $[K(\alpha):K]=d$, 由 $n=[F:K]=[F:K(\alpha)][K(\alpha):K]$ 得知 $d\mid n$, 故 α 在 K 上的极小多项式的次数, 即 α 的次数 $\deg\alpha$, 为 n 的因子. 对任意正整数 ℓ, 若 $\ell = ud+r$, 其中 $0\le r\le d-1$, 则 $\alpha^{q^\ell}=\alpha^{q^r}$.

若 α 为 F 的本原元素, 则 α 在 K 上的极小多项式称为 K 上的本原多项式, 这时因为 $\mathrm{ord}(\alpha)=q^n-1$, 故 $\deg\alpha=n$. 换句话说, 有限域 $\mathbb{F}_q$ 上的 n 次本原多项式即 $\mathbb{F}_q$ 上的 n 次首一不可约多项式且以 $\mathbb{F}_q$ 的 n 次扩张 $\mathbb{F}_{q^n}$ 的本原元素为根. 注意到一个不可约多项式的根彼此共轭, 它们有相同的阶, 所以 $\mathbb{F}_q$ 上的 n 次本原多项式的每个根都是 $\mathbb{F}_{q^n}$ 的本原元素. $\mathbb{F}_{q^n}$ 中有 $\phi(q^n-1)$ 个本原元素, 而每个 n 次本原多项式有 n 个根, 由此得到如下定理.

定理 2.11: 有限域 $\mathbb{F}_q$ 上的 n 次本原多项式的个数为

$$\frac{1}{n}\phi(q^n-1),$$

其中 ϕ 为 Euler ϕ-函数. □

例如, $\mathbb{F}_2$ 上的 4 次不可约多项式 (一定首一) 的个数为 $I_2(4)=\frac{1}{4}(2^4-2^2)=3$, 而 $\mathbb{F}_2$ 上的 4 次本原多项式的个数为 $\frac{1}{4}\phi(2^4-1)=2$.

例 2.6: 设 $q=2$, $n=4$. 容易知道 x^4+x+1 为 $\mathbb{F}_2$ 上的本原多项式, 令 $F=\mathbb{F}_2[x]/(x^4+x+1)$, 记 α 为 F 中的元素 $\bar{x}$, 即向量 $(0,0,1,0)$, α 为域 F 的本原元素. 我们计算 F 中非零元素在 $\mathbb{F}_2$

上的极小多项式如下表:

i	α^i	$\mathrm{ord}(\alpha^i)$	$\deg(\alpha^i)$	极小多项式
0	0001	1	1	$x+1$
1	0010	15	4	$(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$ $=x^4+x+1$
2	0100	15	4	x^4+x+1
3	1000	5	4	$(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$ $=x^4+x^3+x^2+x+1$
4	0011	15	4	x^4+x+1
5	0110	3	2	$(x-\alpha^5)(x-\alpha^{10})=x^2+x+1$
6	1100	5	4	$x^4+x^3+x^2+x+1$
7	1011	15	4	x^4+x^3+1
8	0101			
9	1010			
10	0111			(其余的可由前面的结果给出)
11	1110			
12	1111			
13	1101			
14	1001			

如上计算的几点注记:

- $i=0$. 元素 1 的极小多项式为 $x-1$. 自然在特征为 2 的域上, $x-1$ 和 $x+1$ 是一样的.
- $i=1$. 因为 α 为元素 $\overline{x}$, 所以 α 的极小多项式就是定义这个域的不可约多项式, 本例中, 多项式 x^4+x+1 定义了域 F, 所以 α 的极小多项式为 $f_\alpha(x)=x^4+x+1$. 当然 α 的极小多项式也可以通过直接计算 $(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$ 来得到.
- $i=2$. 因为 $\alpha,\alpha^2,\alpha^4,\alpha^8$ 彼此共轭, 它们有相同的极小多项式. 所以 α^2 (以及 α^4 和 α^8) 的极小多项式为 x^4+x+1.
- $i=3$. 通过直接计算 $(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$ 得到 α^3 的极小多项式为 $x^4+x^3+x^2+x+1$. 我们也可以通过 $(\alpha^3)^5=1$ 知 α^3 为多项式 x^5-1 的根, 又 $\alpha^3\neq 1$, 所以 α^3 一定是多项式 $(x^5-1)/(x-1)=x^4+x^3+x^2+x+1$ 的根, 因为 $\deg\alpha^3=4$, 所以 α^3 的极小多项式为 $x^4+x^3+x^2+x+1$.
- $i=7$. 通过直接计算 $(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})$ 得到 α^7 的极小多项式为 $f_{\alpha^7}(x)=x^4+x^3+1$. 另外注意到 $f_{\alpha^7}(x)$ 的根, 即 $\alpha^7,\alpha^{11},\alpha^{13},\alpha^{14}$, 恰好为 $f_\alpha(x)$ 的根的逆, 具有这样性质的两个多项式有重要的联系. 设 $f(x)=a_0+a_1x+\cdots+a_mx^m\in\mathbb{F}_q[x]$ 且 $a_0a_m\neq 0$, 定义 $\tilde{f}(x)=x^mf(1/x)=a_0x^m+a_1x^{m-1}+\cdots+a_m$, 称其为多项式 $f(x)$

的互反多项式. 显然 $f(\alpha)=0$ 当且仅当 $\tilde{f}(\alpha^{-1})=0$, 所以以 $f(x)$ 的全部根的逆为根的多项式就是 $f(x)$ 的互反多项式 $\tilde{f}(x)$, 也就是把 $f(x)$ 的系数反方向写出来得到的多项式. 由于 α 与 α^{-1} 有相同的阶, 所以若 $f(x)$ 是 $\mathbb{F}_q$ 上的 m 次本原多项式, 则 $f(0)^{-1}\tilde{f}(x)$ 也是 $\mathbb{F}_q$ 上的 m 次本原多项式. 现在 $f_{\alpha^7}(x)$ 就是 $f_\alpha(x)=x^4+x+1$ 的互反多项式, 即 $f_{\alpha^7}(x)=x^4+x^3+1$. 由于 x^4+x+1 是 $\mathbb{F}_2$ 上的本原多项式, x^4+x^3+1 也是 $\mathbb{F}_2$ 上的本原多项式.

- $i>7$. 这时 α^i 与某个 α^j 共轭, 其中 $j\le 7$, 它们的阶、次数以及极小多项式均相同. □

由此例, 我们得到二元域 $\mathbb{F}_2$ 上的 2 个 4 次本原多项式为 x^4+x+1 和 x^4+x^3+1, 再加上 $x^4+x^3+x^2+x+1$, 就得到所有的 (3 个) $\mathbb{F}_2$ 上的 4 次不可约多项式. 另外多项式 $f(x)$ 称为是自互反的若 $\tilde{f}(x)=f(x)$.

下面依然设 $F=\mathbb{F}_{q^n}$ 是 $K=\mathbb{F}_q$ 的 n 次扩张, 我们来求 F 关于 K 的 Galois 群, 即 F 关于 K 的所有自同构构成的群.

定理 2.12: 域 $\mathbb{F}_{q^n}$ 关于 $\mathbb{F}_q$ 的自同构恰为如下映射 $\sigma_0,\sigma_1,\dots,\sigma_{n-1}$, 其中 σ_j 定义为对任意 $\alpha\in\mathbb{F}_{q^n}$, $\sigma_j(\alpha)=\alpha^{q^j}$, $0\le j\le n-1$. 进一步地, 这些自同构互不相同.

证明: 容易验证 σ_j 保持加法和乘法运算, 即 σ_j 为自同态, 而域的自同态一定是单同态, 又 $\mathbb{F}_{q^n}$ 为有限集合, 单射一定是满射, 所以 σ_j 为域 $\mathbb{F}_{q^n}$ 的自同构. 再注意到 $\mathbb{F}_q$ 中每个元素 a 满足 $a^q=a$, 所以对 $a\in\mathbb{F}_q$, $\sigma_j(a)=a$. 故 σ_j 是 $\mathbb{F}_{q^n}$ 的 $\mathbb{F}_q$-自同构, $0\le j\le n-1$. 这些自同构 $\sigma_0,\sigma_1,\dots,\sigma_{n-1}$ 互不相同是因为它们在 $\mathbb{F}_{q^n}$ 的本原元素上的像不同.

另一方面, 设 σ 是一个 $\mathbb{F}_{q^n}$ 关于 $\mathbb{F}_q$ 的自同构. 取 α 为 $\mathbb{F}_{q^n}$ 的一个本原元素且设 α 在 $\mathbb{F}_q$ 上的极小多项式为 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in\mathbb{F}_q[x]$. 由

$$0=\sigma(0)=\sigma(\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_0)=\sigma(\alpha)^n+a_{n-1}\sigma(\alpha)^{n-1}+\cdots+a_0$$

得知 $\sigma(\alpha)$ 也是 $f(x)$ 在域 $\mathbb{F}_{q^n}$ 中的根, 而 $f(x)$ 的根为 α 的共轭元, 故存在某个 $0\le j\le n-1$, 使得 $\sigma(\alpha)=\alpha^{q^j}$. 因为 σ 保持乘法且 α 生成群 $\mathbb{F}_{q^n}^*$, 又 $\sigma(0)=0=0^{q^j}$, 所以对任意 $\beta\in\mathbb{F}_{q^n}$ 有 $\sigma(\beta)=\beta^{q^j}$, 即 $\sigma=\sigma_j$. □

实际上, $\alpha\in\mathbb{F}_{q^n}$ 关于 $\mathbb{F}_q$ 的共轭元可以通过 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的所有自同构作用在元素 α 上得到. 另外, $\sigma_j=\sigma_1^j$, $0\le j\le n-1$, 所以 $\mathbb{F}_{q^n}$ 关于 $\mathbb{F}_q$ 的 Galois 群为由 σ_1 生成的 n 阶循环群, 即 $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)=\langle\sigma_1\rangle$. σ_1 为映射 $\alpha\mapsto\alpha^q$, 常称为 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的 Frobenius 自同构. 又显然扩张 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 为 Galois 扩张.

注意到素域的自同构只有恒等映射. 设 p 为素数, 则有 $\mathrm{Aut}(\mathbb{F}_{p^n})=\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)=\langle\tau\rangle$, 其中 $\tau(\alpha)=\alpha^p$ 对所有 $\alpha\in\mathbb{F}_{p^n}$, 即任意有限域的自同构群为循环群. 进一步地, 设 $m\mid n$, 则 $\mathbb{F}_{p^m}$ 为 $\mathbb{F}_{p^n}$ 的子域, 且 $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})=\langle\tau^m\rangle$.

一个多项式可约与否与对应的域有关, 设 $f(x)\in F[x]$, $f(x)$ 在域 F 上不可约, 但在 F 的扩域上有可能是可约的, 比如 $f(x)$ 在它的分裂域上一定可约. 下面我们看有限域的情形, 设

$K=\mathbb{F}_q$, $L=\mathbb{F}_{q^m}$ 为 K 的 m 次扩张, $f(x)\in K[x]$ 是 K 上的 n 次 (首一) 不可约多项式, 那么 $f(x)$ 看成域 L 上的多项式在 L 上可约或不可约情况如何?

设 α 是 $f(x)$ 的一个根 (α 在域 $\mathbb{F}_{q^n}$ 中), 则 $f(x)$ 就是 α 在 K 上的极小多项式, 其次数 n 为满足 $q^n\equiv 1 \pmod{\mathrm{ord}(\alpha)}$ 的最小正整数, 记 $t=\mathrm{ord}(\alpha)$, 所以 n 为 q 模 t 的乘法阶 $\mathrm{ord}_t(q)$. 我们把 α 也看成是 L 的某个扩域中的元素, 比如 L 的扩域 $\mathbb{F}_{q^{mn}}$, $f(x)\in L[x]$ 为 α 的零化多项式, 所以 α 在域 L 上的极小多项式 $f_\alpha(x)\in L[x]$ 就是 $f(x)$ 在 L 上的不可约因式. 注意到 $f_\alpha(x)$ 的次数 d 是 $\mathrm{ord}_t(q^m)$, 由 $\mathrm{ord}_t(q)=n$ 可得 $d=\mathrm{ord}_t(q^m)=\frac{n}{\gcd(m,n)}$. 如果 $d<n$, 我们可以取 $f(x)$ 的根 β, 且 β 不是 $f_\alpha(x)$ 的根, 则 β 在域 L 上的极小多项式 $f_\beta(x)$ 也是 $f(x)$ 在 L 上的不可约因式. 由于 $\mathrm{ord}(\beta)=\mathrm{ord}(\alpha)$, 所以 $f_\beta(x)$ 的次数依然是 d. 以此类推, 我们可以推出, 多项式 $f(x)$ 可以分解成 $\frac{n}{d}$ 个域 L 上的 d 次首一不可约多项式的乘积. 这便证明了如下定理.

定理 2.13: 设 $f(x)$ 是 $\mathbb{F}_q$ 上的 n 次不可约多项式, m 为正整数, $s=\gcd(m,n)$, $d=\frac{n}{s}$, 则 $f(x)$ 可以分解成 s 个 $\mathbb{F}_{q^m}$ 上的 d 次不可约多项式的乘积. □

推论 2.14: 域 $\mathbb{F}_q$ 上的 n 次不可约多项式在 $\mathbb{F}_{q^m}$ 上依然不可约当且仅当 m 与 n 互素. □

2.4 有限域中元素的表示

要实现有限域中的运算, 就必须首先对元素进行表示, 所以有限域中元素的表示是有限域实际应用时需要解决的基础问题. 有限域中的元素可以有不同的表示形式, 表示形式的不同会带来有限域中运算效率的变化, 我们第三章中将学习有限域的基也对应着有限域中元素的表示形式.

有限域中非零元素可表为该有限域一个本原元素的方幂, 设 $\alpha\in\mathbb{F}_q$ 是 $\mathbb{F}_q$ 的一个本原元素 (本章第 1 节给出了如何求一个有限域的本原元素), 则 $\mathbb{F}_q=\{0,\alpha^0=1,\alpha,\alpha^2,\ldots,\alpha^{q-2}\}$. 对于 $\beta\in\mathbb{F}_q^*$, 存在唯一整数 r 满足 $0\le r\le q-2$ 使得 $\beta=\alpha^r$, 这个唯一的整数 r 称为以 α 为底 β 的对数, 记作 $\log_\alpha\beta$, 有些文献也称其为 β 关于 α 的指数, 记为 $\mathrm{ind}_\alpha(\beta)$, 在本原元素 α 取定且上下文清楚的情况下, 元素 β 的对数或指数也可以简记为 $\log\beta$ 或 $\mathrm{ind}(\beta)$. 类似于例 1.4, 我们可以列出域 $\mathbb{F}_q$ 的对数表和指数表. 在有限域元素的这种表示方式下, 我们容易计算域中两个元素的乘积, 也容易计算非零元素的逆, 事实上, 对于 $\beta,\gamma\in\mathbb{F}_q^*$, 显然有 $\mathrm{ind}(\beta\gamma)\equiv\mathrm{ind}(\beta)+\mathrm{ind}(\gamma)\pmod{q-1}$ 和 $\mathrm{ind}(\beta^{-1})=q-1-\mathrm{ind}(\beta)$. 但是要做域中的加法就不容易了, 这时我们可以利用所谓的 Jacobi 对数, 对于 $r\in\mathbb{Z}_{q-1}$, 定义 $L(r)$ 满足 $1+\alpha^r=\alpha^{L(r)}$, 去掉 $\alpha^r=-1$ 的情形 (即若 q 为奇数, 则去掉 $r=\frac{q-1}{2}$, 若 q 为偶数, 则去掉 $r=0$). 对于有限域 $\mathbb{F}_q$, 可以预先列出它的 Jacobi 对数表, 这样就容易得到

$$\alpha^r+\alpha^s=\alpha^r(1+\alpha^{s-r})=\alpha^{r+L(s-r)}.$$

例 2.7: 设 $\mathbb{F}_{16}=\mathbb{F}_2[x]/(x^4+x+1)$, 令 $\alpha=\overline{x}$, 则 α 是 $\mathbb{F}_{16}$ 的本原元素, 我们可得 $\mathbb{F}_{16}$ 的 Jacobi

对数表如下:

i	$L(i)$	i	$L(i)$	i	$L(i)$	i	$L(i)$	i	$L(i)$
0	*	3	14	6	13	9	7	12	11
1	4	4	1	7	9	10	5	13	6
2	8	5	10	8	2	11	12	14	3

利用此 Jacobi 对数表, 我们来计算 $(\alpha^6+\alpha^{10}+\alpha^{14})(1+\alpha^9)^{-1}+\alpha^8$. 由于 $\alpha^6+\alpha^{10}=\alpha^{6+L(4)}=\alpha^7$, $\alpha^7+\alpha^{14}=\alpha^{7+L(7)}=\alpha^{16}$, $1+\alpha^9=\alpha^{L(9)}=\alpha^7$, 故 $(\alpha^6+\alpha^{10}+\alpha^{14})(1+\alpha^9)^{-1}=\alpha^{16}\alpha^{-7}=\alpha^9$, 再由 $\alpha^9+\alpha^8=\alpha^{9+L(-1)}=\alpha^{9+L(14)}=\alpha^{12}$ 就得到 $(\alpha^6+\alpha^{10}+\alpha^{14})(1+\alpha^9)^{-1}+\alpha^8=\alpha^{12}$, 这里要注意到 L 定义在 $\mathbb{Z}_{15}$ 上, 所以对 $L(r)$ 中的 r 要做模 15 的运算. □

设 p 为素数, $q=p^n$, 取 $f(x)$ 为 $\mathbb{F}_p$ 上的一个 n 次首一不可约多项式, 令 $\mathbb{F}_q=\mathbb{F}_p[x]/(f(x))$ 和 $\alpha=\overline{x}$, 则 $\mathbb{F}_q$ 中每一元素可以唯一地表示成 $a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0$ 的形式, 其中 $a_i\in\mathbb{F}_p$, $0\le i\le n-1$, 我们也可以利用 $\mathbb{F}_p$ 上的 n-维向量 $(a_{n-1},\ldots,a_1,a_0)$ 来表示这个元素 (如例 1.4). 在这种表示下, 域 $\mathbb{F}_q$ 中的加法就是通常向量的加法, 即对应分量相加 (分量相加是在 $\mathbb{F}_p$ 中), 但是乘法和求逆则比较繁琐, 我们可以如下进行. 对于 $\beta,\gamma\in\mathbb{F}_q$, 设 $\beta=(b_{n-1},\ldots,b_1,b_0)=b_{n-1}\alpha^{n-1}+\cdots+b_1\alpha+b_0$, $\gamma=(c_{n-1},\ldots,c_1,c_0)=c_{n-1}\alpha^{n-1}+\cdots+c_1\alpha+c_0$, 其中 b_i, $c_i\in\mathbb{F}_p$, $i=0,1,2,\ldots,n-1$. 令 $b(x)=b_{n-1}x^{n-1}+\cdots+b_1x+b_0$, $c(x)=c_{n-1}x^{n-1}+\cdots+c_1x+c_0$, 则 $b(x),c(x)\in\mathbb{F}_p[x]$ 且 $b(\alpha)=\beta$, $c(\alpha)=\gamma$. 在 $\mathbb{F}_p[x]$ 中作带余除法, 设

$$b(x)c(x)=q(x)f(x)+r(x),$$

其中 $q(x),r(x)\in\mathbb{F}_p[x]$ 且 $\deg r(x)<n$. 记 $r(x)=r_{n-1}x^{n-1}+\cdots+r_1x+r_0$, 带入 $x=\alpha$ 得到

$$\beta\gamma=b(\alpha)c(\alpha)=q(\alpha)f(\alpha)+r(\alpha)=r(\alpha)=r_{n-1}\alpha^{n-1}+\cdots+r_1\alpha+r_0,$$

即

$$(b_{n-1},\ldots,b_1,b_0)\cdot(c_{n-1},\ldots,c_1,c_0)=(r_{n-1},\ldots,r_1,r_0).$$

设 $\beta\ne0$, 为计算 β^{-1}, 注意到 $\gcd(b(x),f(x))=1$, 对 $b(x)$ 和 $f(x)$ 施行 Euclid 算法, 我们得到

$$g(x)b(x)+h(x)f(x)=1,$$

其中 $g(x),h(x)\in\mathbb{F}_p[x]$ 且 $\deg g(x)<\deg f(x)$, $\deg h(x)<\deg b(x)$. 带入 $x=\alpha$ 得到 $g(\alpha)b(\alpha)=1$, 所以 $\beta^{-1}=g(\alpha)$. 记 $g(x)=g_{n-1}x^{n-1}+\cdots+g_1x+g_0$, 则有

$$(b_{n-1},\ldots,b_1,b_0)^{-1}=(g_{n-1},\ldots,g_1,g_0).$$

$\mathbb{F}_q$ 中的元素除了可用 $\mathbb{F}_p$ 上的 n-维向量表示外, 还可以用 $\mathbb{F}_p$ 上的 n 阶矩阵来表示. 我们依然设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{F}_p[x]$ 为 $\mathbb{F}_p$ 的一个 n 次首一不可约多项式,

定义 $\mathbb{F}_p$ 上的 n 阶矩阵

$$A=\begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{bmatrix},$$

称矩阵 A 为多项式 $f(x)$ 的伴随矩阵 (或友矩阵). 容易验证矩阵 A 的特征多项式 $\det(xI-A)$ 就是多项式 $f(x)$, 从而 $f(A)=0$, 又由 $f(x)$ 不可约得到 $f(x)$ 也是矩阵 A 的极小多项式. 令 $F=\{g(A)\mid g(x)\in\mathbb{F}_p[x]\}$, 运算为通常的矩阵加法和乘法, 设 α 为 $f(x)$ 的一个根, 则容易验证 $\alpha\mapsto A$ 可诱导出 $\mathbb{F}_p(\alpha)=\mathbb{F}_p[x]/(f(x))$ 到 F 的同构 $g(\alpha)\mapsto g(A)$, 其中 $g(x)\in\mathbb{F}_p[x]$. 这表明 F 在通常的矩阵加法和乘法下构成一个 q 元域, 我们令 $\mathbb{F}_q=F$, 这时 $\mathbb{F}_q$ 中每个元素都是矩阵 A 的系数在 $\mathbb{F}_p$ 中的多项式, 故为 $\mathbb{F}_p$ 上的 n 阶矩阵, 而运算就是通常的矩阵运算. 注意到对任意 $g(A)\in F$, 我们可以要求其对应的多项式 $g(x)\in\mathbb{F}_p[x]$ 满足 $\deg(g(x))<n$, 因为对任意 $g(x)\in\mathbb{F}_p[x]$, 作带余除法 $g(x)=h(x)f(x)+r(x)$, 其中 $\deg(r(x))<n$, 则 $g(A)=r(A)$. 进一步地, 类似于 $\mathbb{F}_p(\alpha)$ 中的元素用 α 的多项式形式表示, 域 F 中所有元素与 $\mathbb{F}_p$ 上所有次数小于 n 的多项式之间有一一对应的关系, 即 F 中的每个元素可以唯一地表示为 $g(A)$, 其中 $\deg(g(x))<n$.

例 2.8: 设 $f(x)=x^2+1\in\mathbb{F}_3[x]$, $f(x)$ 为 $\mathbb{F}_3$ 上的不可约多项式, $f(x)$ 的伴随矩阵为

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

由此我们得到 9 元域

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

或者详细表出为

$$\begin{aligned}\mathbb{F}_9 \;=\; &\left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix},\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix},\right. \\ &\left.\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix},\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix},\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix},\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}\right\}.\end{aligned}$$

通过通常的矩阵运算可以得到

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

□

类似于有限域中每个非零元素都是此域一个本原元素的方幂, 若我们取 $f(x)$ 为 $\mathbb{F}_p$ 上的 n 次本原多项式, A 为 $f(x)$ 的伴随矩阵, 则 $\mathbb{F}_q$ 中每个非零元可以表为矩阵 A 的方幂. 例如取

$f(x) = x^2 + x + 2$, 则 $f(x)$ 是 $\mathbb{F}_3$ 上的本原多项式, 它的伴随矩阵为

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

则有

$$\mathbb{F}_9 = \{0, A, A^2, A^3, A^4, A^5, A^6, A^7, A^8 = I\}.$$

在这种表示下乘法运算依然容易, 而加法是矩阵的加法，需要把具体的矩阵求出来, 例如可以计算出

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

2.5 习题

2.1 找出最小素数 p 使得 2 和 3 都是域 $\mathbb{F}_p$ 的本原元素.

2.2 在域 $\mathbb{F}_{73}$ 中,

a. 计算 $\mathrm{ord}(2)$ 和 $\mathrm{ord}(3)$.

b. 构造一个元素使其阶为 $\mathrm{lcm}(\mathrm{ord}(2), \mathrm{ord}(3))$.

c. 设 α 为 (b) 中构造的元素, 则 $\{1, 2, \ldots, 72\}$ 中不是 α 方幂的最小数是什么? 这个数的阶是什么?

d. 计算 $\sqrt[30]{64}$ 和 $\sqrt[30]{59}$.

2.3 方程 $x^2 - 1 = 0$ 在环 $\mathbb{Z}_{2^n}$ 中有多少个根?

2.4 设域 $\mathbb{F}_{49} = \mathbb{Z}_7[x]/(x^2 - 3)$, 令 α 为 x 所在的等价类.

a. 计算 α 在此域中的阶.

b. 找此域中的一个本原元素, 并把 α 表为该本原元素的方幂.

c. 给出 (b) 中所求本原元素的极小多项式.

2.5 利用 $\mathbb{F}_3$ 上的本原多项式 $x^3 + 2x + 1$ 构作域 $\mathbb{F}_{27}$, 列出它的 27 个元素, 并对每个元素计算其极小多项式和阶.

2.6 把分数 $1/7$ 用循环十进制小数表示, 即 $1/7 = 0.14285714\cdots$, 其循环周期为 6, 而分数 $1/11 = 0.090909\cdots$, 循环周期为 2. 一般说来, 设 p 为不等于 5 的奇素数, $1 \le k \le p-1$, 则分数 k/p 表示为循环十进制小数的循环周期等于域 $\mathbb{F}_p$ 中元素 10 的阶, 试证明之, 并说明为什么 $p \ne 5$?

2.7 设 F 是域, 定义映射 $\psi : F \to F$ 为 $\psi(a) = a^{-1}$ 若 $a \ne 0$ 而 $\psi(0) = 0$, 证明 ψ 是 F 的一个自同构当且仅当 F 有至多 4 个元素.

2.8 证明 $\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^{\gcd(m,n)}}$ 和 $\mathbb{F}_{p^m}\mathbb{F}_{p^n} = \mathbb{F}_{p^{\mathrm{lcm}(m,n)}}$.

2.9 类似于例 2.5, 分别画出域 $\mathbb{F}_{p^{16}}$, $\mathbb{F}_{p^{20}}$ 和 $\mathbb{F}_{p^{24}}$ 的子域构成的格, 其中 p 为素数.

2.10 设有限域 $\mathbb{F}_q$ 的特征为素数 p, $f(x) \in \mathbb{F}_q[x]$. 证明 $f'(x) = 0$ 当且仅当 $f(x)$ 为 $\mathbb{F}_q[x]$ 中某个多项式的 p 次幂.

2.11 设 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{F}_q[x]$ 不可约, $a_0 \neq 0$, 且 $\alpha \in \mathbb{F}_{q^n}$ 是 $f(x)$ 的一个根. 证明如下论断:

a. 元素 $\alpha^{-1} \in \mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的极小多项式为 $f^*(x) = a_0^{-1}\tilde{f}(x)$, 其中 $\tilde{f}(x)$ 是 $f(x)$ 的互反多项式.

b. $f(x) = f^*(x)$ 当且仅当对某个非负整数 $m \geq 0$ 有 $\alpha^{q^m+1} = 1$.

c. 若 $f(x) = f^*(x)$, 则或者 $n = 1$ 且 $f(x) = x \pm 1$ 或者 n 为偶数且 $a_0 = 1$.

2.12 构作域 $\mathbb{F}_9$ 和 $\mathbb{F}_{17}$ 的 Jacobi 对数表.

2.13 利用 $\mathbb{F}_2$ 上的不可约多项式 $f(x) = x^3 + x + 1$, 给出域 $\mathbb{F}_8$ 的矩阵表示. (由于 $f(x)$ 为 $\mathbb{F}_2$ 上的本原多项式, 所以 $\mathbb{F}_8$ 中每个非零元可以表为它的伴随矩阵的方幂.)

2.14 设 k 为正整数, $\alpha \in \mathbb{F}_q^*$, 证明 α 为 $\mathbb{F}_q$ 中某个元素的 k 次幂当且仅当 $\alpha^{\frac{q-1}{d}} = 1$, 其中 $d = \gcd(k, q-1)$. 进一步地, 证明 $\mathbb{F}_q$ 中每个元素都是 $\mathbb{F}_q$ 中某个元素的 k 次幂当且仅当 $\gcd(k, q-1) = 1$.

2.15 证明对任意 $a \in \mathbb{F}_q$ 和任意正整数 n, 在 $\mathbb{F}_q[x]$ 中 $x^{q^n} - x + na$ 可被 $x^q - x + a$ 整除.

2.16 设 F 为任意域, 证明 F 的乘法群 F^* 的每个有限子群都是循环群. 进一步地, 若 F^* 为循环群, 则 F 一定有限.

2.17 设 n 为奇数, $a, b \in \mathbb{F}_{2^n}$ 满足 $a^2 + ab + b^2 = 0$, 证明 $a = b = 0$.

第三章　迹, 范数和基

本章中设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$, 则 K 为 F 的子域且 $[F:K]=n$.

3.1　迹与范数

对于 $\alpha\in F$, 定义 α 在 K 上的迹为

$$\mathrm{Tr}_{F/K}(\alpha)=\alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}}, \tag{3.1}$$

而 α 在 K 上的范数为

$$\mathrm{N}_{F/K}(\alpha)=\alpha\cdot\alpha^q\cdot\alpha^{q^2}\cdot\cdots\cdot\alpha^{q^{n-1}}, \tag{3.2}$$

设 σ 为 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的 Frobenius 自同构, 即对任意 $\alpha\in\mathbb{F}_{q^n}$, $\sigma(\alpha)=\alpha^q$, 则 $\mathrm{Gal}(F/K)=\langle\sigma\rangle$, 从而

$$\mathrm{Tr}_{F/K}(\alpha)=\sum_{i=0}^{n-1}\sigma^i(\alpha)=\sum_{\varphi\in\mathrm{Gal}(F/K)}\varphi(\alpha),\quad \mathrm{N}_{F/K}(\alpha)=\prod_{i=0}^{n-1}\sigma^i(\alpha)=\prod_{\varphi\in\mathrm{Gal}(F/K)}\varphi(\alpha),$$

所以, α 在 K 上的迹为群 $\mathrm{Gal}(F/K)$ 中的元素作用到 α 上所得元素之和, 而 α 在 K 上的范数是这些所得元素之积. 迹与范数显然与相应的域有关, 所以在符号中我们列出了相应的域, 但当上下文中考虑的域清楚时, 我们也可以在符号中省略相应的域而只记为 Tr 和 N, 如同下面这个定理表示的这样.

定理 3.1: 对所有 $\alpha,\beta\in F$, 我们有

(a). $\mathrm{Tr}(\alpha)\in K$, $\mathrm{N}(\alpha)\in K$, 所以 Tr 和 N 都是 F 到 K 的映射, 分别称为 F 到 K 的迹映射和范数映射.

(b). $\mathrm{Tr}(\alpha+\beta)=\mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)$, $\mathrm{N}(\alpha\beta)=\mathrm{N}(\alpha)\mathrm{N}(\beta)$.

(c). 若 $a\in K$, 则 $\mathrm{Tr}(a\alpha)=a\mathrm{Tr}(\alpha)$, $\mathrm{N}(a\alpha)=a^n\mathrm{N}(\alpha)$.

(d). $\mathrm{Tr}(\alpha^q)=\mathrm{Tr}(\alpha)$, $\mathrm{N}(\alpha^q)=\mathrm{N}(\alpha)$. 进一步地, 若 $\beta\in F$ 为 α 的共轭元素, 则 $\mathrm{Tr}(\beta)=\mathrm{Tr}(\alpha)$ 且 $\mathrm{N}(\beta)=\mathrm{N}(\alpha)$.

(e). Tr 是 F 到 K 的满线性函数 (把 F 看成 K 上的线性空间), N 是群 F^* 到 K^* 的满同态.

证明: 我们只对迹的情形进行证明, 范数情形的证明是类似的.

(a) 因为 $\alpha^{q^n}=\alpha$, 所以

$$\mathrm{Tr}(\alpha)^q=(\alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}})^q=\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}}+\alpha=\mathrm{Tr}(\alpha).$$

由定理 2.2, $\mathrm{Tr}(\alpha)\in K$.

(b) 由定理 1.2 以及 q 为域 F 的特征的方幂知对于任意 $i\geq 0$ 有 $(\alpha+\beta)^{q^i}=\alpha^{q^i}+\beta^{q^i}$.

(c) 依然根据定理 2.2 知对任意 $a\in K$ 和 $i\geq 0$, 有 $a^{q^i}=a$.

(d) 因为 $\alpha^{q^n}=\alpha$, 我们有

$$\mathrm{Tr}(\alpha^q)=\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}}+\alpha^{q^n}=\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}}+\alpha=\mathrm{Tr}(\alpha).$$

(e) 由上面的 (a), (b) 和 (c) 知映射 Tr 为 F 到 K 的线性映射, 由线性映射基本定理有 $F/\mathrm{Ker}(\mathrm{Tr})\cong\mathrm{Tr}(F)\leq K$. 注意到 $\mathrm{Ker}(\mathrm{Tr})=\{\alpha\in F\mid \alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}}=0\}$, 又多项式 $x+x^q+x^{q^2}+\cdots+x^{q^{n-1}}$ 在 F 中有至多 q^{n-1} 个根, 所以 $|\mathrm{Ker}(\mathrm{Tr})|\leq q^{n-1}$. 这样 $|\mathrm{Tr}(F)|\geq q$, 再由 $\mathrm{Tr}(F)\leq K$ 得知 $\mathrm{Tr}(F)=K$, 所以 $\mathrm{Tr}:F\to K$ 为满射. □

由上面 (e) 的证明得到 $|\mathrm{Ker}(\mathrm{Tr})|=q^{n-1}$. 对于任意 $a\in K$, a 在 Tr 下的原像为子空间 $\mathrm{Ker}(\mathrm{Tr})$ 的一个陪集 $\alpha+\mathrm{Ker}(\mathrm{Tr})$, 其中 $\mathrm{Tr}(\alpha)=a$. 由此得知, 对于任意 $a\in K$, 恰有 F 中 q^{n-1} 个元素的迹为 a. 类似地, 0 的范数为 0, 而对任意 $a\in K$, $a\neq 0$, 则恰有 F 中 $\frac{q^n-1}{q-1}$ 个元素的范数为 a.

例 3.1: 设 $K=\mathbb{F}_2$, $F=\mathbb{F}_{2^4}=\mathbb{F}_2[x]/(f(x))$, 其中 $f(x)=x^4+x^3+x^2+x+1$ 在 $\mathbb{F}_2$ 上不可约. 令 $\alpha=\overline{x}$, 则 α 为 $f(x)$ 的根且对任意 $\beta\in F$, β 可以唯一表为

$$\beta=a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3,$$

其中 $a_i\in K$. 定理 3.1 的 (b) 和 (c) 给出

$$\mathrm{Tr}(\beta)=a_0\mathrm{Tr}(1)+a_1\mathrm{Tr}(\alpha)+a_2\mathrm{Tr}(\alpha^2)+a_3\mathrm{Tr}(\alpha^3).$$

所以为计算 $\mathrm{Tr}(\beta)$, 只需计算 $\mathrm{Tr}(1)$, $\mathrm{Tr}(\alpha)$, $\mathrm{Tr}(\alpha^2)$ 和 $\mathrm{Tr}(\alpha^3)$ 即可. 显然 $\mathrm{Tr}(1)=1+1+1+1=0$. 现在 $\mathrm{Tr}(\alpha)=\alpha+\alpha^2+\alpha^4+\alpha^8$, 这可以在域 F 中直接计算. 但是注意到 α 的极小多项式为 $f(x)$, 所以 $f(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)=x^4+c_3x^3+c_2x^2+c_1x+c_0$, 故 $\mathrm{Tr}(\alpha)=-c_3=c_3$ (特征为 2), 由 $f(x)=x^4+x^3+x^2+x+1$ 得到 $\mathrm{Tr}(\alpha)=1$. 利用定理 3.1 的 (d) 有 $\mathrm{Tr}(\alpha^2)=\mathrm{Tr}(\alpha)=1$. 最后因为 $\alpha^5=1$, 所以 $\alpha^3=\alpha^8$, 即 α^3 与 α 共轭, 所以 $\mathrm{Tr}(\alpha^3)=\mathrm{Tr}(\alpha)=1$. 综合起来我们得到

$$\mathrm{Tr}(1)=0,\quad \mathrm{Tr}(\alpha)=\mathrm{Tr}(\alpha^2)=\mathrm{Tr}(\alpha^3)=1,$$

所以若 $\beta=a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3$, 则

$$\mathrm{Tr}(\beta)=a_1+a_2+a_3.$$

类似地, 下面设 $F=\mathbb{F}_{2^4}=\mathbb{F}_2[x]/(x^4+x+1)$, 依然令 $\alpha=\overline{x}$, 则对任意 $\beta\in F$, β 也可以唯一表为

$$\beta=a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3,$$

其中 $a_i \in \mathbb{F}_2$. 这时 $\mathrm{Tr}(1) = 0$, $\mathrm{Tr}(\alpha) = 0$ (多项式 $x^4 + x + 1$ 中 x^3 的系数), $\mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha) = 0$ (α^2 与 α 共轭). 这只需计算 $\mathrm{Tr}(\alpha^3)$. 若 $\mathrm{Tr}(\alpha^3) = 0$, 则推出对所有 $\beta \in F$ 有 $\mathrm{Tr}(\beta) = 0$, 与 Tr 为满射矛盾, 所以一定有 $\mathrm{Tr}(\alpha^3) = 1$, 这时 $\mathrm{Tr}(\beta) = a_3$. □

下面设 $K \subseteq L \subseteq F$ 是有限域的扩张链, 其中 $K = \mathbb{F}_q$, $L = \mathbb{F}_{q^d}$, $F = \mathbb{F}_{q^n}$, 则显然有 d 为 n 的因子. 这时需要考虑三个迹映射

$$\begin{aligned} \mathrm{Tr}_{F/K}(\alpha) &= \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}, \\ \mathrm{Tr}_{L/K}(\alpha) &= \alpha + \alpha^q + \cdots + \alpha^{q^{d-1}}, \\ \mathrm{Tr}_{F/L}(\alpha) &= \alpha + \alpha^{q^d} + \cdots + \alpha^{q^{d(\frac{n}{d}-1)}}, \end{aligned}$$

也有三个范数映射

$$\begin{aligned} \mathrm{N}_{F/K}(\alpha) &= \alpha^{1+q+\cdots+q^{n-1}}, \\ \mathrm{N}_{L/K}(\alpha) &= \alpha^{1+q+\cdots+q^{d-1}}, \\ \mathrm{N}_{F/L}(\alpha) &= \alpha^{1+q^d+\cdots+q^{d(\frac{n}{d}-1)}}. \end{aligned}$$

通过直接计算, 可以证明如下定理.

定理 3.2: 对任意 $\alpha \in F$, 有 $\mathrm{Tr}_{F/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{F/L}(\alpha))$ 和 $\mathrm{N}_{F/K}(\alpha) = \mathrm{N}_{L/K}(\mathrm{N}_{F/L}(\alpha))$, 即作为映射来说, $\mathrm{Tr}_{F/K} = \mathrm{Tr}_{L/K}\mathrm{Tr}_{F/L}$ 和 $\mathrm{N}_{F/K} = \mathrm{N}_{L/K}\mathrm{N}_{F/L}$.

证明: 现在用 Galois 群的写法证明, 记 $t = \frac{n}{d}$. 设 σ 为 $\mathbb{F}_{q^n}$ 的 $\mathbb{F}_q$ 上的 Frobenius 自同构, 即对任意 $\alpha \in \mathbb{F}_{q^n}$, $\sigma(\alpha) = \alpha^q$, 则 $\mathrm{Gal}(F/K) = \langle\sigma\rangle$, $\mathrm{Gal}(F/L) = \langle\sigma^d\rangle$, 以及 $\mathrm{Gal}(L/K) = \langle\sigma'\rangle$, 其中 $\sigma' = \sigma|_L$. 所以, 对任意 $\alpha \in F$, 有

$$\begin{aligned} \mathrm{Tr}_{L/K}(\mathrm{Tr}_{F/L}(\alpha)) &= \mathrm{Tr}_{L/K}\left(\sum_{i=0}^{t-1}\sigma^{di}(\alpha)\right) = \sum_{j=0}^{d-1}\sigma^j\left(\sum_{i=0}^{t-1}\sigma^{di}(\alpha)\right) \\ &= \sum_{i=0}^{t-1}\sum_{j=0}^{d-1}\sigma^{di+j}(\alpha) = \sum_{k=0}^{n-1}\sigma^k(\alpha) = \mathrm{Tr}_{F/K}(\alpha). \end{aligned}$$

对范数映射的证明是类似的. □

下面继续讨论映射 $\mathrm{Tr}_{F/K}$ 和 $\mathrm{N}_{F/K}$, 其中 $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^n}$. 对于 $\alpha \in F$, 设 α 在 K 上的共轭元素为 $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$, 其中 $d \mid n$, 则 α 在 K 上的极小多项式为

$$(x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{d-1}}) = x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0 \in K[x]. \tag{3.3}$$

下面这个定理表明 $\mathrm{Tr}_{F/K}(\alpha)$ 和 $\mathrm{N}_{F/K}(\alpha)$ 可以由 α 在 K 上的极小多项式的系数表出.

定理 3.3: 设 $\alpha \in F$ 在 K 上的极小多项式为 $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$, 则

$$\mathrm{Tr}_{F/K}(\alpha) = -\frac{n}{d}c_{d-1}, \quad \mathrm{N}_{F/K}(\alpha) = (-1)^n c_0^{\frac{n}{d}}.$$

证明: 设 $L = K(\alpha)$, 则 $L = \mathbb{F}_{q^d}$ 是 $F = \mathbb{F}_{q^n}$ 的子域. 因为 $\alpha \in L$, 所以 $\mathrm{Tr}_{F/L}(\alpha) = \frac{n}{d} \cdot \alpha$, 故

$$\mathrm{Tr}_{F/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{F/L}(\alpha)) = \mathrm{Tr}_{L/K}\left(\frac{n}{d}\cdot\alpha\right) = \frac{n}{d}\mathrm{Tr}_{L/K}(\alpha).$$

式 (3.3) 给出 $\mathrm{Tr}_{L/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{d-1}} = -c_{d-1}$, 所以 $\mathrm{Tr}_{F/K}(\alpha) = -\frac{n}{d} \cdot c_{d-1}$. 对 $\mathrm{N}_{F/K}(\alpha)$ 的证明是类似的. □

例 3.2: 设 $K=\mathbb{F}_2$, $F=\mathbb{F}_{2^4}=\mathbb{F}_2[x]/(x^4+x+1)$. 记 $\alpha=\overline{x}$, 参考例 2.6, 我们得到 F 中所有非零元素的迹如下表:

i	α^i 的极小多项式	$\mathrm{Tr}(\alpha^i)$	注释
0	$x+1$	0	$c_{d-1}=1$, $n/d=4$.
1	x^4+x+1	0	$c_{d-1}=0$, $n/d=1$.
2	x^4+x+1	0	α^2 共轭于 α.
3	$x^4+x^3+x^2+x+1$	1	$c_{d-1}=1$, $n/d=1$.
4	x^4+x+1	0	α^4 共轭于 α.
5	x^2+x+1	0	$c_{d-1}=1$, $n/d=2$.
6	$x^4+x^3+x^2+x+1$	1	α^6 共轭于 α^3.
7	x^4+x^3+1	1	$c_{d-1}=1$, $n/d=1$.
8	x^4+x+1	0	α^8 共轭于 α.
9	$x^4+x^3+x^2+x+1$	1	α^9 共轭于 α^3.
10	x^2+x+1	0	α^{10} 共轭于 α^5.
11	x^4+x^3+1	1	α^{11} 共轭于 α^7.
12	$x^4+x^3+x^2+x+1$	1	α^{12} 共轭于 α^3.
13	x^4+x^3+1	1	α^{13} 共轭于 α^7.
14	x^4+x^3+1	1	α^{14} 共轭于 α^7.

又显然在本例中, $N(0)=0$, 而对任意 $0\le i\le 14$, 有 $N(\alpha^i)=1$. □

迹和范数也可以用线性变换来刻画. 设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$, 则 F 是 K 上的 n-维线性空间. 对于 $\alpha\in F$, 定义变换 T_α 为

$$\begin{array}{rccc} T_\alpha: & F & \to & F \\ & \beta & \mapsto & \alpha\beta, \end{array} \tag{3.4}$$

则 T_α 是 F 上的线性变换. 线性代数中我们知道线性变换的迹和行列式就是此线性变换在线性空间的任一组基下矩阵的迹和行列式 (与基的选取无关). 下面我们计算线性变换 T_α 的迹和行列式.

设 $L=K(\alpha)$ 且 α 在 K 上的极小多项式为 $f(x)=x^d+c_{d-1}x^{d-1}+\cdots+c_1x+c_0$, 则 $d\mid n$, 且 $\{1,\alpha,\ldots,\alpha^{d-1}\}$ 是 L 在 K 上的一组基, 显然

$$T_\alpha(1,\alpha,\cdots,\alpha^{d-1})=(1,\alpha,\cdots,\alpha^{d-1})A,$$

其中矩阵

$$A=\begin{pmatrix} 0 & & & & -c_0 \\ 1 & 0 & & & -c_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -c_{d-2} \\ & & & 1 & -c_{d-1} \end{pmatrix}.$$

记 $t=\frac{n}{d}$ 并设 $\{v_1,v_2,\ldots,v_t\}$ 是 F 在 L 上的一组基, 则 $\{v_1,v_1\alpha,\ldots,v_1\alpha^{d-1},v_2,v_2\alpha,\ldots,v_2\alpha^{d-1},\ldots,v_t,v_t\alpha,\ldots,v_t\alpha^{d-1}\}$ 是 F 在 K 上的一组基, 线性变换 T_α 在 F 的这组基下的矩阵为

$$M_\alpha=\begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix},$$

所以线性变换 T_α 的迹为 $\mathrm{Tr}(T_\alpha)=\mathrm{Tr}(M_\alpha)=t\mathrm{Tr}(A)=-\frac{n}{d}c_{d-1}$, 而 T_α 的行列式为 $\det(T_\alpha)=\det(M_\alpha)=\det(A)^t=((-1)^dc_0)^t=(-1)^nc_0^{\frac{n}{d}}$. 由定理 3.3, 我们有如下定理.

定理 3.4: 设 $\alpha\in F$ 且域 F 上的线性变换 T_α 由式 (3.4) 给出, 则 $\mathrm{Tr}_{F/K}(\alpha)=\mathrm{Tr}(T_\alpha)$, $\mathrm{N}_{F/K}(\alpha)=\det(T_\alpha)$. □

设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$, 则 F 是 K 上的 n-维线性空间, 迹映射 $\mathrm{Tr}_{F/K}$ 为 F 到 K 的线性映射, 反之每个 F 到 K 的线性映射一定为迹映射.

定理 3.5: 设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$, 对给定的 $\alpha\in F$, 定义映射 $L_\alpha:F\to K$ 为对任意 $\beta\in F$ 有 $L_\alpha(\beta)=\mathrm{Tr}_{F/K}(\alpha\beta)$, 则 L_α 为线性映射, 反之, 每个 F 到 K 的线性映射一定为某个 L_α.

证明: 显然 L_α 为线性映射. 另一方面, 对于 $\alpha,\gamma\in F$, 若 $\alpha\neq\gamma$, 则 $L_\alpha\neq L_\gamma$. 事实上, 若 $L_\alpha=L_\gamma$, 则对任意 $\beta\in F$ 有 $L_\alpha(\beta)=L_\gamma(\beta)$, 即 $\mathrm{Tr}_{F/K}((\alpha-\gamma)\beta)=0$, 由于 $\alpha-\gamma\neq0$, 当 β 跑遍 F 时, $(\alpha-\gamma)\beta$ 也跑遍 F, 故对任意 $\beta\in F$ 有 $\mathrm{Tr}_{F/K}(\beta)=0$, 与 $\mathrm{Tr}_{F/K}$ 为满射矛盾. 这样集合 $\mathcal{L}=\{L_\alpha\mid\alpha\in F\}$ 中有 q^n 个元素, 又由线性代数知从 F 到 K 的线性映射恰有 q^n 个, 所以 $\mathcal{L}$ 中的元素就是所有的 F 到 K 的线性映射. □

下面我们求迹映射和范数映射的核, 它们分别为 F 到 K 的线性映射和 F^* 到 K^* 的群同态.

定理 3.6: (Hilbert 定理 90) 设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$. 则 $\mathrm{Tr}_{F/K}(\alpha)=0$ 当且仅当存在 $\beta\in F$ 使得 $\alpha=\beta-\beta^q$, 即 $\mathrm{Ker}(\mathrm{Tr}_{F/K})=\{\beta-\beta^q\mid\beta\in F\}$. 类似地, $\mathrm{N}_{F/K}(\alpha)=1$ 当且仅当存在 $\beta\in F^*$ 使得 $\alpha=\beta^{1-q}$, 即 $\mathrm{Ker}(\mathrm{N}_{F/K})=\{\beta^{1-q}\mid\beta\in F^*\}$.

证明: 首先注意到映射 $\rho:\beta\mapsto\beta-\beta^q$ 是线性空间 F 上的线性变换, 此线性变换的核为 $\mathrm{Ker}(\rho)=\{\beta\in F\mid\beta=\beta^q\}$, 它恰为子域 K, 也是 F 的 1-维子空间. 故 ρ 的像 $\rho(F)=\{\beta-\beta^q\mid$

$\beta \in F\}$ 为 F 的 $n-1$ 维子空间, 又对任意 $\alpha = \beta - \beta^q \in \rho(F)$, $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\beta) - \mathrm{Tr}(\beta^q) = \mathrm{Tr}(\beta) - \mathrm{Tr}(\beta) = 0$, 所以 $\mathrm{Ker}(\mathrm{Tr}_{F/K}) \supseteq \rho(F)$. 由定理 3.1 的 (e) 得知 $\mathrm{Ker}(\mathrm{Tr}_{F/K})$ 也是 F 的 $n-1$ 维子空间, 所以 $\mathrm{Ker}(\mathrm{Tr}_{F/K}) = \rho(F) = \{\beta - \beta^q \mid \beta \in F\}$. 而对范数的相应结果, 证明是类似的. □

我们知道 Galois 群 $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ 为 n 阶循环群, 设 ψ 为此群的一个生成元, 则被 ψ 固定的 $\mathbb{F}_{q^n}$ 中的元素也一定被群 $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ 中每个元素固定, 又域扩张 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 为 Galois 扩张, 所以 $\{\beta \in \mathbb{F}_{q^n} \mid \psi(\beta) = \beta\} = \mathbb{F}_q$. 注意到 $\psi(\beta)$ 与 β 有相同的极小多项式, 由定理 3.3, $\psi(\beta)$ 与 β 的迹相等, 范数也相等. 所以类似于如上证明, 我们可以得到 $\mathrm{Ker}(\mathrm{Tr}_{F/K}) = \{\beta - \psi(\beta) \mid \beta \in \mathbb{F}_{q^n}\}$ 和 $\mathrm{Ker}(\mathrm{N}_{F/K}) = \{\beta\psi(\beta)^{-1} \mid \beta \in \mathbb{F}_{q^n}^*\}$. 取 ψ 为 $\mathbb{F}_q$ 上的 Frobenius 自同构就得到定理 3.6 的内容.

定理 3.6 的证明不是构造性的, 即若 $\mathrm{Tr}(\alpha) = 0$, 则使得 $\alpha = \beta - \beta^q$ 的 $\beta \in F$ 是存在的, 但上述证明并没有给出求得 β 的方法. 基于如下引理, Hilbert 给出定理 3.6 的一个构造性证明.

引理 3.7: 设 $\alpha, \theta \in F$. 定义 $\beta \in F$ 为

$$\beta = \alpha\theta^q + (\alpha + \alpha^q)\theta^{q^2} + \cdots + (\alpha + \alpha^q + \cdots + \alpha^{q^{n-2}})\theta^{q^{n-1}}, \tag{3.5}$$

则 $\beta - \beta^q = \alpha\mathrm{Tr}(\theta) - \theta\mathrm{Tr}(\alpha)$.

证明: 由 β 的定义得到 $\beta^q = \alpha^q\theta^{q^2} + (\alpha^q + \alpha^{q^2})\theta^{q^3} + \cdots + (\alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}})\theta^{q^n}$, 所以, $\beta - \beta^q = \alpha(\theta^q + \theta^{q^2} + \cdots + \theta^{q^{n-1}}) - (\alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}})\theta^{q^n}$. 由 $\theta^{q^n} = \theta$, $\theta^q + \theta^{q^2} + \cdots + \theta^{q^{n-1}} = \mathrm{Tr}(\theta) - \theta$, 和 $\alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} = \mathrm{Tr}(\alpha) - \alpha$ 可得证明. □

下面给出 Hilbert 关于定理 3.6 的构造性证明. 选取 F 中的一个元素 θ 满足 $\mathrm{Tr}(\theta) = 1$ (这样的 θ 一定存在, 实际上有 q^{n-1} 个). 则若 $\mathrm{Tr}(\alpha) = 0$, 由 (3.5) 给出的 β 就满足 $\alpha = \beta - \beta^q$. 如上说明多项式 $x^q - x + \alpha$ 在 F 中有根当且仅当 $\mathrm{Tr}(\alpha) = 0$, 又由 (3.5) 给出此多项式的一个根 β 后, $x^q - x + \alpha$ 的所有根就是 $\beta + a$, 其中 $a \in K$.

定理 3.6 还告诉我们如何来解特征为 2 的域上的二次方程 (这非常重要, 因为解一般二次方程 $Ax^2 + Bx + C = 0$ 的求根公式 $x = (-B \pm \sqrt{B^2 - 4AC})/2A$ 在特征 2 时无效!). 设小域 $K = \mathbb{F}_2$, 大域 $F = \mathbb{F}_{2^n}$, 定理 3.6 告诉我们对 $\alpha \in \mathbb{F}_{2^n}$, 方程

$$x^2 + x = \alpha \tag{3.6}$$

在 $\mathbb{F}_{2^n}$ 中有根当且仅当 $\mathrm{Tr}(\alpha) = 0$. 进一步地, 设 $\mathrm{Tr}(\alpha) = 0$, 选取元素 $\theta \in \mathbb{F}_{2^n}$ 使得 $\mathrm{Tr}(\theta) = 1$, 则由式 (3.5) 给出的 β 是方程 (3.6) 的一个根, 再由 $(\beta + 1)^2 + (\beta + 1) = \beta^2 + \beta$ 知方程 (3.6) 的另一个根为 $\beta + 1$.

例 3.3: 考虑域 $\mathbb{F}_{2^5}$ 上的方程 (3.6), 这时我们可以简洁地取 $\theta = 1$, 故 Hilbert 的解答给出 $\beta = \alpha^2 + \alpha^8$. 一般地, 若 n 为奇数, 则对 $\alpha \in \mathbb{F}_{2^n}$ 满足 $\mathrm{Tr}(\alpha) = 0$, 则方程 $x^2 + x = \alpha$ 的一个根为 $\beta = \alpha^2 + \alpha^8 + \alpha^{32} + \cdots + \alpha^{2^{n-2}}$. □

例 3.4: 设 $F=\mathbb{F}_{2^4}=\mathbb{F}_2[x]/(x^4+x+1)$, 记 $\alpha=\overline{x}$. 下表给出 F 中的所有非零元.

i	α^i	i	α^i	i	α^i	i	α^i	i	α^i
0	0001	3	1000	6	1100	9	1010	12	1111
1	0010	4	0011	7	1011	10	0111	13	1101
2	0100	5	0110	8	0101	11	1110	14	1001

下面考虑方程 $x^2+x=\gamma$, 其中 $\gamma\in\mathbb{F}_{2^4}$, 此方程有根 $\beta\in\mathbb{F}_{2^4}$ 当且仅当 $\mathrm{Tr}(\gamma)=0$. 若记 $\gamma=a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0=(a_3,a_2,a_1,a_0)$, 其中 $a_i\in\mathbb{F}_2$, 由例 3.1 知 $\mathrm{Tr}(1)=\mathrm{Tr}(\alpha)=\mathrm{Tr}(\alpha^2)=0$, $\mathrm{Tr}(\alpha^3)=1$, 所以 $\mathrm{Tr}(\gamma)=a_3$. 所以上述方程有根当且仅当 $a_3=0$, 即当且仅当 $\gamma=0$ 以及 $\gamma=\alpha^i$, 其中 $i=0,1,2,4,5,8,10$. 由上表知道 $\mathrm{Tr}(\alpha^3)=1$, 所以在 Hilbert 构造中取 $\theta=\alpha^3$. 现在式 (3.5) 为

$$\beta=\gamma\theta^2+(\gamma+\gamma^2)\theta^4+(\gamma+\gamma^2+\gamma^4)\theta^8=\gamma(\theta^2+\theta^4+\theta^8)+\gamma^2(\theta^4+\theta^8)+\gamma^4\theta^8.$$

由 $\theta=\alpha^3$, 可以容易计算出 $\theta^2+\theta^4+\theta^8=\alpha^3+1=(1001)$, $\theta^4+\theta^8=\alpha^2+1=(0101)$ 和 $\theta^8=\alpha^3+\alpha=(1010)$, 所以当 $\mathrm{Tr}(\gamma)=0$ 时, 方程 $x^2+x=\gamma$ 的一个根为

$$\beta=\gamma(\alpha^3+1)+\gamma^2(\alpha^2+1)+\gamma^4(\alpha^3+\alpha).$$

由此式易知映射 $\gamma\mapsto\beta$ 是线性映射, 又 $\gamma=(a_3,a_2,a_1,a_0)$ 满足 $\mathrm{Tr}(\gamma)=0$ 当且仅当 $a_3=0$, 所以为了给出一般的根的公式我们只需讨论当 $\gamma=1$, α 和 α^2 的情形. 简单的计算可给出: $\gamma=1:\ \beta_0=\alpha^2+\alpha=(0110)$, $\gamma=\alpha:\ \beta_1=\alpha^3+\alpha+1=(1011)$, $\gamma=\alpha^2:\ \beta_2=\alpha^3+1=(1001)$. 所以若 $\gamma=(0,a_2,a_1,a_0)=a_2\alpha^2+a_1\alpha+a_0$, 方程 $x^2+x=\gamma$ 的一个根为

$$\beta=a_2\beta_2+a_1\beta_1+a_0\beta_0=(0,a_2,a_1,a_0)\cdot\begin{bmatrix}*\\ \beta_2\\ \beta_1\\ \beta_0\end{bmatrix}=(0,a_2,a_1,a_0)\cdot\begin{bmatrix}* & * & * & *\\ 1 & 0 & 0 & 1\\ 1 & 0 & 1 & 1\\ 0 & 1 & 1 & 0\end{bmatrix}.$$

例如, 对于方程 $x^2+x=\alpha^{10}=(0111)$, 我们可得它的一个根为

$$\beta=(0,1,1,1)\cdot\begin{bmatrix}* & * & * & *\\ 1 & 0 & 0 & 1\\ 1 & 0 & 1 & 1\\ 0 & 1 & 1 & 0\end{bmatrix}=(0,1,0,0)=\alpha^2.$$

而方程 $x^2+x=\alpha^{10}$ 的另一个根为 $\alpha^2+1=(0101)$. □

如上讨论的是特殊的二次方程 (3.6), 下面来看特征为 2 的域上的一般二次方程

$$Ax^2+Bx+C=0, \tag{3.7}$$

其中 $A,B,C\in\mathbb{F}_{2^n}$, $A\neq0$.

- 情形 1. $B\neq0$. 设 $y=AB^{-1}\cdot x$, $\gamma=ACB^{-2}$, 则方程 (3.7) 化为 $y^2+y=\gamma$, 故方程 (3.7) 有根当且仅当 $\mathrm{Tr}(\frac{AC}{B^2})=0$, 这时方程 (3.7) 的根为 $x=\frac{B}{A}y$ 和 $\frac{B}{A}(y+1)$, 其中 y 为方程

$y^2+y=\gamma$ 的一个根. (这时 $\frac{AC}{B^2}$ 称为方程 (3.7) 的判别式, 二次方程 (3.7) 有根当且仅当其判别式的迹为 0.)

- 情形 2. $B=0$. 设 $\gamma=CA^{-1}$, 方程 (3.7) 化为 $x^2=\gamma$. 此方程在域 $\mathbb{F}_{2^n}$ 中有一个 (2 重) 根 $x=\gamma^{2^{n-1}}$. 事实上, 由于 $(\gamma^{2^{n-1}})^2=\gamma^{2^n}=\gamma$, $\gamma^{2^{n-1}}$ 为方程 $x^2=\gamma$ 的根. 进一步地, 若 x_1,x_2 都是方程 $x^2=\gamma$ 的根, 则 $(x_1+x_2)^2=x_1^2+x_2^2=0$, 所以 $x_1=x_2$.

综合如上讨论, 我们得到方程 (3.7) 的根的情形如下.

$$\begin{array}{lll} \text{若 } B=0, & \text{一个 (2 重)根.} & \\ \text{若 } B\neq 0, & \mathrm{Tr}(\frac{AC}{B^2})=1, & \text{无根.} \\ & \mathrm{Tr}(\frac{AC}{B^2})=0, & \text{两个根.} \end{array}$$

最后, 如果 $\mathrm{Tr}_{F/K}(\frac{AC}{B^2})=1$, 令 $K=\mathbb{F}_2$, $F=\mathbb{F}_{2^n}$, $E=\mathbb{F}_{2^{2n}}$, 则

$$\mathrm{Tr}_{E/K}\left(\frac{AC}{B^2}\right)=\mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}\left(\frac{AC}{B^2}\right)\right)=\mathrm{Tr}_{F/K}\left(\frac{AC}{B^2}+\left(\frac{AC}{B^2}\right)^{2^n}\right)=\mathrm{Tr}_{F/K}(0)=0,$$

这时方程 (3.7) 在 $\mathbb{F}_{2^n}$ 的二次扩域 $\mathbb{F}_{2^{2n}}$ 中有两个根.

3.2 基

设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$ 是 K 的 n 次扩张, 则 F 是域 K 上的一个 n 维线性空间, 给定 F 在 K 上的一组基 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$, 则任意 $\alpha\in F$ 可以唯一地表示成 $\alpha=a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n$, 其中 $a_i\in K$, $1\leq i\leq n$. 在计算机、通信、编码以及密码等实际应用中, 我们经常需要在很大的域 (如 $\mathbb{F}_{2^{1000}}$) 中做代数运算, 比如加法、乘法、方幂、求逆等运算, 而特别的基可以使某些运算更快捷, 本章后面的内容将考虑基的问题. 注意到如果算上基中元素的次序, 则 F 在 K 上的不同基的个数为 $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$. 首先我们来讨论 F 中什么样的 n 个元素才能成为 F 在 K 上的一组基.

设向量组 $\alpha_1,\alpha_2,\ldots,\alpha_n\in F$, 定义 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 的判别式 $\Delta_{F/K}(\alpha_1,\alpha_2,\ldots,\alpha_n)$ 为

$$\Delta_{F/K}(\alpha_1,\alpha_2,\ldots,\alpha_n)=\begin{vmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_n) \\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_n) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_n\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_n\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_n\alpha_n) \end{vmatrix}.$$

由于此行列式中的每个元素都在 K 中, 故 $\Delta_{F/K}(\alpha_1,\alpha_2,\ldots,\alpha_n)\in K$. 下面结论给出向量组为基的一个刻画.

定理 3.8: 设 K 为有限域, F 是 K 的一个 n 次扩张且 $\alpha_1,\alpha_2,\ldots,\alpha_n\in F$. 则向量组 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 构成 F 在 K 上的一组基当且仅当 $\Delta_{F/K}(\alpha_1,\alpha_2,\ldots,\alpha_n)\neq 0$.

证明: 设 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 构成 F 在 K 上的一组基, 我们来证明 $\Delta_{F/K}(\alpha_1,\alpha_2,\ldots,\alpha_n)$ 中的行向量组在 K 上线性无关, 从而 $\Delta_{F/K}(\alpha_1,\alpha_2,\ldots,\alpha_n)\neq 0$. 设有 $c_1,c_2,\ldots,c_n\in K$ 使得对所有 $1\leq j\leq n$ 有

$$c_1\mathrm{Tr}(\alpha_1\alpha_j)+c_2\mathrm{Tr}(\alpha_2\alpha_j)+\cdots+c_n\mathrm{Tr}(\alpha_n\alpha_j)=0.$$

记 $\beta=c_1\alpha_1+c_2\alpha_2+\cdots+c_n\alpha_n$, 则有 $\mathrm{Tr}(\beta\alpha_j)=0$, $1\leq j\leq n$, 再由 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 张成 F, 可知对所有 $\alpha\in F$ 有 $\mathrm{Tr}(\beta\alpha)=0$. 由迹映射为满射可得 $\beta=0$, 即 $c_1\alpha_1+c_2\alpha_2+\cdots+c_n\alpha_n=0$, 从而 $c_1=c_2=\cdots=c_n=0$.

反之, 设 $\Delta_{F/K}(\alpha_1,\alpha_2,\ldots,\alpha_n)\neq 0$. 若存在 $c_1,c_2,\ldots,c_n\in K$, 使得

$$c_1\alpha_1+c_2\alpha_2+\cdots+c_n\alpha_n=0,$$

则对每个 $1\leq j\leq n$, 有 $c_1\alpha_1\alpha_j+c_2\alpha_2\alpha_j+\cdots+c_n\alpha_n\alpha_j=0$, 两边取迹得到

$$c_1\mathrm{Tr}(\alpha_1\alpha_j)+c_2\mathrm{Tr}(\alpha_2\alpha_j)+\cdots+c_n\mathrm{Tr}(\alpha_n\alpha_j)=0,$$

即

$$\begin{bmatrix}\mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_n)\\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_n)\\ \vdots & \vdots & & \vdots\\ \mathrm{Tr}_{F/K}(\alpha_n\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_n\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_n\alpha_n)\end{bmatrix}\begin{bmatrix}c_1\\ c_2\\ \vdots\\ c_n\end{bmatrix}=0.$$

因为此齐次线性方程组系数矩阵的行列式非零, 由此推出 $c_1=c_2=\cdots=c_n=0$, 所以向量组 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 在 K 上线性无关, 即此向量组构成 F 在 K 上的一组基. □

注意到要计算判别式 $\Delta_{F/K}(\alpha_1,\alpha_2,\ldots,\alpha_n)$, 我们需要计算 $\frac{1}{2}n(n+1)$ 个迹 $\mathrm{Tr}(\alpha_i\alpha_j)$, $1\leq i\leq j\leq n$. 下面我们用 F 中的元素给出另一种刻画. 对于 $\alpha_1,\alpha_2,\ldots,\alpha_n\in F$, 定义 $n\times n$ 矩阵 $C=(c_{ij})$, 其中 $c_{ij}=\alpha_j^{q^{i-1}}$, 则容易计算得到 $C^T\cdot C=A$, 其中 $A=(a_{ij})$ 为 $n\times n$ 矩阵且 $a_{ij}=\mathrm{Tr}(\alpha_i\alpha_j)$. 取行列式得到 $\det(C)^2=\Delta_{F/K}(\alpha_1,\alpha_2,\ldots,\alpha_n)$. 由定理 3.8 立得下面的推论.

推论 3.9: 设 $K=\mathbb{F}_q$, F 是 K 的 n 次扩张且 $\alpha_1,\alpha_2,\ldots,\alpha_n\in F$. 则向量组 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 构成 F 在 K 上的一组基当且仅当

$$\det(C)=\begin{vmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_n^q\\ \vdots & \vdots & & \vdots\\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}}\end{vmatrix}\neq 0.$$

□

注意虽然计算 $\det(C)$ 不需要计算迹, 但是它的计算是在大域 F 中进行的, 通常说来在 F 中做代数运算比在它的子域 K 中做代数运算要复杂的多.

设 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 是 F 在 K 上的一组基, 向量组 $\{\beta_1,\beta_2,\ldots,\beta_n\}$ 被 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 表

示为

$$\beta_j = u_{1j}\alpha_1 + u_{2j}\alpha_2 + \cdots + u_{nj}\alpha_n, \tag{3.8}$$

$j = 1, 2, \ldots, n$, 其中 $u_{ij} \in K$. 记矩阵 $U = (u_{ij})_{n\times n}$, 则 (3.8) 可以形式地写成

$$(\beta_1, \beta_2, \cdots, \beta_n) = (\alpha_1, \alpha_2, \cdots, \alpha_n)U.$$

由线性代数得到向量组 $\{\beta_1, \beta_2, \ldots, \beta_n\}$ 也构成 F 在 K 上的一组基当且仅当矩阵 U 可逆, 或者当且仅当 $\det(U) \neq 0$, 这时也称可逆矩阵 U 为从基 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 到基 $\{\beta_1, \beta_2, \ldots, \beta_n\}$ 的过渡矩阵.

下面我们来讨论如何利用基来进行有限域中的代数运算. 设 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 为 $F = \mathbb{F}_{q^n}$ 在 $K = \mathbb{F}_q$ 上的一组基. 对于 $\beta, \gamma \in F$, 设 β 和 γ 被基 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 线性表出如下:

$$\begin{aligned} \beta &= b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n, \\ \gamma &= c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n, \end{aligned}$$

其中 $b_i, c_i \in K$, $i = 1, 2, \ldots, n$. 则有

$$\beta \pm \gamma = (b_1 \pm c_1)\alpha_1 + (b_2 \pm c_2)\alpha_2 + \cdots + (b_n \pm c_n)\alpha_n,$$

即 F 中的加法和减法运算是非常容易进行的, 只需把对应元素在基下的系数 (在子域 K 中) 相加减即可. 对于乘法, 我们有

$$\beta\gamma = \sum_{i=1}^{n} b_i\alpha_i \sum_{j=1}^{n} c_j\alpha_j = \sum_{i=1}^{n}\sum_{j=1}^{n} b_ic_j\alpha_i\alpha_j,$$

设 $\alpha_i\alpha_j$ 被给定的基 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 表示为

$$\alpha_i\alpha_j = \sum_{k=1}^{n} c_{ijk}\alpha_k,$$

其中 $c_{ijk} \in K$, 则

$$\beta\gamma = \sum_{i=1}^{n}\sum_{j=1}^{n} b_ic_j \sum_{k=1}^{n} c_{ijk}\alpha_k = \sum_{k=1}^{n}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} b_ic_jc_{ijk}\right)\alpha_k.$$

从而在进行乘法运算时, 需要先计算这 n^3 个常数 c_{ijk}, $1 \leq i, j, k \leq n$, 再计算 $\sum_{i=1}^{n}\sum_{j=1}^{n} b_ic_jc_{ijk}$, 所以一般说来乘法运算是比较复杂的. 但是对某些特殊的基来说, 这 n^3 个常数 c_{ijk} 有可能容易计算.

选取 $\alpha \in F$ 使其在 K 上的次数 $\deg\alpha = n$ (这样的元素一定存在, 比如 F 的本原元素), 则 $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ 是 F 在 K 上的一组基, 这种形式的基称为多项式基. 这时由

$$\alpha^i\alpha^j = \sum_{k=0}^{n-1} c_{ijk}\alpha^k$$

可以看出一些常数 c_{ijk} 为 0, 所以用多项式基计算乘法比用一般的基要简单. 事实上, 我们也可以用在 §2.4 中提到的方法来做域 F 中的加、减、乘和求逆运算, 这需要首先求出 α 在 K 上的极小多项式, 再通过多项式加法、减法、带余除法以及 Euclid 算法完成, 具体细节可见如下例子.

例 3.5: 设 $K=\mathbb{F}_2$, $F=\mathbb{F}_{2^3}=\mathbb{F}_2[x]/(x^3+x+1)$. 记 $\alpha=\overline{x}$, 则 α 为 K 上的 3 次元素且 α 在 K 上的极小多项式为 $f(x)=x^3+x+1$. 这时 $\{1,\ \alpha,\ \alpha^2\}$ 是 $\mathbb{F}_{2^3}$ 在 $\mathbb{F}_2$ 上的多项式基. 设 $\beta=1+\alpha^2$, $\gamma=1+\alpha+\alpha^2$, 则 $\beta+\gamma=\alpha$. 下面来计算 $\beta\gamma$. 为此设 $b(x)=1+x^2$, $c(x)=1+x+x^2$, 所以 $b(x)c(x)=1+x+x^3+x^4$, 用 $f(x)=x^3+x+1$ 去除 x^4+x^3+x+1 得到

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

所以 $\beta\gamma=b(\alpha)c(\alpha)=\alpha+\alpha^2$. 为计算 β^{-1}, 对 $b(x)=x^2+1$ 和 $f(x)=x^3+x+1$ 施行 Euclid 算法得到

$$xb(x)+f(x)=1,$$

所以 $\beta^{-1}=b(\alpha)^{-1}=\alpha$. □

域 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的两组基在计算上可能没有什么区别, 一般说来, 设 $\{\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n\}$ 和 $\{\beta_1,\ \beta_2,\ \ldots,\ \beta_n\}$ 是 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的两组基, 它们称之为是等价的, 若存在元素 $c\in\mathbb{F}_q^*$ 使得对所有 $i=1,\ 2,\ \ldots,\ n$, 均有 $\alpha_i=c\beta_i$; 而它们称之为是弱等价的, 若存在元素 $\delta\in\mathbb{F}_{q^n}^*$ 使得 $\alpha_i=\delta\beta_i$ 对所有 $i=1,\ 2,\ \ldots,\ n$ 成立.

3.3 对偶基

设 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 是 $F=\mathbb{F}_{q^n}$ 在 $K=\mathbb{F}_q$ 上的一组基, 则任一 $\alpha\in F$ 可由 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 唯一线性表出, 即存在唯一的 $c_j(\alpha)\in K$, $1\le j\le n$, 使得

$$\alpha=c_1(\alpha)\alpha_1+c_2(\alpha)\alpha_2+\cdots+c_n(\alpha)\alpha_n. \tag{3.9}$$

易知 $c_j:\alpha\mapsto c_j(\alpha)$ 是 F 到 K 的线性映射, 由定理 3.5, 存在 $\beta_j\in F$ 使得 $c_j=L_{\beta_j}$, 即对任意 $\alpha\in F$ 有 $c_j(\alpha)=\mathrm{Tr}(\beta_j\alpha)$. 取 $\alpha=\alpha_i$, $1\le i\le n$, 则有

$$\mathrm{Tr}(\beta_j\alpha_i)=c_j(\alpha_i)=\delta_{ij}=\begin{cases}1 & \text{若 } i=j,\\ 0 & \text{若 } i\ne j,\end{cases}\qquad 1\le i,\ j\le n. \tag{3.10}$$

这表明对 F 在 K 上的任一组基 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$, 存在 $\beta_1,\beta_2,\ldots,\beta_n\in F$ 使得对任意 $1\le i,j\le n$ 有 $\mathrm{Tr}(\beta_j\alpha_i)=\delta_{ij}$. 注意到这样的 $\{\beta_1,\beta_2,\ldots,\beta_n\}$ 也是 F 在 K 上的一组基. 事实上, 若对 $d_i\in K$, $1\le i\le n$, 有

$$d_1\beta_1+d_2\beta_2+\cdots+d_n\beta_n=0,$$

两边同时乘以 α_i 并取迹映射 Tr, 可以得到 $d_i=0$, 即 $\{\beta_1,\beta_2,\ldots,\beta_n\}$ 在 K 上线性无关, 构成 F 在 K 上的基. 进一步地, 若向量组 $\{\theta_1,\theta_2,\ldots,\theta_n\}$ 也满足 (3.10), 即对所有 $1\le i,j\le n$, 有 $\mathrm{Tr}(\theta_j\alpha_i)=\delta_{ij}$, 则对某个固定的 $1\le j\le n$ 和所有 $1\le i\le n$, 有 $\mathrm{Tr}((\theta_j-\beta_j)\alpha_i)=0$. 因为 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 是 F 的一组基, 故可推出对任意 $\alpha\in F$ 有 $\mathrm{Tr}((\theta_j-\beta_j)\alpha)=0$, 又由 Tr 为满射得到 $\theta_j-\beta_j=0$, 即 $\theta_j=\beta_j$, 即基 $\{\beta_1,\beta_2,\ldots,\beta_n\}$ 是被基 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 所唯一确定的. 满

足条件 (3.10) 的 $\{\beta_1, \beta_2, \ldots, \beta_n\}$ 称为基 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 的对偶基. 显然对偶基是互相的, 即 $\{\beta_1, \beta_2, \ldots, \beta_n\}$ 的对偶基就是 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. 如上讨论给出如下定理.

定理 3.10: 域 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的任一组基都存在对偶基, 且其对偶基唯一. □

下面我们来具体求出一组基的对偶基. 设 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 是 F 在 K 上的一组基. 令矩阵 $A = (a_{ij})_{n\times n}$, 其中 $a_{ij} = \mathrm{Tr}(\alpha_i\alpha_j)$, 由定理 3.8 知矩阵 A 可逆, 设 $B = A^{-1}$, 令

$$(\beta_1, \beta_2, \cdots, \beta_n) = (\alpha_1, \alpha_2, \cdots, \alpha_n)B,$$

则 $\{\beta_1, \beta_2, \ldots, \beta_n\}$ 是 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 的对偶基. 事实上, 记 $B = (b_{ij})_{1\le i,j\le n}$, 则对 $j = 1, 2, \ldots, n$, 有

$$\beta_j = \sum_{k=1}^{n} b_{kj}\alpha_k,$$

所以对 $i, j = 1, 2, \ldots, n$, 有

$$\mathrm{Tr}(\alpha_i\beta_j) = \sum_{k=1}^{n} b_{kj}\mathrm{Tr}(\alpha_i\alpha_k) = \sum_{k=1}^{n} b_{kj}a_{ik} = \delta_{ij}.$$

另外, 式 (3.10) 也可以写成

$$\begin{pmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} \\ \vdots & \vdots & & \vdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_n^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}} \end{pmatrix} = I_n,$$

所以, 若我们令 $C = (c_{ij})_{1\le i,j\le n}$, 其中 $c_{ij} = \alpha_j^{q^{i-1}}$, 则由推论 3.9 可知矩阵 C 可逆, 上式表明 C^{-1} 的第一列就构成了基 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 的对偶基. 注意上面两种求对偶基的方法都需要求逆矩阵, 但是求 A^{-1} 是在子域 K 上进行的而求 C^{-1} 是在大域 F 上进行的.

例 3.6: 设 $K = \mathbb{F}_2$, $F = \mathbb{F}_{2^3} = \mathbb{F}_2[x]/(x^3 + x + 1)$. 记 $\alpha = \overline{x}$, 则 α 是 F 的一个本原元素且 $\{1, \alpha, \alpha^2\}$ 是 F 在 K 上的一组基 (多项式基). 易知 $\mathrm{Tr}(1) = 1$, $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha^2) = 0$. 所以若 $\beta = a_2\alpha^2 + a_1\alpha + a_0$, 则 $\mathrm{Tr}(\beta) = a_0$, α 的方幂的迹如下表:

i	α^i	$\mathrm{Tr}(\alpha^i)$
0	001	1
1	010	0
2	100	0
3	011	1
4	110	0
5	111	1
6	101	1

所以可以求出矩阵 A 为

$$A=\begin{bmatrix} \mathrm{Tr}(\alpha^0) & \mathrm{Tr}(\alpha^1) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha^1) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

从而

$$B=A^{-1}=A^T=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

由

$$(\beta_0,\beta_1,\beta_2)=(1,\alpha,\alpha^2)B=(1,\alpha^2,\alpha)$$

便求出基 $\{1,\alpha,\alpha^2\}$ 的对偶基为 $\{1,\alpha^2,\alpha\}$. □

下面的定理给出求多项式基的对偶基的方法, 此法不需要求逆矩阵.

定理 3.11: 设 $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ 是 F 在 K 上的一组多项式基, $\{\beta_0, \beta_1, \beta_2, \ldots, \beta_{n-1}\}$ 是它的对偶基. 设 $f(x)=(x-\alpha)(\gamma_0+\gamma_1 x+\cdots+\gamma_{n-1}x^{n-1})$ 是 α 在 K 上的极小多项式, 其中 $\gamma_{n-1}=1$, 则 $\beta_i=\gamma_i(f'(\alpha))^{-1}$, $0\le i\le n-1$.

证明: 记矩阵 $P=(p_{ij})_{0\le i,j\le n-1}$, $Q=(q_{ij})_{0\le i,j\le n-1}$, 其中 $p_{ij}=\alpha^{iq^j}$, $q_{ij}=\beta_j^{q^i}$, $0\le i,j\le n-1$, 则有 $PQ=I_n$, 即 $Q=P^{-1}$. 设多项式 $\beta(x)=\beta_0+\beta_1x+\cdots+\beta_{n-1}x^{n-1}$, 则由 $QP=I_n$ 得到 (看 Q 的第一行与 P 的各列相乘)

$$\beta(\alpha^{q^i})=\begin{cases} 1, & \text{若 } i=0, \\ 0, & \text{若 } 1\le i\le n-1. \end{cases} \tag{3.11}$$

由 Lagrange 插值公式 (定理 1.12), 满足 (3.11) 的次数小于 n 的唯一多项式为

$$\beta(x)=\frac{(x-\alpha^q)(x-\alpha^{q^2})\cdots(x-\alpha^{q^{n-1}})}{(\alpha-\alpha^q)(\alpha-\alpha^{q^2})\cdots(\alpha-\alpha^{q^{n-1}})},$$

由第二章定理 2.10 知 α 的极小多项式为 $f(x)=(x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$, 所以 $f'(\alpha)=(\alpha-\alpha^q)(\alpha-\alpha^{q^2})\cdots(\alpha-\alpha^{q^{n-1}})$, 故

$$\beta(x)=\frac{f(x)}{(x-\alpha)f'(\alpha)}=\frac{1}{f'(\alpha)}(\gamma_0+\gamma_1x+\cdots+\gamma_{n-1}x^{n-1}),$$

所以 $\beta_i=\gamma_i(f'(\alpha))^{-1}$, $0\le i\le n-1$. □

设 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 是 F 在 K 上的一组基, $\{\beta_1,\beta_2,\ldots,\beta_n\}$ 是它的对偶基, 我们可以称 $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 为原始基而 $\{\beta_1,\beta_2,\ldots,\beta_n\}$ 为对偶基. 任意 $x\in F$ 可以表示为

$$x=\sum_{i=1}^{n}x_i\alpha_i=\sum_{i=1}^{n}x_i'\beta_i,$$

我们称 $x_1,x_2,\ldots,x_n$ 为 x 的原始坐标而 $x_1',x_2',\ldots,x_n'$ 称为 x 的对偶坐标. 通过计算得到对任

意 $1 \le i \le n$, 有

$$\mathrm{Tr}(x\beta_i) = \mathrm{Tr}\left(\left(\sum_{j=1}^{n} x_j\alpha_j\right)\beta_i\right) = \sum_{j=1}^{n} x_j\delta_{ji} = x_i,$$

即 x 的原始坐标可由对偶基表出. 类似地有 $x'_i = \mathrm{Tr}(x\alpha_i)$, $1 \le i \le n$, 即 x 的对偶坐标可由原始基表出.

例 3.7: 设 $K = \mathbb{F}_2$, $F = \mathbb{F}_{2^3} = \mathbb{F}_2[x]/(x^3+x^2+1)$. 记 $\alpha = \overline{x}$, 则 $\{\alpha, \alpha^2, 1+\alpha+\alpha^2\}$ 是 F 在 K 上的一组基. 容易计算出它的对偶基仍然是 $\{\alpha, \alpha^2, 1+\alpha+\alpha^2\}$ (与其对偶基相同的基称为是自对偶的). 元素 $\alpha^5 \in \mathbb{F}_8$ 可以唯一表示成 $\alpha^5 = c_1\alpha + c_2\alpha^2 + c_3(1+\alpha+\alpha^2)$, 其中 $c_1, c_2, c_3 \in \mathbb{F}_2$, 则这些坐标为 $c_1 = \mathrm{Tr}(\alpha\cdot\alpha^5) = 0$, $c_2 = \mathrm{Tr}(\alpha^2\cdot\alpha^5) = 1$, $c_3 = \mathrm{Tr}((1+\alpha+\alpha^2)\alpha^5) = 1$, 所以 $\alpha^5 = \alpha^2 + (1+\alpha+\alpha^2)$. □

例 3.8: 设 $K = \mathbb{F}_2$, $F = \mathbb{F}_{2^4} = \mathbb{F}_2[x]/(x^4+x+1)$. 记 $\alpha = \overline{x}$, 则 α 是 F 的一个本原元素且 $\{1, \alpha, \alpha^2, \alpha^3\}$ 是 F 在 K 上的一组基, 计算可得它的对偶基为 $\{\beta_0, \beta_1, \beta_2, \beta_3\}$, 其中 $\beta_0 = \alpha^3+1$, $\beta_1 = \alpha^2$, $\beta_2 = \alpha$, $\beta_3 = 1$ (可用例 3.6 的方法或者利用定理 3.11). 对任意 $x \in \mathbb{F}_{2^4}$, 表示 x 为

$$x = \sum_{i=0}^{3} x_i\alpha^i = \sum_{i=0}^{3} x'_i\beta_i,$$

即

$$x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3 = x'_0(\alpha^3+1) + x'_1\alpha^2 + x'_2\alpha + x'_3 = x'_0\alpha^3 + x'_1\alpha^2 + x'_2\alpha + (x'_0+x'_3),$$

所以 $x'_0 = x_3$, $x'_1 = x_2$, $x'_2 = x_1$, $x'_3 = x_0 + x_3$. □

设 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 是 $F = \mathbb{F}_{q^n}$ 在 $K = \mathbb{F}_q$ 上的多项式基, 其对偶基为 $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$. 我们可以看到在对偶坐标系统下 F 中的乘法可以更容易. 设 $x \in F$ 表为

$$x = x'_0\beta_0 + x'_1\beta_1 + x'_2\beta_2 + \cdots + x'_{n-1}\beta_{n-1},$$

其中 $x'_i \in K$, $i = 0, 1, 2, \ldots, n-1$, 则 $x'_i = \mathrm{Tr}(x\alpha^i)$, $i = 0, 1, 2, \ldots, n-1$. 下面我们计算 αx, 表 αx 为

$$\alpha x = (\alpha x)'_0\beta_0 + (\alpha x)'_1\beta_1 + (\alpha x)'_2\beta_2 + \cdots + (\alpha x)'_{n-1}\beta_{n-1},$$

其中 $(\alpha x)'_i \in K$, $i = 0, 1, 2, ..., n-1$, 则有

$$(\alpha x)'_i = \mathrm{Tr}(\alpha x\cdot\alpha^i) = \mathrm{Tr}(x\alpha^{i+1}).$$

设 $f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0$ 为 α 在 K 上的极小多项式, 则

$$\begin{aligned}(\alpha x)'_{n-1} &= \mathrm{Tr}(x\alpha^n) = -\mathrm{Tr}(c_{n-1}x\alpha^{n-1} + c_{n-2}x\alpha^{n-2} + \cdots + c_1x\alpha + c_0x)\\ &= -(c_{n-1}x'_{n-1} + c_{n-2}x'_{n-2} + \cdots + c_1x'_1 + c_0x'_0).\end{aligned}$$

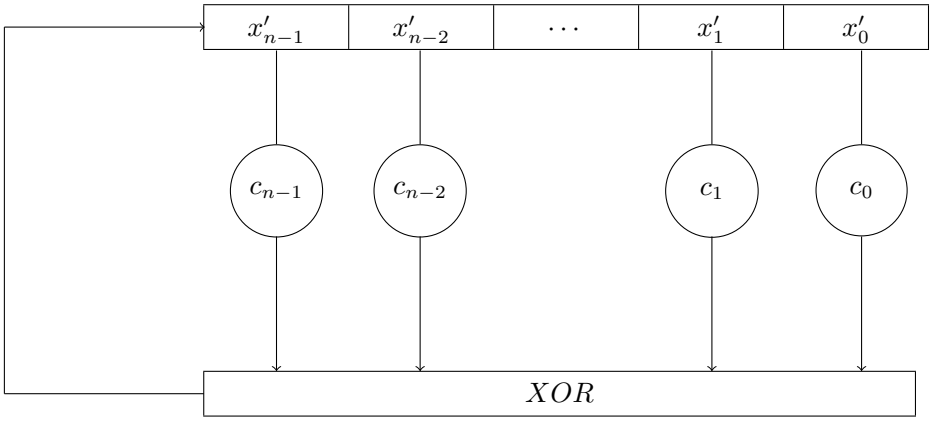
从而

$$(\alpha x)'_i = \begin{cases} x'_{i+1}, & i = 0, 1, 2, \ldots, n-2,\\ -c_{n-1}x'_{n-1} - c_{n-2}x'_{n-2} - \cdots - c_1x'_1 - c_0x'_0, & i = n-1.\end{cases}$$

特别地, 设 $q=2$, 则 $F=\mathbb{F}_{q^n}=\mathbb{F}_{2^n}=\mathbb{F}_2(\alpha)$, 其中 α 是 $\mathbb{F}_2$ 上的 n 次元素, 则上面的公式可以写成

$$(\alpha x)'_i=\begin{cases} x'_{i+1}, & i=0,\,1,\,2,\,\ldots,\,n-2,\\ c_{n-1}x'_{n-1}+c_{n-2}x'_{n-2}+\cdots+c_1x'_1+c_0x'_0, & i=n-1. \end{cases}$$

我们可以用如下图显示的这个简单的移位寄存器来计算 αx. 设从左到右数第 i 个触发器里填上对偶坐标 x'_{n-i}, $1\leq i\leq n$, 具有元素 XOR 的盒子表示 $\mathbb{F}_2$ 上的加法器, 称为 XOR-门, 具有元素 $c_{n-i}=1$ 或者 0 表示存在或者不存在一条从第 i 个触发器连到 XOR-门的线, 一个移位时钟脉冲进行后, 每个触发器的内容向右传递, 第 n 个触发器里的内容移出, 第 1 个触发器填上在 XOR-门中计算后的内容 $c_{n-1}x'_{n-1}+c_{n-2}x'_{n-2}+\cdots+c_1x'_1+c_0x'_0$, 这样一个脉冲后这 n 个触发器里的内容就从 x 的对偶坐标变成 αx 的对偶坐标. 这种执行 $\mathbb{F}_{2^n}$ 中乘法运算的有效电路的设计来源于 Elwyn Berlekamp. (Berlekamp 是美国著名数学家、代数编码学家, 生于 1940 年 9 月 6 日, 1977 年当选美国国家工程院院士, 1999 年当选美国国家科学院院士, 其著作《代数编码理论》曾荣获美国电子学会信息论组的最佳科研著作奖. Berlekamp 于 2019 年 4 月 9 日逝世, 我们后面将给出他提出的有限域上多项式的分解算法.)



一般 q 元域情形下, 乘积 αx 的对偶坐标也可由 x 的对偶坐标用线性反馈移位寄存器得到. 进一步地, 设 $x,y\in F$, 要计算 x 与 y 的乘积. 用对偶坐标系统表示 x 为 $x=x'_0\beta_0+x'_1\beta_1+\cdots+x'_{n-1}\beta_{n-1}$, 用原始坐标系统表示 y 为 $y=y_0+y_1\alpha+\cdots+y_{n-1}\alpha^{n-1}$, 其中 $x'_i,\,y_i\in K$, $0\leq i\leq n-1$, 则

$$yx=\sum_{i=0}^{n-1}y_i\alpha^i x=\sum_{i=0}^{n-1}y_i\left(\sum_{j=0}^{n-1}(\alpha^i x)'_j\beta_j\right)=\sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1}y_i(\alpha^i x)'_j\right)\beta_j,$$

故 $(yx)'_j=\sum_{i=0}^{n-1}y_i(\alpha^i x)'_j$.

3.4 正规基

设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$. 域 F 在 K 上的形如 $\{\alpha,\alpha^q,\ldots,\alpha^{q^{n-1}}\}$ 的基称为 F 在 K 上的正规基. 例如, 例 3.7 中的基 $\{\alpha,\alpha^2,1+\alpha+\alpha^2\}$ 就是正规基, 因为 $1+\alpha+\alpha^2=\alpha^4$. 正规基即一个 F 中的元素 α 在 K 上的所有共轭元组成的基, 这样的元素 α 称为 F 在 K 上的正规元素 (或称 α 生成一个正规基). 显然若 α 是 F 在 K 上的一个正规元素, 则 $\deg\alpha=n$ 且 $\mathrm{Tr}_{F/K}(\alpha)\neq 0$. 正规基在计算 F 中元素的方幂时非常有用, 若 $\beta\in F$ 被一组正规基 $\{\alpha,\alpha^q,\ldots,\alpha^{q^{n-1}}\}$ 表示为 $\beta=a_0\alpha+a_1\alpha^q+\cdots+a_{n-1}\alpha^{q^{n-1}}$, 即 β 可由向量 $(a_0,a_1,\ldots,a_{n-1})$ 表示, 则 β^q 的表示向量为 $(a_{n-1},a_0,\ldots,a_{n-2})$, 即把 β 的表示向量循环右移一位得到, 这表明在正规基下, 计算一个元素的 q 次幂异常容易. 当然在正规基下做加法运算也很容易, 就是对应的表示向量分量相加即可.

下面我们将证明 F 在 K 上的正规基一定存在, 但在此之前, 我们来看在正规基下的 F 中的乘法. 设 $\{\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{n-1}}\}$ 是 F 在 K 上的一组正规基, 元素 $\xi,\eta\in F$ 用此正规基表示为 $\xi=x_0\alpha+x_1\alpha^q+\cdots+x_{n-1}\alpha^{q^{n-1}}$, $\eta=y_0\alpha+y_1\alpha^q+\cdots+y_{n-1}\alpha^{q^{n-1}}$, 其中 x_i, $y_i\in K$, $0\leq i\leq n-1$. 则

$$\xi\eta=\sum_{i,j=0}^{n-1}x_iy_j\alpha^{q^i}\alpha^{q^j}=\sum_{i,j=0}^{n-1}x_iy_j\alpha^{q^i+q^j}=\sum_{i,j=0}^{n-1}x_iy_j(\alpha^{q^{i-j}+1})^{q^j}.$$

所以如果知道如何将 $\alpha^{q^m}\alpha$ 在此正规基 $\{\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{n-1}}\}$ 下表示出来, $0\leq m\leq n-1$, 我们就可以做任意的元素相乘了, 设

$$\alpha^{q^m}\alpha=\alpha^{q^m+1}=\sum_{k=0}^{n-1}t_{k,m}\alpha^{q^k},$$

其中 $t_{k,m}\in K$, 则有

$$\xi\eta=\sum_{i,j,k=0}^{n-1}x_iy_jt_{k,i-j}\alpha^{q^{k+j}}=\sum_{i,j,m=0}^{n-1}x_iy_jt_{m-j,i-j}\alpha^{q^m}.$$

注意到上式中 t 的两个下标都是模 n 意义下的. 前面第 2 节中我们知道在一般基下计算 F 中元素乘积需要 K 中的 n^3 个常数 c_{ijk}, $i,j,k=1,2,\ldots,n$, 但在正规基下我们只需要 K 中的 n^2 个常数 $t_{i,j}$, $0\leq i,j\leq n-1$.

用 σ 表示 F 在 K 上的 Frobenius 自同构, 即对 $\alpha\in F$, 有 $\sigma(\alpha)=\alpha^q$, 则正规基就是一个合适的元素 α 在 σ 下的轨道做成的基. 把 F 看作 K 上的 n 维线性空间, 则 σ 是 F 在 K 上的线性变换. 显然 $\sigma^n=\mathrm{id}_F$, 所以 x^n-1 为 σ 的零化多项式. 下面我们证明不存在 K 上的次数小于 n 的多项式 $f(x)$ 使得 $f(\sigma)=0$. 事实上, 若存在 $f(x)=x^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0\in K[x]$ 使得 $f(\sigma)=0$, 其中 $m<n$, 则对任意 $\beta\in F$ 有

$$0=f(\sigma)(\beta)=\sigma^m(\beta)+a_{m-1}\sigma^{m-1}(\beta)+\cdots+a_1\sigma(\beta)+a_0\beta=\beta^{q^m}+a_{m-1}\beta^{q^{m-1}}+\cdots+a_1\beta^q+a_0\beta,$$

这表明 q^m 次多项式 $g(x)=x^{q^m}+a_{m-1}x^{q^{m-1}}+\cdots+a_1x^q+a_0x$ 在域 F 中有 q^n 个根, 矛盾. 这表明 σ 在 K 上的极小多项式为 x^n-1, 自然这也是 σ 的特征多项式, 即 σ 的特征多项式就

是它极小多项式. 所以存在 F 在 K 上的一组基 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 使得 σ 在这组基下的矩阵为 (因为具有相同的不变因子)

$$\begin{pmatrix} 0 & & & & 1 \\ 1 & 0 & & & 0 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & 0 \\ & & & 1 & 0 \end{pmatrix}.$$

显然 $\alpha_{i+1} = \sigma(\alpha_i) = \alpha_i^q$, $1 \leq i \leq n-1$, 记 $\alpha = \alpha_1$, 则 $\alpha_{i+1} = \alpha^{q^i}$, $1 \leq i \leq n-1$, 这表明基 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 恰为正规基. 我们证明了如下定理.

定理 3.12: (正规基定理) 对任意素数幂 q 和正整数 n, 存在 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的正规基. □

定理 3.13: 正规基的对偶基依然是正规基.

证明: 设 $\{\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\}$ 是 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的一组正规基且 $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ 是它的对偶, 即对任意 $0 \leq i, j \leq n-1$, 有 $\mathrm{Tr}(\sigma^i(\alpha)\beta_j) = \delta_{ij}$. 记矩阵

$$P = \begin{pmatrix} \alpha & \sigma(\alpha) & \cdots & \sigma^{n-1}(\alpha) \\ \sigma(\alpha) & \sigma^2(\alpha) & \cdots & \alpha \\ \vdots & \vdots & & \vdots \\ \sigma^{n-1}(\alpha) & \alpha & \cdots & \sigma^{n-2}(\alpha) \end{pmatrix}$$

和

$$Q = \begin{pmatrix} \beta_0 & \beta_1 & \cdots & \beta_{n-1} \\ \sigma(\beta_0) & \sigma(\beta_1) & \cdots & \sigma(\beta_{n-1}) \\ \vdots & \vdots & & \vdots \\ \sigma^{n-1}(\beta_0) & \sigma^{n-1}(\beta_1) & \cdots & \sigma^{n-1}(\beta_{n-1}) \end{pmatrix},$$

则有 $PQ = I_n$, 即 $Q = P^{-1}$. 注意到 P 为对称矩阵, 所以 Q 也是对称矩阵, 故 $\beta_i = \sigma^i(\beta_0)$, $0 \leq i \leq n-1$, 所以 $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\} = \{\beta_0, \sigma(\beta_0), \ldots, \sigma^{n-1}(\beta_0)\}$ 是正规基. □

设 $\alpha \in F$, 记 $t_i = \mathrm{Tr}_{F/K}(\alpha\alpha^{q^i})$, $0 \leq i \leq n-1$, 则由

$$\mathrm{Tr}_{F/K}(\alpha\alpha^{q^i}) = \mathrm{Tr}_{F/K}(\alpha^{q^n}\alpha^{q^i}) = \mathrm{Tr}_{F/K}\left(\left(\alpha\alpha^{q^{n-i}}\right)^{q^i}\right) = \mathrm{Tr}_{F/K}(\alpha\alpha^{q^{n-i}})$$

得到 $t_i = t_{n-i}$, $1 \leq i \leq n-1$, 且容易计算出 $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ 的判别式为

$$\Delta_{F/K}(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}) = \begin{vmatrix} t_0 & t_1 & \cdots & t_{n-2} & t_{n-1} \\ t_{n-1} & t_0 & \cdots & t_{n-3} & t_{n-2} \\ \vdots & \vdots & & \vdots & \vdots \\ t_2 & t_3 & \cdots & t_0 & t_1 \\ t_1 & t_2 & \cdots & t_{n-1} & t_0 \end{vmatrix}. \tag{3.12}$$

由定理 3.8 知 $\alpha \in F$ 为 F 在 K 上的正规元素当且仅当上面这个行列式非零.

定理 3.14: 设 $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^n}$, $\alpha \in F$, 记 $t_i = \mathrm{Tr}_{F/K}(\alpha\alpha^{q^i})$, $0 \le i \le n-1$, 则 α 生成 F 在 K 上的正规基当且仅当 K 上的两个多项式 $f(x) = x^n - 1$ 与 $g(x) = t_0x^{n-1} + t_1x^{n-2} + \cdots + t_{n-2}x + t_{n-1}$ 互素.

证明: 考虑多项式 $f(x)$ 和 $g(x)$ 的结式 $R(f,g)$, 这是一个 $2n-1$ 阶的行列式, 把它详细写出为

$$R(f,g) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & -1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & -1 \\ t_0 & t_1 & t_2 & \cdots & t_{n-2} & t_{n-1} & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & t_0 & t_1 & \cdots & t_{n-3} & t_{n-2} & t_{n-1} & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & t_0 & t_1 & t_2 & t_3 & \cdots & t_{n-2} & t_{n-1} \end{vmatrix}.$$

把 $R(f,g)$ 的第 $(n+j)$ 列加到第 j 列, $1 \le j \le n-1$, 则容易计算出

$$R(f,g) = (-1)^{n^2-1} \begin{vmatrix} t_0 & t_1 & \cdots & t_{n-2} & t_{n-1} \\ t_{n-1} & t_0 & \cdots & t_{n-3} & t_{n-2} \\ \vdots & \vdots & & \vdots & \vdots \\ t_2 & t_3 & \cdots & t_0 & t_1 \\ t_1 & t_2 & \cdots & t_{n-1} & t_0 \end{vmatrix}. \tag{3.13}$$

我们知道 $f(x)$ 与 $g(x)$ 互素当且仅当 $R(f,g) \ne 0$, 由 (3.12) 和 (3.13) 知 $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ 是 F 在 K 上的一组基当且仅当 $R(f,g) \ne 0$, 这也等价于 $f(x)$ 与 $g(x)$ 互素. □

注意到两个多项式互素当且仅当它们没有公共根, 由此得到两个多项式互素当且仅当它们的互反多项式互素. 因为 $f(x) = x^n - 1$ 的互反多项式为 $\tilde{f}(x) = -f(x)$, 而 $g(x)$ 的互反多项式为 $\tilde{g}(x) = t_{n-1}x^{n-1} + t_{n-2}x^{n-2} + \cdots + t_1x + t_0$. 这里应当指出, 一般说来, 互反多项式的定义要求常数项非零, 但由于 $f(x)$ 无零根, 即使 $t_0 = 0$ 或者 $t_{n-1} = 0$, 也不影响这里的讨论. 所以我们有如下推论.

推论 3.15: 设 $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^n}$, $\alpha \in F$, 记 $t_i = \mathrm{Tr}_{F/K}(\alpha\alpha^{q^i})$, $0 \le i \le n-1$, 则 α 生成 F 在 K 上的正规基当且仅当 K 上的两个多项式 $f(x) = x^n - 1$ 与 $t(x) = t_{n-1}x^{n-1} + t_{n-2}x^{n-2} + \cdots + t_1x + t_0$ 互素. □

下面我们来求一个正规基的对偶基. 设 $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ 是 F 在 K 上的一组正规基. 记 $t_i = \mathrm{Tr}_{F/K}(\alpha\alpha^{q^i})$, $0 \le i \le n-1$, $t(x) = \sum_{i=0}^{n-1} t_ix^i$, 由推论 3.15 知多项式 $t(x)$ 与 $x^n - 1$ 互素, 故存在唯一多项式 $d(x) \in K[x]$ 满足 $t(x)d(x) \equiv 1 \pmod{(x^n-1)}$ 且 $\deg d(x) \le n-1$. 记

$d(x)=\sum_{i=0}^{n-1}d_ix^i$, 由于

$$t(x)d(x)=\sum_{0\le i,j\le n-1}t_id_jx^{i+j}\equiv\sum_{i=0}^{n-1}\left(\sum_{k=0}^{n-1}d_kt_{i-k}\right)x^i\,(\mathrm{mod}\,(x^n-1)),$$

其中的下标是模 n 意义下的. 由 $t(x)d(x)\equiv 1(\mathrm{mod}\,(x^n-1))$ 得到

$$\sum_{k=0}^{n-1}d_kt_{i-k}=\delta_{i0}.$$

令 $\beta=\sum_{i=0}^{n-1}d_i\alpha^{q^i}$, 则对任意 $0\le i,j\le n-1$ 有

$$\begin{aligned}\mathrm{Tr}(\alpha^{q^i}\beta^{q^j}) &= \mathrm{Tr}\left(\alpha^{q^i}\left(\sum_{k=0}^{n-1}d_k\alpha^{q^{j+k}}\right)\right)=\sum_{k=0}^{n-1}d_k\mathrm{Tr}(\alpha^{q^i}\alpha^{q^{j+k}})\\ &= \sum_{k=0}^{n-1}d_k\mathrm{Tr}(\alpha\alpha^{q^{j+k-i}})=\sum_{k=0}^{n-1}d_kt_{j+k-i}=\sum_{k=0}^{n-1}d_kt_{i-j-k}=\delta_{i-j,0}=\delta_{ij}.\end{aligned}$$

所以 $\{\beta,\beta^q,\ldots,\beta^{q^{n-1}}\}$ 是一组 F 在 K 上的正规基且为正规基 $\{\alpha,\alpha^q,\ldots,\alpha^{q^{n-1}}\}$ 的对偶基.

利用推论 3.9, 类似于定理 3.14 的证明, 我们可以得到正规元素的另一个刻画, 只是这时的多项式是大域 F 上的多项式.

定理 3.16: 设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$, $\alpha\in F$, 则 α 生成 F 在 K 上的正规基当且仅当 F 上的两个多项式 $f(x)=x^n-1$ 与 $g(x)=\alpha x^{n-1}+\alpha^qx^{n-2}+\cdots+\alpha^{q^{n-2}}x+\alpha^{q^{n-1}}$ 互素, 也当且仅当多项式 $f(x)=x^n-1$ 与 $\tilde{g}(x)=\alpha^{q^{n-1}}x^{n-1}+\alpha^{q^{n-2}}x^{n-2}+\cdots+\alpha^qx+\alpha$ 互素. □

推论 3.17: 设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$, 其中 $n=p^e$, 而 $p=\mathrm{char}F$, 则 $\alpha\in F$ 生成 F 在 K 上的正规基当且仅当 $\mathrm{Tr}_{F/K}(\alpha)\ne 0$.

证明: 必要性显然, 下面证明充分性. 由 $\mathrm{Tr}_{F/K}(\alpha)\ne 0$ 易知 1 不是多项式 $g(x)=\alpha x^{n-1}+\alpha^qx^{n-2}+\cdots+\alpha^{q^{n-2}}x+\alpha^{q^{n-1}}$ 的根. 又 $n=p^e$, 所以 $f(x)=x^n-1=(x-1)^{p^e}$, 故 $f(x)$ 与 $g(x)$ 无公共根, 所以 $f(x)$ 与 $g(x)$ 互素, 由定理 3.16 知 α 生成 F 在 K 上的正规基. □

设 σ 为 F 在 K 上的 Frobenius 自同构, 即对 $\alpha\in F$, 有 $\sigma(\alpha)=\alpha^q$, 对于多项式 $f(x)=a_0+a_1x+\cdots+a_mx^m\in K[x]$, 定义

$$f(\sigma)(\alpha)=a_0\alpha+a_1\sigma(\alpha)+\cdots+a_m\sigma^m(\alpha).$$

对于 $\alpha\in F$, 若 $f(\sigma)(\alpha)=0$, 则称多项式 $f(x)$ σ-零化 α. 显然 σ 的极小多项式 x^n-1 σ-零化 F 中任意元素, 从而 σ-零化 α 的多项式中有次数最低的首一非零多项式, 容易证明这样的多项式唯一且整除每一个 σ-零化 α 的多项式. 注意到 α 是 F 在 K 上的正规元素当且仅当 $\alpha,\sigma(\alpha),\sigma^2(\alpha),\ldots,\sigma^{n-1}(\alpha)$ 在 K 上线性无关, 即 σ- 零化 α 的次数最低的首一非零多项式为 x^n-1.

定理 3.18: 设 $K=\mathbb{F}_q$, $F=\mathbb{F}_{q^n}$, 其中 n 为异于 $\mathrm{char}F$ 的素数且 q 为模 n 的原根, 则 $\alpha\in F$ 生成 F 在 K 上的正规基当且仅当 $\alpha\notin K$ 且 $\mathrm{Tr}_{F/K}(\alpha)\ne 0$.

证明: 必要性显然, 下面证明充分性. 显然 $x^n-1=(x-1)(x^{n-1}+\cdots+x+1)$. 设 $\xi\in E$ 是 $e(x)=x^{n-1}+\cdots+x+1$ 在 K 的扩域 E 中的一个根, 则 ξ^q, ξ^{q^2}, ... 也是 $e(x)$ 在 E 中的

根. 我们断言 $\xi, \xi^q, \xi^{q^2}, \ldots, \xi^{q^{n-2}}$ 是互不相同的. 设对于 $0 \le i, j \le n-2$, 有 $\xi^{q^i} = \xi^{q^j}$, 则有 $\xi^{q^j - q^i} = 1$. 注意到 $\xi^n = 1$, 又 n 为素数且 $\xi \ne 1$, 所以 ξ 在 E^* 中的阶为 n. 故 $n \mid (q^j - q^i)$, 从而 $q^j \equiv q^i \pmod n$. 因为 q 为模 n 的原根, 即 q 模 n 的乘法阶为 $\phi(n) = n-1$, 由此得 $i = j$. 这表明 ξ 在 K 上的极小多项式就是 $e(x)$, 所以 $x^{n-1} + \cdots + x + 1$ 在 K 上不可约. 由于 $\alpha \notin K$, 即 $\alpha^q \ne \alpha$, 所以 $x - 1$ 不能 σ-零化 α. 又 $e(\sigma)(\alpha) = \mathrm{Tr}_{F/K}(\alpha) \ne 0$, 故 $e(x)$ 也不能 σ-零化 α. 因为 σ-零化 α 的次数最低的首一非零多项式整除 $x^n - 1$, 所以 σ- 零化 α 的次数最低的首一非零多项式恰为 $x^n - 1$, 从而 α 可生成 F 在 K 上的正规基. □

综合推论 3.17 和定理 3.18, 我们有如下定理.

定理 3.19: 设 p 为素数, q 为 p 的方幂, $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^n}$, 其中 $n = p^e$, $e \ge 1$, 或者 n 为不等于 p 的素数且 q 为模 n 的原根, 则满足 $\mathrm{Tr}_{F/K}(\alpha) \ne 0$ 的所有 n 次元素 $\alpha \in F$ 都可生成 F 在 K 上的正规基. □

如上定理的逆依然成立, 我们下面列出这个结论但是不给出证明.

定理 3.20: 设 p 为素数, q 为 p 的方幂, $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^n}$, 若满足 $\mathrm{Tr}_{F/K}(\alpha) \ne 0$ 的所有 n 次元素 $\alpha \in F$ 都可生成 F 在 K 上的正规基, 则一定有 $n = p^e$, $e \ge 1$, 或者 n 为不等于 p 的素数且 q 为模 n 的原根. □

设 $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^n}$, F 在 K 上的正规基 $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ 称为是本原正规基, 若 α 为 F 的本原元素. 篇幅所限, 下面我们依然列出结论但是不给出证明.

定理 3.21: (本原正规基定理) 对任意素数幂 q 和正整数 n, 存在 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的本原正规基. □

3.5 习题

3.1 给出定理 3.1, 3.2, 3.3 和 3.6 中关于范数部分的证明.

3.2 利用 $\mathbb{F}_2$ 上的不可约多项式 $x^5 + x^2 + 1$ 构作有限域 $\mathbb{F}_{2^5}$, 给出其中求迹 $\mathrm{Tr}_{\mathbb{F}_{2^5}/\mathbb{F}_2}$ 的公式.

3.3 设 $K = \mathbb{F}_q$, F 是 K 的 n 次扩张, 把 F 中的元素看成为分量在域 K 中的 n-维向量. 对任意给定的 $\alpha \in F$, 映射 $T(\beta) = \alpha \cdot \beta$, 其中 $\cdot$ 为向量的内积, 满足定理 3.1 中的性质 (a), (b), (c), 和 (e). 证明若映射 T 还满足定理 3.1 中的性质 (d), 即对任意 $\beta \in F$ 有 $T(\beta) = T(\beta^q)$, 则存在 $c \in \mathbb{F}_q^*$ 使得 $T = c\mathrm{Tr}$. (此结论来源于 Anselm Blumer.)

3.4 设 $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^n}$, 且 $\alpha \in K$. 证明 $\mathrm{Tr}_{F/K}(\alpha) = n \cdot \alpha$, $\mathrm{N}_{F/K}(\alpha) = \alpha^n$.

3.5 类似于定理 3.3, 对于 $\alpha \in F$, 给出并证明利用 α 的极小多项式的次数和系数给出计算 $\mathrm{Tr}_{F/K}(\alpha^{-1})$ 和 $\mathrm{N}_{F/K}(\alpha^{-1})$ 的公式.

3.6 设域 $\mathbb{F}_{2^6}$ 有本原元素 α 满足 $\alpha^6 + \alpha + 1 = 0$. 找出 $\mathbb{F}_{2^6}$ 中一个元素 θ 使其迹为 1, 并由此给出二次方程 $x^2 + x = \alpha$ 的根.

3.7 设域 $F_m = \mathbb{F}_{8^m}$, $m = 1, 2, \ldots$.

a. 证明方程 $x^7 = 1$ 在每个这样的域中都恰有 7 个根.
b. 用 a_m 表示方程 $x^7 = 1$ 的迹为 0 的根 (这里的迹是 F_m 到 $\mathbb{F}_2$ 的), 对所有 $m \geq 1$ 计算 a_m.

3.8 设域 $\mathbb{F}_{2^5}$ 有本原元素 α 满足 $\alpha^5 = \alpha^2 + 1$. 对 $\gamma \in \mathbb{F}_{2^5}$, 给出方程 $y^2 + y = \gamma$ 在域 $\mathbb{F}_{2^5}$ 中有两个根的一个充要条件, 这个条件用 γ 被 $\mathbb{F}_{2^5}$ 的基 $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ 表示的系数给出.

3.9 设域 $\mathbb{F}_{3^3}$ 中有本原元素 α 满足 $\alpha^3 = \alpha + 2$.
a. 把任一元素 γ 表示为 $\gamma = a_2\alpha^2 + a_1\alpha + a_0$, 其中 $a_i \in \mathbb{F}_3$. 找出向量 $\mathbf{t} = (t_2, t_1, t_0)$ 使得 $\mathrm{Tr}(\gamma) = a_2t_2 + a_1t_1 + a_0t_0$.
b. 给出三个方程 $y^3 - y = \alpha^3$, $y^3 - y = \alpha^8$, 和 $y^3 - y = 2\alpha + 2$ 的根.

3.10 本题给出定理 3.6 中关于范数部分的 Hilbert 构造式证明. 给定元素 $\alpha, \theta \in \mathbb{F}_{q^n}$, 定义

$$\beta = \theta + \alpha\theta^q + \alpha^{1+q}\theta^{q^2} + \cdots + \alpha^{1+q+\cdots+q^{n-2}}\theta^{q^{n-1}}.$$

a. 证明 $\alpha\beta^q + \theta = \beta + \mathrm{N}(\alpha) \cdot \theta$.
b. 证明对任意给定的 α, 存在 θ 使得 $\beta \neq 0$.
c. 证明若 $\mathrm{N}(\alpha) = 1$, 则存在 β 使得 $\alpha = \beta^{1-q}$.

3.11 设域 $\mathbb{F}_{3^3} = \mathbb{F}_3[x]/(x^3 + 2x + 1)$, 给出 $\mathbb{F}_{3^3}$ 中所有 13 个范数为 1 的元素, 并对每个范数为 1 的元素 α, 找出元素 β 使得 $\alpha = \beta^{-2}$.

3.12 证明若 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 是 $F = \mathbb{F}_{q^n}$ 在 $K = \mathbb{F}_q$ 上的一组基, 则存在至少一个 i, $1 \leq i \leq n$, 使得 $\mathrm{Tr}(\alpha_i) \neq 0$.

3.13 设 β 是 $\mathbb{F}_{2^n}$ 在 $\mathbb{F}_2$ 上的一个定义元素, 即 $\{1, \beta, \ldots, \beta^{n-1}\}$ 是 $\mathbb{F}_{2^n}$ 在 $\mathbb{F}_2$ 上的一组基. 证明

(a) 存在 k, $0 \leq k \leq n-1$, 使得 $\mathrm{Tr}(\beta^k) = 1$.
(b) 对每个 $i = 0, 1, \ldots, n-1$, 存在 $\alpha_i \in \mathbb{F}_{2^n}$ 使得

$$\alpha_i^2 + \alpha_i = \begin{cases} \beta^i & \text{若 } \mathrm{Tr}(\beta^i) = 0, \\ \beta^i + \beta^k & \text{若 } \mathrm{Tr}(\beta^i) = 1. \end{cases}$$

(c) 设 $\gamma = \sum_{i=0}^{n-1} c_i\beta^i$, $c_i \in \mathbb{F}_2$, 且 $\mathrm{Tr}(\gamma) = 0$, 则 $x^2 + x + \gamma$ 的根为 $\sum_{i=0}^{m-1} c_i\alpha_i$ 和 $1 + \sum_{i=0}^{m-1} c_i\alpha_i$.

3.14 设 α 是 $\mathbb{F}_2$ 上本原多项式 $x^3 + x + 1$ 的一个根, 考虑 $\mathbb{F}_8$ 在 $\mathbb{F}_2$ 上的基 $\alpha, \alpha^2, \alpha^3$, 找出类似于例 3.6 中的矩阵 A 和 B, 并给出该基的对偶基.

3.15 找出下面两个 $\mathbb{F}_2$ 的扩域关于基 $1, \alpha, \ldots, \alpha^{n-1}$ 的对偶基:

a. $\mathbb{F}_{32}$ 且满足 $\alpha^5 = \alpha^2 + 1$.
b. $\mathbb{F}_{64}$ 且满足 $\alpha^6 = \alpha + 1$.

3.16 设 α 是 $K=\mathbb{F}_q$ 上一个 n 次首一不可约多项式 $f(x)$ 的一个根, 设 $\{1,\alpha,\dots,\alpha^{n-1}\}$ 是 $F=\mathbb{F}_{q^n}$ 在 K 上的一组多项式基. 证明基 $\{1,\alpha,\dots,\alpha^{n-1}\}$ 的对偶基仍为多项式基当且仅当 $f(x)$ 是一个二项式且 $n\equiv 1 \pmod{p}$, 这里 p 是域 F 的特征.

3.17 证明存在 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的自对偶基当且仅当或者 q 为偶数或者 q 和 n 都是奇数.

3.18 设 σ 是 $F=\mathbb{F}_{q^n}$ 在 $K=\mathbb{F}_q$ 上的 Frobenius 自同构, $\{\alpha,\sigma(\alpha),\dots,\sigma^{n-1}(\alpha)\}$ 是 F 在 K 上的一个正规基. 设 $C=(c_{ij})_{0\le i,j\le n-1}$ 是 K 上的一个非退化矩阵, 令

$$\beta_i=\sum_{j=0}^{n-1}c_{ij}\sigma^j(\alpha),\quad i=0,1,\dots,n-1.$$

证明

(a) $\{\beta_0,\beta_1,\dots,\beta_{n-1}\}$ 是 F 在 K 上的正规基当且仅当 C 是循环矩阵, 即对所有的 $i,j=0,1,\dots,n-1$ 有 $c_{i+1,j+1}=c_{ij}$, 这里的下标 i,j 是模 n 意义下的.

(b) F 在 K 上正规基的个数等于域 K 上非退化循环矩阵的个数除以 n.

(c) F 在 K 上正规基的个数等于 $\frac{1}{n}\Phi_q(x^n-1)$, 这里 $\Phi_q(x^n-1)$ 是 $K[x]$ 中次数小于 n 且与 x^n-1 互素的多项式的个数, 也是环 $K[x]/(x^n-1)$ 的乘法群的阶.

第四章　有限域上的多项式

我们已经看到, 多项式在有限域的研究中起着重要的作用. 例如给定 q 元域 $\mathbb{F}_q$ 上的一个 n 次不可约多项式, 我们可以构造出 q^n 元域. 前面我们也求出了 $\mathbb{F}_q$ 上的 n 次首一不可约多项式的个数以及 n 次本原多项式的个数. 我们还知道可以通过分解 $x^{q^n}-x$ 来得到 $\mathbb{F}_q$ 上的所有 d 次首一不可约多项式, 其中 $d \mid n$. 本章就来讨论有限域上多项式的分解问题以及有限域上多项式的其它性质.

4.1　分圆多项式

设 $F=\mathbb{F}_q$ 为 q 元域, 记 $I_{q,n}(x)$ 为 $F[x]$ 中所有 n 次首一不可约多项式的乘积, 式 (2.1) 为

$$x^{q^n}-x=\prod_{d|n} I_{q,d}(x).$$

在域 F 上的所有有理函数组成的域 $F(x)=\{\frac{p(x)}{q(x)} \mid p(x),q(x)\in F[x], q(x)\neq 0\}$ 的乘法群中利用 Möbius 反演公式得到

$$I_{q,n}(x)=\prod_{d|n}(x^{q^{\frac{n}{d}}}-x)^{\mu(d)}, \tag{4.1}$$

其中 μ 为 Möbius 函数.

例 4.1: 设 $q=2$, $n=6$. 则由 (4.1) 得到

$$I_{2,6}(x)=\frac{(x^2-x)(x^{64}-x)}{(x^4-x)(x^8-x)}=\frac{(x-1)(x^{63}-1)}{(x^3-1)(x^7-1)}=\text{一个 54 次多项式}. \tag{4.2}$$

□

式 (4.2) 中的这个 54 次多项式是 9 个 $\mathbb{F}_2$ 上的 6 次 (首一) 不可约多项式的乘积. 但是如何找到这些 6 次不可约多项式? 由 (4.2) 我们看到这需要分解形如 x^m-1 的多项式, 类比在有理数域 $\mathbb{Q}$ 上分解多项式 x^m-1, 下面我们引入有限域上的分圆多项式.

设 n 为正整数, 多项式 $x^n-1\in F[x]$ 的根 (在 F 的扩域中) 称为 n 次单位根, 而 n 次本原单位根就是域的乘法群中阶为 n 的元素, 即 n 次本原单位根 ζ 满足 $\zeta^n=1$ 但是对任意 $1\leq k\leq n-1$, 都有 $\zeta^k\neq 1$. 显然任意特征为 0 的域的某个扩域中一定存在 n 次本原单位根.

设 $\mathrm{char}F=p$, 若 $p\mid n$, 则 $x^n-1=(x^{\frac{n}{p}}-1)^p$, 即 x^n-1 的根一定是 $x^{\frac{n}{p}}-1$ 的根, 所以这时 F 的扩域中就不存在 n 次本原单位根. 设 $F=\mathbb{F}_q$ 为 q 元域. 若 q 与 n 不互素, 则 F 的特征整除 n, 从而 F 的扩域中不存在 n 次本原单位根. 反之若 q 与 n 互素, 则 $\overline{q}\in U(n)$, 设 q 模 n 的乘法阶为 m, 则 $q^m\equiv 1\,(\mathrm{mod}\ n)$. 取 F 的 m 次扩域 $\mathbb{F}_{q^m}$ 的本原元素 θ, 令 $\zeta=\theta^{\frac{q^m-1}{n}}$, 则 $\zeta\in\mathbb{F}_{q^m}$ 就是 n 次本原单位根. 这样我们证明了q 元域 $F=\mathbb{F}_q$ 的某个扩域中存在 n 次本原单位根当且仅当 q 与 n 互素.

下面我们只考察有限域 $F=\mathbb{F}_q$. 设 n 为与 q 互素的正整数且 ζ 为 n 次本原单位根, ζ 在 F 的扩域 E 中, 则 x^n-1 在 $E[x]$ 中可以完全分解为

$$x^n-1=\prod_{j=0}^{n-1}(x-\zeta^j). \tag{4.3}$$

由于 $\mathrm{ord}(\zeta^j)=n/\gcd(j,n)$, 所以对于 $0\le j\le n$, $\mathrm{ord}(\zeta^j)=n$ 当且仅当 $\gcd(j,n)=1$, 故共有 $\phi(n)$ 个 n 次本原单位根. 我们定义第 n 个分圆多项式 $\Phi_n(x)$ 为以所有 n 次本原单位根为根的首一多项式, 这是一个E 上的 $\phi(n)$ 次多项式且可写成

$$\Phi_n(x)=\prod_{0\le j\le n-1,\ \gcd(j,n)=1}(x-\zeta^j). \tag{4.4}$$

考察 x^n-1 的分解式 (4.3), 对任意 $0\le j\le n-1$, $\mathrm{ord}(\zeta^j)$ 为 n 的因子. 反之对任意 $d\mid n$, 有 $\phi(d)$ 个 j 满足 $0\le j\le n-1$ 且 $\mathrm{ord}(\zeta^j)=d$ (恰为满足 $\gcd(j,n)=n/d$ 的那些 j), 这样的单位根为 d 次本原单位根. 由此我们可得

$$x^n-1=\prod_{d\mid n}\Phi_d(x),$$

再利用 Möbius 反演公式得到

$$\Phi_n(x)=\prod_{d\mid n}(x^d-1)^{\mu(\frac{n}{d})}. \tag{4.5}$$

例如, 若 $n=p$ 为素数, 则

$$\Phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1.$$

进一步地, 由式 (4.5) 我们可以看出分圆多项式 $\Phi_n(x)$ 可以写成一个分式, 分子是满足 $\mu(\frac{n}{d})=+1$ 的那些项 x^d-1 的乘积, 分母是满足 $\mu(\frac{n}{d})=-1$ 的那些项 x^d-1 的乘积, 所以这个分式的分子和分母都是首一多项式, 且系数都在 F 中 (实际上都在 F 的素子域 $\mathbb{F}_p$ 中). 由长除我们知道一个 F 上的首一多项式除以一个 F 上的首一多项式结果依然是 F 上的首一多项式, 所以分圆多项式 $\Phi_n(x)$ 是一个 F 上的首一多项式, 虽然定义中 $\Phi_n(x)$ 的根在 F 的扩域 E 中. (我们也可以利用 $\Phi_n(x)^q=\Phi_n(x^q)$ 推出 $\Phi_n(x)\in F[x]$.)

下面我们来计算分圆多项式 (假定在给定的有限域上涉及的分圆多项式都存在), 例如求 $\Phi_{18}(x)$. 由 (4.5) 我们有

$$\Phi_{18}(x)=\frac{(x^{18}-1)(x^3-1)}{(x^9-1)(x^6-1)},$$

这是一个 21 次多项式除以一个 15 次多项式, 做长除可以求出结果. 下面我们通过此例来说明一个由 Berlekamp 给出的求分圆多项式的方法, 因为 $\deg \Phi_{18}(x) = \phi(18) = 6$, 所以此多项式模 x^7 并不会影响结果. 由

$$\begin{aligned}\Phi_{18}(x) &\equiv \frac{(-1)(x^3-1)}{(-1)(x^6-1)} \pmod{x^7} \equiv \frac{(1-x^3)(1-x^{12})}{(1-x^6)} \pmod{x^7} \\ &\equiv (1-x^3)(1+x^6) \pmod{x^7} \equiv 1-x^3+x^6 \pmod{x^7}\end{aligned}$$

可得 $\Phi_{18}(x) = x^6 - x^3 + 1$. 下表列出前几个分圆多项式:

n	$\Phi_n(x)$
1	$x-1$
2	$x+1$
3	x^2+x+1
4	x^2+1
5	$x^4+x^3+x^2+x+1$
6	x^2-x+1
7	$x^6+x^5+x^4+x^3+x^2+x+1$
8	x^4+1
9	x^6+x^3+1.

定理 4.1: 设 p 为素数, m 为正整数且 $p \nmid m$. 则对任意 $k \geq 1$,

$$\Phi_{mp^k}(x) = \Phi_{mp}(x^{p^{k-1}}) = \frac{\Phi_m(x^{p^k})}{\Phi_m(x^{p^{k-1}})}.$$

证明: 利用 (4.5) (交换其中的 d 和 $\frac{n}{d}$) 我们有

$$\Phi_{mp^k}(x) = \prod_{d|mp^k} (x^{\frac{mp^k}{d}} - 1)^{\mu(d)} = \prod_{d|mp} (x^{\frac{mp^k}{d}} - 1)^{\mu(d)} = \prod_{d|mp} ((x^{p^{k-1}})^{\frac{mp}{d}} - 1)^{\mu(d)} = \Phi_{mp}(x^{p^{k-1}}).$$

现在我们把上面式子中 mp 的因子 d 按是否能被 p 整除分成不相交的两部分, 不能被 p 整除的那些因子给出

$$\prod_{d|m} (x^{\frac{mp^k}{d}} - 1)^{\mu(d)} = \Phi_m(x^{p^k}),$$

而能被 p 整除的那些因子给出

$$\prod_{dp|mp} (x^{\frac{mp^k}{dp}} - 1)^{\mu(dp)} = \prod_{d|m} (x^{\frac{mp^{k-1}}{d}} - 1)^{\mu(pd)} = \prod_{d|m} (x^{\frac{mp^{k-1}}{d}} - 1)^{-\mu(d)} = \Phi_m(x^{p^{k-1}})^{-1},$$

所以

$$\Phi_{mp^k}(x) = \frac{\Phi_m(x^{p^k})}{\Phi_m(x^{p^{k-1}})}.$$

□

例 4.2: 考虑 $\Phi_{72}(x)$. 由定理 4.1 得到

$$\Phi_{72}(x) = \Phi_{8\cdot 9}(x) = \Phi_{8\cdot 3}(x^3) = \Phi_{3\cdot 2}((x^3)^4) = \Phi_6(x^{12}) = x^{24} - x^{12} + 1.$$

类似地, 对任意素数 p 和 $k \geq 1$, 在定理 4.1 中取 $m = 1$, 则有

$$\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}}) = x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \cdots + x^{p^{k-1}} + 1.$$

特别地, 对任意 $k \geq 1$, 有 $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$. □

继续例 4.1, 我们得到

$$I_{2,6}(x) = \frac{(x-1)(x^{63}-1)}{(x^3-1)(x^7-1)} = \frac{\Phi_1 \cdot \Phi_1 \cdot \Phi_3 \cdot \Phi_7 \cdot \Phi_9 \cdot \Phi_{21} \cdot \Phi_{63}}{\Phi_1 \cdot \Phi_3 \cdot \Phi_1 \cdot \Phi_7} = \Phi_9 \cdot \Phi_{21} \cdot \Phi_{63},$$

其中多项式 $\Phi_9(x)$ 的次数为 $\phi(9) = 6$, $\Phi_{21}(x)$ 的次数为 $\phi(21) = 12$, 而 $\Phi_{63}(x)$ 的次数为 $\phi(63) = 36$. 由此得到在域 $\mathbb{F}_2$ 上, $\Phi_9(x) = x^6 + x^3 + 1$ 不可约, $\Phi_{21}(x)$ 是 2 个 6 次不可约多项式的乘积, 而 Φ_{63} 为 6 个 6 次不可约多项式的乘积. 一般地, 由式 (4.1) 可看出 $I_{q,n}(x)$ 是一些分圆多项式的乘积, 所以为了完全分解 $I_{q,n}(x)$, 我们需要分解分圆多项式.

我们知道对所有 $n \geq 1$, 分圆多项式 $\Phi_n(x)$ 在有理数域 $\mathbb{Q}$ 上不可约, 但在有限域上, 情况不是这样简单. 例如 $\Phi_4(x) = x^2 + 1$ 在 $\mathbb{F}_3$ 和 $\mathbb{F}_7$ 上不可约, 但在 $\mathbb{F}_5$ 上可约, 因为在 $\mathbb{F}_5$ 上有 $x^2 + 1 = (x+2)(x+3)$.

设 $F = \mathbb{F}_q$, $\gcd(n, q) = 1$, 下面考虑分圆多项式 $\Phi_n(x)$ 在域 F 上的分解. 设 $m = \mathrm{ord}_n(q)$ 为 q 模 n 的乘法阶, 即满足 $q^m \equiv 1 \pmod{n}$ 的最小正整数 m, 则在 F 的 m 次扩域 $E = \mathbb{F}_{q^m}$ 中存在 n 次本原单位根 ζ, 所以 $\Phi_n(x)$ 的全部根为 ζ^j, 其中 $0 \leq j \leq n-1$ 且 $\gcd(j, n) = 1$. 对于 $\Phi_n(x)$ 的每个根 ζ^j, 显然 ζ^j 在 F 上的极小多项式是 $\Phi_n(x)$ 在 F 上的不可约因子.

先看 ζ 在 F 上的极小多项式, 由定理 2.10 知此极小多项式的次数 d 是满足 $q^d \equiv 1 \pmod{\mathrm{ord}(\zeta)}$ 的最小正整数 d, 由于 $\mathrm{ord}(\zeta) = n$, 即 d 为 q 模 n 的乘法阶, 从而 $d = m$, 这样我们得到 $\Phi_n(x)$ 在 F 上有一个 m 次不可约因子, 即 ζ 在 F 上的极小多项式 $f_\zeta(x)$. 如果 $m \neq \phi(n)$, 则存在 $\Phi_n(x)$ 的根但不是 $f_\zeta(x)$ 的根. 取一个这样的根 ξ, 再求 ξ 在 F 上的极小多项式 $f_\xi(x)$, 由于 $\mathrm{ord}(\xi) = n$, 所以 $\deg f_\xi(x) = m$. 如果需要就继续这个过程, 可以得到, 分圆多项式 $\Phi_n(x)$ 在 F 上的每个不可约因子的次数都是 m. 这样我们便证明了如下定理.

定理 4.2: 设 $F = \mathbb{F}_q$, $\gcd(n, q) = 1$. 则分圆多项式 $\Phi_n(x)$ 在域 F 上可以分解为 $\frac{\phi(n)}{m}$ 个 m 次首一不可约多项式的乘积, 其中 $m = \mathrm{ord}_n(q)$. □

例 4.3: 考虑 $\Phi_7(x)$ 在 $\mathbb{F}_2$ 上的分解. 容易算出 $\mathrm{ord}_7(2) = 3$, 又 $\deg \Phi_7(x) = \phi(7) = 6$, 所以 $\Phi_7(x)$ 分解为 $\mathbb{F}_2$ 上 2 个 3 次不可约多项式的乘积. 下面我们需要在域 $\mathbb{F}_{2^3}$ 中找 7 阶元素, 不妨设 $E = \mathbb{F}_{2^3} = \mathbb{F}_2[x]/(x^3+x+1)$, 令 $\zeta = \overline{x}$, 则容易计算得到 $\mathrm{ord}(\zeta) = 7$ (ζ 为域 E 的本原元), 所以 ζ 在 $\mathbb{F}_2$ 上的极小多项式为 $f_\zeta(x) = (x-\zeta)(x-\zeta^2)(x-\zeta^4) = x^3 + x + 1$. 利用 $\Phi_7(x)$ 的另外一个根 ζ^3, 我们求出它在 $\mathbb{F}_2$ 上的极小多项式为 $f_{\zeta^3}(x) = (x-\zeta^3)(x-\zeta^6)(x-\zeta^5) = x^3 + x^2 + 1$. 故我们得到 $\Phi_7(x)$ 在 $\mathbb{F}_2$ 上的分解为

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1).$$

更一般地, 考虑 $\Phi_{q^m-1}(x)$ 在 $\mathbb{F}_q$ 上的分解. 由于 $n = q^m - 1$, 所以 q 模 n 的乘法阶就是 m. 而在域 $\mathbb{F}_{q^m}$ 中阶为 $n = q^m - 1$ 的元素就是 $\mathbb{F}_{q^m}$ 的本原元, 这样我们得到 $\Phi_{q^m-1}(x)$ 的根就是

域 $\mathbb{F}_{q^m}$ 的所有本原元, 所以 $\Phi_{q^m-1}(x)$ 在 $\mathbb{F}_q$ 上的每个首一不可约因式都是域 $\mathbb{F}_q$ 上的 m 次本原多项式, 而 $\mathbb{F}_q$ 上的每个 m 次本原多项式也是 $\Phi_{q^m-1}(x)$ 在 $\mathbb{F}_q$ 上的首一不可约因式, 从而分圆多项式 $\Phi_{q^m-1}(x)$ 可分解为 $\mathbb{F}_q$ 上的所有 m 次本原多项式的乘积. 例如我们已经知道 $\mathbb{F}_2$ 上的两个 4 次本原多项式分别为 x^4+x+1 和 x^4+x^3+1, 这样可给出 $\Phi_{15}(x)$ 在 $\mathbb{F}_2$ 上的分解为 $\Phi_{15}(x)=(x^4+x+1)(x^4+x^3+1)$. □

由定理 4.2 易知, 分圆多项式 $\Phi_n(x)$ 在域 $\mathbb{F}_q$ 上不可约当且仅当 $m=\phi(n)$, 这也等价于整数模 n 的乘法群 $U(n)$ 为循环群且 $\bar{q}$ 为 $U(n)$ 的一个生成元. 若正整数 a 与 n 互素, 称 a 为模 n 的一个原根若剩余类 $\bar{a}$ 在群 $U(n)$ 中的阶为群 $U(n)$ 的阶 $\phi(n)$ (这隐含着群 $U(n)$ 为循环群). 由初等数论可知, $U(n)$ 为循环群当且仅当 $n=1,\,2,\,4,\,r^s,\,2r^s$, 其中 r 为奇素数, s 为正整数. 由此我们得到如下推论.

推论 4.3: 设 $F=\mathbb{F}_q$, $\gcd(n,q)=1$. 则分圆多项式 $\Phi_n(x)$ 在域 F 上不可约当且仅当 q 为模 n 的原根. 所以若 $\Phi_n(x)$ 在域 F 上不可约, 则有 $n=1,\,2,\,4,\,r^s,\,2r^s$, 其中 r 为奇素数, s 为正整数. □

推论 4.3 表明若 n 不等于 $1,\,2,\,4,\,r^s,\,2r^s$ 中的一个, 其中 r 为奇素数, s 为正整数, 则 $\Phi_n(x)$ 在任意有限域上都可约, 例如 $\Phi_8(x)=x^4+1$ 就在任意有限域上都可约. 另外虽然 $n=7$ 为素数, 但是 2 并不是模 7 的原根, 故 $\Phi_7(x)$ 在 $\mathbb{F}_2$ 上可约 (我们已在例 4.3 中给出了 $\Phi_7(x)$ 在 $\mathbb{F}_2$ 上的分解). 进一步地, 3 是模 7 的原根, 所以 $\Phi_7(x)$ 在 $\mathbb{F}_3$ 上不可约. 同时易知, 当且仅当素数幂 q 满足 $q\equiv 3 \pmod 7$ 或者 $q\equiv 5 \pmod 7$ 时, $\Phi_7(x)$ 在 $\mathbb{F}_q$ 上不可约, 例如, $q=5,\,17,\,19,\,31,\,59,\,61$ 等等. 对于奇数 n, 分圆多项式 $\Phi_n(x)$ 在 $\mathbb{F}_2$ 上不可约当且仅当 2 为模 n 的原根, 比如 n 取如下素数幂时就是如此: $n=3,\,5,\,9,\,11,\,13,\,19,\,25,\,29,\,\ldots$, 这便给出 $\mathbb{F}_2$ 上的不可约多项式, 其次数 d 为 $2,\,4,\,6,\,10,\,12,\,18,\,20,\,28,\,\ldots$.

设 $p=\mathrm{char}\mathbb{F}_q$, 即 q 为 p 的方幂. 注意到对正整数 n, 若 $p\mid n$, 则分圆多项式 $\Phi_n(x)$ 在 $\mathbb{F}_q$ 上并没有定义. 为了完整性, 我们可以有如下定义: 设 $n=p^kn'$, 其中 $k\geq 1$ 且 $p\nmid n'$, 则定义 $\Phi_n(x)=\Phi_{n'}(x)^{p^k-p^{k-1}}$. 这时依然有 $\deg\Phi_n(x)=\phi(n)$. 而此时在 $\mathbb{F}_q$ 上有 $x^n-1=(x^{n'}-1)^{p^k}$, 即 x^n-1 的分解也转化为 $x^{n'}-1$ 的分解. 这表明我们上面假设 q 与 n 互素也并不影响一般性.

4.2 分解多项式的 Berlekamp 算法

上节中我们利用分圆多项式 $\Phi_n(x)$ 的根在 F 上的极小多项式来分解 $\Phi_n(x)$, 这需要在 F 的扩域中进行, 但通常说来找出扩域以及完成扩域中的运算都是不方便的. 下面给出有限域上分解多项式的一个算法, 此算法来源于 Berlekamp, 它对任意多项式都适合. 下面依然设 $F=\mathbb{F}_q$ 为 q 元域.

定理 4.4: 设 $f(x)$ 是域 F 上的首一多项式且 $\deg f(x)=n\geq 1$, 设 $h(x)\in F[x]$ 满足

$$h(x)^q\equiv h(x)\ (\mathrm{mod}\ f(x)), \tag{4.6}$$

则有

$$f(x)=\prod_{s\in F}\gcd(f(x),h(x)-s).$$

证明: 因为 F 中元素就是多项式 y^q-y 的根, 我们有 $y^q-y=\prod_{s\in F}(y-s)$, 用多项式 $h(x)$ 来替换其中的不定元 y 得到

$$h(x)^q-h(x)=\prod_{s\in F}(h(x)-s).$$

这样条件 (4.6) 可以写成 $f(x)\mid\prod_{s\in F}(h(x)-s)$, 由此可得

$$f(x)\mid\gcd\left(f(x),\prod_{s\in F}(h(x)-s)\right).$$

注意到当 $s_1\neq s_2\in F$ 时, $h(x)-s_1$ 与 $h(x)-s_2$ 互素, 故 $\gcd\left(f(x),\prod_{s\in F}(h(x)-s)\right)=\prod_{s\in F}\gcd(f(x),h(x)-s)$. 这样我们有

$$f(x)\mid\prod_{s\in F}\gcd(f(x),h(x)-s). \tag{4.7}$$

另一方面, 对每个 $s\in F$, 我们有 $\gcd(f(x),h(x)-s)\mid f(x)$. 进一步地, 由于当 $s_1\neq s_2$ 时, $h(x)-s_1$ 与 $h(x)-s_2$ 互素, 所以 $\gcd(f(x),h(x)-s_1)$ 与 $\gcd(f(x),h(x)-s_2)$ 互素, 故

$$\prod_{s\in F}\gcd(f(x),h(x)-s)\mid f(x). \tag{4.8}$$

由于 $f(x)$ 首一, 综合式 (4.7) 和 (4.8) 就得到定理的证明. □

注意到若存在 $h(x)\in F[x]$ 满足 (4.6) 且 $0<\deg h(x)<n$, 则对每个 $s\in F$ 都有 $\deg\gcd(f(x),h(x)-s)<\deg f(x)$, 这时定理 4.4 给出的就是 $f(x)$ 的一个非平凡分解. 我们称满足 (4.6) 且 $0<\deg h(x)<\deg f(x)$ 的多项式 $h(x)\in F[x]$ 为 f-约化多项式. 下面我们证明若多项式 $f(x)$ 的互不相同的首一不可约因式多于一个, 则 f-约化多项式一定存在, 我们还将给出求 f-约化多项式的方法.

设 $f(x)\in F[x]$ 首一且 $\deg f(x)=n\geq 1$, $R=F[x]/(f(x))$, 这是域 F 上的一元多项式环模多项式 $f(x)$ 的剩余类环, 其中的元素可表为 F 上次数小于 n 的多项式, 容易验证 R 在多项式加法以及把数乘定义为多项式乘法 (F 中的元素也是 F 上的多项式) 下构成域 F 上的线性空间且 $1,x,x^2,\ldots,x^{n-1}$ 为空间 R 的一组基. 记 $R(f):=\{h(x)\in R\mid h(x)^q=h(x)\}$, 其中的 $h(x)^q$ 表示 $h(x)^q$ 模 $f(x)$ 的那个唯一的次数 $<n$ 的多项式, 即 $R(f)$ 是满足 (4.6) 的次数 $<n$ 的多项式构成的集合. 显然 $F\subseteq R(f)$, 而 $R(f)\setminus F$ 中的元素就是那些 f-约化多项式. 对任意 $s_1,s_2\in F$, $h_1(x),h_2(x)\in R(f)$, 有 $(s_1h_1(x)+s_2h_2(x))^q=s_1^qh_1(x)^q+s_2^qh_2(x)^q=s_1h_1(x)+s_2h_2(x)$, 所以 $R(f)$ 是线性空间 R 的一个子空间. 设 $f(x)$ 有 m 个互不相同的首一不可约因式 $p_i(x)$, $1\leq i\leq m$, 并设 $f(x)$ 的标准分解式为 $f(x)=\prod_{i=1}^m p_i(x)^{e_i}$, 其中 $e_i\geq 1$, $1\leq i\leq m$.

定理 4.5: 子空间 $R(f)$ 的维数等于 m, 即 $f(x)$ 的互不相同的首一不可约因式的个数.

证明: 显然 $h(x) \in R(f)$ 当且仅当 $\deg h(x) < n$ 且

$$f(x) \mid \prod_{s\in F}(h(x)-s).$$

对于 $h(x) \in R(f)$, 我们有

$$\prod_{i=1}^{m} p_i(x)^{e_i} \mid \prod_{s\in F}(h(x)-s),$$

即对每个 $i \in \{1,2,\ldots,m\}$, 有 $p_i(x)^{e_i} \mid \prod_{s\in F}(h(x)-s)$, 由于对 $s \neq s' \in F$, $h(x)-s$ 与 $h(x)-s'$ 互素, 所以存在唯一的 $s_i \in F$ 使得 $p_i(x)^{e_i} \mid h(x)-s_i$, 即 $h(x) \equiv s_i \pmod{p_i(x)^{e_i}}$. 这样我们证明了对于任意 $h(x) \in R(f)$, 存在唯一的 $(s_1,s_2,\ldots,s_m) \in F^m$ 使得

$$\begin{cases} h(x) \equiv s_1 \pmod{p_1(x)^{e_1}}, \\ h(x) \equiv s_2 \pmod{p_2(x)^{e_2}}, \\ \quad\vdots \\ h(x) \equiv s_m \pmod{p_m(x)^{e_m}}. \end{cases} \tag{4.9}$$

反之, 任给 $(s_1,s_2,\ldots,s_m) \in F^m$, 由中国剩余定理, 存在唯一的 $h(x) \in F[x]$ 满足 (4.9) 且 $\deg h(x) < n$. 由此对于每个 $1 \le i \le m$, 有 $p_i(x)^{e_i} \mid h(x)-s_i$, 从而 $f(x) \mid \prod_{s\in F}(h(x)-s)$, 所以满足 (4.9) 且 $\deg h(x) < n$ 的多项式 $h(x)$ 满足 $h(x) \in R(f)$.

定义映射 $R(f) \to F^m$ 为 $h(x) \mapsto (s_1,s_2,\ldots,s_m)$, 其中 $h(x)$ 满足 (4.9). 由上面的证明得知这个映射为双射, 故 $R(f)$ 中有 q^m 个元素, 即 $\dim_F R(f) = m$. □

若 $m \ge 2$, 即 $f(x)$ 的互不相同的首一不可约因式多于一个, 则 $R(f) \setminus F \neq \varnothing$, 故一定存在 f-约化多项式. 下面我们来看如何具体求出 f-约化多项式.

设 $h(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in F[x]$, 则 $h(x)^q = a_0 + a_1x^q + \cdots + a_{n-1}x^{(n-1)q}$. 对于每个 $0 \le j \le n-1$, 设

$$x^{jq} \equiv \sum_{i=0}^{n-1} b_{ij}x^i \pmod{f(x)}, \tag{4.10}$$

记矩阵 $B = (b_{ij})_{0\le i,j\le n-1}$, 则有

$$h(x)^q = (1,x^q,\cdots,x^{(n-1)q}) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \equiv (1,x,\cdots,x^{n-1})B \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \pmod{f(x)},$$

所以 $h(x)^q \equiv h(x) \pmod{f(x)}$ 当且仅当

$$(B-I) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = 0,$$

其中 I 为 n 阶单位矩阵, 即满足 $h(x)^q \equiv h(x) \pmod{f(x)}$ 且 $\deg h(x) < n$ 的多项式 $h(x) \in F$ 的系数构成的向量 $(a_0, a_1, \cdots, a_{n-1})^T$ 是齐次线性方程组 $(B-I)X = 0$ 的解向量. 由定理 4.5 知道此齐次线性方程组解空间的维数是 m, 或者矩阵 $B-I$ 的秩为 $n-m$. 故通过求 $\mathrm{rank}(B-I)$, 我们也可以得到 $f(x)$ 的互不相同的首一不可约因式的个数. 解这个齐次线性方程组 $(B-I)X = 0$, 我们就可以求出 f-约化多项式. 注意到矩阵 $B-I$ 的第一列为零向量, 所以 $\mathrm{rank}(B-I) \leq n-1$ 且 $(a_0, 0, \ldots, 0)^T$ 是方程组 $(B-I)X = 0$ 的解, 这个解对应的是常数多项式 a_0, 并不是 f-约化多项式. 该方程组的满足 $(a_1, \ldots, a_{n-1}) \neq (0, \ldots, 0)$ 的解 $(a_0, a_1, \cdots, a_{n-1})^T$ 才对应 f-约化多项式, 实际上我们只需求出形如 $(0, a_1, \cdots, a_{n-1})^T$ 的非零解即可.

Berlekamp 算法: 给定任一首一多项式 $f(x) \in F[x]$, 其中 $\deg f(x) = n > 0$. 下面的步骤可以给出 $f(x)$ 的非平凡分解或者确认 $f(x)$ 不可约.

G1. 计算 $d(x) = \gcd(f(x), f'(x))$. 若 $\deg d(x) > 0$, 则 $f(x) = d(x) \cdot \frac{f(x)}{d(x)}$ 是 $f(x)$ 的非平凡分解. 若 $\deg d(x) = 0$, 则进入步骤 G2.

G2. 计算由式 (4.10) 定义的矩阵 B.

G3. 若 $\mathrm{rank}(B-I) = n-1$, 则 $f(x)$ 不可约. 若 $\mathrm{rank}(B-I) \leq n-2$, 求出齐次线性方程组 $(B-I)X = 0$ 的一组非零解 $(0, a_1, \cdots, a_{n-1})^T$, 令 $h(x) = a_1 x + \cdots + a_{n-1}x^{n-1}$.

G4. 对每个 $s \in F$, 计算 $\gcd(f(x), h(x) - s)$, 则 $f(x) = \prod_{s \in F} \gcd(f(x), h(x) - s)$ 就是 $f(x)$ 的一个非平凡分解.

例 4.4: 考虑多项式 $f(x) = x^5 + x + 1$ 在 $\mathbb{F}_2$ 上的分解. 容易得到 $\gcd(f(x), f'(x)) = 1$, 且在模 $f(x)$ 下有

$$\begin{aligned}
x^0 &\equiv 1, \\
x^2 &\equiv x^2, \\
x^4 &\equiv x^4, \\
x^6 &\equiv x + x^2, \\
x^8 &\equiv x^3 + x^4,
\end{aligned}$$

所以

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

可求出齐次线性方程组 $(B-I)X = 0$ 的基础解系为 $[1,0,0,0,0]^T$ 和 $[0,1,0,1,1]^T$. 这表明 $f(x)$ 有 2 个互不相同的不可约因式, 取 $[0,1,0,1,1]^T$ 对应的多项式 $h(x) = x + x^3 + x^4$. 通

过 Euclid 算法可计算出 $\gcd(f(x),h(x)) = \gcd(x^5+x+1, x^4+x^3+x) = x^3+x^2+1$ 和 $\gcd(f(x),h(x)+1) = \gcd(x^5+x+1, x^4+x^3+x+1) = x^2+x+1$. 所以

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

是 $f(x)$ 在 $\mathbb{F}_2$ 上的一个非平凡分解. 但是由上面计算我们知道 $f(x)$ 共有 2 个互不相同的不可约因式, 所以如上分解也是 $f(x)$ 在 $\mathbb{F}_2$ 上的完全分解. □

考虑多项式的分解时我们可以假设多项式没有重因式, 因为对于任意多项式 $f(x)$, $f(x)/\gcd(f(x),f'(x))$ 与 $f(x)$ 有相同的不可约因式, 但是没有重因式. 注意到利用 Berlekamp 算法我们需要计算 q 个最大公因式, 所以此算法在 q 较小时有效.

另外, Berlekamp 算法给出了多项式的非平凡分解, 但不一定是完全分解. 显然如果一个无重因式的多项式的互不相同的首一不可约因式只有 2 个, 则非平凡分解就是它的完全分解. 若多项式 $f(x)$ 有 m 个互不相同的首一不可约因式, 则齐次线性方程组 $(B-I)X=0$ 的基础解系中有 m 个向量, 它们可对应着 $R(f)$ 中线性无关的多项式 $h_0(x)=1$, $h_1(x)$, $h_2(x),\ldots,h_{m-1}(x)$. 我们可利用 $h_1(x)$ 给出 $f(x)$ 的一个非平凡分解

$$f(x) = \prod_{s\in F} \gcd(f(x), h_1(x)-s) = f_1(x)f_2(x)\cdots f_k(x).$$

如果这不是 $f(x)$ 的完全分解 (即 $k<m$), 则一定存在 $f(x)$ 的某个因式有至少 2 个不同的首一不可约因式. 这时一定存在某个 $h_i(x)$ 和 $f_j(x)$, $2\le i\le m-1$, $1\le j\le k$, 使得对所有 $s\in F$, 都有 $h_i(x)\not\equiv s \pmod{f_j(x)}$, 即这时通过 $h_i(x)$ 利用 Berlekamp 算法可得到 $f_j(x)$ 的非平凡分解. 事实上, 若对所有的 i, j, $2\le i\le m-1$, $1\le j\le k$, 都存在 $s_{ij}\in F$ 使得 $h_i(x)\equiv s_{ij} \pmod{f_j(x)}$. 不妨设 $f_1(x)$ 有至少 2 个不同的首一不可约因式, 则有 $\dim_F R(f_1)\ge 2$, 故存在多项式 $g_1(x)\in F[x]$ 满足 $g_1(x)^q \equiv g_1(x) \pmod{f_1(x)}$ 且 $1\le \deg g_1(x) < \deg f_1(x)$. 由中国剩余定理, 存在 $g(x)\in F[x]$ 使得 $g(x)\equiv g_1(x) \pmod{f_1(x)}$ 和对所有 $2\le j\le k$ 有 $g(x)\equiv 0 \pmod{f_j(x)}$ 且 $\deg g(x) < n$. 显然 $g(x)$ 满足 $g(x)^q \equiv g(x) \pmod{f(x)}$, 故 $g(x)\in R(f)$, 从而存在 $c_0,c_1,\ldots,c_{m-1}\in F$ 使得

$$g(x) = c_0 + c_1h_1(x) + \cdots + c_{m-1}h_{m-1}(x).$$

注意到存在某个 $s_0\in F$ 使得 $f_1(x) = \gcd(f(x),h_1(x)-s_0)$, 即 $h_1(x)\equiv s_0 \pmod{f_1(x)}$, 这样

$$g(x) \equiv c_0 + c_1s_0 + c_2s_{21} + \cdots + c_{m-1}s_{m-1,1} \pmod{f_1(x)},$$

与 $g(x)\equiv g_1(x) \pmod{f_1(x)}$ 且 $1\le \deg g_1(x) < \deg f_1(x)$ 矛盾. 所以如果利用 $h_1(x)$ 给出 $f(x)$ 的非平凡分解 $f(x) = f_1(x)f_2(x)\cdots f_k(x)$ 不是完全分解, 则对每个因式 $f_j(x)$, $1\le j\le k$, 我们可以利用 $h_2(x)$ 继续利用 Berlekamp 算法来分解 $f_j(x) = \prod_{s\in F}\gcd(f_j(x),h_2(x)-s)$. 这个过程可以继续下去, 直至得到 $f(x)$ 的完全分解.

下面考虑多项式 $f(x)=x^n-1$ 在域 $F=\mathbb{F}_q$ 上的分解, 根据 4.1 节末的说明, 我们可以假设 $\gcd(q,n)=1$, 这时 x^n-1 无重因式. 下面的定理说明, 这时也可以在不解方程组的情况下求出 Berlekamp 算法中需要的多项式 $h(x)$.

定理 4.6: 多项式 $h(x)=\sum_{i=0}^{n-1}a_ix^i$ 满足 $h(x)^q\equiv h(x)\,(\mathrm{mod}\ (x^n-1))$ 当且仅当对所有 $i=0,1,\ldots,n-1$, 有 $a_{iq\,(\mathrm{mod}\ n)}=a_i$.

证明: 计算得知

$$h(x)^q\equiv\sum_{i=0}^{n-1}a_ix^{iq\,(\mathrm{mod}\ n)}\ (\mathrm{mod}\ (x^n-1)),$$

比较 $h(x)^q\ (\mathrm{mod}\ (x^n-1))$ 和 $h(x)$ 中 $x^{iq\,(\mathrm{mod}\ n)}$ 的系数可得结论. □

注意到因为 $\gcd(q,n)=1$, 映射 $\pi:\ i\mapsto iq\ (\mathrm{mod}\ n)$ 是 $\mathbb{Z}_n=\{0,1,\ldots,n-1\}$ 上的一个置换, 可把它写成互不相交的轮换的乘积. 置换 π 的每个轮换因子中的元素构成的集合称为分圆陪集. 显然包含元素 i 的分圆陪集为 $\{i,iq,iq^2,\ldots,iq^{k-1}\}$, 其中 k 为满足 $iq^k\equiv i\ (\mathrm{mod}\ n)$ 的最小正整数. 设 $\mathbb{Z}_n$ 在乘以 q 下 (即映射 π 的作用下) 得到的分圆陪集为 $C_0=\{0\}$, C_1, …, C_{m-1}, 令 $h_i(x)=\sum_{k\in C_i}x^k$. 则由定理 4.6 知 $h_i\in R(f)$ 且 $R(f)$ 中每个元素都可由 $h_0(x)$, $h_1(x)$, …, $h_{m-1}(x)$ 在 F 上线性表出. 由于当 $0\le i\ne j\le m-1$ 时, C_i 与 C_j 不相交, 故 $h_i(x)$ 和 $h_j(x)$ 中出现的各项的次数完全不同, 故 $h_0(x)$, $h_1(x)$, …, $h_{m-1}(x)$ 在 F 上线性无关, 所以 $h_0(x)$, $h_1(x)$, …, $h_{m-1}(x)$ 就构成 $R(f)$ 在 F 上的一组基. 由 $\dim_F R(f)=m$ 得到 x^n-1 在 F 上的互不相同的首一不可约因式的个数等于分圆陪集的个数, 即把置换 π 写成互不相交的轮换乘积时的轮换个数.

例 4.5: 考察 $x^{20}-1$ 在 $\mathbb{F}_3$ 上的分解. 这时 $n=20$, $q=3$, 对应的置换 π 写成互不相交的轮换乘积为 $\pi=(0)(1,3,9,7)(2,6,18,14)(4,12,16,8)(5,15)(10)(11,13,19,17)$. π 的轮换分解中有 7 个轮换, 所以 $x^{20}-1$ 在 $\mathbb{F}_3$ 上有 7 个互不相同的首一不可约因式. 由前面的讨论可得 $R(f)$ 的一组基 $h_0(x)=1$, $h_1(x)=x+x^3+x^7+x^9$, $h_2(x)=x^2+x^6+x^{14}+x^{18}$, $h_3(x)=x^4+x^8+x^{12}+x^{16}$, $h_4(x)=x^5+x^{15}$, $h_5(x)=x^{10}$ 和 $h_6(x)=x^{11}+x^{13}+x^{17}+x^{19}$. 自然我们可以通过 Berlekamp 算法来做分解, 但是由 4.1 节的讨论, 我们也可以先把多项式 x^n-1 分解为分圆多项式的乘积.

我们知道,

$$x^{20}-1=\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_5(x)\Phi_{10}(x)\Phi_{20}(x),$$

其中 $\Phi_1(x)=x-1$, $\Phi_2(x)=x+1$, $\Phi_4(x)=x^2+1$, $\Phi_5(x)=x^4+x^3+x^2+x+1$, $\Phi_{10}(x)=\frac{\Phi_2(x^5)}{\Phi_2(x)}=(x^5+1)/(x+1)=x^4-x^3+x^2-x+1$, $\Phi_{20}(x)=\Phi_{10}(x^2)=x^8-x^6+x^4-x^2+1$. 通过计算 3 模对应整数的乘法阶容易得到 $\Phi_1(x)$, $\Phi_2(x)$, $\Phi_4(x)$, $\Phi_5(x)$, $\Phi_{10}(x)$ 均在 $\mathbb{F}_3$ 上不可约, 而 $\Phi_{20}(x)$ 是 $\mathbb{F}_3$ 上两个 4 次不可约多项式的乘积, 所以我们只需分解 $\Phi_{20}(x)$ 即可.

由于 $\Phi_{20}(x)\mid x^{20}-1$ 且对每个 $0\le i\le 6$, 有 $h_i(x)^3\equiv h_i(x)\,(\mathrm{mod}\ x^{20}-1)$, 所以 $h_i(x)^3\equiv h_i(x)\,(\mathrm{mod}\ \Phi_{20}(x))$. 故我们通过 Berlekamp 算法来分解 $\Phi_{20}(x)$ 时, 也可以用之前得到的这些 $h_i(x)$. 比如取 $h_1(x)=x^9+x^7+x^3+x$, 虽然这时 $h_1(x)$ 的次数大于 $\Phi_{20}(x)$ 的次数, 但这并不影响我们的计算. 计算得到 $\gcd(\Phi_{20}(x),h_1(x))=1$, $\gcd(\Phi_{20}(x),h_1(x)+1)=x^4+x^3-x+1$, $\gcd(\Phi_{20}(x),h_1(x)+2)=x^4-x^3+x+1$. 这样我们得到 $\Phi_{20}(x)$ 在 $\mathbb{F}_3$ 上的分解为

$$\Phi_{20}(x)=(x^4+x^3-x+1)(x^4-x^3+x+1).$$

当然因为我们知道 $\Phi_{20}(x)$ 是 $\mathbb{F}_3$ 上两个 4 次不可约多项式的乘积, 当我们求出它的一个非平凡因子 x^4+x^3-x+1 后, 利用长除法就可以求出它的另一个因式 (这时不需要求最大公因式). 或者注意到 $\Phi_{20}(x)$ 在 $\mathbb{F}_3$ 上两个不可约因式是互反的 (为什么?), 从一个也可以求出另一个. 最后我们得到 $x^{20}-1$ 在 $\mathbb{F}_3$ 上的完全分解为

$$x^{20}-1=(x-1)(x+1)(x^2+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)(x^4+x^3-x+1)(x^4-x^3+x+1).$$

□

本节的最后再来看域 $\mathbb{F}_2$ 上的 6 次不可约多项式. 在 4.1 节我们知道 $\mathbb{F}_2$ 上的所有 6 次不可约多项式的乘积为 $I_{2,6}(x)=\Phi_9(x)\Phi_{21}(x)\Phi_{63}(x)$, 且 $\Phi_9(x)=x^6+x^3+1$ 在 $\mathbb{F}_2$ 上是不可约的, 而 $\Phi_{21}(x)$ 和 $\Phi_{63}(x)$ 在 $\mathbb{F}_2$ 上可约. 简单计算得到

$$\Phi_{21}(x)=\frac{\Phi_3(x^7)}{\Phi_3(x)}=x^{12}+x^{11}+x^9+x^8+x^6+x^4+x^3+x+1,$$

且 $\Phi_{21}(x)$ 为 $\mathbb{F}_2$ 上两个 6 次不可约多项式的乘积. 注意到 $\{3,6,12\}$ 为乘 2 下 $\mathbb{Z}_{21}$ 的一个分圆陪集, 我们取 $h(x)=x^3+x^6+x^{12}$. 计算得到 $\gcd(\Phi_{21}(x),h(x))=x^6+x^5+x^4+x^2+1$, 类似于例 4.5 中的说明, 可得 $\Phi_{21}(x)$ 的另一个不可约因式为 $x^6+x^4+x^2+x+1$, 所以

$$\Phi_{21}(x)=(x^6+x^5+x^4+x^2+1)(x^6+x^4+x^2+x+1).$$

下面再看 $\Phi_{63}(x)$, 由于 $\Phi_{63}(x)=\Phi_{21}(x^3)$, 由已得到的 $\Phi_{21}(x)$ 的分解有

$$\Phi_{63}(x)=(x^{18}+x^{15}+x^{12}+x^6+1)(x^{18}+x^{12}+x^6+x^3+1),$$

等式右端的每一个因式都是 3 个 $\mathbb{F}_2$ 上的 6 次不可约多项式的乘积, 它们的完全分解作为习题. 注意到通过完全分解 $\Phi_{63}(x)$, 我们可以得到 $\mathbb{F}_2$ 上的 6 个 6 次本原多项式.

4.3 多项式的阶

除了次数, 还有一个重要的整数附属于有限域上的多项式, 即多项式的阶. 本节中我们依然设 $F=\mathbb{F}_q$ 为 q 元域. 设 $f(x)\in F[x]$, $\deg f(x)=n\geq 1$ 且其常数项 $f(0)\neq 0$. 这样 x 与 $f(x)$ 互素, 从而 $\bar{x}$ 包含在剩余类环 $F[x]/(f(x))$ 的乘法群中. 定义多项式 $f(x)$ 的阶, 记为 $\mathrm{ord}(f(x))$ 或简写为 $\mathrm{ord}(f)$, 为 $\bar{x}$ 在剩余类环 $F[x]/(f(x))$ 的乘法群中的阶, 或者等价地说, $\mathrm{ord}(f)$ 是满足 $f(x)\mid x^e-1$ 的最小正整数 e. 多项式 $f(x)$ 的阶也称为 $f(x)$ 的周期 (以 $f(x)$ 为极小多项式的 F 上的线性递归序列的周期恰为 $\mathrm{ord}(f(x))$). 一个不可约多项式的阶可由下面另一种表达来刻画.

定理 4.7: 设 $f(x)$ 是域 $\mathbb{F}_q$ 上的 n 次不可约多项式且 $f(0)\neq 0$, 则 $\mathrm{ord}(f(x))$ 等于 $f(x)$ 的任一根在 $\mathbb{F}_{q^n}$ 的乘法群中的阶.

证明: 显然 $f(x)$ 的根在域 $\mathbb{F}_{q^n}$ 中, 由 $f(0)\neq 0$ 知 $f(x)$ 的根非零. 设 $\alpha\in\mathbb{F}_{q^n}^*$ 是 $f(x)$ 的一个根, 因为 $f(x)$ 不可约, 所以 $f(x)$ 的根为 α 的共轭元素, 即 $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$, 它们在群 $\mathbb{F}_{q^n}^*$ 中有相同的阶, 所以我们只看 α 的阶即可. 显然 $\alpha^e=1$ 当且仅当 α 是多项式 x^e-1 的根, 这也

当且仅当 α 的极小多项式 ($f(x)$ 的常数倍使其首一) 整除 x^e-1, 即当且仅当 $f(x)\mid x^e-1$. 由于 α 在群 $\mathbb{F}_{q^n}^*$ 中的阶 $\mathrm{ord}(\alpha)$ 是满足 $\alpha^e=1$ 的最小正整数 e, 而 $\mathrm{ord}(f(x))$ 是满足 $f(x)\mid x^e-1$ 的最小正整数 e, 由上面两者的等价性得到 $\mathrm{ord}(f(x))=\mathrm{ord}(\alpha)$. □

推论 4.8: 设 $f(x)$ 是域 $\mathbb{F}_q$ 上的 n 次不可约多项式且 $f(0)\neq 0$, 则 $\mathrm{ord}(f(x))\mid(q^n-1)$ 且 $\gcd(\mathrm{ord}(f(x)),p)=1$, 其中 $p=\mathrm{char}\mathbb{F}_q$.

证明: 因为群 $\mathbb{F}_{q^n}^*$ 的阶为 q^n-1, 所以 $f(x)$ 的根 α 的阶一定为 q^n-1 的因子. 由定理 4.7 立得 $\mathrm{ord}(f(x))\mid(q^n-1)$. 由于 q 为 p 的方幂, 所以 $\gcd(q^m-1,p)=1$, 再由 $\mathrm{ord}(f(x))\mid(q^n-1)$ 便立刻推出 $\gcd(\mathrm{ord}(f(x)),p)=1$. □

设 $f(x)$ 是域 $\mathbb{F}_q$ 上的不可约多项式且 $f(0)\neq 0$, 设 $\mathrm{ord}(f(x))=e$, 则 $f(x)$ 根的阶为 e, 而分圆多项式 $\Phi_e(x)$ 是以所有 e 阶元为根的多项式, 从而 $f(x)\mid\Phi_e(x)$. 反之设 $f(x)\in\mathbb{F}_q[x]$ 是 $\Phi_e(x)$ 的一个不可约因式, 因为 $\Phi_e(0)\neq 0$, 所以 $f(0)\neq 0$. 进一步地, 又 $f(x)$ 根的阶为 e, 故 $\mathrm{ord}(f(x))=e$. 由此我们证明了常数项非零的不可约多项式 $f(x)$ 的阶为 e 当且仅当 $f(x)\mid\Phi_e(x)$. 由定理 4.2 知 $\Phi_e(x)$ 在 $\mathbb{F}_q$ 上的不可约因式的次数为 $\mathrm{ord}_e(q)$, 即 q 模 e 的乘法阶, 而 $\Phi_e(x)$ 有 $\frac{\phi(e)}{\mathrm{ord}_e(q)}$ 个不同的首一不可约因式. 这样我们可得如下定理.

定理 4.9: 常数项非零且阶为 e 的 $\mathbb{F}_q$ 上的不可约多项式的次数为 $\mathrm{ord}_e(q)$, 进一步地, 常数项非零且阶为 e 的 $\mathbb{F}_q$ 上的 $n=\mathrm{ord}_e(q)$ 次首一不可约多项式的个数为 $\frac{\phi(e)}{n}$. □

下面来考察如何计算多项式的阶.

引理 4.10: 设 $f(x)\in F[x]$ 满足 $f(0)\neq 0$, 则 $f(x)\mid(x^\ell-1)$ 当且仅当 $\mathrm{ord}(f(x))\mid\ell$.

证明: 设 $e=\mathrm{ord}(f(x))\mid\ell$, 则 $f(x)\mid(x^e-1)$ 且 $(x^e-1)\mid(x^\ell-1)$, 从而 $f(x)\mid(x^\ell-1)$. 反之, 若 $f(x)\mid(x^\ell-1)$, 由 e 的最小性得到 $\ell\geq e$. 做带余除法 $\ell=se+r$, 其中 s 为正整数且 $0\leq r<e$. 由 $x^\ell-1=(x^{se}-1)x^r+(x^r-1)$ 可知 $f(x)\mid(x^r-1)$, 仍由正整数 e 的最小性得到 $r=0$, 故有 $e\mid\ell$. □

引理 4.11: 设 $f(x)\in F[x]$ 满足 $f(0)\neq 0$, 若 $f(x)$ 可分解为 $f(x)=f_1(x)f_2(x)$, 其中 $\deg(f_1),\deg(f_2)\geq 1$ 且 $\gcd(f_1(x),f_2(x))=1$, 则 $\mathrm{ord}(f(x))=\mathrm{lcm}(\mathrm{ord}(f_1(x)),\mathrm{ord}(f_2(x)))$, 即 $f(x)$ 的阶是 $f_1(x)$ 的阶和 $f_2(x)$ 的阶的最小公倍数.

证明: 记 $e_i=\mathrm{ord}(f_i(x))$, $i=1,2$, 和 $e=\mathrm{lcm}(e_1,e_2)$. 则有 $f_1(x)\mid(x^{e_1}-1)\mid(x^e-1)$ 且 $f_2(x)\mid(x^{e_2}-1)\mid(x^e-1)$, 再由 $\gcd(f_1(x),f_2(x))=1$ 得到 $f(x)\mid(x^e-1)$. 由引理 4.10 可得 $\mathrm{ord}(f(x))\mid e$.

另一方面, 由 $f(x)\mid(x^{\mathrm{ord}(f(x))}-1)$ 我们有 $f_1(x)\mid(x^{\mathrm{ord}(f(x))}-1)$ 和 $f_2(x)\mid(x^{\mathrm{ord}(f(x))}-1)$. 仍由引理 4.10 得 $e_1\mid\mathrm{ord}(f(x))$ 且 $e_2\mid\mathrm{ord}(f(x))$, 从而 e_1 和 e_2 的最小公倍数还是 $\mathrm{ord}(f(x))$ 的因子, 即 $e\mid\mathrm{ord}(f(x))$.

综合起来便有 $\mathrm{ord}(f(x))=e=\mathrm{lcm}(\mathrm{ord}(f_1(x)),\mathrm{ord}(f_2(x)))$. □

引理 4.12: 设 $p(x)\in F[x]$ 不可约且满足 $p(0)\neq 0$, $b\geq 1$. 再设 t 为满足 $p^t\geq b$ 的最小非负整数, 其中 $p=\mathrm{char}F$. 则 $\mathrm{ord}(p(x)^b)=\mathrm{ord}(p(x))p^t$.

证明: 由 $p(x) \mid (x^{\mathrm{ord}(p(x))}-1)$ 我们有

$$p(x)^b \mid (x^{\mathrm{ord}(p(x))}-1)^b \mid (x^{\mathrm{ord}(p(x))}-1)^{p^t} = x^{\mathrm{ord}(p(x))p^t}-1,$$

所以 $\mathrm{ord}(p(x)^b) \mid \mathrm{ord}(p(x))p^t$.

另一方面, 设 $\mathrm{ord}(p(x)^b) = p^i j$, 其中 $\gcd(j,p)=1$, 则有 $p(x)^b \mid (x^{p^i j}-1) = (x^j-1)^{p^i}$. 显然 $\gcd(x^j-1,(x^j-1)')=1$, 所以 x^j-1 没有重因式. 由于 $p(x)$ 不可约, 由多项式的唯一因式分解得到 $p(x) \mid (x^j-1)$ 且 $b \le p^i$. 从而有引理 4.10 有 $\mathrm{ord}(p(x)) \mid j$, 再由 t 的最小性得出 $i \ge t$. 所以 $\mathrm{ord}(p(x)^b) = p^i j \ge p^t \mathrm{ord}(p(x))$, 结论得证. □

利用如上引理我们可立得下面结论.

定理 4.13: 设 $f(x) \in F[x]$ 满足 $f(0) \neq 0$, 设 $f(x)$ 的标准分解式为

$$f(x) = p_1(x)^{b_1} p_2(x)^{b_2} \cdots p_r(x)^{b_r},$$

其中 $p_1(x), p_2(x), \ldots, p_r(x)$ 是域 F 上的 r 个互不相伴的不可约多项式, $b_1, b_2, \ldots, b_r$ 为 r 个正整数. 令 $p = \mathrm{char}F$, 并设 t 为对所有 i, $1 \le i \le r$, 都满足 $p^t \ge b_i$ 的最小非负整数. 则 $\mathrm{ord}(f(x)) = \mathrm{lcm}(\mathrm{ord}(p_1(x)), \mathrm{ord}(p_2(x)), \ldots, \mathrm{ord}(p_r(x)))p^t$.

证明: 利用引理 4.11, 对 r 作归纳可得

$$\mathrm{ord}(f(x)) = \mathrm{lcm}(\mathrm{ord}(p_1(x)^{b_1}), \mathrm{ord}(p_2(x)^{b_2}), \ldots, \mathrm{ord}(p_r(x)^{b_r})).$$

再由引理 4.12, 对每个 i, 我们有 $\mathrm{ord}(p_i(x)^{b_i}) = \mathrm{ord}(p_i(x))p^{t_i}$, 其中 t_i 是满足 $p^{t_i} \ge b_i$ 的最小非负整数. 进一步地, 由于 $\gcd(\mathrm{ord}(p_i(x)), p) = 1$, 我们有

$$\begin{aligned} \mathrm{ord}(f(x)) &= \mathrm{lcm}(\mathrm{ord}(p_1(x)), \mathrm{ord}(p_2(x)), \ldots, \mathrm{ord}(p_r(x)))\mathrm{lcm}(p^{t_1}, p^{t_2}, \ldots, p^{t_r}) \\ &= \mathrm{lcm}(\mathrm{ord}(p_1(x)), \mathrm{ord}(p_2(x)), \ldots, \mathrm{ord}(p_r(x)))p^t. \end{aligned}$$

□

例 4.6: 计算 $f(x) = x^{10}+x^9+x^3+x^2+1 \in \mathbb{F}_2[x]$ 的阶. 多项式 $f(x)$ 在 $\mathbb{F}_2$ 上的分解为 $f(x) = (x^2+x+1)^3(x^4+x+1)$. 容易计算出 $\mathrm{ord}(x^2+x+1)=3$, $\mathrm{ord}(x^4+x+1)=15$, 又满足 $2^t \ge 3$ 的最小非负整数为 $t=2$. 所以 $\mathrm{ord}(f(x)) = \mathrm{lcm}(3,15)\cdot 2^2 = 60$. 注意到这时 $\mathrm{ord}(f(x))$ 不整除 $2^{10}-1$, 这表明推论 4.8 对可约多项式不再成立.

现在我们考虑如何计算不可约多项式的阶. 设 $f(x) \in \mathbb{F}_q$ 满足 $f(0) \neq 0$ 且设 $\deg f(x) = n$, 推论 4.8 告诉我们 $\mathrm{ord}(f(x)) \mid (q^n-1)$. 设 $q^n-1 = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ 是正整数 q^n-1 的标准分解, 其中 $p_1, p_2, \ldots, p_r$ 互不相同的素数, $e_1, e_2, \ldots, e_r$ 为正整数, 故此 $\mathrm{ord}(f(x)) = p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$, 其中 ℓ_i 为非负整数且 $\ell_i \le e_i$, $1 \le i \le r$. 对每个 i, $1 \le i \le r$, 因为 $x^{q^n-1} \equiv 1 \pmod{f(x)}$, 则存在非负整数 f_i 满足 $f_i \le e_i$ 且 $x^{(q^n-1)/p_i^{f_i}} \equiv 1 \pmod{f(x)}$ 和 $x^{(q^n-1)/p_i^{f_i+1}} \not\equiv 1 \pmod{f(x)}$. 注意这里虽然 $(q^n-1)/p_i^{e_i+1}$ 不是整数但是我们认为 $x^{(q^n-1)/p_i^{e_i+1}} \not\equiv 1 \pmod{f(x)}$, 即若 $x^{(q^n-1)/p_i^{e_i}} \equiv 1 \pmod{f(x)}$, 则取 $f_i = e_i$. 这样我们有 $\mathrm{ord}(f(x)) \mid (q^n-1)/p_i^{f_i}$ 但是 $\mathrm{ord}(f(x)) \nmid (q^n-1)/p_i^{f_i+1}$, 所以 $\ell_i = e_i - f_i$, 即 $\mathrm{ord}(f(x)) = p_1^{e_1-f_1}p_2^{e_2-f_2}\cdots p_r^{e_r-f_r}$. 这样我们可以按如下步骤来求不可约多项式 $f(x)$ 的阶.

(1) 给出 q^n-1 的标准分解. 设 $q^n-1=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, 其中 $p_1,p_2,\ldots,p_r$ 是互不相同的素数, $e_1,e_2,\ldots,e_r$ 是正整数.

(2) 对每个 $i=1,2,\ldots,r$, 计算 $x^{(q^n-1)/p_i} \pmod{f(x)}$, $x^{(q^n-1)/p_i^2} \pmod{f(x)}$, $\ldots$, 直到找到非负整数 f_i 满足 $f_i\le e_i$ 且 $x^{(q^n-1)/p_i^{f_i}}\equiv 1 \pmod{f(x)}$ 但是 $x^{(q^n-1)/p_i^{f_i+1}}\not\equiv 1 \pmod{f(x)}$, 这里 $g(x) \pmod{f(x)}$ 表示那个唯一的次数 $<\deg(f(x))$ 且模 $f(x)$ 下同余于 $g(x)$ 的多项式. 则可计算出

$$\operatorname{ord}(f(x))=p_1^{e_1-f_1}p_2^{e_2-f_2}\cdots p_r^{e_r-f_r}.$$

为了计算 $x^{(q^n-1)/p_i^s} \pmod{f(x)}$ 对每个 $s=1,2,\ldots$ 和 $i=1,2,\ldots,r$, 我们可如下进行.

2.1) 如同计算 Berlekamp 算法中的 (4.10) 式, 计算 $x^0 \pmod{f(x)}$, $x^q \pmod{f(x)}$, $x^{2q} \pmod{f(x)}$, $\ldots$, $x^{(n-1)q} \pmod{f(x)}$. 设

$$x^{jq}\equiv\sum_{i=0}^{n-1}b_{ij}x^i \pmod{f(x)},$$

$j=0,1,\ldots,n-1$. 记 $B=(b_{ij})_{0\le i,j\le n-1}$, 这是 $\mathbb{F}_q$ 上的一个 n 阶矩阵.

2.2) 计算 $x \pmod{f(x)}$, $x^q \pmod{f(x)}$, $x^{q^2} \pmod{f(x)}$, $\ldots$, $x^{q^{n-1}} \pmod{f(x)}$. 注意到若 $q^i\le(n-1)q$, $x^{q^i} \pmod{f(x)}$ 在 2.1) 步已经计算出. 进一步地, 若 $x^{q^i} \pmod{f(x)}$ 已被算出, 不妨设

$$x^{q^i}\equiv\sum_{j=0}^{n-1}b_jx^j \pmod{f(x)},$$

则

$$x^{q^{i+1}}\equiv\left(\sum_{j=0}^{n-1}b_jx^j\right)^q=\sum_{j=0}^{n-1}b_jx^{jq}\equiv\sum_{k=0}^{n-1}\sum_{j=0}^{n-1}b_{kj}b_jx^k \pmod{f(x)}.$$

所以, 若记

$$x^{q^{i+1}}\equiv\sum_{k=0}^{n-1}b'_kx^k \pmod{f(x)},$$

则

$$\begin{pmatrix}b'_0\\b'_1\\\vdots\\b'_{n-1}\end{pmatrix}=B\begin{pmatrix}b_0\\b_1\\\vdots\\b_{n-1}\end{pmatrix}.$$

2.3) 表正整数 $(q^n-1)/p_i^s$ 为 q-进制数, 设

$$(q^n-1)/p_i^s=a_0+a_1q+a_2q^2+\cdots+a_{n-1}q^{n-1},$$

其中 $0\le a_i\le q-1$. 则有

$$x^{(q^n-1)/p_i^s}\equiv x^{a_0}(x^q)^{a_1}(x^{q^2})^{a_2}\cdots(x^{q^{n-1}})^{a_{n-1}} \pmod{f(x)}.$$

注意到在如上算法中, 除第一步正整数 q^n-1 的标准分解外, 其它的计算都不复杂, 但是整数的分解确是一个非常困难的问题.

例 4.7: 确定多项式 $f(x)=x^9+x+1\in\mathbb{F}_2[x]$ 的阶. 容易验证 $f(x)$ 在 $\mathbb{F}_2$ 上不可约 (比如用 Berlekamp 算法), 这时 $2^9-1=511=7\cdot 73$. 我们计算出 2.1) 步的矩阵 B 为

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

(容易计算出 $\mathrm{rank}(B-I)=8$, 故 $f(x)$ 的不可约因式只有 1 个, 再由 $f(x)$ 与 $f'(x)$ 互素得到 $f(x)$ 在 $\mathbb{F}_2$ 上不可约). 利用此矩阵 B, 我们可计算出 $x^{q^j}\pmod{f(x)}$, $0\le j\le 8$,

$$\begin{aligned}
x^{2^0} &\equiv x,\\
x^{2^1} &\equiv x^2,\\
x^{2^2} &\equiv x^4,\\
x^{2^3} &\equiv x^8,\\
x^{2^4} &\equiv x^7+x^8,\\
x^{2^5} &\equiv x^5+x^6+x^7+x^8,\\
x^{2^6} &\equiv x+x^2+x^3+x^4+x^5+x^6+x^7+x^8,\\
x^{2^7} &\equiv x+x^3+x^5+x^7,\\
x^{2^8} &\equiv x+x^5.
\end{aligned}$$

对于 $p_1=7$, 我们有

$$\frac{511}{7}=73=2^0+2^3+2^6,$$

所以

$$x^{73}=x\cdot x^{2^3}\cdot x^{2^6}\equiv x\cdot x^8\cdot(x+x^2+x^3+x^4+x^5+x^6+x^7+x^8)\equiv 1\,(\mathrm{mod}\ f(x)),$$

即 $f_1=1$. 又显然 $x^{511/73}=x^7\not\equiv 1\,(\mathrm{mod}\ f(x))$, 故 $f_2=0$. 所以我们最后得出 $\mathrm{ord}(f(x))=7^0\cdot 73=73$.

设多项式 $f(x)\in\mathbb{F}_q[x]$ 满足 $f(0)\neq 0$, 则一定存在正整数 r 满足

$$x^r\equiv a\,(\mathrm{mod}\ f(x)),\tag{4.11}$$

其中 $a\in\mathbb{F}_q^*$ (显然 $\mathrm{ord}(f(x))$ 就是其中之一). 设 r 为满足式 (4.11) 的最小正整数, 则显然

$r \le \mathrm{ord}(f(x))$, 而这时的 $a \in \mathbb{F}_q^*$ 也是唯一的.

定理 4.14: 设多项式 $f(x) \in \mathbb{F}_q[x]$ 满足 $f(0) \neq 0$, 设 r 为满足式 (4.11) 的最小正整数, 则 $\mathrm{ord}(f(x)) = \mathrm{ord}(a)r$, 其中 $\mathrm{ord}(a)$ 是 a 在群 $\mathbb{F}_q^*$ 中的阶.

证明: 记 $e = \mathrm{ord}(f(x))$, 因为 $x^e \equiv 1 \,(\mathrm{mod}\ f(x))$, 所以 $e \ge r$. 由带余除法, 设 $e = sr + t$, 其中 $s \in \mathbb{N}$ 且 $0 \le t < r$. 由于

$$1 \equiv x^e = (x^r)^s x^t \equiv a^s x^t \,(\mathrm{mod}\ f(x)), \tag{4.12}$$

所以 $x^t \equiv a^{-s} \,(\mathrm{mod}\ f(x))$. 由 r 的最小性得到 $t = 0$, 故 (4.12) 变成 $a^s \equiv 1 \,(\mathrm{mod}\ f(x))$, 从而 $a^s = 1$. 所以 $s \ge \mathrm{ord}(a)$, 这便得出 $e \ge \mathrm{ord}(a)r$. 另一方面, 由 $x^{\mathrm{ord}(a)r} \equiv a^{\mathrm{ord}(a)} = 1 \,(\mathrm{mod}\ f(x))$ 就得出 $e = \mathrm{ord}(a)r$. □

显然 $\mathbb{F}_q$ 上 n 次多项式的阶至多为 $q^n - 1$, 下面我们来刻画 $\mathbb{F}_q$ 上阶恰为 $q^n - 1$ 的 n 次多项式. 我们知道本原多项式是本原元素的极小多项式, 即 $\mathbb{F}_q$ 上的 n 次本原多项式是以 $\mathbb{F}_{q^n}$ 的本原元素为根的首一不可约多项式.

定理 4.15: 多项式 $f(x)$ 是 $\mathbb{F}_q$ 上的 n 次本原多项式当且仅当 $f(x)$ 首一, $f(0) \neq 0$ 且 $\mathrm{ord}(f(x)) = q^n - 1$.

证明: 设 $f(x)$ 在 $\mathbb{F}_q$ 上本原, 则显然 $f(x)$ 首一且它的根非零, 故 $f(0) \neq 0$. 又因为 $f(x)$ 在 $\mathbb{F}_q$ 不可约, 它的根为域 $\mathbb{F}_{q^n}$ 的本原元素, 即在群 $\mathbb{F}_{q^n}^*$ 中的阶为 $q^n - 1$. 由定理 4.7 立得 $\mathrm{ord}(f(x)) = q^n - 1$.

反之, 设 $\mathbb{F}_q$ 上的 n 次首一多项式 $f(x)$ 满足 $f(0) \neq 0$ 且 $\mathrm{ord}(f(x)) = q^n - 1$. 这时因为剩余类环 $R = \mathbb{F}_q[x]/(f(x))$ 中的非零元有 $q^n - 1$ 个元素, 故 R 的乘法群就是由 R 的全部非零元组成的乘法群, 所以 $\mathbb{F}_q$ 上所有次数小于 n 的非零多项式都与 $f(x)$ 互素, 故 $f(x)$ 在 $\mathbb{F}_q$ 上不可约. 由定理 4.7 知 $f(x)$ 的根的阶为 $q^n - 1$, 自然为 $\mathbb{F}_{q^n}$ 的本原元素, 所以 $f(x)$ 为 $\mathbb{F}_q$ 上的本原多项式. □

例如, 多项式 $f(x) = x^4+x^3+x^2+x+1$ 在 $\mathbb{F}_2$ 上不可约, 容易计算出 $\mathrm{ord}(f(x)) = 5 \neq 2^4-1$, 所以 $f(x)$ 不是 $\mathbb{F}_2$ 上的本原多项式. 由定理 4.9 和定理 4.15 也可以又一次得到 $\mathbb{F}_q$ 上 n 次本原多项式的个数为 $\frac{1}{n}\phi(q^n - 1)$. 上述定理还可以得到下面的推论.

推论 4.16: 设首一多项式 $f(x) \in \mathbb{F}_q[x]$, $\deg f(x) = n$, 且 $f(0) \neq 0$, 再设 $p_1, p_2, \ldots, p_r$ 是正整数 $q^n - 1$ 的所有互不相同的素因子, 则 $f(x)$ 本原当且仅当对每个 $i = 1, 2, \ldots, r$, 均有 $x^{(q^n-1)/p_i} \not\equiv 1 \,(\mathrm{mod}\ f(x))$. □

定理 4.17: 设多项式 $f(x) \in \mathbb{F}_q[x]$ 首一且 $\deg f(x) = n$, 则 $f(x)$ 是 $\mathbb{F}_q$ 上的本原多项式当且仅当 $(-1)^n f(0)$ 是域 $\mathbb{F}_q$ 的本原元素且满足式 (4.11) 的最小正整数 $r = \frac{q^n-1}{q-1}$.

证明: 设 $f(x)$ 本原, α 是 $f(x)$ 的一个根, 则 α 是 $\mathbb{F}_{q^n}$ 的本原元素. 注意到 $f(x)$ 的全部根为 $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$, 即 $f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$, 所以

$$(-1)^n f(0) = \alpha\alpha^q \cdots \alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}} (= \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)). \tag{4.13}$$

由于 $\mathrm{ord}(\alpha)=q^n-1$, 所以 $\mathrm{ord}((-1)^nf(0))=q-1$, 故 $(-1)^nf(0)$ 是域 $\mathbb{F}_q$ 的本原元素. 进一步地, 由于 α 是多项式 $x^{\frac{q^n-1}{q-1}}-(-1)^nf(0)\in\mathbb{F}_q[x]$ 的根, 而 $f(x)$ 是 α 在 $\mathbb{F}_q$ 上的极小多项式, 所以 $x^{\frac{q^n-1}{q-1}}\equiv(-1)^nf(0)\pmod{f(x)}$, 故 $r\le\frac{q^n-1}{q-1}$. 由于 $\mathbb{F}_q^*$ 中元素的阶最大为 $q-1$, 由定理 4.14 得到 $\mathrm{ord}(f(x))\le(q-1)r$. 又 $f(x)$ 本原, 故 $\mathrm{ord}(f(x))=q^n-1$, 从而 $r\ge\frac{q^n-1}{q-1}$. 所以满足式 (4.11) 的最小正整数 $r=\frac{q^n-1}{q-1}$.

反之, 设 $(-1)^nf(0)$ 是域 $\mathbb{F}_q$ 的本原元素且满足式 (4.11) 的最小正整数 $r=\frac{q^n-1}{q-1}$. 由定理 4.14 知 $\mathrm{ord}(f(x))=r\mathrm{ord}(a)$, 其中 $a\in\mathbb{F}_q^*$ 满足式 (4.11). 由于 r 和 $\mathrm{ord}(a)$ 都与 q 互素, 故可推出 $\mathrm{ord}(f(x))$ 与 q 互素, 这样根据定理 4.13 知道 $f(x)$ 无重因式. 设 $f(x)$ 的标准分解为 $f(x)=p_1(x)\cdots p_k(x)$, 其中 $p_1(x),\ldots,p_k(x)$ 是 $\mathbb{F}_q$ 上互不相同的首一不可约多项式且 $\deg p_i(x)=n_i$, $1\le i\le k$. 由推论 4.8 有 $\mathrm{ord}(p_i(x))\mid(q^{n_i}-1)$. 若 $k\ge2$, 记

$$d=\frac{1}{(q-1)^{k-1}}\prod_{i=1}^{k}(q^{n_i}-1).$$

则显然对每个 i, $1\le i\le k$, 有 $(q^{n_i}-1)\mid d$, 所以 $\mathrm{ord}(p_i(x))\mid d$. 由于 $\mathrm{ord}(f(x))=\mathrm{lcm}(\mathrm{ord}(p_1(x)),\ldots,\mathrm{ord}(p_k(x)))$, 故 $\mathrm{ord}(f(x))\mid d$, 故 $x^d\equiv1\pmod{f(x)}$. 注意到

$$d<\frac{1}{q-1}(q^{n_1+\cdots+n_k}-1)=\frac{q^n-1}{q-1}=r,$$

与 r 的选取矛盾, 故 $k=1$, 推出 $f(x)$ 是 $\mathbb{F}_q$ 上的首一不可约多项式. 设 $\beta\in\mathbb{F}_{q^n}$ 是 $f(x)$ 的一个根, 则类似于 (4.13) 有 $\beta^r=(-1)^nf(0)$. 由于 $f(x)$ 是 β 在 $\mathbb{F}_q$ 上的极小多项式, 所以 $x^r\equiv(-1)^nf(0)\pmod{f(x)}$. 又 $(-1)^nf(0)$ 在 $\mathbb{F}_q^*$ 中的阶为 $q-1$, 利用定理 4.14 得到 $\mathrm{ord}(f(x))=(q-1)r=q^n-1$. 故 $f(x)$ 是 $\mathbb{F}_q$ 上的本原多项式. □

我们定义常数项为 0 的多项式的阶如下, 设 $f(x)\in F[x]$ 满足 $f(0)=0$, 则存在整数 $k\ge1$ 使得 $f(x)=x^kg(x)$, 其中 $g(x)\in F[x]$ 且 $g(0)\ne0$. 定义 $f(x)$ 的阶为 $\mathrm{ord}(f(x)):=\mathrm{ord}(g(x))$, 而非零常数多项式的阶定义为 1. 注意到常数项为 0 的首一不可约多项式只有 x, 它的阶为 1. 如果不考虑常数项是否为 0, 定理 4.9 关于给定阶数的首一不可约多项式的个数的结果需要略微修改一下.

4.4 线性化多项式

本节我们讨论一类在理论和应用上都非常重要的多项式, 如之前一样, 本节中 q 是一个素数幂. 形如

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

的多项式称为域 $\mathbb{F}_{q^m}$ 上的 q-多项式, 其中 $\alpha_i\in\mathbb{F}_{q^m}$, $0\le i\le n$. 设 F 是 $\mathbb{F}_{q^m}$ 的一个扩域, 容易验证对任意 $\beta,\gamma\in F$ 和 $c\in\mathbb{F}_q$, 有 $L(\beta+\gamma)=L(\beta)+L(\gamma)$ 和 $L(c\beta)=cL(\beta)$. 从而若把 F 看成是域 $\mathbb{F}_q$ 上的线性空间, 则 q-多项式 $L(x)$ 就诱导出 F 上的一个线性变换 $L:\beta\mapsto L(\beta)$, 对

所有 $\beta \in F$. 这样若 q 是一个固定的素数幂或者在上下文中清楚是哪一个 q, 我们也称多项式 $L(x)$ 为线性化多项式.

设 q-多项式 $L(x)$ 的全部根都在 $\mathbb{F}_{q^m}$ 的扩域 F 中, F 是 $\mathbb{F}_q$ 上的线性空间. 因为 L 是 F 上的 $\mathbb{F}_q$-线性变换, 而 $L(x)$ 的所有根的集合就是 L 的核, 所以多项式 $L(x)$ 的所有根构成的集合 $U = \{\alpha \in F \mid L(\alpha) = 0\}$ 是 F 的子空间, 即 U 也是 $\mathbb{F}_q$ 上的线性空间. 进一步地, 设 $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$, 则有 $L'(x) = \alpha_0$. 若 $\alpha_0 \neq 0$, 则 $\gcd(L(x), L'(x)) = 1$, 这时 $L(x)$ 无重根. 若 $\alpha_0 = 0$, 不妨设 $\alpha_0 = \cdots = \alpha_{k-1} = 0$, 而 $\alpha_k \neq 0$, 则

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

令 $L_1(x) = \sum_{i=k}^{n} \alpha_i^{q^{(m-1)k}} x^{q^{i-k}} = \sum_{j=0}^{n-k} \alpha_{j+k}^{q^{(m-1)k}} x^{q^j}$, 则 $L_1(x)$ 依然是 $\mathbb{F}_{q^m}$ 上的 q-多项式, 其 x 的系数非零. 所以 $L_1(x)$ 的根集为 $\mathbb{F}_q$ 上的一个线性空间, 且 $L_1(x)$ 的根都是单根. 这时, $L(x) = L_1(x)^{q^k}$, 从而 $L(x)$ 的每个根的重数都是 q^k 且 $L(x)$ 的根集就是 $L_1(x)$ 的根集. 这便证明了如下定理.

定理 4.18: 设 $L(x) \in \mathbb{F}_{q^m}[x]$ 是非零 q-多项式, 则 $L(x)$ 的所有根组成 $\mathbb{F}_q$ 上的一个线性空间, 且 $L(x)$ 的每个根 (在 $\mathbb{F}_{q^m}$ 的扩域中) 都有相同的重数, 该重数或为 1 或为 q 的方幂. □

反之, 如果一个多项式的根组成一个 $\mathbb{F}_q$ 上的线性空间, 那么这个多项式形式如何? 首先我们给出如下引理.

引理 4.19: 设 $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{F}_{q^m}$, 则

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

证明: 对 n 做归纳, $n = 1$ 时结论显然成立. 假设结论对 n 成立, 下面考虑 $n+1$ 的情形. 构造

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

把 $D(x)$ 按第 $n+1$ 列展开得到

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

其中 $\alpha_i \in \mathbb{F}_{q^m}$. 若 $\beta_1, \beta_2, \ldots, \beta_n$ 在 $\mathbb{F}_q$ 上线性无关, 显然它们都是 $D(x)$ 的根, 又 $D(x)$ 为 $\mathbb{F}_{q^m}$ 上的 q-多项式, 所以对于任意的 $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$, $c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n$ 也是 $D(x)$ 的根.

这样我们就得到了 $D(x)$ 的 q^n 个根, 而 $\deg D(x) \leq q^n$, 所以这时 $D_n \neq 0$ (这也是推论 3.9), 且

$$D(x) = D_n \prod_{c_1,c_2,\ldots,c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k \beta_k \right). \tag{4.14}$$

若 $\beta_1, \beta_2, \ldots, \beta_n$ 在 $\mathbb{F}_q$ 上线性相关, 则存在不全为 0 的 $b_1, b_2, \ldots, b_n \in \mathbb{F}_q$ 使得 $b_1\beta_1 + b_2\beta_2 + \cdots + b_n\beta_n = 0$. 从而对任意的 $0 \leq j \leq n$ 有

$$\sum_{i=1}^{n} b_i \beta_i^{q^j} = \left(\sum_{i=1}^{n} b_i \beta_i \right)^{q^j} = 0.$$

所以 D_n 的 n 列以及 $D(x)$ 的前 n 列都在 $\mathbb{F}_q$ 上线性相关, 故 $D_n = 0$ 且 $D(x) = 0$. 这表明此时式 (4.14) 依然成立, 即 (4.14) 在任何情形下都成立. 在 (4.14) 中令 $x = \beta_{n+1}$, 则有

$$D_{n+1} = D(\beta_{n+1}) = D_n \prod_{c_1,c_2,\ldots,c_n \in \mathbb{F}_q} \left(\beta_{n+1} - \sum_{k=1}^{n} c_k \beta_k \right).$$

故结论对 $n+1$ 成立, 由归纳法原理, 结论得证. □

引理 4.19 中出现的行列式 D_n 称为 Moore 行列式, 可作为著名的 Vandermonde 行列式在有限域上的推广. 设 U 是 $\mathbb{F}_q$ 上的一个线性空间, $\beta_1, \beta_2, \ldots, \beta_n$ 是 U 在 $\mathbb{F}_q$ 上的一组基, 则由 (4.14) 有

$$\prod_{\beta \in U} (x - \beta) = \prod_{c_1,c_2,\ldots,c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k \beta_k \right) = D_n^{-1} D(x).$$

如果一个多项式的根集 U 构成 $\mathbb{F}_q$ 上的 n 维线性空间且每个根都是单根, 上式表明此多项式是 q-多项式, 而若此多项式每个根的重数都是 q^k, 则此多项式为

$$\prod_{\beta \in U} (x - \beta)^{q^k} = \prod_{c_1,c_2,\ldots,c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k \beta_k \right)^{q^k} = \left(D_n^{-1} D(x) \right)^{q^k},$$

仍是 q-多项式. 注意到若 $U \subseteq \mathbb{F}_{q^m}$, 则得到的 q-多项式是域 $\mathbb{F}_{q^m}$ 上多项式. 我们有下面定理.

定理 4.20: 设 U 是 $\mathbb{F}_{q^m}$ 的一个 $\mathbb{F}_q$-子空间. 多项式 $L(x) \in \mathbb{F}_{q^m}[x]$ (在 $\mathbb{F}_{q^m}$ 的充分大的扩域中) 的根集为 U, 每个根的重数都相同且此重数或为 1 或为 q 的方幂, 则 $L(x)$ 是 $\mathbb{F}_{q^m}$ 上的 q- 多项式. □

用 $\mathcal{L}_{q^m}[x]$ 表示 $\mathbb{F}_{q^m}$ 上的所有线性化多项式构成的集合, 显然线性化多项式的乘积不一定还是线性化多项式, 所以普通的多项式乘法并不是 $\mathcal{L}_{q^m}[x]$ 上的运算. 注意到线性空间上两个线性变换的合成仍为线性变换, 我们定义 $\mathcal{L}_{q^m}[x]$ 中两个元素的符号乘法为它们的合成, 即设 $L_1(x), L_2(x) \in \mathcal{L}_{q^m}[x]$, 定义 $L_1(x) \otimes L_2(x) = L_1(L_2(x))$, 称为 $L_1(x)$ 与 $L_2(x)$ 的符号乘积, 符号乘法的符号记为 "$\otimes$". 设 $L_1(x) = \sum_{i=0}^{s} \alpha_i x^{q^i}$, $L_2(x) = \sum_{j=0}^{t} \beta_j x^{q^j}$, 则

$$L_1(x) \otimes L_2(x) = \sum_{i=0}^{s} \alpha_i \left(\sum_{j=0}^{t} \beta_j x^{q^j} \right)^{q^i} = \sum_{i=0}^{s} \sum_{j=0}^{t} \alpha_i \beta_j^{q^i} x^{q^{i+j}} = \sum_{k=0}^{s+t} \left(\sum_{i=0}^{s} \alpha_i \beta_{k-i}^{q^i} \right) x^{q^k},$$

其中当 $k<i$ 时, $\beta_{k-i}=0$, 而

$$L_2(x)\otimes L_1(x)=\sum_{k=0}^{s+t}\left(\sum_{j=0}^{t}\alpha_{k-j}^{q^j}\beta_j\right)x^{q^k},$$

其中当 $k<j$ 时, $\alpha_{k-j}=0$, 所以通常说来符号乘法是不交换的. 容易验证, $\mathcal{L}_{q^m}[x]$ 在多项式的通常加法和如上定义的符号乘法下构成一个环, 单位元为多项式 x.

设 F 是 $\mathbb{F}_{q^m}$ 的有限次扩域, $\beta\in F$, 则存在 $\mathbb{F}_{q^m}$ 上的非零 q-多项式 $L(x)$ 使得 β 为 $L(x)$ 的根. 事实上, 设 $g(x)$ 为 β 在 $\mathbb{F}_{q^m}$ 上的极小多项式且 $\deg g(x)=n$. 对每个 i, $0\leqslant i\leqslant n$, 求出唯一的 $r_i(x)\in\mathbb{F}_{q^m}[x]$ 使得 $x^{q^i}\equiv r_i(x)\pmod{g(x)}$ 且 $\deg r_i(x)<n$. 再找出不全为零的 $\alpha_0,\alpha_1,\cdots,\alpha_n\in\mathbb{F}_{q^m}$ 使得 $\sum_{i=0}^{n}\alpha_i r_i(x)=0$ (这样的 $\alpha_0,\alpha_1,\cdots,\alpha_n\in\mathbb{F}_{q^m}$ 一定存在). 令 $L(x)=\sum_{i=0}^{n}\alpha_i x^{q^i}$, 则由 $g(x)\mid L(x)$ 知 $L(x)$ 是 $\mathbb{F}_{q^m}$ 上的非零 q-多项式且以 β 为根.

定理 4.21: 设 F 是 $\mathbb{F}_{q^m}$ 的有限次扩域, $\beta\in F$, 设 $M(x)\in\mathcal{L}_{q^m}[x]$ 是以 β 为根的次数最低的首一 q-多项式 (当然非零). 则 $K(x)\in\mathcal{L}_{q^m}[x]$ 以 β 为根当且仅当存在 $L(x)\in\mathcal{L}_{q^m}[x]$ 使得 $K(x)=L(x)\otimes M(x)$.

证明: 充分性显然, 下证必要性. 设 $M(x)=\sum_{j=0}^{t}\gamma_j x^{q^j}$, 其中 $\gamma_t=1$. 设 $K(x)=\sum_{k=0}^{r}\alpha_k x^{q^k}$, 则有 $r\geqslant t$. 令 $s=r-t$, 并设在 $j<0$ 时定义 $\gamma_j=0$. 考察如下以 $\beta_0,\beta_1,\ldots,\beta_s$ 为未知量的线性方程组

$$\begin{cases}
\beta_0+\beta_1\gamma_{t-1}^{q}+\beta_2\gamma_{t-2}^{q^2}+\cdots+\beta_{s-1}\gamma_{t-s+1}^{q^{s-1}}+\beta_s\gamma_{t-s}^{q^s}=\alpha_t,\\
\beta_1+\beta_2\gamma_{t-1}^{q^2}+\cdots+\beta_{s-1}\gamma_{t-s+2}^{q^{s-1}}+\beta_s\gamma_{t-s+1}^{q^s}=\alpha_{t+1},\\
\vdots\\
\beta_{s-1}+\beta_s\gamma_{t-1}^{q^s}=\alpha_{r-1},\\
\beta_s=\alpha_r,
\end{cases}\tag{4.15}$$

此方程组有 $s+1$ 个未知量, $s+1$ 个方程, 其系数矩阵是主对角线上元素均为 1 的上三角矩阵, 故 (4.15) 有唯一解 $(\beta_0,\beta_1,\cdots,\beta_s)$. 令 $L(x)=\sum_{i=0}^{s}\beta_i x^{q^i}$, 则

$$L(x)\otimes M(x)=\sum_{k=0}^{r}\left(\sum_{i=0}^{s}\beta_i\gamma_{k-i}^{q^i}\right)x^{q^k}.$$

由 (4.15) 知 q-多项式 $L(x)\otimes M(x)$ 和 $K(x)$ 在 x^{q^k} 时的系数相等, 其中 $t\leqslant k\leqslant r$. 令 $R(x)=K(x)-L(x)\otimes M(x)$, 则 $R(x)\in\mathcal{L}_{q^m}[x]$ 且以 β 为根. 由于 $\deg R(x)<q^t$ 以及 $M(x)$ 次数的极小性, 所以 $R(x)=0$, 故 $K(x)=L(x)\otimes M(x)$. □

由定理 4.21 容易推出以 β 为根的 $\mathbb{F}_{q^m}$ 上首一且次数最低的非零 q-多项式一定唯一, 而它的存在性是显然的. 称这样的多项式为 β 在 $\mathbb{F}_{q^m}$ 上的极小 q-多项式. 设 $L(x)\in\mathcal{L}_{q^m}[x]$ 非零, 若 β 是 $L(x)$ 的根但不是 $\mathcal{L}_{q^m}[x]$ 中次数更低的非零 q-多项式的根, 则称 β 为 $L(x)$ 在 $\mathbb{F}_{q^m}$ 上的 q-本原根. 设 β 在 $\mathbb{F}_{q^m}$ 上的极小多项式为 $g(x)$, 则 β 为 $L(x)$ 在 $\mathbb{F}_{q^m}$ 上的 q-本原根当且仅当 $g(x)\mid L(x)$ 但是 $g(x)\nmid K(x)$ 对任意满足 $K(x)\neq 0$ 且 $\deg K(x)<\deg L(x)$ 的 $K(x)\in\mathcal{L}_{q^m}[x]$. 显然若 $M(x)$ 是 β 在 $\mathbb{F}_{q^m}$ 上的极小 q-多项式, 则 β 是 $M(x)$ 在 $\mathbb{F}_{q^m}$ 上的 q-本原根.

下面考察 $\mathbb{F}_q$ 上的 q-多项式. 设 $L_1(x)=\sum_{i=0}^{s}a_ix^{q^i}$, $L_2(x)=\sum_{j=0}^{t}b_jx^{q^j}$, 其中 $a_i,b_j\in\mathbb{F}_q$, $0\le i\le s$, $0\le j\le t$. 则有

$$L_1(x)\otimes L_2(x)=\sum_{i=0}^{s}a_i\left(\sum_{j=0}^{t}b_jx^{q^j}\right)^{q^i}=\sum_{i=0}^{s}\sum_{j=0}^{t}a_ib_jx^{q^{i+j}}=\sum_{k=0}^{s+t}\left(\sum_{i=0}^{s}a_ib_{k-i}\right)x^{q^k},\qquad(4.16)$$

其中当 $k<i$ 时, $b_{k-i}=0$. 类似地可以求出 $L_2(x)\otimes L_1(x)$, 由此可得到 $L_1(x)\otimes L_2(x)=L_2(x)\otimes L_1(x)$, 即这时的符号乘法可交换, 还容易得到 $(\mathcal{L}_q[x],+,\otimes)$ 是一个整环. 由式 (4.16) 我们可得如下定理.

定理 4.22: 映射

$$\begin{array}{rccc}\psi: & \mathbb{F}_q[x] & \to & \mathcal{L}_q[x]\\ & \sum_{i=0}^{n}a_ix^i & \mapsto & \sum_{i=0}^{n}a_ix^{q^i}\end{array}$$

是一个环同构. □

在如上环同构 ψ 下对应的 $\mathbb{F}_q[x]$ 与 $\mathcal{L}_q[x]$ 中的元素称为是互为 q-相伴的, 即多项式 $l(x)=\sum_{i=0}^{n}a_ix^i$ 和 $L(x)=\sum_{i=0}^{n}a_ix^{q^i}$ 是互为 q-相伴的. 或称 $l(x)$ 为 $L(x)$ 的常规 q-相伴多项式而 $L(x)$ 为 $l(x)$ 的线性化 q-相伴多项式. 由于 ψ 为环同构, 所以若 $L_1(x)$ 和 $L_2(x)$ 分别为 $l_1(x)$ 和 $l_2(x)$ 的线性化 q-相伴多项式, 则 $L(x)=L_1(x)\otimes L_2(x)$ 为 $l(x)=l_1(x)l_2(x)$ 的线性化 q-相伴多项式, 反之亦然. 对于 $L_1(x),L(x)\in\mathcal{L}_q[x]$, 若存在某个 $L_2(x)\in\mathcal{L}_q[x]$ 使得 $L(x)=L_2(x)\otimes L_1(x)(=L_1(x)\otimes L_2(x))$, 则称 $L_1(x)$ 符号整除 $L(x)$ (或 $L(x)$ 被 $L_1(x)$ 符号整除), 也称 $L_1(x)$ 是 $L(x)$ 的符号因式. 由此我们有如下推论.

推论 4.23: 设 $L_1(x),L(x)\in\mathcal{L}_q[x]$, $L_1(x)$ 和 $L(x)$ 的常规 q-相伴多项式分别为 $l_1(x)$ 和 $l(x)$, 则 $L_1(x)$ 符号整除 $L(x)$ 当且仅当 $l_1(x)$ 整除 $l(x)$. □

考虑 $\mathbb{F}_q$ 上的 q-多项式 $x^{q^n}-x$. 设 $L(x)\in\mathcal{L}_q[x]$ 符号整除 $x^{q^n}-x$, 即存在 $L_1(x)\in\mathcal{L}_q[x]$ 使得 $x^{q^n}-x=L_1(x)\otimes L(x)=L_1(L(x))$. 则对 $\alpha\in\mathbb{F}_{q^n}$, $L(x)-\alpha$ 在 $\mathbb{F}_{q^n}$ 中有根当且仅当 $L_1(\alpha)=0$. 事实上, 若 $L(x)-\alpha$ 在 $\mathbb{F}_{q^n}$ 中有根 β, 即 $L(\beta)=\alpha$, 则 $L_1(\alpha)=L_1(L(\beta))=\beta^{q^n}-\beta=0$. 反之, 设 $L_1(\alpha)=0$, γ 为 $L(x)-\alpha$ 在 $\mathbb{F}_{q^n}$ 的扩域中的根. 则 $\gamma^{q^n}-\gamma=L_1(L(\gamma))=L_1(\alpha)=0$, 即 $\gamma^{q^n}=\gamma$, 从而 $\gamma\in\mathbb{F}_{q^n}$. (实际上我们也证明了若 $L(x)-\alpha$ 在 $\mathbb{F}_{q^n}$ 中有根, 则它的根都在 $\mathbb{F}_{q^n}$ 中.) 特别地, 取 $L(x)=x^q-x$, 则 $L(x)$ 符号整除 $x^{q^n}-x$. 由它们对应的常规 q-相伴多项式可以容易求出满足 $x^{q^n}-x=L_1(x)\otimes(x^q-x)$ 的 q-多项式 $L_1(x)$ 为 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)=x^{q^{n-1}}+\cdots+x^q+x$. 由上面的结论就得到对于 $\alpha\in\mathbb{F}_{q^n}$, $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)=0$ 当且仅当 $x^q-x-\alpha$ 在 $\mathbb{F}_{q^n}$ 中有根, 也当且仅当存在 $\beta\in\mathbb{F}_{q^n}$ 使得 $\alpha=\beta^q-\beta$. 这就是定理 3.6 关于迹映射的结果.

注意到符号乘法和普通乘法是完全不同的运算, 但令人惊奇的是对 $\mathbb{F}_q$ 上的 q-多项式来说, 对应的两种整除是等价的.

定理 4.24: 设 $L_1(x),L(x)\in\mathcal{L}_q[x]$, 则 $L_1(x)$ 符号整除 $L(x)$ 当且仅当 $L_1(x)\mid L(x)$.

证明: 设 $L_1(x)$ 符号整除 $L(x)$, 则存在 $L_2(x) \in \mathcal{L}_q[x]$ 使得 $L(x) = L_2(x) \otimes L_1(x)$. 设 $L_2(x) = \sum_{i=0}^{s} a_i x^{q^i}$, 则有

$$L(x) = a_s L_1(x)^{q^s} + \cdots + a_1 L_1(x)^q + a_0 L_1(x),$$

从而 $L_1(x) \mid L(x)$.

反之, 设 $L_1(x) \mid L(x)$, 不妨设 $L_1(x) \neq 0$. 设 $l_1(x)$ 和 $l(x)$ 分别为 $L_1(x)$ 和 $L(x)$ 的常规 q-相伴多项式, 则 $l_1(x) \neq 0$. 做带余除法, 设 $l(x) = q(x)l_1(x) + r(x)$, 其中 $q(x), r(x) \in \mathbb{F}_q[x]$ 且 $\deg r(x) < \deg l_1(x)$. 设 $Q(x)$ 和 $R(x)$ 分别为 $q(x)$ 和 $r(x)$ 的线性化 q-相伴多项式, 则有 $L(x) = Q(x) \otimes L_1(x) + R(x)$. 由前面必要性的证明得知 $L_1(x) \mid Q(x) \otimes L_1(x)$, 故由 $L_1(x) \mid L(x)$ 就有 $L_1(x) \mid R(x)$. 由 $\deg r(x) < \deg l_1(x)$ 得到 $\deg R(x) < \deg L_1(x)$, 所以 $R(x) = 0$. 这样 $L(x) = Q(x) \otimes L_1(x)$, 即 $L_1(x)$ 符号整除 $L(x)$. □

类似于通常的多项式的最大公因式, 我们可以定义 $\mathbb{F}_q$ 上的 q-多项式的最大公共符号因式. 设 $L_1(x), L_2(x) \in \mathcal{L}_q[x]$, 称 $L_1(x)$ 和 $L_2(x)$ 的次数最高且符号整除 $L_1(x)$ 和 $L_2(x)$ 的首一 q-多项式为 $L_1(x)$ 和 $L_2(x)$ 的最大公共符号因式. 我们先考察 $L_1(x)$ 和 $L_2(x)$ 的最大公因式 $D(x) = \gcd(L_1(x), L_2(x))$. 注意到 $D(x)$ 的根集为 $L_1(x)$ 和 $L_2(x)$ 的根集的交, 假设 $L_1(x)$ 和 $L_2(x)$ 的根都在 $\mathbb{F}_q$ 的某个扩域 F 中, 则 $L_1(x)$ 和 $L_2(x)$ 的根集都是 F 的 $\mathbb{F}_q$-子空间, 它们的交依然是 F 的 $\mathbb{F}_q$-子空间. 又 $L_1(x)$ 的每个根的重数都相同, 该重数或为 1 或为 q 的方幂, $L_2(x)$ 的根的情况也是如此, 所以 $D(x)$ 的每个根的重数也都相同, 这个重数也是或为 1 或为 q 的方幂, 故由定理 4.20 得到 $D(x)$ 为首一 q-多项式. 定理 4.24 表明 $D(x)$ 是 $L_1(x)$ 和 $L_2(x)$ 的公共符号因式, 另一方面, 给定 $L_1(x)$ 和 $L_2(x)$ 的公共符号因式 $E(x)$, 则由 $E(x)$ 符号整除 $L_1(x)$ 和 $L_2(x)$ 得到 $E(x)$ 整除 $L_1(x)$ 和 $L_2(x)$, 即 $E(x)$ 是 $L_1(x)$ 和 $L_2(x)$ 的公因式. 所以 $E(x) \mid D(x)$, 即 $\deg E(x) \leq \deg D(x)$, 从而 $D(x)$ 是 $L_1(x)$ 和 $L_2(x)$ 的次数最高的首一公共符号因式, 即 $L_1(x)$ 和 $L_2(x)$ 的最大公共符号因式. 上述结果表明 $\mathbb{F}_q$ 上的 q-多项式的最大公共符号因式就是它们的最大公因式. 进一步地, 如果我们要求出 $L_1(x)$ 和 $L_2(x)$ 的最大公共符号因式 (或最大公因式), 可以先写出 $L_1(x)$ 和 $L_2(x)$ 的常规 q- 相伴多项式 $l_1(x)$ 和 $l_2(x)$, 再求出 $d(x) = \gcd(l_1(x), l_2(x))$, 则 $d(x)$ 的线性化 q-相伴多项式 $D(x)$ 即为所求 (容易验证).

设 $f(x) \in \mathbb{F}_q[x]$ 不可约, $F[x]$ 是 $f(x)$ 的线性化 q-相伴多项式, 则显然 $F(x)$ 有因子 x. 那么 $\frac{F[x]}{x}$ 在 $\mathbb{F}_q[x]$ 中的分解如何? 显然若 $f(x)$ 的常数项为 0, 则 $f(x) = cx$, 其中 $c \in \mathbb{F}_q^*$. 这时 $F(x)/x = cx^{q-1}$, 它的不可约因子是 x, 次数为 1. 一般地, 若 $f(0) \neq 0$, 我们有如下结论.

定理 4.25: 设 $f(x) \in \mathbb{F}_q[x]$ 不可约且 $f(0) \neq 0$, 设 $F[x]$ 是 $f(x)$ 的线性化 q-相伴多项式, 则 $\frac{F(x)}{x}$ 在 $\mathbb{F}_q[x]$ 中每个不可约因式的次数为 $\mathrm{ord}(f(x))$.

证明: 设 $e = \mathrm{ord}(f(x))$, $h(x)$ 是 $\frac{F(x)}{x}$ 的一个不可约因式且 $\deg h(x) = d$. 由于 $f(x) \mid x^e - 1$, 由推论 4.23 和定理 4.24 有 $F(x) \mid x^{q^e} - x$. 由定理 2.4 得到 $x^{q^e} - x$ 的不可约多项式的次数整除 e, 故 $d \mid e$.

另一方面, 设 $x^d-1=q(x)f(x)+r(x)$, 其中 $q(x),r(x)\in\mathbb{F}_q[x]$ 且 $\deg r(x)<\deg f(x)$. 设 $Q(x)$ 和 $R(x)$ 分别为 $q(x)$ 和 $r(x)$ 的线性化 q-相伴多项式, 则有

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

由 $h(x)\mid x^{q^d}-x$ 和 $h(x)\mid F(x)$ 得到 $h(x)\mid R(x)$. 若 $r(x)\neq 0$, 则由 $\deg r(x)<\deg f(x)$ 和 $f(x)$ 不可约有 $r(x)$ 与 $f(x)$ 互素, 故存在 $u(x),v(x)\in\mathbb{F}_q[x]$ 使得 $u(x)r(x)+v(x)f(x)=1$. 令 $U(x)$ 和 $V(x)$ 分别为 $u(x)$ 和 $v(x)$ 的线性化 q-相伴多项式, 则有

$$U(x)\otimes R(x)+V(x)\otimes F(x)=x.$$

再由 $h(x)\mid R(x)$ 和 $h(x)\mid F(x)$ 得到 $h(x)\mid x$. 注意到 $h(x)\mid \frac{F(x)}{x}\mid x^{q^e-1}-1$, $h(x)$ 的常数项非零, 与 $h(x)\mid x$ 矛盾. 所以 $r(x)=0$, 故 $f(x)\mid(x^d-1)$. 这样 $e\mid d$, 与上面得到的 $d\mid e$ 联合起来就得到 $d=e=\mathrm{ord}(f(x))$. □

注意到定理 4.25 的结论对常数项为 0 不可约多项式 $f(x)=cx$ 依然成立, 其中 $c\in\mathbb{F}_q^*$. 另外若 $\deg f(x)=n$, 则 $\deg\left(\frac{F(x)}{x}\right)=q^n-1$. 由此得到下面的推论.

推论 4.26: 设 $f(x)\in\mathbb{F}_q[x]$ 首一不可约且 $f(0)\neq 0$, $F[x]$ 是 $f(x)$ 的线性化 q-相伴多项式, 则 $\frac{F(x)}{x}$ 在 $\mathbb{F}_q$ 上依然不可约当且仅当 $f(x)$ 为本原多项式. □

设 $L(x)\in\mathcal{L}_q[x]$, 称 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约若它的常规 q-相伴多项式 $l(x)$ 在 $\mathbb{F}_q$ 上不可约. 所以 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约即 $\deg L(x)\geq q$ 且若有 $L_1(x),L_2(x)\in\mathcal{L}_q[x]$ 满足 $L(x)=L_1(x)\otimes L_2(x)$, 则 $L_1(x)$ 和 $L_2(x)$ 中恰有一个的次数为 1. 显然次数为 q 的 q-多项式一定符号不可约. 由于任一次数大于 0 的多项式都可以唯一地写成不可约多项式的乘积, 所以 $\mathbb{F}_q$ 上的每个次数大于 1 的 q-多项式也可以唯一地写成 $\mathbb{F}_q$ 上符号不可约的 q-多项式的符号乘积 (唯一性指的是我们不考虑符号乘积的次序以及符号不可约 q-多项式的非零常数倍), 而这样的符号不可约 q-多项式的符号乘积表达式也称为符号分解式. 显然我们要找出一个次数大于 1 的 q-多项式 $L(x)$ 的符号分解式, 我们只需将 $L(x)$ 的常规 q-相伴多项式 $l(x)$ 在 $\mathbb{F}_q$ 上做不可约分解, 再把 $l(x)$ 的每个不可约因式的线性化 q-相伴多项式写回即可. 例如, 我们来符号分解 $\mathbb{F}_2$ 上的 2-多项式 $L(x)=x^{16}+x^8+x^2+x$. $L(x)$ 的常规 2-相伴多项式为 $l(x)=x^4+x^3+x+1$, $l(x)$ 在 $\mathbb{F}_2$ 上的标准分解式为 $l(x)=(x+1)^2(x^2+x+1)$, 所以 $L(x)$ 在 $\mathbb{F}_2$ 上的符号分解式为 $L(x)=(x^2+x)\otimes(x^2+x)\otimes(x^4+x^2+x)$.

我们知道 $\mathbb{F}_q$ 上的非零 q-多项式的根集一定包含在 $\mathbb{F}_q$ 的某个扩域中且构成 $\mathbb{F}_q$ 上的一个有限维线性空间, 那么一个有限维线性空间要满足什么性质才能保证以其中元素为根的首一 q-多项式一定在 $\mathbb{F}_q$ 上? 注意到 $\mathbb{F}_q$ 上多项式根的 q 次幂依然是该多项式的根, 由此我们给出下面定义. 设 M 是 $\mathbb{F}_q$ 上的一个有限维线性空间且包含在 $\mathbb{F}_q$ 的某个扩域 F 中, 若对每个 $\beta\in M$ 都有 $\beta^q\in M$, 则称 M 为一个 q-模块. 注意到 M 中非零元的阶与 q 互素, 故 $\beta\mapsto\beta^q$ 是 M 到 M 的单射, 进而为双射, 所以 $M^q:=\{\beta^q\mid\beta\in M\}=M$.

定理 4.27: 首一多项式 $L(x)$ 是 $\mathbb{F}_q$ 上的 q-多项式当且仅当 $L(x)$ 的根集 M 构成一个 q-模块并

且 $L(x)$ 的每个根都有相同的重数, 同时这个重数或为 1 或为 q 的方幂.

证明: 必要性由前面的说明已证, 下证充分性. 设 $L(x)$ 的根集 M 构成一个 q-模块并且 $L(x)$ 的每个根都有相同的重数, 这个重数或为 1 或为 q 的方幂, 则存在某个非负整数 k 使得

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

由定理 4.20 得知 $L(x)$ 是一个 q-多项式. 记

$$L_1(x) = \prod_{\beta\in M}(x-\beta) = \sum_{i=0}^{n}\alpha_i x^{q^i},$$

一方面, 由于 M 是 q-模块, 所以 $M^q = M$, 从而

$$L_1(x)^q = \prod_{\beta\in M}(x^q-\beta^q) = \prod_{\beta\in M}(x^q-\beta) = L_1(x^q).$$

由

$$\sum_{i=0}^{n}\alpha_i^q x^{q^{i+1}} = L_1(x)^q = L_1(x^q) = \sum_{i=0}^{n}\alpha_i x^{q^{i+1}}$$

得到对每个 i, $0\le i\le n$, 都有 $\alpha_i^q = \alpha_i$, 故 $\alpha_i\in\mathbb{F}_q$. 这便证出 $L_1(x)$ 是 $\mathbb{F}_q$ 上的 q-多项式, 从而 $L(x) = L_1(x)^{q^k}$ 也是 $\mathbb{F}_q$ 上的 q-多项式. □

下面我们用多项式的根来刻画 $\mathbb{F}_q$ 上的符号不可约首一 q-多项式. 注意到 q 次首一 q-多项式一定符号不可约, 所以我们只讨论次数大于 q 的 q-多项式.

定理 4.28: 设 $L(x)$ 是 $\mathbb{F}_q$ 上的首一 q-多项式且 $\deg L(x) > q$, 则 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约当且仅当 $L(x)$ 的每个根都是单根且其根集构成的 q-模块 M 没有非平凡的子 q-模块 (即 M 的子 q-模块只有 $\{0\}$ 和 M).

证明: 设 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约, 若 $L(x)$ 的每个根不是单根, 设其重数为 q^k, $k\ge 1$, 则由定理 4.27 的证明知存在 $L_1(x)\in\mathcal{L}_q[x]$ 使得 $L(x) = L_1(x)^{q^k}$. 这时 $L(x) = (L_1(x)^{q^{k-1}})^q = x^q\otimes L_1(x)^{q^{k-1}}$. 由于 $\deg L(x) > q$, 所以 $\deg L_1(x)^{q^{k-1}} > 1$, 与 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约矛盾. 从而 $L(x)$ 的每个根都是单根, 故 $\deg L(x) = |M|$. 进一步地, 设 N 为 M 的子 q-模块, 令 $S(x) = \prod_{\beta\in N}(x-\beta)$, 则显然 $\deg S(x) = |N|$ 且由定理 4.27 知 $S(x)$ 是 $\mathbb{F}_q$ 上的 q-多项式. 由 $N\subseteq M$ 知 $S(x)\mid L(x)$, 所以 $S(x)$ 符号整除 $L(x)$, 即存在 $T(x)\in\mathcal{L}_q[x]$ 使得 $L(x) = S(x)\otimes T(x)$. 又 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约, 所以有 $\deg S(x) = 1$ 或 $\deg T(x) = 1$. 若 $\deg S(x) = 1$, 则 $N = \{0\}$. 若 $\deg T(x) = 1$, 则 $\deg S(x) = \deg L(x)$, 故 $|N| = |M|$, 从而 $N = M$.

反之, 设 $L(x)$ 的每个根都是单根且其根集构成的 q-模块 M 没有非平凡的子 q-模块, 显然 $\deg L(x) = |M|$. 若 $L(x) = S(x)\otimes T(x)$, 其中 $S(x), T(x)\in\mathcal{L}_q[x]$. 设 $S(x)$ 的根构成的 q-模块为 N, 由于 $S(x)$ 符号整除 $L(x)$, 故 $S(x)\mid L(x)$, 所以 $S(x)$ 的根也都是单根, 故 $\deg S(x) = |N|$ 且 N 为 M 的子 q-模块, 从而 $N = \{0\}$ 或 $N = M$. 若 $N = \{0\}$, 则 $\deg S(x) = 1$. 若 $N = M$, 则 $\deg S(x) = \deg L(x)$, 由此推出 $\deg T(x) = 1$. 这便证出 $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约. □

下面考察 $\mathbb{F}_q$ 上 q-多项式的 q-本原根的个数问题. 设 $L(x)$ 是 $\mathbb{F}_q$ 上的 q-多项式, 记 N_L 为 $L(x)$ 在 $\mathbb{F}_q$ 上的 q-本原根的个数. 首先若 $L(x)$ 有重根, 则存在 $L_1(x) \in \mathcal{L}_q[x]$ 使得 $L(x) = L_1(x)^{q^k}$, 其中 $k \geq 1$. 这时 $L(x)$ 的根一定是 $L_1(x)$ 的根, 又 $\deg L_1(x) < \deg L(x)$, 所以 $L(x)$ 无 q-本原根, 即 $N_L = 0$. 下面我们假设 $L(x)$ 无重根且首一, 所以 $L(x)$ 的全部根的个数就是 $\deg L(x)$. 若 $\deg L(x) = 1$, 即 $L(x) = ax$, 其中 $a \in \mathbb{F}_q^*$, $L(x)$ 的唯一根 0 是它的本原根, 这时 $N_L = 1$. 下面设 $\deg L(x) = q^n > 1$, 且 $L(x)$ 的符号分解为

$$L(x) = \underbrace{L_1(x) \otimes \cdots \otimes L_1(x)}_{e_1} \otimes \underbrace{L_2(x) \otimes \cdots \otimes L_2(x)}_{e_2} \otimes \cdots \otimes \underbrace{L_r(x) \otimes \cdots \otimes L_r(x)}_{e_r}, \tag{4.17}$$

其中 $L_i(x)$ 为 $\mathbb{F}_q$ 上的符号不可约 q-多项式且 $e_i \geq 1$, $1 \leq i \leq r$. 对每个 i, 令

$$K_i(x) = \underbrace{L_1(x) \otimes \cdots \otimes L_1(x)}_{e_1} \otimes \cdots \otimes \underbrace{L_i(x) \otimes \cdots \otimes L_i(x)}_{e_i - 1} \otimes \cdots \otimes \underbrace{L_r(x) \otimes \cdots \otimes L_r(x)}_{e_r},$$

则有 $L(x) = L_i(x) \otimes K_i(x)$. 设 $\deg L_i(x) = q^{n_i}$, 则 $\deg K_i(x) = q^{n-n_i}$. 设 ξ 为 $L(x)$ 的任一根, $M(x)$ 是 ξ 在 $\mathbb{F}_q$ 上的极小 q-多项式. 若 ξ 不是 $L(x)$ 的 q-本原根, 则 $\deg M(x) < q^n$ 且 $M(x)$ 符号整除 $L(x)$, 故 $M(x)$ 符号整除某个 $K_i(x)$, 即 ξ 是 $K_i(x)$ 的根. 进一步地, 设 $i_1, \ldots, i_s$ 是 $\{1, 2, \ldots, r\}$ 中互不相同的元素, 则 $K_{i_1}(x), \ldots, K_{i_s}(x)$ 的公共根的个数也就是它们的最大公因式的次数. $K_{i_1}(x), \ldots, K_{i_s}(x)$ 的最大公因式也是它们的最大公共符号因式, 由它们的符号分解容易得到 $K_{i_1}(x), \ldots, K_{i_s}(x)$ 的最大公共符号因式的次数为 $q^{n-n_1-\cdots-n_s}$. 显然 $L(x)$ 的 q-本原根的个数就是 $L(x)$ 的所有根的个数减去那些非 q-本原根的个数, 即减去所有 $K_i(x)$ 的根的个数, $1 \leq i \leq r$. 注意到 $i \neq j$, $K_i(x)$ 的根与 $K_j(x)$ 的根可能有重复 (比如若 $\gcd(K_i(x), K_j(x)) \neq 1$, 则 $\gcd(K_i(x), K_j(x))$ 的根就是重复). 利用容斥原理, 我们可得 $L(x)$ 在 $\mathbb{F}_q$ 上的 q-本原根个数为

$$N_L = q^n - \sum_{i=1}^{r} q^{n-n_i} + \sum_{1 \leq i < j \leq r} q^{n-n_i-n_j} \mp \cdots + (-1)^r q^{n-n_1-\cdots-n_r} = q^n \prod_{i=1}^{r} (1 - q^{-n_i}). \tag{4.18}$$

设 $L(x)$ 和 $L_i(x)$ 的常规 q-相伴多项式为 $l(x)$ 和 $l_i(x)$, $1 \leq i \leq r$, 则 $L(x)$ 的符号分解式 (4.17) 可以给出 $l(x)$ 在 $\mathbb{F}_q$ 上的标准分解为

$$l(x) = l_1(x)^{e_1} l_2(x)^{e_2} \cdots l_r(x)^{e_r}.$$

由于 $\deg L_i(x) = q^{n_i}$, 所以 $\deg l_i(x) = n_i$, $1 \leq i \leq r$. 由定理 1.20 可知, 式 (4.18) 中的数恰为 $\Phi_q(l(x))$, 即次数小于 $\deg l(x) (= n)$ 且与 $l(x)$ 互素的 $\mathbb{F}_q$ 上的多项式的个数. 由此我们证明了如下定理.

定理 4.29: 设 $L(x)$ 是 $\mathbb{F}_q$ 上的非零 q-多项式且其常规 q-相伴多项式为 $l(x)$, 则 $L(x)$ 在 $\mathbb{F}_q$ 上的 q-本原根个数 N_L 为

$$N_L = \begin{cases} 0, & \text{若 } L(x) \text{ 有重根,} \\ \Phi_q(l(x)), & \text{若 } L(x) \text{ 无重根.} \end{cases}$$

□

由于对任一非零多项式 $l(x) \in \mathbb{F}_q[x]$, 有 $\Phi_q(l(x)) > 0$. 我们可立得如下推论.

推论 4.30: 任一 $\mathbb{F}_q$ 上无重根的非零 q-多项式一定有 $\mathbb{F}_q$ 上的 q-本原根. □

设 $\mathbb{F}_q$ 上非零 q-多项式 $L(x)$ 的常规 q-相伴多项式为 $l(x)$, 注意到 $L(x)$ 没有重根当且仅当其 x 项的系数非零, 也即当且仅当 $l(x)$ 的常数项非零. 所以我们得到 $\mathbb{F}_q$ 上非零 q-多项式有 q-本原根当且仅当其常规 q-相伴多项式的常数项非零.

设 $F = \mathbb{F}_{q^n}$ 是 $\mathbb{F}_q$ 的 n 次扩张, 显然 $L(x) = x^{q^n} - x = \prod_{\beta \in F}(x - \beta)$ 是 $\mathbb{F}_q$ 上的 q-多项式. 设 $\alpha \in F$ 是 $L(x)$ 的一个 q-本原根, 若存在不全为零的元素 $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_q$ 使得 $a_0\alpha + a_1\alpha^q + \cdots + a_{n-1}\alpha^{q^{n-1}} = 0$, 则有 $\mathbb{F}_q$ 上次数更低的非零 q-多项式 $a_0x + a_1x^q + \cdots + a_{n-1}x^{q^{n-1}}$ 以 α 为根, 与 α 是 $L(x)$ 的 q-本原根矛盾. 从而 $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ 是 F 在 $\mathbb{F}_q$ 上的一组基, 即 α 为 F 在 $\mathbb{F}_q$ 上的正规元素. 由于 $x^{q^n} - x$ 无重根, 由推论 4.30 得知 F 在 $\mathbb{F}_q$ 上的正规元素一定存在, 这样我们再次证明了正规基定理, 即定理 3.12. 进一步地, 若 $\xi \in F$ 不是 $L(x)$ 的一个 q-本原根, 则存在 $\mathbb{F}_q$ 上一个次数小于 q^n 的非零 q-多项式以 ξ 为根, 这便得到 $\xi, \xi^q, \ldots, \xi^{q^{n-1}}$ 在 $\mathbb{F}_q$ 上线性相关, 即 ξ 不是 F 在 $\mathbb{F}_q$ 上的正规元素. 所以 $\alpha \in F$ 是 F 在 $\mathbb{F}_q$ 上的正规元素当且仅当 α 是 $L(x) = x^{q^n} - x$ 在 $\mathbb{F}_q$ 上的 q-本原根, 由于 $L(x)$ 的常规 q-相伴多项式为 $l(x) = x^n - 1$, 由定理 4.29 知 F 在 $\mathbb{F}_q$ 上的正规元素的个数为 $\Phi_q(x^n - 1)$. 注意到 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的一组正规基中含有 n 个不同的正规元素, 它们彼此共轭, 如果我们把共轭元素生成的正规基看成是相同的 (因为这样的正规基中的元素是完全一样的, 只是写出来次序不同), 我们可得到下面定理.

定理 4.31: 对任意素数幂 q 和正整数 n, 域 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的正规基个数为 $\frac{1}{n}\Phi_q(x^n - 1)$. □

4.5 习题

4.1 证明若 $n \geq 3$ 为奇数, 则 $\Phi_{2n}(x) = \Phi_n(-x)$.

4.2 注意到除 $\Phi_1(x)$ 外, 我们计算出的分圆多项式的常数项都是 $+1$, 这是一个巧合还是一个定理?

4.3 证明除 $\Phi_1(x)$ 外, 分圆多项式都是自互反的.

4.4 计算下面分圆多项式: $\Phi_{24}(x)$, $\Phi_{35}(x)$, $\Phi_{40}(x)$, $\Phi_{60}(x)$, 和 $\Phi_{105}(x)$.

4.5 设 m 为正整数, p 为素数且 $p \mid m$, 证明 $\Phi_{mp}(x) = \Phi_m(x^p)$.

4.6 证明

$$\Phi_n(1) = \begin{cases} 0, & \text{若 } n = 1, \\ p, & \text{若 } n = p^e, \text{其中 } p \text{ 是素数, } e \geq 1, \\ 1, & \text{若 } n \text{ 有至少两个不同的素因子}, \end{cases}$$

和

$$\Phi_n(-1)=\begin{cases}-2, & \text{若 } n=1,\\ 0, & \text{若 } n=2,\\ p, & \text{若 } n=2p^e,\ \text{其中 } p \text{ 是素数},\ e\geq 1,\\ 1, & \text{其它}.\end{cases}$$

4.7 在所给的域上完全分解如下分圆多项式: 在 $\mathbb{F}_2$ 上分解 $\Phi_{17}(x)$, 在 $\mathbb{F}_3$ 上分解 $\Phi_{11}(x)$, 在 $\mathbb{F}_5$ 上分解 $\Phi_{13}(x)$, 在 $\mathbb{F}_7$ 上分解 $\Phi_{19}(x)$.

4.8 分解多项式 $x^{16}-x$ 为不可约因子的乘积:

a. 在域 $\mathbb{F}_{16}$ 上.

b. 在域 $\mathbb{F}_2$ 上.

c. 在域 $\mathbb{F}_4=\{0,1,\omega,\omega^2\}$ 上, 其中 $\omega^2=\omega+1$.

4.9 分别在域 $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_5$, 和 $\mathbb{F}_7$ 上完全分解 $x^{24}-1$.

4.10 设 $\mathrm{char}\mathbb{F}_q=p$, 正整数 $n=p^em$, 其中 $p\nmid m$. 证明

$$\Phi_q(x^n-1)=q^n\prod_{d|m}\left(1-q^{-\mathrm{ord}_d(q)}\right)^{\phi(d)/\mathrm{ord}_d(q)},$$

这里 $\mathrm{ord}_d(q)$ 是 q 模 d 的乘法阶.

4.11 设 $I_{q,n}(x)$ 为域 $\mathbb{F}_q$ 上所有 n 次首一不可约多项式的乘积, 证明

$$I_{q,n}(x)=\prod_m \Phi_m(x),$$

这里的乘积跑遍 q^n-1 的所有正因子 m 使得 q 模 m 的乘法阶为 n.

4.12 利用 Berlekamp 算法分解 $\mathbb{F}_3$ 上的多项式 $f(x)=x^{11}+2x^7+2x^5+2x^4+x+2$.

4.13 利用 Berlekamp 算法找出 $\Phi_{63}(x)$ 在 $\mathbb{F}_2$ 上的 6 个 6 次不可约因式.

4.14 证明多项式 $f(x)$ 和它的互反多项式 $\tilde{f}(x)$ 有相同的阶.

4.15 证明若 2^m-1 是素数, 则 $\mathbb{F}_2$ 上的 m 次不可约多项式一定本原. (注意到若 2^m-1 为素数, 则 m 必须为素数. 进一步地对于素数 p, 若 2^p-1 也是素数, 则 2^p-1 称为 Mersenne 素数, 记为 $M_p=2^p-1$. 现在已知的 Mersenne 素数有 51 个, 其中最大的是 $M_{82589933}$.)

4.16 确定 $\mathbb{F}_2$ 上多项式 $(x^2+x+1)^5(x^3+x+1)$ 的阶.

4.17 证明多项式 $x^8+x^7+x^3+x+1$ 在 $\mathbb{F}_2$ 上不可约并确定它的阶.

4.18 证明对正整数 n, $\mathrm{ord}(\Phi_n(x))=n$.

4.19 设 q 为奇素数幂, $f(x)\in\mathbb{F}_q[x]$ 的次数为正整数且 $f(0)\neq 0$. 试给出 $f(x)$ 的阶与 $f(-x)$ 的阶之间的关系.

4.20 证明对 $\mathbb{F}_{q^m}$ 上的任一正次数多项式 $f(x)$, 存在 $\mathbb{F}_{q^m}$ 上可被 $f(x)$ 整除的非零 q-多项式.

4.21 证明 $\mathbb{F}_{q^m}$ 上的两个或多个非零 q-多项式的最大公因式仍为 q-多项式, 但是它们的最小公倍式则不一定为 q-多项式.

4.22 证明 $\mathbb{F}_{q^m}$ 上的 q-多项式 $L_1(x)$ 整除 q-多项式 $L(x)$ 当且仅当存在 $\mathbb{F}_{q^m}$ 上的 q-多项式 $L_2(x)$ 使得 $L(x) = L_2(x) \otimes L_1(x)$.

4.23 设 ζ 是 $\mathbb{F}_{q^m}$ 的某个有限扩张中的元素, 证明 $\mathbb{F}_{q^m}$ 上的某个 q-多项式$K(x)$ 以 ζ 为根当且仅当 $K(x)$ 可被 ζ 在 $\mathbb{F}_{q^m}$ 上的极小 q-多项式整除.

4.24 确定下面线性化多项式的最大公因式:

a. $\mathbb{F}_2$ 上的多项式 $L_1(x) = x^{64} + x^{16} + x^8 + x^4 + x^2 + x$ 和 $L_2(x) = x^{32} + x^8 + x^2 + x$.

b. $\mathbb{F}_3$ 上的多项式 $L_1(x) = x^{243} - x^{81} - x^9 + x^3 + x$ 和 $L_2(x) = x^{81} + x$.

4.25 把下面线性化多项式写成符号不可约多项式的符号乘积:

a. $L(x) = x^{32} + x^{16} + x^8 + x^4 + x^2 + x \in \mathbb{F}_2[x]$.

b. $L(x) = x^{81} - x^9 - x^3 - x \in \mathbb{F}_3[x]$.

4.26 对任一非零多项式 $f(x) \in \mathbb{F}_q[x]$, 证明

$$\sum_{g(x)} \Phi_q(g(x)) = q^{\deg f(x)},$$

其中求和跑遍 $f(x)$ 的所有首一因式 $g(x) \in \mathbb{F}_q[x]$.

4.27 设 $L(x) = \alpha_0 x + \alpha_1 x^q + \cdots + \alpha_{m-1} x^{q^{m-1}} \in \mathcal{L}_{q^m}[x]$, 定义

$$A(L) = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{m-1} \\ \alpha_{m-1}^q & \alpha_0^q & \cdots & \alpha_{m-2}^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_0^{q^{m-1}} \end{pmatrix}.$$

证明 $L(\mathbb{F}_{q^m})$ 是 $\mathbb{F}_q$ 上的线性空间且 $L(\mathbb{F}_{q^m})$ 在 $\mathbb{F}_q$ 上的维数等于矩阵 $A(L)$ 的秩.

4.28 设 $L(x)$ 是 $\mathbb{F}_{q^m}$ 上的 q-多项式, $\alpha \in \mathbb{F}_{q^m}$, 则多项式 $A(x) = L(x) - \alpha$ 称为 $\mathbb{F}_{q^m}$ 上的仿射 q-多项式. 设 $A(x)$ 是 $\mathbb{F}_{q^m}$ 上的一个正次数仿射 q-多项式, 并且 $\mathbb{F}_{q^m}$ 的扩域 $\mathbb{F}_{q^s}$ 包含了 $A(x)$ 的所有根. 证明 $A(x)$ 的每个根有相同的重数, 该重数或为 1 或为 q 的方幂, 且 $A(x)$ 的所有根组成 $\mathbb{F}_{q^s}$ 的某个线性子空间的平移, 这里 $\mathbb{F}_{q^s}$ 看成是 $\mathbb{F}_q$ 上的线性空间.

4.29 设 $A_1(x) = L_1(x) - \alpha_1$ 和 $A_2(x) = L_2(x) - \alpha_2$ 是 $\mathbb{F}_{q^m}$ 上的仿射 q-多项式且 $A_1(x)$ 整除 $A_2(x)$, 证明 q-多项式 $L_1(x)$ 整除 q-多项式 $L_2(x)$.

第五章　有限域上的不可约多项式

本章继续讨论有限域上的多项式, 集中在不可约多项式的具体构造方面. 有限域上的不可约多项式在理论和应用方面都起着重要的作用, 例如为了构造 $q = p^n$ 元域, 我们需要 p 元域 $\mathbb{F}_p$ 上的 n 次不可约多项式. 前面我们已经给出可以通过多项式的分解或者求扩域中一个元素的极小多项式得到不可约多项式, 本章将给出其它的一些构造方法.

注意到不可约多项式可以类比于素数, 我们也可以用类似于素数筛法的方法得到不可约多项式. 如果我们要得到域 $\mathbb{F}_q$ 上的所有 n 次不可约多项式, 我们可以从所有 $\mathbb{F}_q$ 上 n 次多项式中去掉那些可约多项式, 而可约多项式一定有次数更低的因式, 这在 q 和 n 都很小时还是有效的. 例如设 $q = 2$, $n = 4$, $\mathbb{F}_2$ 上的 4 次多项式共 $2^4 = 16$ 个, 其中的可约多项式或有一个 1 次因式, 或有两个 1 次因式, 或有四个 1 次因式, 或有两个 2 次因式. 有一个 1 次因式的多项式有 4 个, 分别为 $x(x^3 + x^2 + 1) = x^4 + x^3 + x$, $x(x^3 + x + 1) = x^4 + x^2 + x$, $(x + 1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$, 和 $(x + 1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$. 有两个 1 次因式的多项式有 3 个, 分别为 $x^2(x^2 + x + 1) = x^4 + x^3 + x^2$, $x(x + 1)(x^2 + x + 1) = x^4 + x$ 和 $(x + 1)^2(x^2 + x + 1) = x^4 + x^3 + x + 1$. 有四个 1 次因式的多项式有 5 个, 分别为 x^4, $x^3(x + 1) = x^4 + x^3$, $x^2(x + 1)^2 = x^4 + x^2$, $x(x + 1)^3 = x^4 + x^3 + x^2 + x$ 和 $(x + 1)^4 = x^4 + 1$. 有两个 2 次因式的多项式有 1 个, 为 $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. 去掉这 13 个 $\mathbb{F}_2$ 上的 4 次可约多项式, 我们得到 3 个 $\mathbb{F}_2$ 上的 4 次不可约多项式, 分别为 $x^4 + x^3 + 1$, $x^4 + x + 1$ 和 $x^4 + x^3 + x^2 + x + 1$. 当然用这种方法时, 我们需要首先知道给定域上所有次数更低的不可约多项式.

5.1　有限域上不可约多项式的判定

要构造有限域上的不可约多项式, 首先我们需要有判断一个多项式是否不可约的方法. 我们已经知道一些方法可以判断多项式的不可约性, 比如利用上一章的 Berlakamp 算法, 或者证明一个首一多项式恰为一个元素的极小多项式等等. 但显然这些方法在某些情形下非常复杂, 下面我们给出一个判断多项式不可约性的充要条件.

定理 5.1: 设 $f(x) \in \mathbb{F}_q[x]$ 且 $\deg f(x) = n$, 则 $f(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $f(x) \mid (x^{q^n} - x)$ 且对任意 $i = 1, 2, \ldots, \lfloor \frac{n}{2} \rfloor$, 有 $\gcd(f(x), x^{q^i} - x) = 1$.

证明: 若 $f(x)$ 不可约, 由定理 2.4 得知 $f(x) \mid (x^{q^n} - x)$. 对每个 $i = 1, 2, \ldots, \lfloor \frac{n}{2} \rfloor$, 因为 $n \nmid i$, 仍由定理 2.4 得到 $f(x) \nmid (x^{q^i} - x)$, 从而 $\gcd(f(x), x^{q^i} - x) = 1$. 反之, 若 $f(x)$ 在 $\mathbb{F}_q$ 上可约, 则 $f(x)$ 有一个不可约因式 $g(x) \in \mathbb{F}_q$ 且 $\deg(g(x)) = m \leq \lfloor \frac{n}{2} \rfloor$. 由定理 2.4 有 $g(x) \mid (x^{q^m} - x)$, 所以 $g(x) \mid \gcd(f(x), x^{q^m} - x)$, 与 $\gcd(f(x), x^{q^m} - x) = 1$ 矛盾. □

我们知道次数为 1 的多项式一定不可约, 下面设 $f(x) \in \mathbb{F}_q[x]$ 且 $\deg f(x) = n \geq 2$. 对于 $a, b, c, d \in \mathbb{F}_q$ 且满足 $ad - bc \neq 0$, 令 $g(x) = (cx + d)^n f(\frac{ax+b}{cx+d})$, 则有 $f(x) = (bc - ad)^{-n}(cx - a)^n g(\frac{-dx+b}{cx-a})$, 由此我们可以得到 $f(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $g(x)$ 在 $\mathbb{F}_q$ 上不可约. 特别地, 令 $a = d = 0$, $b = c = 1$, 则 $g(x)$ 为 $f(x)$ 的互反多项式 $\tilde{f}(x)$, 从而 $f(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当它的互反多项式 $\tilde{f}(x)$ 在 $\mathbb{F}_q$ 上不可约. 下面我们给出多项式不可约的几个必要条件, 它们的证明是明显的.

定理 5.2: 设 $f(x) \in \mathbb{F}_q[x]$ 不可约且 $\deg f(x) = n \geq 2$, 则有

(i) $f(x)$ 的常数项 $f(0) \neq 0$.

(ii) $f(x)$ 的所有系数之和非零.

(iii) $\gcd(f(x), f'(x)) = 1$. □

特别地, 对于 $\mathbb{F}_2$ 上的次数 ≥ 2 的不可约多项式 $f(x)$, $f(x)$ 一定有一个奇数次项的系数为 1. 因为若否, 则 $f(x)$ 就是一个多项式的平方. 进一步地, 由定理 5.2 的 (ii) 还得到 $f(x)$ 的项数一定为奇数 (我们称一个多项式中系数非零的项的个数为该多项式的项数). 一个著名的猜想说对每个正整数 $n \geq 2$, 一定存在 $\mathbb{F}_2$ 上 n 次不可约三项式或 n 次不可约五项式, 当然这个猜想现在还没有解决.

下面我们讨论一类特殊多项式的不可约性, 即含有两项的多项式. 由于若不可约多项式的次数 ≥ 2, 则其常数项一定非零, 所以我们需考虑常数项非零的多项式. 我们称只有两个非零项且其中之一为常数项的首一多项式为二项式, 即形如 $x^t - a \in \mathbb{F}_q[x]$ 的多项式, 其中 $a \in \mathbb{F}_q^*$, $t \geq 1$. 为研究二项式 $x^t - a \in \mathbb{F}_q[x]$ 的不可约性, 其中 $t \geq 2$, $a \in \mathbb{F}_q^*$, 我们先给出如下引理. 设 b 和 n 是互素的两个正整数, 注意到 $\mathrm{ord}_n(b)$ 是剩余类 $\bar{b}$ 在剩余类环 $\mathbb{Z}_n$ 的乘法群 $U(n)$ 中的阶, 即满足 $b^e \equiv 1 \pmod{n}$ 的最小正整数 e, 称为 b 模 n 的乘法阶.

引理 5.3: 设正整数 $q \geq 2$ 和 $m \geq 2$ 互素且 $\mathrm{ord}_m(q) = \ell$, 设正整数 $t \geq 2$ 满足如下条件:

(i) t 的每个素因子都整除 m 但是不整除 $\frac{q^\ell - 1}{m}$.

(ii) 若 $4 \mid t$, 则 $4 \mid (q^\ell - 1)$.

则 $\mathrm{ord}_{mt}(q) = \ell t$.

证明: 对 t 的素因子个数 N_t 做归纳, 其中这个个数不是 t 的互不相同的素因子个数, 而是带有重数的, 即若 t 的标准分解式为 $t = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, 其中 $p_1, p_2, \ldots, p_r$ 是互不相同的素数, $e_i \geq 1$, $1 \leq i \leq r$, 则 $N_t = e_1 + e_2 + \cdots + e_r$.

首先, 看 $N_t = 1$, 即 t 为素数的情形. 因为 $\mathrm{ord}_m(q) = \ell$, 即 $q^\ell \equiv 1 \pmod m$. 记 $d = \frac{q^\ell - 1}{m}$, 则 d 是一个正整数且 $q^\ell = 1 + dm$, 所以

$$q^{\ell t} = (1 + dm)^t = 1 + \sum_{i=1}^{t} \binom{t}{i} (dm)^i. \tag{5.1}$$

由于 t 为素数, 所以对 $i = 1, 2, \ldots, t-1$, 有 $t \mid \binom{t}{i}$, 从而 $mt \mid \binom{t}{i}(dm)^i$. 再由条件 (i) 知 $t \mid m$, 所以 $mt \mid (dm)^t$. 故由式 (5.1) 得到 $q^{\ell t} \equiv 1 \pmod{mt}$. 设 $\mathrm{ord}_{mt}(q) = k$, 则 $k \mid \ell t$. 由 $q^k \equiv 1 \pmod{mt}$ 得到 $q^k \equiv 1 \pmod m$, 从而 $\ell \mid k$, 即存在正整数 s 使得 $k = \ell s$. 由 $k \mid \ell t$ 得到 $s \mid t$, 又 t 为素数, 所以 $s = 1$ 或者 $s = t$, 从而 $k = \ell$ 或者 $k = \ell t$. 若 $k = \ell$, 则有 $q^\ell \equiv 1 \pmod{mt}$, 从而 $mt \mid (q^\ell - 1) = dm$, 故 $t \mid d$, 这与条件 (i) 矛盾. 这样我们便证出 $\mathrm{ord}_{mt}(q) = k = \ell t$.

下面设 t 有至少 2 个素因子 (它们可以相同) 且记 $t = rt_0$, 其中 r 为 t 的素因子, 由前面的证明我们有 $\mathrm{ord}_{mr}(q) = \ell r$. 进一步地, 若 $4 \mid t_0$, 则 $4 \mid t$, 故由条件 (ii) 得到 $4 \mid (q^\ell - 1)$. 又显然 $(q^\ell - 1) \mid (q^{\ell r} - 1)$, 我们有 $4 \mid (q^{\ell r} - 1)$. 所以如果我们能够证明 t_0 的每个素因子都整除 mr 但是不整除 $\frac{q^{\ell r} - 1}{mr}$, 又显然 t_0 的素因子个数比 t 的素因子个数少 1, 则对 t_0 利用归纳假设就得到 $\mathrm{ord}_{mrt_0}(q) = \ell r t_0$, 即 $\mathrm{ord}_{mt}(q) = \ell t$.

下面我们就来证明 t_0 的每个素因子都整除 mr 但是不整除 $\frac{q^{\ell r} - 1}{mr}$. 设 r_0 是 t_0 的一个素因子, 由条件 (i) 得到 $r_0 \mid m$, 故 $r_0 \mid mr$. 这样我们只需证明 $r_0 \nmid \frac{q^{\ell r} - 1}{mr}$. 记 $q^{\ell r} - 1 = c(q^\ell - 1)$, 其中 $c = q^{\ell(r-1)} + q^{\ell(r-2)} + \cdots + q^\ell + 1$, 设 $d_0 = \frac{q^{\ell r} - 1}{mr}$, $d = \frac{q^\ell - 1}{m}$, 所以 $d_0 = \frac{c(q^\ell - 1)}{mr} = \frac{cd}{r}$. 因为 r 是 t 的素因子, 由条件 (i) 得到 $r \mid m$. 故由 $q^\ell \equiv 1 \pmod m$ 得到 $q^\ell \equiv 1 \pmod r$, 所以

$$c = q^{\ell(r-1)} + q^{\ell(r-2)} + \cdots + q^\ell + 1 \equiv r \pmod r \equiv 0 \pmod r,$$

即 $\frac{c}{r} \in \mathbb{Z}$. 因为 r_0 是 t 的素因子, 由条件 (i) 得到 $r_0 \nmid d$. 这样如果我们能证明 $r_0 \nmid \frac{c}{r}$, 则得到我们要证明的 $r_0 \nmid d_0$.

由 $r_0 \mid m$ 和 $q^\ell - 1 = md$, 我们有 $q^\ell \equiv 1 \pmod{r_0}$, 从而 $c \equiv r \pmod{r_0}$. 若 $r_0 \neq r$, 则有 $\frac{c}{r} \equiv 1 \pmod{r_0}$, 所以 $r_0 \nmid \frac{c}{r}$. 下面设 $r_0 = r$, 这时有 $q^\ell \equiv 1 \pmod r$. 我们设 $q^\ell \equiv 1 + br \pmod{r^2}$, 其中 b 为一个整数. 所以对每个 $j \geq 1$, 有

$$q^{\ell j} \equiv (1 + br)^j \equiv 1 + jbr \pmod{r^2},$$

从而

$$c = q^{\ell(r-1)} + q^{\ell(r-2)} + \cdots + q^\ell + 1 \equiv r + br \sum_{j=1}^{r-1} j \equiv r + br\frac{r(r-1)}{2} \pmod{r^2},$$

故 $\frac{c}{r} \equiv 1 + br\frac{r-1}{2} \pmod r$. 若 r 为奇素数, 则有 $\frac{c}{r} \equiv 1 \pmod r$, 这可推出 $r_0 = r \nmid \frac{c}{r}$. 若 r 为偶素数, 即 $r_0 = r = 2$. 由 $rr_0 \mid rt_0 = t$ 得到 $4 \mid t$, 再由条件 (ii) 得到 $4 \mid (q^\ell - 1)$. 这时有 $c = q^\ell + 1 = (q^\ell - 1) + 2$, 所以 $c \equiv 2 \pmod 4$, 故 $\frac{c}{r} = \frac{c}{2} \equiv 1 \pmod 2$, 由此依然得到 $r_0 \nmid \frac{c}{r}$. □

特别地, 取 q 为素数幂且 $m \mid (q-1)$, 则显然有 q 与 m 互素且 $\mathrm{ord}_m(q) = \ell = 1$. 由上面引理我们可立得如下推论.

推论 5.4: 设 q 为素数幂, 正整数 $m \geq 2$ 满足 $m \mid (q-1)$. 设正整数 $t \geq 2$ 满足如下条件:

(i) t 的每个素因子都整除 m 但是不整除 $\frac{q-1}{m}$.

(ii) 若 $4 \mid t$, 则 $4 \mid (q-1)$.

则有 $\mathrm{ord}_{mt}(q) = t$. □

下面给出有限域 $\mathbb{F}_q$ 上二项式不可约性的判定定理.

定理 5.5: (Serret, 1866) 设正整数 $t \geq 2$, $a \in \mathbb{F}_q^*$ 且 a 在群 $\mathbb{F}_q^*$ 中的阶 $\mathrm{ord}(a) = m > 1$. 则二项式 $x^t - a$ 在 $\mathbb{F}_q$ 上不可约当且仅当下面两个条件成立:

(i) t 的每个素因子都整除 m 但是不整除 $\frac{q-1}{m}$.

(ii) 若 $4 \mid t$, 则 $4 \mid (q-1)$.

证明: 首先注意到群 $\mathbb{F}_q^*$ 的阶为 $q-1$, 由 $\mathrm{ord}(a) = m$ 得到 $m \mid (q-1)$, 所以 $\frac{q-1}{m}$ 是一个整数.

先证明充分性, 假设条件 (i) 和 (ii) 成立. 在 $\mathbb{F}_q$ 的某个扩域中选取 $x^t - a$ 的一个根 θ, 设 $f(x)$ 是 θ 在 $\mathbb{F}_q$ 上的极小多项式且 $\deg f(x) = d$, 由定理 2.10 知 d 为 q 模 $\mathrm{ord}(\theta)$ 的乘法阶. 下面我们来求 $\mathrm{ord}(\theta)$, 显然 $\theta^{tm} = a^m = 1$. 如果 $\mathrm{ord}(\theta) < tm$, 则有 tm 的一个素因子 r 满足 $\theta^{\frac{tm}{r}} = 1$. 因为 r 为素数, 由 $r \mid tm$ 可推出 $r \mid t$ 或 $r \mid m$. 条件 (i) 告诉我们若 $r \mid t$, 也必有 $r \mid m$, 故我们一定有 $r \mid m$. 这时 $a^{\frac{m}{r}} = (\theta^t)^{\frac{m}{r}} = \theta^{\frac{tm}{r}} = 1$, 与 $\mathrm{ord}(a) = m$ 矛盾, 所以我们有 $\mathrm{ord}(\theta) = tm$. 因为 $m \mid (q-1)$ 且条件 (i) 和 (ii) 成立, 由推论 5.4 有 $d = \mathrm{ord}_{tm}(q) = t$. 由于 $f(x) \mid (x^t - a)$, 又 $\deg f(x) = t$, 所以 $x^t - a = f(x)$, 故 $x^t - a$ 在 $\mathbb{F}_q$ 上不可约.

我们用反证法来证明必要性. 假设条件 (i) 不成立, 即存在 t 的一个素因子 r 或者整除 $\frac{q-1}{m}$ 或者不整除 m. 记 $t = rt_1$, 其中 t_1 为正整数. 若 r 整除 $\frac{q-1}{m}$, 则存在正整数 s 使得 $\frac{q-1}{m} = rs$. 设 ξ 是 $\mathbb{F}_q$ 的一个本原元素, 即 $\mathbb{F}_q^* = \langle \xi \rangle$, 则显然 $\mathrm{ord}(\xi^{rs}) = \frac{q-1}{rs} = m$. 又 $\mathrm{ord}(a) = m$, 所以 a 一定是 ξ^{rs} 的方幂. 设 $a = (\xi^{rs})^{s_1}$, 再记 $b = \xi^{ss_1}$, 则 $b \in \mathbb{F}_q^*$ 且 $a = b^r$. 所以 $x^t - a = x^{rt_1} - b^r$ 具有因式 $x^{t_1} - b$, 即 $x^t - a$ 在 $\mathbb{F}_q$ 上可约. 下面假设 r 既不整除 $\frac{q-1}{m}$ 也不整除 m. 由于 r 为素数, 所以 $r \nmid (q-1)$, 从而 r 与 $q-1$ 互素. 设正整数 r_1 满足 $r_1 r \equiv 1 \pmod{q-1}$ (这样的 r_1 一定存在), 则 $x^t - a = x^{rt_1} - a^{r_1 r}$ 具有因式 $x^{t_1} - a^{r_1}$, 故 $x^t - a$ 可约. 这便证出若条件 (i) 不成立, 则二项式 $x^t - a$ 在 $\mathbb{F}_q$ 上可约.

最后我们假设条件 (i) 成立但是条件 (ii) 不成立, 即 $4 \mid t$ 但是 $4 \nmid (q-1)$, 这样存在正整数 t_2 使得 $t = 4t_2$. 由于 $2 \mid t$, 由条件 (i) 可得 $2 \mid m$, 再由 $m \mid (q-1)$ 可推出 q 一定是奇数. 注意到 $4 \nmid (q-1)$, 所以 $4 \mid (q+1)$ 且 $m \equiv 2 \pmod 4$, 即 $\frac{m}{2}$ 为奇数. 令 $d = \frac{m}{2} + 1$, 则 d 为偶数. 因为 $\mathrm{ord}(a) = m$, 所以 $a^{\frac{m}{2}} = -1$. 从而 $x^t - a = x^t + a^{\frac{m}{2}+1} = x^t + a^d$. 令 $c = (2^{-1}a^{\frac{d}{2}})^{\frac{q+1}{4}}$, 则有 $c \in \mathbb{F}_q^*$ 且

$$a^d = 4(2^{-1}a^{\frac{d}{2}})^2 = 4(2^{-1}a^{\frac{d}{2}})^2(2^{-1}a^{\frac{d}{2}})^{q-1} = 4(2^{-1}a^{\frac{d}{2}})^{q+1} = 4c^4,$$

所以

$$x^t - a = x^t + a^d = x^{4t_2} + 4c^4 = (x^{2t_2} + 2cx^{t_2} + 2c^2)(x^{2t_2} - 2cx^{t_2} + 2c^2),$$

故二项式 $x^t - a$ 在 $\mathbb{F}_q$ 上可约. □

推论 5.6: 设 $a \in \mathbb{F}_q^*$ 且 $\mathrm{ord}(a) = m$, r 为 $q-1$ 的一个素因子但是 r 不整除 $\frac{q-1}{m}$, 设 k 为非负整数, 当 $r = 2$ 且 $k \geq 2$ 时还假设 $4 \mid (q-1)$. 则二项式 $x^{r^k} - a$ 在 $\mathbb{F}_q$ 上不可约.

证明: 显然由 $\mathrm{ord}(a) = m$ 可得 $m \mid (q-1)$. 设 $t = r^k$, 则 t 的素因子只有 r. 由 $r \mid (q-1)$ 但是 $r \nmid \frac{q-1}{m}$ 可推出 $r \mid m$, 即定理 5.5 中的条件 (i) 成立. 若 $4 \mid t$, 则有 $r = 2$ 且 $k \geq 2$, 由假设得 $4 \mid (q-1)$, 从而定理 5.5 中的条件 (ii) 也成立. 故由定理 5.5 立得二项式 $x^{r^k} - a$ 在 $\mathbb{F}_q$ 上不可约. □

例 5.1: 设 $k \geq 0$ 为非负整数,

(a) 在 $\mathbb{F}_5^*$ 中, $\mathrm{ord}(2) = \mathrm{ord}(3) = 4$, 由推论 5.6 知二项式 $x^{2^k} - 2$ 和 $x^{2^k} - 3$ 均在 $\mathbb{F}_5$ 上不可约.

(b) 在 $\mathbb{F}_7^*$ 中, $\mathrm{ord}(2) = \mathrm{ord}(4) = 3$, $\mathrm{ord}(3) = \mathrm{ord}(5) = 6$, 由推论 5.6 知二项式 $x^{3^k} - 2$, $x^{3^k} - 3$, $x^{3^k} - 4$ 和 $x^{3^k} - 5$ 均在 $\mathbb{F}_7$ 上不可约.

(c) 类似地, 由推论 5.6 知二项式 $x^{3^k} + \alpha$ 和 $x^{3^k} + \alpha^2$ 都在 $\mathbb{F}_4$ 上不可约, 其中 $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, 而 α 为 $x^2 + x + 1$ 的一个根. 这样 $x^{2\cdot 3^k} + x^{3^k} + 1 = (x^{3^k} + \alpha)(x^{3^k} + \alpha^2)$ 就在 $\mathbb{F}_2$ 上不可约, 这表明对于任意 $k \geq 0$, 存在 $\mathbb{F}_2$ 上 $2 \cdot 3^k$ 次不可约三项式.

形如 $x^n + ax^k + b$ 的多项式称为 $\mathbb{F}_q$ 上的三项式, 其中 $n > k > 0$ 且 $a, b \in \mathbb{F}_q^*$. 对于一般的三项式, 还没有如定理 5.5 那样好的充要条件, 下面我们给出三项式不可约性的部分结果.

定理 5.7: 设 p 为素数, $q = p^m$, $b \in \mathbb{F}_q^*$, 则下面说法等价.

(i) 三项式 $x^p - x - b$ 在 $\mathbb{F}_q$ 上不可约.

(ii) 三项式 $x^p - x - b$ 在 $\mathbb{F}_q$ 中无根.

(iii) $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$.

证明: (i) ⇒ (ii) 显然, 而由定理 3.6 知 (ii) ⇒ (iii) 也显然, 下面我们证明 (iii) ⇒ (i). 设 θ 是 $x^p - x - b \in \mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 的扩域中的一个根, 即 $\theta^p = \theta + b$, 我们来求 θ 在 $\mathbb{F}_q$ 上的极小多项式. 由 $\theta^p = \theta + b$ 得 $\theta^{p^2} = \theta^p + b^p = \theta + b + b^p$, 以此类推, 对任意 $i = 1, 2, \ldots$, 我们得到

$$\theta^{p^i} = \theta + b + b^p + \cdots + b^{p^{i-1}}.$$

从而

$$\theta^q = \theta^{p^m} = \theta + b + b^p + \cdots + b^{p^{m-1}} = \theta + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b). \tag{5.2}$$

由于 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) \in \mathbb{F}_p$, 所以 $(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b))^q = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b)$. 式 (5.2) 两端同时 q 次幂得到 $\theta^{q^2} = \theta^q + (\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b))^q = \theta + 2 \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b)$. 继续下去, 对任意 $i = 1, 2, \ldots$, 我们得到

$$\theta^{q^i} = \theta + i \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b).$$

由 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$, 我们得到 $\theta, \theta^q, \theta^{q^2}, \ldots, \theta^{q^{p-1}}$ 两两不同但是 $\theta^{q^p} = \theta$. 所以 θ 在 $\mathbb{F}_q$ 上有 p 个互不相同的共轭元素, 即 θ 在 $\mathbb{F}_q$ 上的极小多项式的次数为 p. 故 $x^p - x - b$ 就是 θ 在 $\mathbb{F}_q$ 上的极小多项式, 从而 $x^p - x - b$ 在 $\mathbb{F}_q$ 上不可约. □

推论 5.8: 设 $p=\mathrm{char}\mathbb{F}_q$, $a,b\in\mathbb{F}_q^*$, 则三项式 x^p-ax-b 在 $\mathbb{F}_q$ 上不可约当且仅当存在 $a_0\in\mathbb{F}_q^*$ 使得 $a=a_0^{p-1}$ 且 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{b}{a_0^p})\neq 0$.

证明: 设存在 $a_0\in\mathbb{F}_q^*$ 使得 $a=a_0^{p-1}$, 则有

$$x^p-ax-b=a_0^p\left(\left(\frac{x}{a_0}\right)^p-\frac{x}{a_0}-\frac{b}{a_0^p}\right).$$

由定理 5.7 知 $\left(\frac{x}{a_0}\right)^p-\frac{x}{a_0}-\frac{b}{a_0^p}$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{b}{a_0^p})\neq 0$, 从而 x^p-ax-b 在 $\mathbb{F}_q$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{b}{a_0^p})\neq 0$.

现在设对任意 $a_0\in\mathbb{F}_q^*$ 都有 $a\neq a_0^{p-1}$, 则线性化多项式 $L(x)=x^p-ax$ 在 $\mathbb{F}_q$ 中无非零根. 把 $\mathbb{F}_q$ 看作 $\mathbb{F}_p$ 上的线性空间, 则对 $\alpha\in\mathbb{F}_q$, 定义为 $\alpha\mapsto L(\alpha)$ 的映射 L 为线性变换. 由 $L(x)$ 在 $\mathbb{F}_q$ 中无非零根得到线性变换 L 的核为 $\{0\}$, 故 L 为单射. 又 $\mathbb{F}_q$ 是有限集, L 又为满射. 故对 $b\in\mathbb{F}_q^*$, 存在 $c\in\mathbb{F}_q$ 使得 $L(c)=b$, 即多项式 x^p-ax-b 在 $\mathbb{F}_q$ 中有根 c, 所以 x^p-ax-b 在 $\mathbb{F}_q$ 上可约. □

在上面推论中, 对于 $a\in\mathbb{F}_q^*$, 存在 $a_0\in\mathbb{F}_q^*$ 使得 $a=a_0^{p-1}$ 当且仅当 $\mathrm{ord}(a)\mid\frac{q-1}{p-1}$. 事实上, 若 $a=a_0^{p-1}$, 则 $a^{\frac{q-1}{p-1}}=a_0^{q-1}=1$, 故 $\mathrm{ord}(a)\mid\frac{q-1}{p-1}$. 反之, 设 $\mathbb{F}_q$ 的一个本原元素为 ξ 并设 $a=\xi^k$. 由于 $\mathrm{ord}(a)=\frac{q-1}{\gcd(q-1,k)}$, 由 $\mathrm{ord}(a)\mid\frac{q-1}{p-1}$ 可得 $(p-1)\mid\gcd(q-1,k)$, 从而 $(p-1)\mid k$. 令 $a_0=\xi^{\frac{k}{p-1}}$, 则有 $a_0\in\mathbb{F}_q^*$ 且 $a=\xi^k=a_0^{p-1}$. 注意到 $\mathrm{ord}(a)\mid\frac{q-1}{p-1}$ 当且仅当 $a^{\frac{q-1}{p-1}}=1$, 从而我们得到对于 $a\in\mathbb{F}_q^*$, 存在 $a_0\in\mathbb{F}_q^*$ 使得 $a=a_0^{p-1}$ 的充要条件是 $a^{\frac{q-1}{p-1}}=1$.

特别地在推论 5.8 中, 若 $p=2$, 则条件"存在 $a_0\in\mathbb{F}_q^*$ 使得 $a=a_0^{p-1}$" 是显然的并且 $a_0=a$, 所以我们有 x^2+ax+b 在 $\mathbb{F}_{2^m}$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\frac{b}{a^2})\neq 0$, 这就是第 3.1 节最后面的结论.

设 p 为素数, 下面我们给出素域 $\mathbb{F}_p$ 上一个 p 次三项式本原的充要条件. 首先注意到对任意 $b\in\mathbb{F}_p^*$, 由定理 5.7 知三项式 x^p-x-b 一定在 $\mathbb{F}_p$ 上不可约.

定理 5.9: 设 p 为素数, $b\in\mathbb{F}_p^*$, 则三项式 $f(x)=x^p-x-b$ 在 $\mathbb{F}_p$ 上本原当且仅当 b 为 $\mathbb{F}_p$ 的本原元素且三项式 x^p-x-1 的阶为 $\frac{p^p-1}{p-1}$.

证明: 设 β 是 $g(x)=x^p-x-1$ 在 $\mathbb{F}_p$ 的扩域 $\mathbb{F}_{p^p}$ 中的根, 由 $g(x)$ 在 $\mathbb{F}_p$ 上不可约得到

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

比较 $g(x)$ 的常数项有 $\beta^{\frac{p^p-1}{p-1}}=1$. 令 $\alpha=b\beta$, 则由

$$f(\alpha)=(b\beta)^p-b\beta-b=b(\beta^p-\beta-1)=bg(\beta)=0$$

知 α 为 $f(x)$ 的根.

设 $f(x)=x^p-x-b$ 在 $\mathbb{F}_p$ 上本原, 由定理 4.17 知 b 为 $\mathbb{F}_p$ 的本原元素. 下面我们求 β 的阶, 若存在正整数 $k<\frac{p^p-1}{p-1}$ 使得 $\beta^k=1$. 则有 $\alpha^{k(p-1)}=(b^{p-1})^k(\beta^k)^{p-1}=1$, 而 $k(p-1)<p^p-1$, 这与 α 为 $\mathbb{F}_{p^p}$ 的本原元素矛盾. 所以 β 在群 $\mathbb{F}_{p^p}^*$ 中的阶为 $\frac{p^p-1}{p-1}$, 由定理 4.7 知 $\mathrm{ord}(x^p-x-1)=\frac{p^p-1}{p-1}$.

反之, 设 b 为 $\mathbb{F}_p$ 的本原元素且 x^p-x-1 的阶为 $\frac{p^p-1}{p-1}$, 则在群 $\mathbb{F}_{p^p}^*$ 中, $\mathrm{ord}(b)=p-1$ 且 $\mathrm{ord}(\beta)=\frac{p^p-1}{p-1}$. 注意到

$$\frac{p^p-1}{p-1}=p^{p-1}+\cdots+p+1\equiv 1+\cdots+1+1=p\equiv 1\,(\mathrm{mod}\ (p-1)),$$

故 $p-1$ 与 $\frac{p^p-1}{p-1}$ 互素, 所以 $\mathrm{ord}(\alpha)=\mathrm{ord}(b\beta)=\mathrm{ord}(b)\cdot\mathrm{ord}(\beta)=p^p-1$. 故 α 为 $\mathbb{F}_{p^p}$ 的本原元素, 从而 $f(x)=x^p-x-b$ 在 $\mathbb{F}_p$ 上本原. □

前面给出一类特殊三项式不可约性判定的充要条件, 下面我们考虑更一般一点的三项式.

定理 5.10: 设域 $K=\mathbb{F}_r$ 是域 $F=\mathbb{F}_q$ 的子域, $b\in\mathbb{F}_r^*$, 则三项式 x^q-x-b 在 $\mathbb{F}_q$ 上有如下分解

$$x^q-x-b=\prod_{j=1}^{\frac{q}{r}}(x^r-x-\beta_j),\tag{5.3}$$

其中 $\beta_1,\beta_2,\ldots,\beta_{\frac{q}{r}}$ 为满足 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(\beta_j)=b$ 的 $\mathbb{F}_q$ 中的所有元素.

证明: 设 $p=\mathrm{char}\mathbb{F}_q$, $r=p^d$, $q=p^m$, 由于 $\mathbb{F}_r$ 为 $\mathbb{F}_q$ 的子域, 我们有 $d\mid m$. 由定理 3.1 的证明知满足 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(\beta)=b$ 的 $\beta\in\mathbb{F}_q$ 共有 $\frac{q}{r}=p^{m-d}=r^{\frac{m}{d}-1}$ 个, 记其为 $\beta_1,\beta_2,\ldots,\beta_{\frac{q}{r}}$.

对任一 β_j, $1\le j\le\frac{q}{r}$, 设 γ_j 是 $x^r-x-\beta_j$ 在 $\mathbb{F}_q$ 的扩域中的一个根, 则有 $\beta_j=\gamma_j^r-\gamma_j$. 由于

$$\begin{aligned}b=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(\beta_j) &= \beta_j+\beta_j^r+\beta_j^{r^2}+\cdots+\beta_j^{r^{\frac{m}{d}-1}}\\ &= (\gamma_j^r-\gamma_j)+(\gamma_j^{r^2}-\gamma_j^r)+(\gamma_j^{r^3}-\gamma_j^{r^2})+\cdots+(\gamma_j^q-\gamma_j^{\frac{q}{r}})=\gamma_j^q-\gamma_j,\end{aligned}$$

所以 γ_j 为 x^q-x-b 的根. 由于 $x^r-x-\beta_j$ 的根都是 x^q-x-b 的根, 又 $x^r-x-\beta_j$ 没有重根, 故 $(x^r-x-\beta_j)\mid(x^q-x-b)$. 注意到当 $j_1\ne j_2$ 时, $x^r-x-\beta_{j_1}$ 与 $x^r-x-\beta_{j_2}$ 互素, 所以

$$\prod_{j=1}^{\frac{q}{r}}(x^r-x-\beta_j)\mid(x^q-x-b).$$

比较上面整除式两边的次数和首项系数便得到分解式 (5.3). □

特别地, 在定理 5.10 中, 若 $r=p=\mathrm{char}\mathbb{F}_q$, 由于 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(\beta_j)=b\ne 0$, 由定理 5.7 知 $x^r-x-\beta_j$ 在 $\mathbb{F}_q$ 上不可约, 故这时式 (5.3) 给出了三项式 x^q-x-b 的完全分解. 例如, 考虑多项式 $x^8+x+1\in\mathbb{F}_8[x]$, 这里 $\mathbb{F}_8=\mathbb{F}_2(\alpha)$, α 为 $x^3+x+1\in\mathbb{F}_2[x]$ 的根. 容易算出满足 $\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\beta)=1$ 的 $\beta\in\mathbb{F}_8$ 为 $\beta=1$, α^3, α^5 和 α^6. 所以 x^8+x+1 在 $\mathbb{F}_8$ 上的标准分解式为

$$x^8+x+1=(x^2+x+1)(x^2+x+\alpha^3)(x^2+x+\alpha^5)(x^2+x+\alpha^6).$$

例 5.2: 本例我们给出一类三项不可约多项式的构造. 设 $p\equiv 3\,(\mathrm{mod}\ 4)$ 是一个素数, 整数 $r\ge 2$ 满足 $2^r\|(p+1)$, 即 $2^r\mid(p+1)$ 但是 $2^{r+1}\nmid(p+1)$, 则有 $2^{r+1}\|(p^2-1)$. 定义元素 $a_1,a_2,\ldots,a_r\in\mathbb{F}_p$ 如下:

$$\begin{aligned}a_1 &= 0,\\ a_i &= \left(\tfrac{a_{i-1}+1}{2}\right)^{\frac{p+1}{4}},\quad i=2,3,\ldots,r-1,\\ a_r &= \left(\tfrac{a_{r-1}-1}{2}\right)^{\frac{p+1}{4}}.\end{aligned}$$

注意到因为 $2^{r+1} \mid (p^2-1)$, 对于 $0 \leq k \leq r$, $\mathbb{F}_{p^2}$ 中包含所有的 2^{k+1} 次单位根. 但由于 $2^2 \nmid (p-1)$, 所以对 $1 \leq k \leq r$, 任意 2^{k+1} 次本原单位根不包含于 $\mathbb{F}_p$ 中, 即任意 2^{k+1} 次本原单位根在 $\mathbb{F}_p$ 上的次数为 2. 我们有下面论断 P_l: 对于 $l = 1, 2, \ldots, r-1$, 有 $x^2 - 2a_l x + 1$ 在 $\mathbb{F}_p$ 上不可约且整除 $x^{2^l} + 1$.

我们对 l 作归纳. 当 $l = 1$ 时, 因为 $p \equiv 3 \pmod 4$, -1 不是 $\mathbb{F}_p$ 中的平方元, 所以 $x^2 + 1$ 在 $\mathbb{F}_p$ 上不可约, 其整除 $x^2 + 1$ 是显然的.

下面设 l 满足 $1 \leq l < r$ 且论断 P_l 成立. 由 $(x^2 - 2a_l x + 1) \mid (x^{2^l} + 1)$ 得到 $(x^4 - 2a_l x^2 + 1) \mid (x^{2^{l+1}} + 1)$. 设 β 是多项式 $x^4 - 2a_l x^2 + 1$ 在 $\mathbb{F}_p$ 的某个扩域中的根, 则 β^2 是 $x^2 - 2a_l x + 1$ 的根, 再由 $x^2 - 2a_l x + 1$ 在 $\mathbb{F}_p$ 上不可约且整除 $x^{2^l} + 1$ 得到 $\operatorname{ord}(\beta^2) = 2^{l+1}$, 从而 $\operatorname{ord}(\beta) = 2^{l+2}$. 由于 $l + 1 \leq r$, 所以 $\beta \in \mathbb{F}_{p^2}$ 且 β 在 $\mathbb{F}_p$ 上的次数为 2, 从而 $x^4 - 2a_l x^2 + 1$ 为 $\mathbb{F}_p$ 上两个 2 次不可约多项式的乘积. 设 β 在 $\mathbb{F}_p$ 上的极小多项式为 $x^2 - 2sx + t$, 其中 $s, t \in \mathbb{F}_p$, 则有 $\beta^2 + t = 2s\beta$ 和 $\beta^4 = 2a_l\beta^2 - 1$. 由此可得到

$$(4s^2 - 2t)\beta^2 - t^2 = 2a_l\beta^2 - 1.$$

因为 $\operatorname{ord}(\beta^2) = 2^{l+1}$, 又 $2^{l+1} \nmid (p-1)$, 所以 $\beta^2 \notin \mathbb{F}_p$, 从而 $\{1, \beta^2\}$ 是 $\mathbb{F}_{p^2}$ 在 $\mathbb{F}_p$ 上的一组基, 故有 $t^2 = 1$ 且 $4s^2 - 2t = 2a_l$.

在用归纳法证明论断 P_{l+1} 时, 若有 $l < r - 1$, 则 $l + 2 \leq r$, 这时我们可以证明 $t = 1$. 如果 $t = -1$, 则 β 在 $\mathbb{F}_p$ 上的极小多项式为 $x^2 - 2sx - 1$. 由于 $\operatorname{ord}(\beta) = 2^{l+2}$, 所以多项式 $x^4 - 2sx^2 - 1$ 的根是 2^{l+3} 次本原单位根. 由 $l + 2 \leq r$ 和上面的讨论知 2^{l+3} 次本原单位根包含在 $\mathbb{F}_{p^2}$ 中且在 $\mathbb{F}_p$ 上的次数为 2. 所以 $x^4 - 2sx^2 - 1$ 是 $\mathbb{F}_p$ 上两个 2 次不可约多项式的乘积. 假设 $x^2 - 2\bar{s}x + \bar{t}$ 是 $x^4 - 2sx^2 - 1$ 在 $\mathbb{F}_p$ 上的一个不可约因式, 类似地, 我们有 $\bar{t}^2 = -1$, 这与 -1 不是 $\mathbb{F}_p$ 中的平方元矛盾.

这时我们有 $t = 1$, 从而 $2s^2 = a_l + 1$. 若 $a_l + 1 = 0$, 则有 $a_{l+1}^2 = s^2 = 0$. 若 $a_l + 1 \neq 0$, 则 $\frac{a_l+1}{2} \in \mathbb{F}_p^{*2}$, 从而 $(\frac{a_l+1}{2})^{\frac{p-1}{2}} = 1$, 所以我们仍有

$$a_{l+1}^2 = \left(\frac{a_l + 1}{2}\right)^{\frac{p+1}{2}} = \left(\frac{a_l + 1}{2}\right)^{\frac{p-1}{2}} \left(\frac{a_l + 1}{2}\right) = \frac{a_l + 1}{2} = s^2.$$

由

$$x^4 - 2a_l x^2 + 1 = x^4 - 2(2a_{l+1}^2 - 1)x^2 + 1 = (x^2 + 1)^2 - (2a_{l+1}x)^2 = (x^2 - 2a_{l+1}x + 1)(x^2 + 2a_{l+1}x + 1)$$

知 $x^2 - 2a_{l+1}x + 1$ 在 $\mathbb{F}_p$ 上不可约, 再由 $(x^4 - 2a_l x^2 + 1) \mid (x^{2^{l+1}} + 1)$ 可得 $(x^2 - 2a_{l+1}x + 1) \mid (x^{2^{l+1}} + 1)$, 由归纳法我们就证明了论断 P_{l+1}.

下面我们考察情形 $l = r - 1$, 这时 $l + 2 = r + 1$, $l + 3 = r + 2 > r + 1$, 我们来证明 $t = -1$. 事实上, 若 $t = 1$, 则有 $2s^2 = a_{r-1} + 1$, 从而

$$x^4 - 2a_{r-1}x^2 + 1 = (x^2 - 2sx + 1)(x^2 + 2sx + 1).$$

多项式 $x^2 - 2sx + 1$ 和 $x^2 + 2sx + 1$ 都在 $\mathbb{F}_p$ 上不可约, 它们的根都是 2^{r+1} 次本原单位根, 故多项式 $x^4 - 2sx^2 + 1$ 和 $x^4 + 2sx^2 + 1$ 的根都是 2^{r+2} 次本原单位根. 由于 $p \equiv 3 \pmod 4$ 和

$2^r \| (p+1)$, 我们有 $2^{r+2} \| (p^4-1)$, 所以 2^{r+2} 次本原单位根在 $\mathbb{F}_p$ 上的次数为 4, 从而多项式 x^4-2sx^2+1 和 x^4+2sx^2+1 均在 $\mathbb{F}_p$ 上不可约. 若存在某个 $\bar{s} \in \mathbb{F}_p$ 使得 $\frac{s+1}{2} = \bar{s}^2$, 则有 $x^4-2sx^2+1 = (x^2-2\bar{s}x+1)(x^2+2\bar{s}x+1)$, 这与 x^4-2sx^2+1 在 $\mathbb{F}_p$ 上不可约矛盾, 所以 $\frac{s+1}{2} \notin \mathbb{F}_p^2$. 类似地, 若存在某个 $\tilde{s} \in \mathbb{F}_p$ 使得 $-\frac{s+1}{2} = \tilde{s}^2$, 则有 $x^4+2sx^2+1 = (x^2-2\tilde{s}x-1)(x^2+2\tilde{s}x-1)$, 与 x^4+2sx^2+1 在 $\mathbb{F}_p$ 上不可约矛盾, 所以 $-\frac{s+1}{2} \notin \mathbb{F}_p^2$. 但是 $-1 \notin \mathbb{F}_p^2$, 由初等数论可知 $\frac{s+1}{2}$ 和 $-\frac{s+1}{2}$ 中必有一个属于 $\mathbb{F}_p^2$, 矛盾.

这时我们有 $t=-1$, 从而 $2s^2 = a_{r-1}-1$, 与上面的讨论类似我们有 $a_r^2 = s^2$ 和

$$x^4 - 2a_{r-1}x^2 + 1 = (x^2 - 2a_r x - 1)(x^2 + 2a_r x - 1).$$

所以 x^2-2a_rx-1 在 $\mathbb{F}_p$ 上不可约且整除 $x^{2^r}+1$.

接下来我们证明对任意 $k \geq 1$, 三项式 $x^{2^k} - 2a_r x^{2^{k-1}} - 1$ 在 $\mathbb{F}_p$ 上不可约且整除 $x^{2^{r+k-1}}+1$.

我们对 k 作归纳, $k=1$ 就是如上已证明的结论. 设结论对任意 $k \geq 1$ 成立, 我们来看 $k+1$ 的情形. 在 $(x^{2^k} - 2a_r x^{2^{k-1}} - 1) \mid (x^{2^{r+k-1}}+1)$ 中以 x^2 代 x 就有

$$(x^{2^{k+1}} - 2a_r x^{2^k} - 1) \mid (x^{2^{r+k}}+1),$$

我们只需证明 $x^{2^{k+1}} - 2a_r x^{2^k} - 1$ 在 $\mathbb{F}_p$ 上不可约即可. 设 α_1, α_2 为二次多项式 x^2-2a_rx-1 的两个根, 则 $\alpha_1, \alpha_2 \in \mathbb{F}_{p^2}$ 且 $\mathrm{ord}(\alpha_1) = \mathrm{ord}(\alpha_2) = 2^{r+1}$. 由推论 5.6 知对任意 $k \geq 1$, $x^{2^k} - \alpha_1$ 和 $x^{2^k} - \alpha_2$ 均在 $\mathbb{F}_{p^2}$ 上不可约, 所以

$$x^{2^{k+1}} - 2a_r x^{2^k} - 1 = (x^{2^k} - \alpha_1)(x^{2^k} - \alpha_2)$$

在 $\mathbb{F}_p$ 上不可约.

类似地可以证明 (请读者完成证明), $x^2 + 2a_rx - 1$ 在 $\mathbb{F}_p$ 上不可约且整除 $x^{2^r}+1$, 从而我们也可以得到对任意 $k \geq 1$, 三项式 $x^{2^k} + 2a_r x^{2^{k-1}} - 1$ 也在 $\mathbb{F}_p$ 上不可约且整除 $x^{2^{r+k-1}}+1$.

进一步地, 由推论 2.14 得到对任意奇数 m 和任意 $k \geq 1$, 三项式 $x^{2^k} - 2a_r x^{2^{k-1}} - 1$ 和 $x^{2^k} + 2a_r x^{2^{k-1}} - 1$ 均在 $\mathbb{F}_{p^m}$ 上不可约. 注意到对任意素数幂 $q = p^m$, 其中 p 为素数, 若 $q \equiv 3 \pmod 4$, 则必有 $p \equiv 3 \pmod 4$ 且 m 为奇数. 所以本例的结论是对任意有限域来说的. □

显然二次三项式 $x^2+x+b \in \mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约当且仅当它在 $\mathbb{F}_q$ 中无根. 若 q 为奇素数幂, x^2+x+b 在 $\mathbb{F}_q$ 中无根当且仅当 $1-4b$ 为 $\mathbb{F}_q$ 中的非平方元. 我们知道 $\mathbb{F}_q$ 中的非平方元素有 $\frac{q-1}{2}$ 个, 所以存在 $\frac{q-1}{2}$ 个 $\mathbb{F}_q$ 中的元素 b 使得 x^2+x+b 在 $\mathbb{F}_q$ 上不可约. 一般说来, 使得 $x^n+x+b \in \mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约的 $b \in \mathbb{F}_q$ 的个数近似于 $\frac{q}{n}$, 下面我们给出一个定理但是略去其证明.

定理 5.11: 设域 $\mathbb{F}_q$ 的特征为 p, 正整数 $n \geq 2$ 且 $p \nmid 2n(n-1)$, 记 $T_n(q)$ 为使得三项式 x^n+x+b 在 $\mathbb{F}_q$ 上不可约的元素 $b \in \mathbb{F}_q$ 的个数, 则有

$$\left| T_n(q) - \frac{q}{n} \right| \leq B_n \sqrt{q},$$

其中 B_n 为仅与 n 相关的常数. □

5.2 多项式的复合

本节我们考虑多项式的复合. 设 $f(x), g(x) \in \mathbb{F}_q[x]$, 设

$$P(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_q[x]$$

的次数为 n. 则下面的复合

$$Q(x) = g(x)^n P\left(\frac{f(x)}{g(x)}\right) = \sum_{i=0}^{n} c_i f(x)^i g(x)^{n-i}$$

仍为一个多项式. 例如, 若取 $f(x) = 1$, $g(x) = x$, 则如上得到的多项式 $Q(x)$ 就是 $P(x)$ 的互反多项式.

设 $d(x) = \gcd(f(x), g(x))$, 则显然有 $d(x)^n \mid Q(x)$. 另一方面, 若 $P(x)$ 在 $\mathbb{F}_q$ 上可约, 不妨设 $P(x) = P_1(x) \cdot P_2(x)$, 其中 $\deg P_i(x) = n_i < n$, $i = 1, 2$. 令 $Q_i(x) = g(x)^{n_i} P_i\left(\frac{f(x)}{g(x)}\right)$, 由于 $n = n_1 + n_2$, 我们有

$$Q(x) = g(x)^{n_1} P_1\left(\frac{f(x)}{g(x)}\right) \cdot g(x)^{n_2} P_2\left(\frac{f(x)}{g(x)}\right) = Q_1(x) \cdot Q_2(x),$$

所以 $Q(x)$ 依然在 $\mathbb{F}_q$ 上可约. 所以, 若复合后的多项式 $Q(x)$ 在 $\mathbb{F}_q$ 上不可约, 则必有多项式 $f(x)$ 与 $g(x)$ 互素且 $P(x)$ 在 $\mathbb{F}_q$ 上不可约.

若 $n = 1$, 即 $P(x) = c_1 x + c_0$, 其中 $c_1 \neq 0$. 则 $Q(x) = c_1 f(x) + c_0 g(x) = c_1(f(x) - (-\frac{c_0}{c_1})g(x))$. 显然 $-\frac{c_0}{c_1}$ 是 $P(x)$ 的唯一根, 所以这时 $Q(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $f(x) - ag(x) \in \mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约, 其中 a 为 $P(x)$ 的根. 类似的结论可以推广到一般的情形, 我们有下面定理.

定理 5.12: 设 $f(x), g(x) \in \mathbb{F}_q[x]$ 互素, $P(x) \in \mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约且 $\deg P(x) = n \geq 1$. 则 $Q(x) = g(x)^n P\left(\frac{f(x)}{g(x)}\right)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $f(x) - \alpha g(x)$ 在 $\mathbb{F}_{q^n}$ 上不可约, 其中 $\alpha \in \mathbb{F}_{q^n}$ 是 $P(x)$ 的任一个根. 进一步地, 若 $n > 1$, 则 $\deg Q(x) = nh$, 其中 $h = \max\{\deg f(x), \deg g(x)\}$.

证明: 首先若 $n = 1$, 前面的讨论已证明了定理. 只是当 $P(0) = 0$ 时有 $Q(x) = c_1 f(x)$, 这时 $\deg Q(x) = \deg f(x)$.

下面假设 $n \geq 2$, 若 $\deg f(x) \neq \deg g(x)$, 容易计算得到 $\deg Q(x) = nh$. 若 $\deg f(x) = \deg g(x) = h$, 设它们的首项系数分别为 a 和 b, 则显然 $\deg Q(x) \leq nh$ 且 $Q(x)$ 的 nh 次项系数为 $b^n P(\frac{a}{b})$, 由于 $n \geq 2$ 次不可约多项式 $P(x)$ 在 $\mathbb{F}_q$ 中没有根, 所以 $b^n P(\frac{a}{b}) \neq 0$, 从而 $\deg Q(x) = nh$. 设 $\alpha \in \mathbb{F}_{q^n}$ 是 $P(x)$ 的一个根, 由 $\alpha \notin \mathbb{F}_q$ 知 $f(x) - \alpha g(x)$ 的次数为 h. 任取 $f(x) - \alpha g(x)$ 在 $\mathbb{F}_{q^n}$ 的某个扩域中的一个根 γ, 则一定有 $g(\gamma) \neq 0$. 事实上, 若 $g(\gamma) = 0$, 则有 $f(\gamma) = f(\gamma) - \alpha g(\gamma) = 0$, 故 γ 为 $f(x)$ 和 $g(x)$ 的公共根, 与 $f(x)$ 与 $g(x)$ 互素矛盾. 所以 $\alpha = \frac{f(\gamma)}{g(\gamma)}$, 从而 $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_q(\gamma)$. 进一步地, 由

$$Q(\gamma) = g(\gamma)^n P\left(\frac{f(\gamma)}{g(\gamma)}\right) = g(\gamma)^n P(\alpha) = 0$$

得到 γ 也是 $Q(x)$ 的根. 显然 $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^n}$, 我们有 $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=n$, 从而

$$[\mathbb{F}_q(\gamma):\mathbb{F}_q]=[\mathbb{F}_q(\gamma):\mathbb{F}_q(\alpha)]\cdot[\mathbb{F}_q(\alpha):\mathbb{F}_q]=n\cdot[\mathbb{F}_q(\gamma):\mathbb{F}_q(\alpha)]=n\cdot[\mathbb{F}_q(\gamma):\mathbb{F}_{q^n}]. \tag{5.4}$$

所以 $Q(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $Q(x)$ 的根 γ 在 $\mathbb{F}_q$ 上的次数为 $\deg Q(x)$, 即 $[\mathbb{F}_q(\gamma):\mathbb{F}_q]=nh$, 由式 (5.4) 知这也当且仅当 $[\mathbb{F}_q(\gamma):\mathbb{F}_{q^n}]=h$, 而后者显然也当且仅当 $f(x)-\alpha g(x)$ 在 $\mathbb{F}_{q^n}$ 上不可约. □

注意到在上面定理中, 若 $n=1$, 则在有些情形下我们也可以不要求 $f(x)$ 与 $g(x)$ 互素. 例如设 $P(x)=x+1$, $f(x)=x-1$, $g(x)=2x-2$, 则这时 $f(x)$ 与 $g(x)$ 不互素, 但是 $Q(x)=3x-3$ 与 $f(x)-(-1)g(x)=3x-3$ 都是不可约的. 特别地, 在定理 5.12 中令 $f(x)=ax+b$, $g(x)=cx+d$, 其中 $a,b,c,d\in\mathbb{F}_q$, 则 $f(x)$ 与 $g(x)$ 互素当且仅当 $ad-bc\neq 0$. 设 $P(x)$ 在 $\mathbb{F}_q$ 上不可约且 $\deg P(x)=n\geq 2$, 则对 $P(x)$ 的任一根 α, $f(x)-\alpha g(x)=(a-c\alpha)x+(b-d\alpha)$ 为一次多项式, 显然在 $\mathbb{F}_{q^n}$ 上不可约. 所以 $Q(x)=(cx+d)^nP(\frac{ax+b}{cx+d})$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $ad-bc\neq 0$. (大家可以对比定理 5.2 上面的一段说明)

下面取 $f(x)=x^t$ 且 $g(x)=1$, 则显然 $f(x)$ 与 $g(x)$ 互素. 设 $P(x)\in\mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约且 $\deg P(x)=n$, 在 $n=1$ 时还要设 $P(0)\neq 0$. 则由定理 5.12, 我们有 $Q(x)=P(x^t)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $x^t-\alpha\in\mathbb{F}_{q^n}[x]$ 在 $\mathbb{F}_{q^n}$ 上不可约, 其中 $\alpha\in\mathbb{F}_{q^n}$ 是 $P(x)$ 的一个根. 设 $e=\mathrm{ord}(\alpha)$, 即不可约多项式 $P(x)$ 的阶. 由定理 5.5, 我们有下面定理.

定理 5.13: 设正整数 $t\geq 2$, $P(x)\in\mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约且 $\deg P(x)=n$, 在 $n=1$ 时还要设 $P(0)\neq 0$, 设 $\mathrm{ord}(P(x))=e$ (e 也是 $P(x)$ 的任一根的阶). 则 $P(x^t)$ 在 $\mathbb{F}_q$ 上不可约当且仅当如下两个条件成立:

(i) t 的每个素因子整除 e 但是不整除 $\frac{q^n-1}{e}$.

(ii) 若 $4\mid t$, 则 $4\mid(q^n-1)$. □

对于任意正整数 $m\geq 2$, 定义 m 的根基 (记为 m^*) 为 m 的互不相同的素因子的乘积. 所以定理 5.13 中的条件 (i) 可以写成 $t^*\mid e$ 且 $\gcd(t^*,\frac{q^n-1}{e})=1$. 进一步地, 若定理 5.13 中的条件 (i) 和 (ii) 成立, 则 $P(x^t)$ 在 $\mathbb{F}_q$ 上不可约且 $\deg P(x^t)=nt$, 我们还容易证明 $\mathrm{ord}(P(x^t))=et$. 事实上, 因为 $P(x)$ 不可约且 $\mathrm{ord}(P(x))=e$, 所以 $P(x)\mid\Phi_e(x)$, 故 $P(x^t)\mid\Phi_e(x^t)$. 条件 (i) 告诉我们 t 的每个素因子都整除 e, 由第四章习题 4.5 有 $\Phi_{et}(x)=\Phi_e(x^t)$. 所以由 $P(x^t)\mid\Phi_{et}(x)$ 可得到 $\mathrm{ord}(P(x^t))=et$. 下面假设 $e\geq 2$ (这时阶为 e 的不可约多项式的常数项一定非零), 由定理 4.9, 域 $\mathbb{F}_q$ 上首一 n 次 e 阶不可约多项式存在当且仅当 $\mathrm{ord}_e(q)=n$ 且这样多项式的个数为 $N=\frac{\phi(e)}{n}$. 若 $P(x)$ 为 $\mathbb{F}_q$ 上首一 n 次 e 阶不可约多项式且 t 满足如上两个条件, 则 $P(x^t)$ 就是 $\mathbb{F}_q$ 上首一 nt 次 et 阶不可约多项式. 进一步地, 由于 $\mathrm{ord}_e(q)=n$, 由引理 5.3 得到 $\mathrm{ord}_{et}(q)=nt$. 同时由 $t^*\mid e$, 我们有 $\phi(et)=t\phi(e)$ (直接计算或者比较 $\Phi_{et}(x)=\Phi_e(x^t)$ 两边的次数), 故 $\mathbb{F}_q$ 上首一 nt 次 et 阶不可约多项式的个数为 $\frac{\phi(et)}{nt}=\frac{\phi(e)}{n}=N$. 这样我们便证明了如下定理.

定理 5.14: 设 $P_1(x), P_2(x), \ldots, P_N(x)$ 是 $\mathbb{F}_q$ 上所有互不相同的首一 n 次 e 阶不可约多项式, 正整数 $t \geq 2$ 满足下面两个条件:

(i) t 的每个素因子整除 e 但是不整除 $\frac{q^n-1}{e}$.

(ii) 若 $4 \mid t$, 则 $4 \mid (q^n-1)$.

则 $P_1(x^t), P_2(x^t), \ldots, P_N(x^t)$ 就是 $\mathbb{F}_q$ 上所有互不相同的首一 nt 次 et 阶不可约多项式. □

注意到在如上定理的叙述中我们并没有写出 $e \geq 2$, 实际上由于 $t \geq 2$ 而 $t^* \mid e$, 这一定有 $e \geq 2$.

在定理 5.12 中取 $f(x) = x^2+1$, $g(x) = x$, 则显然 $f(x)$ 与 $g(x)$ 互素且 $\frac{f(x)}{g(x)} = x + x^{-1}$. 设 $P(x) \in \mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约且 $\deg P(x) = n$, 则显然 $Q(x) = x^n P(x + x^{-1})$ 的次数为 $2n$. 进一步地, 由于

$$\widetilde{Q}(x) = x^{2n}Q(x^{-1}) = x^{2n}x^{-n}P(x^{-1}+x) = Q(x),$$

我们得到 $Q(x)$ 为自互反多项式. 下面我们区分 q 为偶数和奇数两种情形来讨论.

定理 5.15: 设 $q = 2^m$, $P(x) = \sum_{i=0}^{n} c_i x^i$ 为 $\mathbb{F}_q$ 上不可约多项式, $\deg P(x) = n$ 且 $c_0 \neq 0$, 则 $Q(x) = x^n P(x + x^{-1})$ 为 $\mathbb{F}_q$ 上的 $2n$ 次自互反多项式, 进一步地, $Q(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\frac{c_1}{c_0}) = 1$.

证明: 我们只需证定理的后半部分. 由定理 5.12, $Q(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $x^2+1-\alpha x$ 在 $\mathbb{F}_{q^n}$ 上不可约, 其中 $\alpha \in \mathbb{F}_{q^n}$ 是 $P(x)$ 的一个根, 这也等价于 $x^2+1-\alpha x$ 在 $\mathbb{F}_{q^n}$ 中无根. 利用 3.1 节最后的讨论, 这又等价于 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(\alpha^{-2}) = 1$. 由

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(\alpha^{-2}) = (\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(\alpha^{-1}))^2 = (\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^{-1})))^2 = \left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{c_1}{c_0}\right)\right)^2$$

便完成了定理的证明. □

定理 5.16: 设 q 为奇素数幂, $P(x)$ 为 $\mathbb{F}_q$ 上不可约多项式且 $\deg P(x) = n$, 则 $Q(x) = x^n P(x + x^{-1})$ 为 $\mathbb{F}_q$ 上的 $2n$ 次自互反多项式, 进一步地, $Q(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $P(2)P(-2) \notin \mathbb{F}_q^2$, 即 $P(2)P(-2)$ 为 $\mathbb{F}_q$ 中非平方元.

证明: 类似地 $Q(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $x^2-\alpha x+1$ 在 $\mathbb{F}_{q^n}$ 中无根, 其中 $\alpha \in \mathbb{F}_{q^n}$ 是 $P(x)$ 的一个根, 而这又等价于 $\alpha^2-4 \notin \mathbb{F}_{q^n}^2$, 即 $(\alpha^2-4)^{\frac{q^n-1}{2}} = -1$. 设 $P(x)$ 的首项系数为 a, 则有 $P(x) = a\prod_{i=0}^{n-1}(x-\alpha^{q^i})$, 故

$$\begin{aligned} P(2)P(-2) &= a^2\prod_{i=0}^{n-1}(2-\alpha^{q^i})(-2-\alpha^{q^i}) = a^2\prod_{i=0}^{n-1}(2-\alpha)^{q^i}(-2-\alpha)^{q^i} \\ &= a^2\prod_{i=0}^{n-1}(\alpha^2-4)^{q^i} = a^2(\alpha^2-4)^{\frac{q^n-1}{q-1}}. \end{aligned}$$

所以由

$$(\alpha^2-4)^{\frac{q^n-1}{2}} = \left((\alpha^2-4)^{\frac{q^n-1}{q-1}}\right)^{\frac{q-1}{2}} = \left(a^{-2}P(2)P(-2)\right)^{\frac{q-1}{2}} = (P(2)P(-2))^{\frac{q-1}{2}}$$

得知 $(P(2)P(-2))^{\frac{q-1}{2}}=-1$, 此条件等价于 $P(2)P(-2)\notin\mathbb{F}_q^2$. □

推论 5.17: 设 q 为奇素数幂, $P(x)$ 为 $\mathbb{F}_q$ 上不可约多项式且 $\deg P(x)=n$, 则 $R(x)=2^nx^nP(\frac{x+x^{-1}}{2})$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $P(1)P(-1)\notin\mathbb{F}_q^2$.

证明: 令 $P_0(x)=2^nP(\frac{x}{2})$, 在 $P_0(x)$ 上应用定理 5.16 即可. □

设 $p=\mathrm{char}\mathbb{F}_q$, 在定理 5.12 中取 $f(x)=x^p-x-b$, $g(x)=1$, 其中 $b\in\mathbb{F}_q$, 我们有如下结论.

定理 5.18: 设 p 为素数, $\mathrm{char}\mathbb{F}_q=p$, $b\in\mathbb{F}_q$, $P(x)=\sum_{i=0}^n c_ix^i$ 为 $\mathbb{F}_q$ 上首一 n 次不可约多项式, 则 $P(x^p-x-b)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(nb-c_{n-1})\neq 0$.

证明: 设 α 是 $P(x)$ 在 $\mathbb{F}_{q^n}$ 中的一个根, 由定理 5.12, $P(x^p-x-b)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $x^p-x-b-\alpha$ 在 $\mathbb{F}_{q^n}$ 上不可约. 由定理 5.7, 这等价于 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(b+\alpha)\neq 0$. 由

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(b+\alpha)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b+\alpha))=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(nb-c_{n-1}),$$

定理得证. □

设 p 为素数, q 为 p 的方幂. 在定理 5.12 中取 $f(x)=x^p-ax$ 和 $g(x)=1$, 其中 $a\in\mathbb{F}_q^*$. 设 $P(x)=x^n+\sum_{i=0}^{n-1}c_ix^i$ 为 $\mathbb{F}_q$ 上 n 次首一不可约多项式, α 是 $P(x)$ 在 $\mathbb{F}_{q^n}$ 中的一个根. 则 $P(x^p-ax)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $x^p-ax-\alpha\in\mathbb{F}_{q^n}[x]$ 在 $\mathbb{F}_{q^n}$ 上不可约. 由推论 5.8 知此条件等价于存在 $a_0\in\mathbb{F}_{q^n}^*$ 使得 $a=a_0^{p-1}$ 且 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\frac{\alpha}{a_0^p})\neq 0$. 由推论 5.8 后面的讨论可知存在 $a_0\in\mathbb{F}_{q^n}^*$ 使得 $a=a_0^{p-1}$ 当且仅当 $a^{\frac{q^n-1}{p-1}}=1$. 注意到 $a\in\mathbb{F}_q^*$, 所以 $a^{q-1}=1$. 令 $d=\gcd(\frac{q^n-1}{p-1},q-1)$, 则 $a^{\frac{q^n-1}{p-1}}=1$ 当且仅当 $a^d=1$. 由于

$$\frac{q^n-1}{q-1}=1+q+q^2+...+q^{n-1}\equiv n\,(\mathrm{mod}\ (p-1)),$$

所以

$$d=\gcd\left(\frac{q^n-1}{p-1},q-1\right)=\frac{q-1}{p-1}\gcd\left(\frac{q^n-1}{q-1},p-1\right)=\frac{q-1}{p-1}\gcd(n,p-1).$$

由此我们有如下定理.

定理 5.19: 设 p 为素数, $\mathrm{char}\mathbb{F}_q=p$, $a\in\mathbb{F}_q^*$, $P(x)=\sum_{i=0}^n c_ix^i$ 为 $\mathbb{F}_q$ 上 n 次首一不可约多项式, α 是 $P(x)$ 在 $\mathbb{F}_{q^n}$ 中的一个根. 则 $P(x^p-ax)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $a^{\frac{q-1}{p-1}\gcd(n,p-1)}=1$ 且 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\frac{\alpha}{a_0^p})\neq 0$, 其中 $a_0\in\mathbb{F}_{q^n}^*$ 且 $a=a_0^{p-1}$. □

特别地, 在定理 5.19 中, 若存在 $a_0\in\mathbb{F}_q^*$ 使得 $a=a_0^{p-1}$, 则这时 $a^{\frac{q-1}{p-1}\gcd(n,p-1)}=a_0^{(q-1)\gcd(n,p-1)}=1$ 自动成立. 又

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{\alpha}{a_0^p}\right)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\frac{\alpha}{a_0^p}\right)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{1}{a_0^p}\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)\right)=-\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{c_{n-1}}{a_0^p}\right).$$

这样我们便证明了如下推论.

推论 5.20: 设 p 为素数, $\mathrm{char}\mathbb{F}_q=p$, $a_0\in\mathbb{F}_q^*$, $P(x)=\sum_{i=0}^n c_ix^i$ 为 $\mathbb{F}_q$ 上 n 次首一不可约多项式. 则 $P(x^p-a_0^{p-1}x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{c_{n-1}}{a_0^p})\neq 0$. □

注意到定理 5.19 和推论 5.20 中与不可约多项式 $P(x)$ 复合的多项式都是 $\mathbb{F}_q$ 上的线性化多项式, 下面我们考虑一般的线性化多项式. 与前面一样, 设 p 为素数, $\mathrm{char}\mathbb{F}_q = p$. 设 $L(x) = \sum_{i=0}^{v} \ell_i x^{p^i}$, 其中 $\ell_i \in \mathbb{F}_q$, $0 \le i \le v$, 则 $L(x)$ 为 $\mathbb{F}_q$ 上的线性化多项式. 对于 $b \in \mathbb{F}_q$, 我们称 $L(x) - b$ 为 $\mathbb{F}_q$ 上的仿射多项式. 类似于推论 5.8 证明中的讨论, 由线性化多项式 $L(x)$ 确定的 $\mathbb{F}_q$ 到自身的映射 $\alpha \mapsto L(\alpha)$ 是 $\mathbb{F}_q$ 的线性变换 (把 $\mathbb{F}_q$ 看成是 $\mathbb{F}_p$ 上的线性空间). 若 $L(x)$ 在 $\mathbb{F}_q$ 中无非零根, 则 $\mathrm{Ker}(L) = \{0\}$, 故 L 为单射从而也是双射. 所以对任意 $b \in \mathbb{F}_q$, 一定存在 $\beta \in \mathbb{F}_q$ 使得 $L(\beta) = b$, 即仿射多项式 $L(x) - b$ 有根 $\beta \in \mathbb{F}_q$, 从而仿射多项式 $L(x) - b$ 在 $\mathbb{F}_q$ 上可约.

引理 5.21: 设 p 为素数, $\mathrm{char}\mathbb{F}_q = p$, 设 $L(x) = \sum_{i=0}^{v} \ell_i x^{p^i}$ 是 $\mathbb{F}_q$ 上的线性化多项式, 则存在线性化多项式 $G(x) \in \mathbb{F}_q[x]$ 和元素 $r \in \mathbb{F}_q$ 使得 $L(x) = G(x^p - x) + rx$. 进一步地, 若线性化多项式 $L(x)$ 有非零根 $a_0 \in \mathbb{F}_q^*$, 则存在线性化多项式 $G(x) \in \mathbb{F}_q[x]$ 使得 $L(x) = G(x^p - a_0^{p-1}x)$.

证明: 设 $L(x) = \sum_{i=0}^{v} \ell_i x^{p^i} \in \mathbb{F}_q[x]$, 我们对 v 做归纳. $v = 0$ 时结论显然成立. 设 $v \ge 1$, 则

$$L_1(x) = L(x) - \ell_v (x^p - x)^{p^{v-1}} = (\ell_{v-1} + \ell_v) x^{p^{v-1}} + \cdots$$

仍为 $\mathbb{F}_q$ 上的线性化多项式但次数 $\le p^{v-1}$. 由归纳假设存在线性化多项式 $G_1(x) \in \mathbb{F}_q[x]$ 和元素 $r_1 \in \mathbb{F}_q$ 使得 $L_1(x) = G_1(x^p - x) + r_1 x$, 从而

$$L(x) = G_1(x^p - x) + r_1 x + \ell_v (x^p - x)^{p^{v-1}}.$$

令 $G(x) = \ell_v x^{p^{v-1}} + G_1(x)$ 和 $r = r_1$, 则 $G(x)$ 为 $\mathbb{F}_q$ 上的线性化多项式且 $L(x) = G(x^p - x) + rx$.

进一步地, 设 $L(x)$ 有非零根 $a_0 \in \mathbb{F}_q^*$, 则 $L(a_0 x)$ 依然是 $\mathbb{F}_q$ 上的线性化多项式. 由前面的证明知存在线性化多项式 $G_2(x) \in \mathbb{F}_q[x]$ 和元素 $r_2 \in \mathbb{F}_q$ 使得

$$L(a_0 x) = G_2(x^p - x) + r_2 x.$$

在上式中令 $x = 1$, 则有 $0 = G_2(0) + r_2 = r_2$, 所以 $L(a_0 x) = G_2(x^p - x)$. 令 $G(x) = G_2(\frac{x}{a_0^p})$, 则有 $L(x) = G(x^p - a_0^{p-1}x)$. □

定理 5.22: 设 p 为素数, $\mathrm{char}\mathbb{F}_q = p$, 设 $L(x) = \sum_{i=0}^{v} \ell_i x^{p^i}$ 是 $\mathbb{F}_q$ 上的首一线性化多项式且 $\deg L(x) = p^v$, 其中 $v \ge 2$, 设 $b \in \mathbb{F}_q^*$. 则仿射多项式 $L(x) - b$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $p = v = 2$ 且 $L(x)$ 形如

$$L(x) = x(x + a_0)(x^2 + a_0 x + b_0), \tag{5.5}$$

其中 $a_0, b_0 \in \mathbb{F}_q^*$ 并且二次多项式 $x^2 + a_0 x + b_0$ 和 $x^2 + b_0 x + b$ 均在 $\mathbb{F}_q$ 上不可约.

证明: 先证必要性, 假设对 $b \in \mathbb{F}_q^*$, $L(x) - b$ 在 $\mathbb{F}_q$ 上不可约. 则由引理 5.21 前面的说明, 线性化多项式 $L(x)$ 一定有非零根 $a_0 \in \mathbb{F}_q^*$. 有引理 5.21 知存在线性化多项式 $G(x) \in \mathbb{F}_q[x]$ 使得 $L(x) = G(x^p - a_0^{p-1}x)$. 令 $\overline{G}(x) = G(x) - b$, 则 $\overline{G}(x^p - a_0^{p-1}x) = L(x) - b$. 由于 $L(x) - b$ 在 $\mathbb{F}_q$ 上不可约, 则 $\overline{G}(x)$ 也必在 $\mathbb{F}_q$ 上不可约. 由 $L(x)$ 首一显然得到 $G(x)$ 和 $\overline{G}(x)$ 都是首一的,

同时由 $\deg L(x)=p^v$ 可得到 $\deg G(x)=\deg \overline{G}(x)=p^{v-1}$. 记 $n=p^{v-1}$ 且设

$$\overline{G}(x)=x^n+\sum_{i=0}^{n-1}c_ix^i,$$

其中 $c_i\in\mathbb{F}_q$, $0\le i\le n-1$. 因为多项式 $\overline{G}(x)$ 和 $\overline{G}(x^p-a_0^{p-1}x)=L(x)-b$ 均在 $\mathbb{F}_q$ 上不可约, 由推论 5.20 有

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{c_{n-1}}{a_0^p}\right)\neq 0, \tag{5.6}$$

由此可推出 $c_{n-1}\neq 0$. 但是 $\overline{G}(x)$ 为仿射多项式, 次数为 $n=p^{v-1}$, 所以其次高项次数为 $n-1=p^{v-1}-1\le p^{v-2}$, 即 $(p-1)p^{v-2}\le 1$. 由此可推出 $p=v=2$, 从而 $n=2$ 且 $G(x)=x^2+b_0x$, 其中 $b_0\in\mathbb{F}_q$, 所以 $\overline{G}(x)=x^2+b_0x+b$ 且

$$L(x)=G(x^2-a_0x)=(x^2-a_0x)^2+b_0(x^2-a_0x)=x(x-a_0)(x^2-a_0x+b_0).$$

比较多项式 $\overline{G}(x)$ 的各项系数, 我们得到 $b_0=c_{n-1}$, 所以式 (5.6) 可写为 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{b_0}{a_0^2})\neq 0$. 由推论 5.8 得到 $x^2+a_0x+b_0$ 在 $\mathbb{F}_q$ 上不可约, 而 $x^2+b_0x+b=\overline{G}(x)$ 在 $\mathbb{F}_q$ 上的不可约性前面已经得到.

下证充分性. 这时 $p=2$, $L(x)$ 形如

$$L(x)=x(x+a_0)(x^2+a_0x+b_0),$$

其中 $a_0,b_0\in\mathbb{F}_q^*$ 并且二次多项式 $x^2+a_0x+b_0$ 和 x^2+b_0x+b 均在 $\mathbb{F}_q$ 上不可约. 令 $\overline{G}(x)=x^2+b_0x+b$, 则

$$L(x)-b=(x^2+a_0x)^2+b_0(x^2+a_0x)+b=\overline{G}(x^2+a_0x).$$

因为 $x^2+a_0x+b_0$ 在 $\mathbb{F}_q$ 上不可约, 由推论 5.8 得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{b_0}{a_0^2})\neq 0$. 再由 $\overline{G}(x)$ 在 $\mathbb{F}_q$ 上不可约, 由推论 5.20 得到 $\overline{G}(x^2+a_0x)$ 在 $\mathbb{F}_q$ 上不可约, 即仿射多项式 $L(x)-b$ 在 $\mathbb{F}_q$ 上不可约. □

综合定理 5.12 和 5.22, 我们有如下定理.

定理 5.23: 设 p 为素数, $\mathrm{char}\mathbb{F}_q=p$, 设 $L(x)=\sum_{i=0}^{v}\ell_ix^{p^i}$ 是 $\mathbb{F}_q$ 上的首一线性化多项式且 $\deg L(x)=p^v$, 其中 $v\ge 2$, 设 $P(x)=x^n+\sum_{i=0}^{n-1}c_ix^i$ 为 $\mathbb{F}_q$ 上的首一 n 次不可约多项式. 则 $P(L(x))$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $p=v=2$, n 为奇数, $L(x)$ 形如 $L(x)=x(x+a_0)(x^2+a_0x+b_0)$, 其中 $a_0,b_0\in\mathbb{F}_q^*$ 并且二次多项式 $x^2+a_0x+b_0$ 和 $x^2+b_0x+c_{n-1}$ 均在 $\mathbb{F}_q$ 上不可约.

证明: 由定理 5.12, 设 α 是 $P(x)$ 在 $\mathbb{F}_{q^n}$ 中的一个根, 则 $P(L(x))$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $L(x)-\alpha$ 在 $\mathbb{F}_{q^n}$ 上不可约. 由定理 5.22 得到 $P(L(x))$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $p=v=2$, $L(x)$ 形如 $L(x)=x(x+a_0)(x^2+a_0x+b_0)$, 其中 $a_0,b_0\in\mathbb{F}_{q^n}^*$ 并且二次多项式 $x^2+a_0x+b_0$ 和 $x^2+b_0x+\alpha$ 均在 $\mathbb{F}_{q^n}$ 上不可约.

下面设 $p=v=2$, $L(x)$ 形如 $L(x)=x(x+a_0)(x^2+a_0x+b_0)$, 其中 $a_0,b_0\in\mathbb{F}_{q^n}^*$ 并且二次多项式 $x^2+a_0x+b_0$ 在 $\mathbb{F}_{q^n}$ 上不可约. 注意到 $\frac{L(x)}{x}\in\mathbb{F}_q[x]$ 但在 $\mathbb{F}_{q^n}$ 上有 $\frac{L(x)}{x}=(x+a_0)(x^2+a_0x+b_0)$. 如果 $\frac{L(x)}{x}$ 在 $\mathbb{F}_q$ 上不可约, 因为 $\frac{L(x)}{x}$ 在 $\mathbb{F}_{q^n}$ 中有根 a_0, 则 $\frac{L(x)}{x}$ 的

根为 a_0 在 $\mathbb{F}_q$ 上的共轭元素, 依然在 $\mathbb{F}_{q^n}$ 中, 故 $\frac{L(x)}{x}$ 可分解为 $\mathbb{F}_{q^n}$ 上 3 个一次因式之积, 与 $x^2+a_0x+b_0$ 在 $\mathbb{F}_{q^n}$ 上不可约矛盾, 所以 $\frac{L(x)}{x}$ 在 $\mathbb{F}_q$ 上可约. 另外, 若 $\frac{L(x)}{x}$ 可分解为 $\mathbb{F}_q$ 上 3 个一次因式之积, 则 $\frac{L(x)}{x}$ 也可分解为 $\mathbb{F}_{q^n}$ 上 3 个一次因式之积, 同样矛盾. 由此我们得到 $\frac{L(x)}{x}$ 可分解为 $\mathbb{F}_q$ 上 1 个一次因式和 1 个二次不可约因式的乘积. 由于 $\frac{L(x)}{x}$ 在 $\mathbb{F}_{q^n}$ 上的完全分解为 $\frac{L(x)}{x}=(x+a_0)(x^2+a_0x+b_0)$, 再由分解的唯一性得知如上分解也是 $\frac{L(x)}{x}$ 在 $\mathbb{F}_q$ 上的完全分解, 所以 $a_0,b_0\in\mathbb{F}_q^*$. 由于二次多项式 $x^2+a_0x+b_0\in\mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约, 同时在 $\mathbb{F}_{q^n}$ 上也不可约, 由推论 2.14 得到 n 与 2 互素, 所以 n 为奇数. 进一步地, 若 $x^2+a_0x+b_0\in\mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约且 n 为奇数, 则由推论 2.14 可得 $x^2+a_0x+b_0$ 在 $\mathbb{F}_{q^n}$ 上依然不可约. 由于

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{\alpha}{b_0^2}\right)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\frac{\alpha}{b_0^2}\right)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{1}{b_0^2}\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)\right)=-\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{c_{n-1}}{b_0^2}\right),$$

推论 5.8 告诉我们 $x^2+b_0x+\alpha$ 在 $\mathbb{F}_{q^n}$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\frac{\alpha}{b_0^2})\neq 0$, 这也当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{c_{n-1}}{b_0^2})\neq 0$, 仍由推论 5.8, 后者成立当且仅当 $x^2+b_0x+c_{n-1}$ 在 $\mathbb{F}_q$ 上不可约. 这便完成了定理的证明. □

5.3 多项式的复合乘积

本节我们定义两个多项式的另一种复合, 即基于根的复合, 或称为多项式的复合乘积. 我们将通过两个次数互素的不可约多项式得到次数为这两个互素次数乘积的不可约多项式, 这种做法来源于 Brawley 和 Carlitz.

设 Γ 为域 $\mathbb{F}_q$ 的代数闭包, 即 $\mathbb{F}_q$ 上的任一多项式的根都在 Γ 中. 设 σ 为 Γ 的 Frobenius 自同构, 即对任意 $\alpha\in\Gamma$, $\sigma(\alpha)=\alpha^q$. 设 G 是 Γ 的非空子集且在 σ 下不变, 即对任意 $\alpha\in G$, 有 $\sigma(\alpha)=\alpha^q\in G$. 进一步地, 设 G 上有一个二元运算 $\diamond$ 且 σ 保持运算 $\diamond$, 即对任意 $\alpha,\beta\in G$, 有 $\sigma(\alpha\diamond\beta)=\sigma(\alpha)\diamond\sigma(\beta)$. 这表明 σ 是代数结构 $(G,\diamond)$ 的一个自同态 (实际上也是自同构, 因为 σ 在 Γ 上为单射, 自然也是 G 上的单射, 又对任意 $\alpha\in G$, 一定有某个正整数 n 使得 $\alpha\in\mathbb{F}_{q^n}$, 从而 $\alpha^{q^n}=\alpha$, 即 $\sigma(\alpha^{q^{n-1}})=\alpha$, 故 σ 也是 G 上的满射). 记 $M_{G,q}[x]$ 表示所有根在 G 中的 $\mathbb{F}_q$ 上次数 ≥ 1 的首一多项式的集合. 对于 $f(x),g(x)\in M_{G,q}[x]$, 定义

$$(f\diamond g)(x)=\prod_{\alpha}\prod_{\beta}(x-\alpha\diamond\beta), \tag{5.6}$$

其中的乘积跑遍 $f(x)$ 的所有根 α 和 $g(x)$ 的所有根 β (根包括重数), 称 $(f\diamond g)(x)$ 为多项式 $f(x)$ 和 $g(x)$ (由 G 上的运算 $\diamond$ 诱导) 的复合乘积. 显然若 $\deg f(x)=m$ 且 $\deg g(x)=n$, 则 $\deg(f\diamond g)(x)=mn$.

例 5.3: (a) 设 $G=\Gamma\setminus\{0\}$, 对于 $\alpha,\beta\in G$, 定义 $\alpha\diamond\beta=\alpha\beta$, 即运算 $\diamond$ 为域 Γ 中的乘法, 这时代数结构 $(G,\diamond)$ 恰为 Γ 的乘法群, 而式 (5.6) 定义的复合乘积 $\diamond$ 称为复合乘法, 记为 $\odot$, 即式

(5.6) 可改写为

$$(f \odot g)(x) = \prod_{\alpha} \prod_{\beta} (x - \alpha\beta).$$

设 $f(x), g(x) \in \mathbb{F}_q[x]$, $\deg f(x) = m$, $\deg g(x) = n$, 且 $f(x)$ 与 $g(x)$ 无零根, 则容易得到

$$(f \odot g)(x) = \prod_{\alpha} \prod_{\beta} \alpha \left(\frac{x}{\alpha} - \beta\right) = \prod_{\alpha} \alpha^n g\left(\frac{x}{\alpha}\right).$$

同理可得 $(f \odot g)(x) = \prod_{\beta} \beta^m f(\frac{x}{\beta})$. 例如, 设 $q = 2$, $f(x) = x^2 + x + 1$, $g(x) = x^3 + x + 1$, 设 α 为 $f(x)$ 的一个根, β 为 $g(x)$ 的一个根, 则有 $f(x) = (x - \alpha)(x - \alpha^2)$, $g(x) = (x - \beta)(x - \beta^2)(x - \beta^4)$ 且 $\alpha^2 = \alpha + 1$, $\beta^3 = \beta + 1$. 故

$$(f \odot g)(x) = (x^3 + \alpha^2 x + 1)(x^3 + \alpha x + 1) = x^6 + x^4 + x^2 + x + 1.$$

(b) 设 $G = \Gamma$, 对于 $\alpha, \beta \in G$, 定义 $\alpha \diamond \beta = \alpha + \beta$, 这时代数结构 $(G, \diamond)$ 恰为 Γ 的加法群, 而式 (5.6) 定义的复合乘积 $\diamond$ 称为复合加法, 记为 $\oplus$, 即对任意首一多项式 $f(x), g(x) \in \mathbb{F}_q[x]$, 式 (5.6) 可改写为

$$(f \oplus g)(x) = \prod_{\alpha} \prod_{\beta} (x - (\alpha + \beta)).$$

类似地, 我们有 $(f \oplus g)(x) = \prod_{\alpha} g(x - \alpha) = \prod_{\beta} f(x - \beta)$. 例如, 对于上面 (a) 中 $\mathbb{F}_2$ 上的多项式 $f(x) = x^2 + x + 1$ 和 $g(x) = x^3 + x + 1$, 可以计算出 $(f \oplus g)(x) = x^6 + x^5 + x^3 + x^2 + 1$.

(c) 设 G 为 Γ 的一个 σ-不变子集, 对于 $\alpha, \beta \in G$, 定义 $\alpha \diamond \beta = \Psi(\alpha, \beta)$, 其中 $\Psi(x, y) \in \mathbb{F}_q[x, y]$, 即 $\mathbb{F}_q$ 上的二元多项式, 且满足对任意 $\alpha, \beta \in G$, 有 $\Psi(\alpha, \beta) \in G$. 容易验证, σ 保持这里的运算 $\diamond$. 特别地, 取 $G = \Gamma \setminus \{0\}$ 和 $\Psi(x, y) = xy$, 则得到复合乘法, 若取 $G = \Gamma$ 和 $\Psi(x, y) = x + y$, 则得到复合加法. 所以这里的复合乘积是复合乘法和复合加法的推广.

在例 5.3 的 (a) 和 (b) 中我们看到, 虽然定义复合乘积时多项式 $f(x)$ 和 $g(x)$ 的根在 $\mathbb{F}_2$ 的扩域中, 但最后计算出的结果 $(f \odot g)(x)$ 和 $(f \oplus g)(x)$ 却是 $\mathbb{F}_2$ 上的多项式. 事实上, 这对一般的复合乘积也对, 我们有下面定理.

定理 5.24: 设 $f(x), g(x) \in M_{G,q}[x]$, 则 $(f \diamond g)(x)$ 依然属于 $M_{G,q}[x]$.

证明: 多项式 $(f \diamond g)(x)$ 显然首一且次数 ≥ 1, 下面我们只需证明它的系数都在 $\mathbb{F}_q$ 中. 注意到 $\mathbb{F}_q$ 上多项式的根在 σ 作用下依然是此多项式的根, 所以若 α 跑遍多项式 $f(x) \in \mathbb{F}_q[x]$ 的所有根, 则 $\sigma(\alpha) = \alpha^q$ 也跑遍 $f(x)$ 的所有根, 对多项式 $g(x)$ 也如此. 设 $(f \diamond g)(x) = \sum_{i=0}^{h} A_i x^i$, 其中 $A_i \in \Gamma$, $0 \leq i \leq h$. 则由

$$((f \diamond g)(x))^q = \prod_{\alpha} \prod_{\beta} (x - \alpha \diamond \beta)^q = \prod_{\alpha} \prod_{\beta} (x^q - \alpha^q \diamond \beta^q) = \prod_{\alpha} \prod_{\beta} (x^q - \alpha \diamond \beta) = (f \diamond g)(x^q)$$

得到

$$\sum_{i=0}^{h} A_i^q x^{iq} = \sum_{i=0}^{h} A_i x^{iq},$$

所以对任意 $i = 0, 1, \ldots, h$, 有 $A_i^q = A_i$, 即 $A_i \in \mathbb{F}_q$. □

定理 5.24 告诉我们如式 (5.6) 定义的复合乘积 $\diamond$ 也是集合 $M_{G,q}[x]$ 上的运算. 又显然可得若 G 上的运算 $\diamond$ 满足结合律 (或交换律), 则 $M_{G,q}[x]$ 上的运算 $\diamond$ 也满足结合律 (或交换律). 进一步地, 设 $f(x), g(x), h(x) \in M_{G,q}[x]$, 且 $f(x)$ 的所有根为 $\alpha_1, \ldots, \alpha_m$, $g(x)$ 的所有根为 $\beta_1, \ldots, \beta_n$, $h(x)$ 的所有根为 $\beta_{n+1}, \ldots, \beta_{n+k}$, 则 $g(x)h(x)$ 的所有根为 $\beta_1, \ldots, \beta_n, \beta_{n+1}, \ldots, \beta_{n+k}$, 所以

$$(f\diamond(gh))(x) = \prod_{i=1}^{m}\prod_{j=1}^{n+k}(x-\alpha_i\diamond\beta_j) = \prod_{i=1}^{m}\prod_{j=1}^{n}(x-\alpha_i\diamond\beta_j)\prod_{i=1}^{m}\prod_{j=n+1}^{n+k}(x-\alpha_i\diamond\beta_j) = (f\diamond g)(x)(f\diamond h)(x).$$

更一般地, 我们容易证明, 对任意 $f_1(x), \cdots, f_s(x), g_1(x), \ldots, g_t(x) \in M_{G,q}[x]$, 有

$$\left(\prod_{i=1}^{s} f_i \diamond \prod_{j=1}^{t} g_j\right)(x) = \prod_{i=1}^{s}\prod_{j=1}^{t}\left(f_i \diamond g_j\right)(x). \tag{5.7}$$

定理 5.25: 设代数结构 $(G,\diamond)$ 是群, $f(x), g(x) \in M_{G,q}[x]$ 且 $\deg f(x) = m$, $\deg g(x) = n$, 则 $(f \diamond g)(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $f(x)$ 和 $g(x)$ 均在 $\mathbb{F}_q$ 上不可约且 m 与 n 互素.

证明: 设 $(f \diamond g)(x)$ 在 $\mathbb{F}_q$ 上不可约, 则由式 (5.7) 知 $f(x)$ 和 $g(x)$ 均在 $\mathbb{F}_q$ 上不可约. 记 $d = \gcd(m, n)$, 若 $d > 1$, 设 $m = dr$, $n = ds$, 则 r 与 s 互素. 设 α 和 β 分别为 $f(x)$ 和 $g(x)$ 的一个根, 令 $\gamma = \alpha \diamond \beta$, 则 γ 是 $(f \diamond g)(x)$ 的一个根. 由于 $(f \diamond g)(x)$ 在 $\mathbb{F}_q$ 上不可约, 所以 γ 在 $\mathbb{F}_q$ 上的极小多项式为 $(f \diamond g)(x)$, 故 γ 的次数为 $\deg(f \diamond g)(x) = mn$. 但 $drs < mn$, 又

$$\gamma^{q^{drs}} = \alpha^{q^{ms}} \diamond \beta^{q^{nr}} = \alpha \diamond \beta = \gamma,$$

这与 $\deg\gamma = mn$ 矛盾. 所以 $d = 1$, 即 m 与 n 互素.

反之, 设 $f(x)$ 和 $g(x)$ 均在 $\mathbb{F}_q$ 上不可约且 m 与 n 互素. 仍设 α 和 β 分别为 $f(x)$ 和 $g(x)$ 的一个根且令 $\gamma = \alpha \diamond \beta$, 则有 $\deg\alpha = m$, $\deg\beta = n$. 为证明 $(f \diamond g)(x)$ 在 $\mathbb{F}_q$ 上不可约, 我们只需证它的根 γ 的次数为 mn 即可. 记 $k = \deg\gamma$, 由于 $\gamma^{q^{mn}} = \alpha^{q^{mn}} \diamond \beta^{q^{mn}} = \alpha \diamond \beta = \gamma$, 所以 $q^{mn} \equiv 1 \,(\mathrm{mod}\ \mathrm{ord}(\gamma))$, 其中 $\mathrm{ord}(\gamma)$ 是 γ 在 Γ 的乘法群中的阶. 又 k 为 q 模 $\mathrm{ord}(\gamma)$ 的乘法阶, 我们有 $k \mid mn$. 另一方面, 由 $\gamma^{q^k} = \gamma$ 得到 $\alpha^{q^k} \diamond \beta^{q^k} = \alpha \diamond \beta$, 两边同时 q^k 幂得到 $\alpha^{q^{2k}} \diamond \beta^{q^{2k}} = \alpha^{q^k} \diamond \beta^{q^k} = \alpha \diamond \beta$. 继续这个过程, 我们有对任意 $t \geq 0$ 有

$$\alpha^{q^{tk}} \diamond \beta^{q^{tk}} = \alpha \diamond \beta. \tag{5.8}$$

在 (5.8) 中令 $t = m$, 则有 $\alpha^{q^{mk}} \diamond \beta^{q^{mk}} = \alpha \diamond \beta$, 即 $\alpha \diamond \beta^{q^{mk}} = \alpha \diamond \beta$. 由于 $(G,\diamond)$ 为群, 由消去律我们得到 $\beta^{q^{mk}} = \beta$. 再由 q 模 $\mathrm{ord}(\beta)$ 的乘法阶为 n 以及 $q^{mk} \equiv 1 \,(\mathrm{mod}\ \mathrm{ord}(\beta))$ 得到 $n \mid mk$, 又 m 与 n 互素, 所以我们有 $n \mid k$. 同理我们可以得到 $m \mid k$, 仍由 m 与 n 互素就有 $mn \mid k$. 所以 $\deg\gamma = k = mn$. □

复合乘法对应的 G 是 Γ 的乘法群, 复合加法对应的 G 是 Γ 的加法群, 由定理 5.25 我们有下面的推论.

推论 5.26: 设 $f(x)$ 和 $g(x)$ 为 $\mathbb{F}_q$ 上的常数项非零的首一不可约多项式, $\deg f(x) = m$, $\deg g(x) = n$ 且 $\gcd(m, n) = 1$. 则 $(f \odot g)(x)$ 和 $(f \oplus g)(x)$ 都是 $\mathbb{F}_q$ 上的 mn 次不可约多项式. □

常数项为 0 的首一不可约多项式只有 x, 显然对任意首一多项式 $g(x) \in \mathbb{F}_q[x]$ 且 $\deg g(x) = n$, 我们有 $x \odot g(x) = x^n$ 而 $x \oplus g(x) = g(x)$. 下面我们讨论如何计算多项式 $f(x)$ 和 $g(x)$ 的复合乘积 $(f \diamond g)(x)$. 自然我们可以利用定义, 即式 (5.6) 来计算, 但这需要我们要找到 $f(x)$ 与 $g(x)$ 的根, 还要在 $\mathbb{F}_q$ 的某个扩域中做运算. 然而在某些特殊情形下, 通过矩阵的 Kronecker 乘积可使计算在 $\mathbb{F}_q$ 中进行.

设 $A = (a_{ij})_{m\times s}$ 和 $B = (b_{ij})_{n\times t}$ 分别是域 $\mathbb{F}_q$ 上的 $m \times s$ 和 $n \times t$ 矩阵, 定义

$$A \otimes B = (a_{ij}B) = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1s}B \\ a_{21}B & a_{22}B & \cdots & a_{2s}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{ms}B \end{bmatrix},$$

其中 $a_{ij}B$ 是元素 a_{ij} 和矩阵 B 的数量乘积. 显然 $A \otimes B$ 是一个 $\mathbb{F}_q$ 上的 $mn \times st$ 矩阵, 称为矩阵 A 和 B 的 Kronecker 乘积. 容易验证 $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$, 其中 A, B, C, D 是行列数适合如上运算的 $\mathbb{F}_q$ 上的任意矩阵. 所以若 A 和 B 均为 $\mathbb{F}_q$ 上的可逆矩阵, 则 $A \otimes B$ 也可逆且 $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$. 设 α, β 分别为 m 阶矩阵 A 和 n 阶矩阵 B 的特征值, 对应的特征向量分别为 $\mathbf{x}$ 和 $\mathbf{y}$. 则由

$$(A \otimes B)(\mathbf{x} \otimes \mathbf{y}) = A\mathbf{x} \otimes B\mathbf{y} = \alpha\mathbf{x} \otimes \beta\mathbf{y} = \alpha\beta(\mathbf{x} \otimes \mathbf{y}),$$

和 $\mathbf{x} \otimes \mathbf{y} \neq \mathbf{0}$ 得到 $\alpha\beta$ 是 $A \otimes B$ 的特征值. 注意到我们讨论的特征值和特征向量都在 $\mathbb{F}_q$ 的代数闭包 Γ 中考虑, n 阶矩阵必然有 n 个特征值 (包括重数), 所以若矩阵 A 的全部特征值为 $\alpha_1, \alpha_2, \ldots, \alpha_m$, 矩阵 B 的全部特征值为 $\beta_1, \beta_2, \ldots, \beta_n$, 由特征值的个数就得到 $A \otimes B$ 的全部特征值为 $\alpha_i\beta_j$, $1 \leq i \leq m$, $1 \leq j \leq n$. 一般地, 对任意 $c_{st} \in \mathbb{F}_q$, $c_{st}(A^s \otimes B^t)$ 的全部特征值为 $c_{st}\alpha_i^s\beta_j^t$, $1 \leq i \leq m$, $1 \leq j \leq n$, 其中这里的 A^s 和 B^t 是在通常的矩阵乘法 (而不是 Kronecker 乘积) 下的方幂.

给定多项式 $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[x]$, 由第 2.4 节我们知道 $f(x)$ 的伴随矩阵为

$$A = \begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{m-2} \\ & & & 1 & -a_{m-1} \end{bmatrix}, \tag{5.9}$$

其中的空白处为省略的 0. 容易计算得出矩阵 A 的特征多项式 $\det(xI_m - A)$ 就是多项式 $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$, 所以一个多项式的根就是它的伴随矩阵的特征值.

设 $f(x), g(x) \in \mathbb{F}_q[x]$, $\deg f(x) = m$, $\deg g(x) = n$ 且 $f(x)$ 和 $g(x)$ 的伴随矩阵分别为 A 和 B, 由上面的讨论可知 $(f \odot g)(x)$ 就是矩阵 $A \otimes B$ 的特征多项式. 更一般地, 设 $\diamond$ 是由例 5.3 中 (c)

定义的 G 上的运算, 即对于 $\alpha, \beta \in G$, $\alpha \diamond \beta = \Psi(\alpha, \beta)$, 其中 $\Psi(x, y) = \sum_{s,t} c_{st} x^s y^t \in \mathbb{F}_q[x, y]$, 则容易得到 $(f \diamond g)(x)$ 是矩阵 $\sum_{s,t} c_{st}(A^s \otimes B^t)$ 的特征多项式. 由于复合加法 $\oplus$ 就是 $\Psi(x, y) = x + y$ 的情形, 我们有 $(f \oplus g)(x)$ 为矩阵 $A \otimes I_n + I_m \otimes B$ 的特征多项式. 所以我们有如下定理.

定理 5.27: 设 $f(x), g(x) \in \mathbb{F}_q[x]$, $\deg f(x) = m$, $\deg g(x) = n$ 且 A 和 B 分别是 $f(x)$ 和 $g(x)$ 的伴随矩阵, 则 $(f \odot g)(x) = \det(xI_{mn} - A \otimes B)$, $(f \oplus g)(x) = \det(xI_{mn} - (A \otimes I_n + I_m \otimes B))$. □

例 5.4: 设 $q = 2$, $f(x) = x^2 + x + 1$, $g(x) = x^3 + x + 1$, 则 $f(x)$ 和 $g(x)$ 都是 $\mathbb{F}_2$ 上的不可约多项式. 容易得到 $f(x)$ 和 $g(x)$ 的伴随矩阵分别为

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \qquad \text{和} \qquad B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

故有

$$A \otimes B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

和

$$A \otimes I_3 + I_2 \otimes B = \begin{bmatrix} 0 & I_3 \\ I_3 & I_3 \end{bmatrix} + \begin{bmatrix} B & 0 \\ 0 & B \end{bmatrix} = \begin{bmatrix} B & I_3 \\ I_3 & I_3 + B \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

计算它们的特征多项式, 我们得到 $(f \odot g)(x) = x^6 + x^4 + x^2 + x + 1$ 和 $(f \oplus g)(x) = x^6 + x^5 + x^3 + x^2 + 1$. 大家可以对比本例和例 5.3 在计算时所用的方法. 由于 $f(x)$ 与 $g(x)$ 都在 $\mathbb{F}_2$ 上不可约, 又它们的次数互素, 所以得到的 $(f \odot g)(x)$ 和 $(f \oplus g)(x)$ 都是 $\mathbb{F}_2$ 上的 6 次不可约多项式. 进一步地, 可以算出 $\mathrm{ord}((f \odot g)(x)) = 21$ 而 $\mathrm{ord}((f \oplus g)(x)) = 63$, 即多项式 $(f \oplus g)(x)$ 在 $\mathbb{F}_2$ 上本原. □

注意到利用多项式的伴随矩阵的特征多项式来计算复合乘积时需要计算 mn 阶的行列式, 这也是十分复杂的. 下面这个结论可以把要计算的行列式的阶降到 m 或者 n.

定理 5.28: 设 $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j$ 是 $\mathbb{F}_q$ 上两个常数项非零的首一多项式, 次

数分别为 m 和 n, 伴随矩阵分别为 A 和 B. 则有

$$(f \odot g)(x) = \det\left(\sum_{j=0}^{n} b_j x^j A^{n-j}\right) = \det\left(\sum_{i=0}^{m} a_i x^i B^{m-i}\right),$$

和

$$(f \oplus g)(x) = \det\left(\sum_{j=0}^{n} b_j (xI_m - A)^j\right) = \det\left(\sum_{i=0}^{m} a_i (xI_n - B)^i\right).$$

证明: 设 $f(x)$ 的根 (即矩阵 A 的特征值) 为 $\alpha_1, \alpha_2, \ldots, \alpha_m$, 记 D 为上三角矩阵

$$D = \begin{bmatrix} \alpha_1 & * & \cdots & * \\ & \alpha_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & \alpha_m \end{bmatrix}.$$

则存在可逆矩阵 P 使得 $A = PDP^{-1}$, 从而

$$\begin{aligned}
(f \oplus g)(x) &= \det(xI_{mn} - (A \otimes I_n + I_m \otimes B)) \\
&= \det(xI_{mn} - ((PDP^{-1}) \otimes I_n + (PI_mP^{-1}) \otimes B)) \\
&= \det((P \otimes I_n)(xI_{mn} - (D \otimes I_n + I_m \otimes B))(P \otimes I_n)^{-1}) \\
&= \det(xI_{mn} - (D \otimes I_n + I_m \otimes B)) \\
&= \det\begin{pmatrix} xI_n - \alpha_1 I_n - B & & * \\ & \ddots & \\ & & xI_n - \alpha_m I_n - B \end{pmatrix} \\
&= \prod_{i=1}^{m} \det((xI_n - B) - \alpha_i I_n) \\
&= \det\left(\prod_{i=1}^{m} ((xI_n - B) - \alpha_i I_n)\right) \\
&= \det(f(xI_n - B)).
\end{aligned}$$

类似地, 由 $(f \oplus g)(x) = (g \oplus f)(x)$ 可得 $(f \oplus g)(x) = \det(g(xI_m - A))$. 同样地, 可以证明 $(f \odot g)(x)$ 的情形. □

例 5.4: (继续) $f(x) = x^2 + x + 1$, $g(x) = x^3 + x + 1$, 则

$$f(xI_3 - B) = \begin{pmatrix} x & 0 & 1 \\ 1 & x & 1 \\ 0 & 1 & x \end{pmatrix}^2 + \begin{pmatrix} x & 0 & 1 \\ 1 & x & 1 \\ 0 & 1 & x \end{pmatrix} + I_3 = \begin{pmatrix} x^2+x+1 & 1 & 1 \\ 1 & x^2+x & 0 \\ 1 & 1 & x^2+x \end{pmatrix}$$

所以 $(f \oplus g)(x) = \det(f(xI_3 - B)) = x^6 + x^5 + x^3 + x^2 + 1$. □

例 5.5: 设 $\alpha, \beta \in \Gamma^*$ 且 $\mathrm{ord}(\alpha) = s$, $\mathrm{ord}(\beta) = t$, 若 $\gcd(s,t) = 1$, 则 $\mathrm{ord}(\alpha\beta) = st$. 我们知道分圆多项式 $\Phi_s(x)$ 的根为 Γ^* 中所有阶为 s 的元素, $\Phi_t(x)$ 的根为所有阶为 t 的元素. 在 $\gcd(s,t) = 1$ 时所有阶为 s 的元素乘以所有阶为 t 的元素就得到所有阶为 st 的元

素, 从而 $(\Phi_s \odot \Phi_t)(x) = \Phi_{st}(x)$. 这个结论可有助于分解分圆多项式, 例如在 $\mathbb{F}_2$ 上分解 $\Phi_{21}(x)$, 我们有 $\Phi_{21}(x) = (\Phi_3 \odot \Phi_7)(x)$. $\Phi_3(x) = x^2 + x + 1$ 在 $\mathbb{F}_2$ 上不可约, 由例 4.3 知 $\Phi_7(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$ 为 $\mathbb{F}_2$ 上两个 3 次不可约多项式的乘积, 所以

$$\begin{aligned}\Phi_{21}(x) &= (x^2 + x + 1) \odot ((x^3 + x + 1)(x^3 + x^2 + 1)) \\ &= ((x^2 + x + 1) \odot (x^3 + x + 1))((x^2 + x + 1) \odot (x^3 + x^2 + 1)) \\ &= (x^6 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^4 + x^2 + 1).\end{aligned}$$

最后一步得到的两个 6 次多项式一定不可约, 这是因为它们是两个次数互素的不可约多项式的复合乘积. □

5.4 不可约多项式的构作

本节我们首先给出有限域上不可约多项式的几种递归构作方法, 然后再讨论如何构作任意次数的不可约多项式.

定理 5.29: 设 p 为素数, $f(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$ 为 $\mathbb{F}_p$ 上首一 n 次不可约多项式, 设元素 $a \in \mathbb{F}_p^*$ 满足 $(na + c_{n-1})f'(a) \neq 0$ 并记 $g(x) = x^p - x + a \in \mathbb{F}_p[x]$. 定义 $f_0(x) = f(g(x))$, 对于 $k \geq 1$, 递归地构作多项式 $f_k(x)$ 为 $f_k(x) = \widetilde{f}_{k-1}(g(x))$, 其中 $\widetilde{f}_{k-1}(x)$ 为 $f_{k-1}(x)$ 的互反多项式. 则对所有 $k \geq 0$, 有 $\deg f_k(x) = np^{k+1}$ 且 $f_k(x)$ 在 $\mathbb{F}_p$ 上不可约.

证明: 对任意 $k \geq 0$, 记 $\deg f_k(x) = n_k$ 且 $f_k(x) = \sum_{i=0}^{n_k} f_{ki} x^i$. 用 P_k 表示如下论断: $f_{k1} = f_k'(a) \neq 0$, 多项式 $f_k(x)$ 和 $f_k'(x)$ 在 $\mathbb{F}_p$ 上都是常数, $n_k = np^{k+1}$ 且 $f_k(x)$ 在 $\mathbb{F}_p$ 上不可约. 我们对 k 做归纳来证明 P_k.

若 $k = 0$, 则 $f_0(x) = f(g(x))$, 所以 $f_0'(x) = f'(g(x))g'(x) = -f'(g(x))$. 故 $f_{01} = (f_0'(x))|_{x=0} = -f'(g(x))|_{x=0} = -f'(g(0)) = -f'(a)$, $f_0'(a) = -f'(g(x))|_{x=a} = -f'(a)$. 由假设 $(na + c_{n-1})f'(a) \neq 0$, 我们有 $f'(a) \neq 0$, 所以 $f_{01} = f_0'(a) = -f'(a) \neq 0$. 显然, 对任意 $\alpha \in \mathbb{F}_p$, 有 $g(\alpha) = a$, 从而 $g(x)$ 在 $\mathbb{F}_p$ 上为常数, 所以 $f_0(x) = f(g(x))$ 和 $f_0'(x) = -f'(g(x))$ 在 $\mathbb{F}_p$ 上为常数. 显然 $\deg f_0(x) = np$, 即 $n_0 = np$. 由定理 5.18 知多项式 $f_0(x) = f(g(x))$ 在 $\mathbb{F}_p$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_p/\mathbb{F}_p}(na + c_{n-1}) = na + c_{n-1} \neq 0$. 由定理假设有 $na + c_{n-1} \neq 0$, 所以 $f_0(x)$ 在 $\mathbb{F}_p$ 上不可约. 这样我们便证明了论断 P_0.

现在假设论断 P_k 对 $k \geq 0$ 成立, 下面证明 P_{k+1} 也成立. 由归纳假设 $f_k(x)$ 在 $\mathbb{F}_p$ 上不可约且具有次数 $n_k = np^{k+1} > 1$, 所以 $f_k(x)$ 的常数项 $f_{k0} \neq 0$, 故 $\deg \widetilde{f}_k(x) = \deg f_k(x) = np^{k+1}$, 从而 $f_{k+1}(x) = \widetilde{f}_k(g(x))$ 的次数为 np^{k+2}, 即 $n_{k+1} = np^{k+2}$. 由于多项式 $f_{k0}^{-1}\widetilde{f}_k(x) \in \mathbb{F}_p[x]$ 首一且其 x^{n_k-1} 项系数为 $f_{k0}^{-1}f_{k1} \neq 0$, 所以

$$\mathrm{Tr}_{\mathbb{F}_p/\mathbb{F}_p}(n_k a + f_{k0}^{-1} f_{k1}) = f_{k0}^{-1} f_{k1} \neq 0,$$

这里用到 $n_k = np^{k+1}$, 所以在 $\mathbb{F}_p$ 中有 $n_k a = 0$. 由定理 5.18 得到 $f_{k+1}(x) = \widetilde{f}_k(g(x))$ 在 $\mathbb{F}_p$ 上

不可约. 由于

$$f_{k+1}(x)=\widetilde{f}_k(g(x))=\sum_{i=0}^{n_k} f_{ki}g(x)^{n_k-i},$$

和 $g'(x)=-1$, 所以

$$f'_{k+1}(x)=\sum_{i=0}^{n_k-1} f_{ki}(n_k-i)g(x)^{n_k-i-1}g'(x)=\sum_{i=0}^{n_k-1} f_{ki}ig(x)^{n_k-i-1},$$

这表明 $f_{k+1}(x)$ 和 $f'_{k+1}(x)$ 在 $\mathbb{F}_p$ 上为常数, 故 $f_{k+1,1}=f'_{k+1}(x)|_{x=0}=f'_{k+1}(x)|_{x=a}=f'_{k+1}(a)$. 进一步地, 由于 $\widetilde{f}_k(x)=x^{n_k}f_k(\frac{1}{x})$, 我们有

$$\widetilde{f}_k{}'(x)=n_kx^{n_k-1}f_k\left(\frac{1}{x}\right)+x^{n_k}f'_k\left(\frac{1}{x}\right)\left(-\frac{1}{x^2}\right)=-x^{n_k-2}f'_k\left(\frac{1}{x}\right),$$

再利用 $f'_k(x)$ 在 $\mathbb{F}_p$ 上为常数, 我们有 $f'_k(a^{-1})=f'_k(a)$, 所以

$$f_{k+1,1}=f'_{k+1}(x)|_{x=0}=-\widetilde{f}_k{}'(g(x))\,|_{x=0}=-\widetilde{f}_k{}'(a)=a^{n_k-2}f'_k\left(a^{-1}\right)=a^{n_k-2}f'_k(a).$$

由归纳假设 $f'_k(a)\neq 0$, 所以 $f_{k+1,1}=f'_{k+1}(a)=a^{n_k-2}f'_k(a)\neq 0$, 这便证明了论断 P_{k+1}.

由归纳法原理, 论断 P_k 对所有 $k\geq 0$ 成立. 特别地, 对所有 $k\geq 0$, $\deg f_k(x)=np^{k+1}$ 且 $f_k(x)$ 在 $\mathbb{F}_p$ 上不可约. □

例 5.6: 设 p 为任意素数, 取 $f(x)=x$ 和 $a=-1$, 则有 $n=1$, $c_{n-1}=c_0=0$, $f'(x)=1$, 故 $(na+c_{n-1})f'(a)=-1\neq 0$. 这时 $f_0(x)=f(x^p-x-1)=x^p-x-1$, 而当 $k\geq 1$ 时, $f_k(x)=\widetilde{f}_{k-1}(x^p-x-1)$. 由定理 5.29 知对所有 $k\geq 0$, $f_k(x)$ 为 $\mathbb{F}_p$ 上次数为 p^{k+1} 的不可约多项式.

例 5.7: 设 p 为奇素数, $g(x)=x^p-x-1$. 由定理 5.7 知 $g(x)$ 在 $\mathbb{F}_p$ 上不可约, 再由定理 5.12 知多项式

$$f(x)=-(x-1)^pg\left(\frac{1}{x-1}\right)=(x-1)^p+(x-1)^{p-1}-1=x^p+x^{p-1}+\cdots+x-1$$

在 $\mathbb{F}_p$ 上不可约. 显然, $c_{p-1}=1$ 且 $f'(x)=-(x-1)^{p-2}$, 取 $a=-1$, 则 $(pa+c_{p-1})f'(a)\neq 0$. 令 $f_{-1}(x)=f(x)$, $f_0(x)=f(x^p-x-1)$, 对 $k\geq 1$, 定义 $f_k(x)=\widetilde{f}_{k-1}(x^p-x-1)$, 则由定理 5.29 知对所有 $k\geq -1$, $f_k(x)$ 为 $\mathbb{F}_p$ 上次数为 p^{k+2} 的不可约多项式. □

类似于定理 5.29, 我们给出如下结论, 请自己给出证明.

定理 5.30: 设 p 为素数, q 为 p 的方幂, $f(x)=x^n+\sum_{i=0}^{n-1}c_ix^i$ 为 $\mathbb{F}_q$ 上首一 n 次不可约多项式, 设存在元素 $\delta_0\in\mathbb{F}_p$ 使得 $f(\delta_0)\in\mathbb{F}_p^*$ 且满足 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(n\delta_0+c_{n-1})\cdot\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f'(\delta_0))\neq 0$, 记 $g_0(x)=x^p-x+\delta_0$, 当 $k\geq 1$ 时令 $g_k(x)=x^p-x+\delta_k$, 其中 $\delta_k\in\mathbb{F}_p^*$. 定义 $f_0(x)=f(g_0(x))$, 对于 $k\geq 1$, 递归地定义多项式 $f_k(x)$ 为 $f_k(x)=\widetilde{f}_{k-1}(g_k(x))$, 其中 $\widetilde{f}_{k-1}(x)$ 为 $f_{k-1}(x)$ 的互反多项式. 则对所有 $k\geq 0$, 有 $\deg f_k(x)=np^{k+1}$ 且 $f_k(x)$ 在 $\mathbb{F}_q$ 上不可约. □

在定理 5.15 的基础上, 我们有下面的递归构作.

定理 5.31: 设 $q=2^m$, $f(x)=\sum_{i=0}^{n}c_ix^i\in\mathbb{F}_q[x]$ 为 $\mathbb{F}_q$ 上的不可约多项式且 $c_0c_n\neq 0$. 定义 $f_0(x)=f(x)$, 对 $k\geq 1$, 定义 $f_k(x)=x^{2^{k-1}n}f_{k-1}(x+x^{-1})$. 则对 $k\geq 1$, $f_k(x)$ 为 $\mathbb{F}_q$ 上的自互

反多项式且 $\deg f_k(x) = 2^k n$. 进一步地, 我们有

(i) 若 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_1/c_0) \neq 0$, 则 $f_1(x)$ 在 $\mathbb{F}_q$ 上不可约.

(ii) 对于 $k > 1$, 若 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_1/c_0) \neq 0$ 且 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_{n-1}/c_n) \neq 0$, 则 $f_k(x)$ 在 $\mathbb{F}_q$ 上不可约.

证明: 容易验证对于 $k \geq 1$, $f_k(x)$ 是自互反的且次数为 $2^k n$. 由定理 5.15 可以立得结论 (i).

下面来证明结论 (ii). 我们对 k 做归纳来证明对任意 $k \geq 1$, $f_k(x)$ 在 $\mathbb{F}_q$ 上不可约. 由条件 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_1/c_0) \neq 0$ 得到 $f_1(x)$ 在 $\mathbb{F}_q$ 上不可约. 设 $k \geq 1$ 且 $f_k(x)$ 在 $\mathbb{F}_q$ 上不可约. 记 $n_k = 2^k n$ 且对 $k \geq 0$, 设 $f_k(x) = \sum_{i=0}^{n_k} c_{ki} x^i$. 由 $f_k(x)$ 的定义, 我们容易得到 $c_{k0} = c_{k-1,n_{k-1}}$ 和 $c_{k1} = c_{k-1,n_{k-1}-1}$. 由定理 5.15, 多项式 $f_{k+1}(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_{k1}/c_{k0}) \neq 0$. 下面我们来看 c_{k0} 和 c_{k1}, 由于对 $j \geq 1$, $f_j(x)$ 自互反, 所以我们有

$$c_{k0} = c_{k-1,n_{k-1}} = c_{k-1,0} = \cdots = c_{10} = c_{0,n_0} = c_n$$

和

$$c_{k1} = c_{k-1,n_{k-1}-1} = c_{k-1,1} = \cdots = c_{11} = c_{0,n_0-1} = c_{n-1}.$$

由假设 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_{n-1}/c_n) \neq 0$, 从而对任意 $k \geq 1$, $f_{k+1}(x)$ 在 $\mathbb{F}_q$ 上不可约. □

例 5.8: 设 $q = 2$, $f(x) = x + 1 \in \mathbb{F}_2[x]$. 则有 $n = 1$, $c_{n-1} = c_n = c_0 = c_1 = 1$, 从而 $\mathrm{Tr}_{\mathbb{F}_2/\mathbb{F}_2}(c_{n-1}/c_n) = \mathrm{Tr}_{\mathbb{F}_2/\mathbb{F}_2}(c_1/c_0) = 1$. 定义 $f_0(x) = f(x) = x + 1$, 对 $k \geq 1$, 定义 $f_k(x) = x^{2^{k-1}} f_{k-1}(x + x^{-1})$. 则由定理 5.31 知对任意 $k \geq 1$, $f_k(x)$ 在 $\mathbb{F}_2$ 上不可约且次数为 2^k. 例如, 可以计算出 $f_1(x) = x f_0(x+x^{-1}) = x(x+x^{-1}+1) = x^2+x+1$, $f_2(x) = x^4+x^3+x^2+x+1$, $f_3(x) = x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$, 等等. □

类似于定理 5.31, 当 q 为奇数时, 基于推论 5.17 我们有如下构作.

定理 5.32: 设 q 为奇素数幂, $f(x)$ 为 $\mathbb{F}_q$ 上的 n 次不可约多项式且满足 $f(1)f(-1) \notin \mathbb{F}_q^2$, 并且若 $q \equiv 3 \pmod 4$, 还要假设 n 为偶数. 定义 $f_0(x) = f(x)$, 当 $k \geq 1$ 时定义 $f_k(x) = (2x)^{2^{k-1}n} f_{k-1}((x + x^{-1})/2)$. 则对任意 $k \geq 0$, $f_k(x)$ 是 $\mathbb{F}_q$ 上的不可约多项式且次数为 $2^k n$.

证明: 对任意 $k \geq 0$, 容易对 k 作归纳得到 $\deg f_k(x) = 2^k n$. 由已知 $f_0(x) = f(x)$ 在 $\mathbb{F}_q$ 上不可约, 对于 $k \geq 1$, 我们有

$$\begin{aligned} f_k(1)f_k(-1) &= 2^{2^{k-1}n} f_{k-1}(1)(-2)^{2^{k-1}n} f_{k-1}(-1) \\ &= (-1)^{2^{k-1}n} 2^{2\cdot 2^{k-1}n} f_{k-1}(1)f_{k-1}(-1) \\ &= (-1)^{(2^{k-1}+2^{k-2})n} 2^{2(2^{k-1}+2^{k-2})n} f_{k-2}(1)f_{k-2}(-1) \\ &= \cdots \\ &= (-1)^n \left(2^{(2^k-1)n}\right)^2 f_0(1)f_0(-1). \end{aligned}$$

注意到由假设我们或者有 $-1 \in \mathbb{F}_q^{*2}$ (当 $q \equiv 1 \pmod 4$ 时) 或者 n 为偶数, 所以我们总有 $(-1)^n \in \mathbb{F}_q^{*2}$, 故 $f_k(1)f_k(-1) \in f_0(1)f_0(-1)\mathbb{F}_q^{*2}$. 由假设 $f_0(1)f_0(-1) = f(1)f(-1) \notin \mathbb{F}_q^2$, 所以对任意 $k \geq 1$, 有 $f_k(1)f_k(-1) \notin \mathbb{F}_q^2$. 利用推论 5.17 并对 k 做归纳, 我们有对任意 $k \geq 1$, $f_k(x)$ 是 $\mathbb{F}_q$ 上的不可约多项式. □

例 5.9: 利用定理 5.32, 我们有如下几个给定域上的不可约多项式的无穷族:

(i) $q=3$, $f(x)=x^2\pm x-1$.

(ii) $q=5$, $f(x)=x\pm 2$ 或者 $f(x)=x^2\pm x+2$.

(iii) 设素数幂 $q\equiv 1\,(\mathrm{mod}\ 4)$, $f(x)=x-c$ or $f(x)=x^2+2cx+1$, 其中 $c\in\mathbb{F}_q$ 满足 $c^2-1\notin\mathbb{F}_q^2$.

(iv) 设素数幂 $q\equiv 3\,(\mathrm{mod}\ 4)$, $f(x)=x^2+2cx-1$, 其中 $c\in\mathbb{F}_q$ 满足 $c^2+1\notin\mathbb{F}_q^2$. □

前面我们已经给出数种构作有限域上不可约多项式的方法, 设正整数 $n\geq 2$, 下面我们考虑有限域上 n 次不可约多项式的构作问题. 假设 n 的标准分解式为 $n=r_1^{e_1}r_2^{e_2}\dots r_k^{e_k}$, 其中 $r_1,r_2,\dots r_k$ 是互不相同的素数, $e_1,e_2,\dots,e_k$ 为正整数. 如果对每个 i, $1\leq i\leq k$, $\mathbb{F}_q$ 上的 $r_i^{e_i}$ 次不可约多项式可以构作出来, 则利用这些不可约多项式的复合乘法 (或复合加法), 我们便可以得到 $\mathbb{F}_q$ 上的 n 次不可约多项式.

设 p 为素数, 我们来考虑 $\mathbb{F}_p$ 上的 r^e 次不可约多项式的构作, 其中 r 为素数, e 为正整数. 我们区分如下不同的情形.

(a) 若 $r=p$ 且 p 为奇素数, 例 5.6 和 5.7 给出了 $\mathbb{F}_p$ 上 p^e 次不可约多项式, 其中 $e\geq 1$.

(b) 若 $r=p=2$, 例 5.6 和 5.8 给出了 $\mathbb{F}_2$ 上 2^e 次不可约多项式, 其中 $e\geq 1$.

(c) 若 $r=2$ 且 $p\equiv 1\,(\mathrm{mod}\ 4)$, 选取 $a\in\mathbb{F}_p^*$ 使得 a 为 $\mathbb{F}_p$ 中的非平方元, 则显然 $m=\mathrm{ord}(a)$ 不整除 $\frac{p-1}{2}$, 故 $2\nmid\frac{p-1}{m}$. 由推论 5.6, 对任意 $e\geq 1$, 二项式 $x^{2^e}-a$ 在 $\mathbb{F}_p$ 上不可约.

(d) 若 $r=2$ 且 $p\equiv 3\,(\mathrm{mod}\ 4)$, 例 5.2 给出了 $\mathbb{F}_p$ 上 2^e 次不可约多项式, 其中 $e\geq 1$.

(e) 若 r 为奇素数且 $r\neq p$, 下面的定理可以用来构作 $\mathbb{F}_p$ 上的 r^e 次不可约多项式, 其中 $e\geq 1$.

定理 5.33: 设 p 为素数, 奇素数 $r\neq p$, 且 p 模 r 的乘法阶为 n. 选取 $a\in\mathbb{F}_{p^n}^*$, 但是 $a\notin\mathbb{F}_{p^n}^{*r}$, 则对任意正整数 e, $x^{r^e}-a$ 在 $\mathbb{F}_{p^n}$ 上不可约. 进一步地, 设 β 为二项式 $x^{r^e}-a$ 的一个根, 则 $\beta\in\mathbb{F}_{p^{nr^e}}$. 定义

$$\gamma=\mathrm{Tr}_{\mathbb{F}_{p^{nr^e}}/\mathbb{F}_{p^{r^e}}}(\beta)=\sum_{i=0}^{n-1}\beta^{p^{ir^e}},$$

则 $\gamma\in\mathbb{F}_{p^{r^e}}$ 且 γ 在 $\mathbb{F}_p$ 上的次数为 r^e, 从而 γ 在 $\mathbb{F}_p$ 上的极小多项式为 $\mathbb{F}_p$ 上的 r^e 次不可约多项式.

证明: 设 $m=\mathrm{ord}(a)$, 即 a 在群 $\mathbb{F}_{p^n}^*$ 中的阶. 由于 $\mathbb{F}_{p^n}^{*r}$ 是 $\mathbb{F}_{p^n}^*$ 的子群且阶为 $\frac{p^n-1}{r}$, 又 $a\notin\mathbb{F}_{p^n}^{*r}$, 所以 $m\nmid\frac{p^n-1}{r}$, 故 $r\nmid\frac{p^n-1}{m}$. 由推论 5.6 得到对任意 $e\geq 1$, 二项式 $x^{r^e}-a$ 在 $\mathbb{F}_{p^n}$ 上不可约, 从而 $\mathbb{F}_{p^n}(\beta)=\mathbb{F}_{p^{nr^e}}$ 且 $\gamma\in\mathbb{F}_{p^{r^e}}$, 由此可得到 γ 在 $\mathbb{F}_p$ 上的次数整除 r^e.

注意到 $n=\mathrm{ord}_r(p)$, 所以 n 整除 $\phi(r)=r-1$, 故 $\gcd(n,r)=1$, 从而对任意 $t\geq 1$, 有 $\gcd(n,r^t)=1$. 下面我们证明 γ 在 $\mathbb{F}_p$ 上的次数为 r^e, 若否,设 γ 在 $\mathbb{F}_p$ 上的次数为 r^t, 其中

$t < e$. 由于 $\gcd(n, r^t) = 1$, 由推论 2.14 知 γ 在 $\mathbb{F}_{p^n}$ 上的次数也是 r^t, 故 $\gamma \in \mathbb{F}_{p^{nr^t}}$. 注意到 β^r 为 $\mathbb{F}_{p^n}$ 上不可约多项式 $x^{r^{e-1}} - a$ 的根, 故 $\mathbb{F}_{p^n}(\beta^r) = \mathbb{F}_{p^{nr^{e-1}}}$ 且 $[\mathbb{F}_{p^n}(\beta) : \mathbb{F}_{p^n}(\beta^r)] = r$, 从而 β 在 $\mathbb{F}_{p^n}(\beta^r)$ 上的次数为 r. 由 $t \le e-1$ 有 $\gamma \in \mathbb{F}_{p^n}(\beta^r)$. 由于 p 模 r 的乘法阶为 n 以及 $\gcd(n, r^e) = 1$, 我们有 p^{r^e} 模 r 的乘法阶依然为 n. 对每个 i, $0 \le i \le n-1$, 由带余除法, 设 $p^{ir^e} = s_i r + t_i$, 其中 s_i, t_i 为整数且 $0 < t_i < r$, 则由 $\mathrm{ord}_r(p^{r^e}) = n$ 知 $t_0, t_1, \ldots, t_{n-1}$ 互不相同, 所以由

$$\gamma = \sum_{i=0}^{n-1} \beta^{p^{ir^e}} = \sum_{i=0}^{n-1} \beta^{s_i r + t_i}$$

知 β 为 $\mathbb{F}_{p^n}(\beta^r)$ 上的非零多项式

$$h(x) = (\beta^r)^{s_0} x^{t_0} + (\beta^r)^{s_1} x^{t_1} + \cdots + (\beta^r)^{s_{n-1}} x^{t_{n-1}} - \gamma$$

的根, 又 $\deg h(x) < r$, 与 β 在 $\mathbb{F}_{p^n}(\beta^r)$ 上的次数为 r 矛盾, 结论得证. □

前面我们已经看到有限域上多项式 $x^n - 1$ 的分解在理论和实际应用方面都有着重要的意义, 本节的最后我们给出域 $\mathbb{F}_q$ 上 $x^n - 1$ 的一个分解结果, 不失一般性我们依然假设 $\gcd(n, q) = 1$. 对于素数 p 和任意正整数 m, 用 $v_p(m)$ 表示能整除 m 的 p 的最高次幂的指数, 即 $v_p(m) = \max\{r \in \mathbb{N} \mid p^r \mid m\}$, $v_p(m)$ 也常称为正整数 m 的 p-adic 赋值或者 p-adic 阶.

定理 5.34: 设 $\gcd(n, q) = 1$ 且 q 模 n 的乘法阶为 t, 则多项式 $x^n - 1$ 在 $\mathbb{F}_q$ 上可以分解为不可约二项式的乘积当且仅当 $n \mid t(q-1)$.

证明: 设 ζ_n 是 $\mathbb{F}_q$ 的扩域中的一个 n 次本原单位根, 即 $\mathrm{ord}(\zeta_n) = n$. 由于 q 模 n 的乘法阶为 t, 所以 ζ_n 在 $\mathbb{F}_q$ 上的次数为 t. 如果 $x^n - 1$ 在 $\mathbb{F}_q$ 上可以分解为不可约二项式的乘积, 则 ζ_n 在 $\mathbb{F}_q$ 上的极小多项式为一个二项式, 设为 $x^t - a$, 其中 $a \in \mathbb{F}_q^*$, 从而 $\zeta_n^{t(q-1)} = a^{q-1} = 1$, 故 $n \mid t(q-1)$.

反之, 设 $n \mid t(q-1)$. 令 $a = \zeta_n^t$, 则 $a^{q-1} = \zeta_n^{t(q-1)} = 1$, 从而 $a \in \mathbb{F}_q^*$. 注意到 ζ_n 为多项式 $x^t - a \in \mathbb{F}_q[x]$ 的根而 ζ_n 在 $\mathbb{F}_q$ 上的次数为 t, 所以 ζ_n 在 $\mathbb{F}_q$ 上的极小多项式为 $x^t - a$, 故 $x^t - a$ 在 $\mathbb{F}_q$ 上不可约. 显然 $\mathrm{ord}(a) = m = \frac{n}{\gcd(n,t)}$, 由定理 5.5 得到 t 的每个素因子都整除 m 但不整除 $\frac{q-1}{m}$, 并且若 $4 \mid t$ 则 $4 \mid (q-1)$. 多项式 $x^n - 1$ 的每个根形如 ζ_n^k, 其中 $0 \le k \le n-1$. 对每个 k, 令 $t_k = \frac{t}{\gcd(t,k)}$, $a_k = a^{\frac{k}{\gcd(t,k)}} \in \mathbb{F}_q^*$, 则有

$$(\zeta_n^k)^{t_k} = \zeta_n^{\frac{kt}{\gcd(t,k)}} = (\zeta_n^t)^{\frac{k}{\gcd(t,k)}} = a^{\frac{k}{\gcd(t,k)}} = a_k,$$

即 ζ_n^k 为多项式 $x^{t_k} - a_k \in \mathbb{F}_q[x]$ 的根, 下面我们来证明 $x^{t_k} - a_k$ 在 $\mathbb{F}_q$ 上不可约. 首先若 $4 \mid t_k$, 则 $4 \mid t$, 从而 $4 \mid (q-1)$. 记 $s = \frac{kt}{\gcd(t,k)}$, 则 $\mathrm{ord}(a_k) = e = \frac{n}{\gcd(n,s)}$. 设 p 为 t_k 的一个素因子, 则 $p \mid t$, 从而 $p \mid m$ 且 $p \nmid \frac{q-1}{m}$, 故 $v_p(m) \ge 1$ 且 $v_p(\frac{q-1}{m}) = 0$. 由 $v_p(m) = v_p(n) - v_p(\gcd(n,t))$ 有 $v_p(n) > v_p(t)$. 类似地, 由 $p \mid t_k$ 得到 $v_p(t) > v_p(k)$, 从而 $v_p(s) = v_p(kt) - v_p(\gcd(t,k)) = v_p(k) + v_p(t) - v_p(k) = v_p(t)$, 故 $v_p(e) = v_p(n) - v_p(s) = v_p(n) - v_p(t) > 0$, 所以 $p \mid e$. 进一步地, 由 $v_p(\frac{q-1}{e}) = v_p(q-1) - v_p(e) = v_p(q-1) + v_p(s) - v_p(n) = v_p(q-1) + v_p(t) - v_p(n) = v_p(\frac{q-1}{m}) = 0$

得出 $p \nmid \frac{q-1}{e}$. 由定理 5.5, 我们得到对任意 $k = 0, 1, \ldots, n-1$ 有 $x^{t_k} - a_k$ 在 $\mathbb{F}_q$ 上不可约, 所以 $x^n - 1$ 在 $\mathbb{F}_q$ 上分解为不可约二项式的乘积. □

特别地, 当 $q = 2$ 时, 由于 $t = \mathrm{ord}_n(q)$ 为 $\phi(n)$ 的因子, 所以对任意奇数 $n > 1$, $x^n - 1$ 在 $\mathbb{F}_2$ 上一定不能分解为不可约二项式的乘积. 另外如上定理的证明告诉我们, 在定理条件下, $x^n - 1$ 的每个不可约二项因式的次数都是 t 的因子, 对任意 $d \mid t$, $x^n - 1$ 的 d 次不可约二项因式的个数为满足 $0 \le k \le n-1$ 且 $\gcd(t, k) = \frac{t}{d}$ 的 k 的个数除以 d. 例如, 当 $q = 5$, $n = 8$ 时, $t = \mathrm{ord}_8(5) = 2$, 满足条件 $n \mid t(q-1)$, 所以 $x^8 - 1$ 在 $\mathbb{F}_5$ 上可以分解为不可约二项式的乘积. 进一步地, 它的一次因式有 4 个, 二次不可约因式有 2 个. 事实上, $x^8 - 1$ 在 $\mathbb{F}_5$ 上的标准分解式为

$$x^8 - 1 = (x-1)(x+1)(x-2)(x+2)(x^2-2)(x^2+2).$$

5.5 习题

5.1 设 r 为素数, $a \in \mathbb{F}_q$, 证明二项式 $x^r - a$ 或者在 $\mathbb{F}_q$ 上不可约或者在 $\mathbb{F}_q$ 中有根.

5.2 设 r 为奇素数, $a \in \mathbb{F}_q$, 证明对任意 $n \ge 1$, $x^{r^n} - a$ 在 $\mathbb{F}_q$ 上不可约当且仅当 a 不是 $\mathbb{F}_q$ 中元素的 r 次幂.

5.3 设 p 为素数, $b \in \mathbb{F}_p^*$, 证明三项式 $x^p - x - b$ 在 $\mathbb{F}_{p^n}$ 上不可约当且仅当 $p \nmid n$.

5.4 设 $f(x) = x^r - ax - b \in \mathbb{F}_q[x]$, 其中 $r > 2$ 且为 $\mathbb{F}_q$ 的特征的方幂, 设二项式 $x^{r-1} - a$ 在 $\mathbb{F}_q$ 上不可约, 证明 $f(x)$ 为一个 1 次多项式和一个 $r-1$ 次不可约多项式的乘积.

5.5 设 $a, b \in \mathbb{F}_q$ 且 $a \ne 1$, 证明 $x^q - ax - b$ 一定在 $\mathbb{F}_q$ 中有根.

5.6 证明三项式 $x^{2n} + x^n + 1$ 在 $\mathbb{F}_2$ 上不可约当且仅当存在非负整数 k 使得 $n = 3^k$, 而 $x^{4n} + x^n + 1$ 在 $\mathbb{F}_2$ 上不可约当且仅当存在非负整数 k 和 m 使得 $n = 3^k 5^m$.

5.7 设 $p \equiv 3 \pmod 4$ 为素数, $r = v_2(p+1)$, 即能整除 $p+1$ 的 2 的最高次幂的指数, 则 $r \ge 2$. 递归地定义 $\mathbb{F}_p$ 的子集 $H_1, H_2, \ldots, H_r$ 如下:

$$\begin{aligned} H_1 &= \{0\}, \\ H_i &= \{\pm((u+1)/2)^{(p+1)/4} \mid u \in H_{i-1}\},\ i = 2, \ldots, r-1, \\ H_r &= \{\pm((u-1)/2)^{(p+1)/4} \mid u \in H_{r-1}\}. \end{aligned}$$

则对任意的 $1 \le i \le r-1$ 和 $k \ge 0$,

$$x^{2^i} + 1 = \prod_{u \in H_i} (x^2 - 2ux + 1) \ \text{ 和 } \ x^{2^{r+k}} + 1 = \prod_{u \in H_r} \left(x^{2^{k+1}} - 2ux^{2^k} - 1 \right),$$

是 $\mathbb{F}_p$ 上的完全分解.

5.8 设 r 是奇素数, q 是素数幂且为模 r 的一个原根满足 $r^2 \nmid (q^{r-1} - 1)$. 证明对任意 $k \ge 0$, 多项式 $x^{(r-1)r^k} + x^{(r-2)r^k} + \cdots + x^{r^k} + 1$ 在 $\mathbb{F}_q$ 上不可约.

5.9 设 $q=2^m$, $P(x)=\sum_{i=0}^{n}c_ix^i$ 为 $\mathbb{F}_q$ 上不可约多项式且 $\deg P(x)=n$, 证明 $Q(x)=x^n\widetilde{P}(x+x^{-1})$ 为 $\mathbb{F}_q$ 上的 $2n$ 次自互反多项式, 进一步地, $Q(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_{n-1}/c_n)=1$, 其中 $\widetilde{P}(x)$ 为 $P(x)$ 的互反多项式.

5.10 设 q 为奇素数幂, $P(x)$ 为 $\mathbb{F}_q$ 上不可约多项式且 $\deg P(x)=n$, 证明 $Q(x)=x^nP(x+x^{-1})$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $\widetilde{P}(2)\widetilde{P}(-2)\notin\mathbb{F}_q^2$, 其中 $\widetilde{P}(x)$ 为 $P(x)$ 的互反多项式.

5.11 证明二次多项式 $f(x)=x^2+bx+c\in\mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $f(x)$ 整除 x^q+x+b.

5.12 设 $f(x)\in\mathbb{F}_q[x]$ 首一, 次数为 $n\geq 1$. 定义 $h(x,y)\in\mathbb{F}_q[x,y]$ 为

$$h(x,y)=(y-x)(y-x^q)(y-x^{q^2})\cdots(y-x^{q^{n-1}})-f(y),$$

把 $h(x,y)$ 写成 y 的多项式

$$h(x,y)=s_{n-1}(x)y^{n-1}+\cdots+s_1(x)y+s_0(x).$$

证明 $f(x)$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $f(x)$ 整除每一个 $s_j(x)$, $0\leq j\leq n-1$.

5.13 设 $q=2^Au-1$, 其中 $A\geq 2$, u 为奇数. 设正整数 t 可被 2^A 整除, $a\in\mathbb{F}_q^*$ 且在群 $\mathbb{F}_q^*$ 中的阶为 $\mathrm{ord}(a)=e>1$. 再设 t 的每个素因子都整除 e 但是不整除 $(q-1)/e$. 则 $e\equiv 2\,(\mathrm{mod}\,4)$ 且二项式 x^t-a 可以分解为 $\mathbb{F}_q[x]$ 中 $B=2^{A-1}$ 个次数为 t/B 的首一不可约多项式的乘积. 事实上, 设 $d=\frac{e}{2}+1$. 因为 $\gcd(2B,q-1)=2$, 存在 $r\in\mathbb{N}$ 使得 $2Br\equiv d\,(\mathrm{mod}\,(q-1))$. 定义

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

证明

a. $F(x)$ 的根 $c_1,\ldots,c_B$ 均属于 $\mathbb{F}_q$.
b. 在 $\mathbb{F}_q[x]$ 中, x^t-a 的完全分解为

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

其中 $v=t/B$, $b=a^r\in\mathbb{F}_q$.
c. 在 $\mathbb{F}_3[x]$ 中分解 x^8+1, 在 $\mathbb{F}_7[x]$ 中分解 $x^{24}-3$, 在 $\mathbb{F}_{19}[x]$ 中分解 $x^{27}-4$, 在 $\mathbb{F}_{23}[x]$ 中分解 $x^{88}-10$.

5.14 设 q 为奇素数幂, 在定理 5.12 中取 $\mathbb{F}_q$ 上互素的两个多项式 $f(x)=a_1x^2+b_1x+c_1$, $g(x)=a_2x^2+b_2x+c_2$, 其中 a_1, a_2 不全为 0, 设 $P(x)\neq x$ 为 $\mathbb{F}_q$ 上首一 n 次不可约多项式, 则使得 $Q(x)=(g(x))^nP(f(x)/g(x))$ 在 $\mathbb{F}_q$ 上不可约的充要条件是什么?

5.15 设 $q=2^m$, $f(x)=\sum_{i=0}^{n}c_ix^i\in\mathbb{F}_q[x]$ 为 $\mathbb{F}_q$ 上 n 次不可约多项式且 $c_0c_n\neq 0$. 对于 $k\geq 0$, 递归地定义多项式 $f_k(x)$ 为:

$$\begin{aligned}f_0(x)&=f(x),\\ f_k(x)&=(1+x^2)^{2^{k-1}n}f_{k-1}(\tfrac{x}{1+x^2}),\ k\geq 1.\end{aligned}$$

证明对每个 $k>0$, $f_k(x)$ 是 $\mathbb{F}_q$ 上次数为 $2^k n$ 的自互反多项式并且

(i) 若 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_{n-1}/c_n)\neq 0$, 则 $f_1(x)$ 不可约.

(ii) 对于 $k\geq 1$, 若 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_{n-1}/c_n)\neq 0$ 和 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_1/c_0)\neq 0$, 则 $f_k(x)$ 不可约.

5.16 设 $q=2^m$, 递归地定义多项式 $c_k(x), d_k(x)\in\mathbb{F}_q[x]$ 为

$$c_0(x)=x,\quad d_0(x)=1,$$
$$c_{k+1}(x)=c_k^2(x)+d_k^2(x),\quad d_{k+1}(x)=c_k(x)d_k(x),\quad k\geq 0.$$

证明

$$\frac{c_{k+1}(x)}{d_{k+1}(x)}=\frac{1+(c_k(x)/d_k(x))^2}{c_k(x)/d_k(x)}=\frac{c_k(x+x^{-1})}{d_k(x+x^{-1})}$$

和

$$\frac{d_{k+1}(x)}{d_k(x+x^{-1})}=x^{2^k},$$

并由此推出定理 5.31 中定义的多项式 $f_k(x)$ 可以表示为

$$f_k(x)=(d_k(x))^n f(c_k(x)/d_k(x)),\ k\geq 0.$$

5.17 设 $q=2^m$, $f(x)=x^n+\sum_{i=0}^{n-1}c_i x^i$ 为 $\mathbb{F}_q$ 上的首一不可约多项式, 设 $\delta\in\mathbb{F}_q^*$ 且满足 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_1\delta/c_0)=1$ 和 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c_{n-1}/\delta)=1$. 定义 $f_0(x)=f(x)$, 且对 $k\geq 1$, 定义 $f_k(x)=x^{2^{k-1}n}f_{k-1}(x+\delta^2x^{-1})$. 证明对任意 $k\geq 0$, $f_k(x)$ 在 $\mathbb{F}_q$ 上不可约且次数为 $2^k n$.

5.18 设 q 为奇素数幂, $b\in\mathbb{F}_q$, $f(x)$ 为 $\mathbb{F}_q$ 上的不可约多项式且 $\deg f(x)=n$ 满足 $f(-\frac{b}{2})\notin\mathbb{F}_q^2$ 并且若 $q\equiv 3\,(\mathrm{mod}\ 4)$, 还要假设 n 为偶数. 定义 $f_0(x)=f(x)$, 当 $k\geq 1$ 时定义 $f_k(x)=f_{k-1}(x^2+bx+\frac{b^2-2b}{4})$. 证明对任意 $k\geq 0$, $f_k(x)$ 是 $\mathbb{F}_q$ 上的不可约多项式且次数为 $2^k n$.

5.19 设 $A(x)=L(x)-a\in\mathbb{F}_q[x]$ 是次数为 p^k 的仿射 p-多项式满足 $L(x)/x$ 在 $\mathbb{F}_q$ 上不可约, 证明 $A(x)$ 是 $\mathbb{F}_q$ 上一个 1 次多项式和一个 p^k-1 次不可约多项式的乘积.

5.20 设 $q=2^m$, $a,b\in\mathbb{F}_q^*$, $n>k\geq 1$, 证明三项式 x^n+ax^k+b 有重根当且仅当 n 和 k 都是偶数.

5.21 设 $q=2$, 正整数 n 和 k 中至少有一个为奇数且 $n>k>0$, 记 $f_{n,k}(x)=x^n+x^k+1\in\mathbb{F}_2[x]$. 证明:

(i) 设 $n\geq 4$, 若 $n\equiv 1\,(\mathrm{mod}\ 3)$ 且 $k\equiv 2\,(\mathrm{mod}\ 3)$, 或者若 $n\equiv 2\,(\mathrm{mod}\ 3)$ 且 $k\equiv 1\,(\mathrm{mod}\ 3)$, 则有 $(x^2+x+1)\mid f_{n,k}(x)$.

(ii) $f_{n,k}(x)$ 有偶数个不可约因式当且仅当如下三种情况出现:

(a) n 为偶数, k 为奇数, $n\neq 2k$ 且 $\frac{nk}{2}\equiv 0,\ 1\,(\mathrm{mod}\ 4)$.

(b) n 为奇数, k 为偶数, $k\nmid 2n$ 且 $n\equiv\pm 3\,(\mathrm{mod}\ 8)$.

(c) n 为奇数, k 为偶数, $k\mid 2n$ 且 $n\equiv\pm 1\,(\mathrm{mod}\ 8)$.

5.22 证明多项式 $x^n + x^{n-1} + \cdots + x + 1$ 在 $\mathbb{F}_q$ 上不可约当且仅当 $n+1$ 为素数且 q 是模 $n+1$ 的一个原根.

5.23 给出多项式 $x^{3^n} - 1$ 在 $\mathbb{F}_4$ 上的完全分解.

5.24 证明 $\mathbb{F}_q$ 上的任意矩阵在 $\mathbb{F}_q$ 的代数闭域 Γ 上相似于上三角矩阵.

第六章　置换多项式

由定理 1.12 得到, 有限域 $\mathbb{F}_q$ 到其自身的每一个映射都可以用一个次数小于 q 的多项式来唯一表示, 下面我们给出此结论的另一个证明. 首先每个多项式 $f(x) \in \mathbb{F}_q[x]$ 自然地给出 $\mathbb{F}_q$ 到其自身的映射 $f: c \mapsto f(c)$, 对任意 $c \in \mathbb{F}_q$. 进一步地, 对于多项式 $f(x), g(x) \in \mathbb{F}_q[x]$, 若它们给出的 $\mathbb{F}_q$ 到其自身的映射相同, 即对任意 $c \in \mathbb{F}_q$ 均有 $f(c) = g(c)$. 用 $x^q - x$ 去除 $f(x) - g(x)$, 由带余除法有 $f(x) - g(x) = q(x)(x^q - x) + r(x)$, 其中 $\deg(r(x)) < q$. 故对任意 $c \in \mathbb{F}_q$ 有 $r(c) = 0$, 这样多项式 $r(x)$ 在 $\mathbb{F}_q$ 中有 q 个根而其次数小于 q, 从而 $r(x) = 0$. 这便证出若两个 $\mathbb{F}_q$ 上的多项式给出相同的 $\mathbb{F}_q$ 到其自身的映射, 则这两个多项式模 $x^q - x$ 同余, 从而 $\mathbb{F}_q$ 上两个不同的次数小于 q 的多项式给出的 $\mathbb{F}_q$ 到其自身的映射一定不同. 我们知道, $\mathbb{F}_q$ 上次数小于 q 的多项式共有 q^q 个, 而 $\mathbb{F}_q$ 到其自身的映射也共有 q^q 个, 所以每一个这样的映射都可以用一个次数小于 q 的多项式来唯一表示.

记 $\mathbb{F}_q = \{a_0, a_1, \ldots, a_{q-1}\}$, 给定 $\mathbb{F}_q$ 到其自身的映射 φ,

$$f(x) = \sum_{i=0}^{q-1} \varphi(a_i) \prod_{0 \leq k \leq q-1,\, k \neq i} \frac{x - a_k}{a_i - a_k} \tag{6.1}$$

是 $\mathbb{F}_q$ 上的一个次数小于 q 的多项式且给出的 $\mathbb{F}_q$ 到其自身的映射就是 φ, 这个表示称为 Lagrange 插值公式. 另一方面, 容易验证

$$g(x) = \sum_{c \in \mathbb{F}_q} \varphi(c) \left(1 - (x - c)^{q-1}\right) \tag{6.2}$$

也是 $\mathbb{F}_q$ 上的一个次数小于 q 的多项式, 它给出的 $\mathbb{F}_q$ 到其自身的映射也是 φ. 由前面的讨论得知式 (6.1) 和 (6.2) 给出的这两个多项式实际上是一样的, 它们都是映射 φ 的多项式表示.

6.1　置换多项式的判定

设 $f(x) \in \mathbb{F}_q[x]$, 若 $f(x)$ 给出的 $\mathbb{F}_q$ 到其自身的映射 $f: c \mapsto f(c)$ 是 $\mathbb{F}_q$ 上的一个置换 (即双射), 则称 $f(x)$ 为 $\mathbb{F}_q$ 上的一个置换多项式. 由于 $\mathbb{F}_q$ 上的置换共 $q!$ 个, 所以 $\mathbb{F}_q$ 上次数小于 q 的置换多项式共有 $q!$ 个. 因为集合 $\mathbb{F}_q$ 为有限集, 所以 $\mathbb{F}_q$ 到其自身的单射 (或满射) 都是双射, 由置换多项式的定义, 我们容易得到下面的定理.

定理 6.1: 多项式 $f(x)\in\mathbb{F}_q[x]$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当下面条件之一成立.

(i) $\mathbb{F}_q$ 到自身的映射 $f:c\mapsto f(c)$ 是单射.

(ii) $\mathbb{F}_q$ 到自身的映射 $f:c\mapsto f(c)$ 是满射.

(iii) 对任意 $a\in\mathbb{F}_q$, 方程 $f(x)=a$ 在 $\mathbb{F}_q$ 中至少有一个根.

(iv) 对任意 $a\in\mathbb{F}_q$, 方程 $f(x)=a$ 在 $\mathbb{F}_q$ 中至多有一个根.

(v) 对任意 $a\in\mathbb{F}_q$, 方程 $f(x)=a$ 在 $\mathbb{F}_q$ 中有唯一根.

□

例 6.1: (a) 设 $f(x)=ax+b$, 其中 $a,b\in\mathbb{F}_q$ 且 $a\neq 0$. 对于任意 $c\in\mathbb{F}_q$, 方程 $f(x)=c$ 有根 $a^{-1}(c-b)$, 由定理 6.1 (iii) 知 $f(x)$ 是 $\mathbb{F}_q$ 上的置换多项式, 即任意一次多项式都是置换多项式.

(b) 设 n 为正整数, $f(x)=x^n$, 则显然 0 在 f 下有唯一原像 0, 所以 $f(x)$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 $f(\mathbb{F}_q^*)=\mathbb{F}_q^*$. 设 α 为 $\mathbb{F}_q$ 的一个本原元素, 即 $\mathbb{F}_q^*=\langle\alpha\rangle=\{\alpha^i\mid 0\leq i\leq q-2\}$, 则有

$$f(\mathbb{F}_q^*)=\{f(\alpha^i)\mid 0\leq i\leq q-2\}=\{(\alpha^n)^i\mid 0\leq i\leq q-2\}.$$

从而 $f(\mathbb{F}_q^*)=\mathbb{F}_q^*$ 当且仅当 α^n 也是群 $\mathbb{F}_q^*$ 的生成元. 由于 $\mathrm{ord}(\alpha^n)=\frac{q-1}{\gcd(n,q-1)}$, 所以 α^n 是群 $\mathbb{F}_q^*$ 的生成元当且仅当 $\gcd(n,q-1)=1$, 由此得到多项式 $f(x)=x^n$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(n,q-1)=1$.

下面我们给出此结果的另一个证明. 显然映射 $f:c\mapsto f(c)=c^n$ 是群 $\mathbb{F}_q^*$ 的自同态, 所以 f 为 $\mathbb{F}_q^*$ 到自身的单射当且仅当 $|\ker(f)|=1$. 注意到 $\ker(f)=\{c\in\mathbb{F}_q^*\mid c^n=1\}$, 即 $|\ker(f)|$ 为方程 $x^n=1$ 在 $\mathbb{F}_q^*$ 中根的个数. 令 $d=\gcd(n,q-1)$, 则对于 $a\in\mathbb{F}_q^*$, $a^n=1$ 当且仅当 $a^d=1$. 设 α 为域 $\mathbb{F}_q$ 的一个本原元素, 则容易验证对 $0\leq j\leq d-1$, d 个元素 $\alpha^{\frac{q-1}{d}j}$ 都是 $x^d=1$ 在 $\mathbb{F}_q^*$ 中的根, 它们就是 $x^d=1$ 在 $\mathbb{F}_q^*$ 中的所有根, 故 $|\ker(f)|=d$. 所以 $f(x)=x^n$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 f 为 $\mathbb{F}_q^*$ 到自身的单射, 也当且仅当 $\gcd(n,q-1)=1$.

(c) 设 $p=\mathrm{char}\mathbb{F}_q$, $L(x)$ 是 $\mathbb{F}_q$ 上的一个 p-多项式, 则由第 4.4 节知道 $L(x)$ 给出的 $\mathbb{F}_q$ 上的映射 $L:c\mapsto L(c)$ 是 $\mathbb{F}_p$ 上线性空间 $\mathbb{F}_q$ 的线性变换, 所以 L 为单射当且仅当 $\ker(L)=\{0\}$, 即多项式 $L(x)$ 在 $\mathbb{F}_q$ 中有唯一根 0, 故 $L(x)$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 $L(x)$ 在 $\mathbb{F}_q$ 中有唯一根 0. □

由于 $\mathbb{F}_q$ 上两个置换的合成仍为置换, 所以若 $f(x),g(x)\in\mathbb{F}_q[x]$ 是 $\mathbb{F}_q$ 上的置换多项式, 则 $f(g(x))$ 和 $g(f(x))$ 也是 $\mathbb{F}_q$ 上的置换多项式, 即 $\mathbb{F}_q$ 上的置换多项式集合在合成运算下封闭. 由于线性多项式都是置换多项式, 所以若 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式, 则对任意 $b,c,d\in\mathbb{F}_q$ 且 $c\neq 0$, $f_1(x)=cf(x+b)+d$ 也是 $\mathbb{F}_q$ 上的置换多项式. 适当选取 $\mathbb{F}_q$ 中的元素 b, c 和 d, 其中 $c\neq 0$, 我们可使得 $f_1(x)$ 首一且常数项为 0, 同时若 $\mathbb{F}_q$ 的特征 p 不整除 $f_1(x)$ 的次数 n, 我们还可以使得 $f_1(x)$ 中 x^{n-1} 项的系数为 0, 这样形式的 (置换) 多项式 $f_1(x)$ 称为是规范 (置换) 多项式. 例如一次规范的多项式为 x, 它是任意域 $\mathbb{F}_q$ 上的置换多项式. 对二次多项式来说, 若 q

为奇素数幂, 二次规范多项式为 x^2, 由例 6.1 (b) 知道它不是 $\mathbb{F}_q$ 上的置换多项式. 若 q 为 2 的方幂, 则二次规范多项式形为 $f_a(x)=x^2+ax$, 其中 $a\in\mathbb{F}_q$. 若 $a=0$, 由例 6.1 (b) 知道它是 $\mathbb{F}_q$ 上的置换多项式. 而若 $a\neq 0$, 则 $a+1\neq 1$ 但是 $f_a(a+1)=(a+1)^2+a(a+1)=a+1=f_a(1)$, 故 $f_a(x)$ 不是 $\mathbb{F}_q$ 上的置换多项式. 由此我们证明了当 q 为奇素数幂时, 无 $\mathbb{F}_q$ 上的二次置换多项式, 而当 q 为 2 的方幂时, 二次规范置换多项式为 x^2.

由例 6.1 知规范单项式 x^n 是 $\mathbb{F}_q$ 上的置换多项式当且仅当其次数 n 满足 $\gcd(n,q-1)=1$, 下面我们考察一类两项式.

定理 6.2: 设 q 为奇素数幂, $f(x)=x^{\frac{q+1}{2}}+ax$, 其中 $a\in\mathbb{F}_q$. 定义 $\mathbb{F}_q$ 到自身的映射 η 为 $\eta(\alpha)=\alpha^{\frac{q-1}{2}}$, 对任意 $\alpha\in\mathbb{F}_q$, 则 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\eta(a^2-1)=1$.

证明: 我们来证明由 $f(x)$ 给出的 $\mathbb{F}_q$ 上的映射 f 不是单射当且仅当 $\eta(a^2-1)\neq 1$.

首先设 f 不是单射, 若存在 $c\in\mathbb{F}_q^*$ 使得 $f(c)=f(0)$, 即 $c^{\frac{q+1}{2}}+ac=0$, 故 $a=-c^{\frac{q-1}{2}}$, 从而 $a^2-1=c^{q-1}-1=0$, 即 $\eta(a^2-1)=0$. 若存在 $b,c\in\mathbb{F}_q^*$, $b\neq c$ 使得 $f(b)=f(c)\neq f(0)=0$, 则有

$$b(a+b^{\frac{q-1}{2}})=c(a+c^{\frac{q-1}{2}}), \tag{8.3}$$

且 $a+b^{\frac{q-1}{2}}\neq 0$, $a+c^{\frac{q-1}{2}}\neq 0$. 若 $b^{\frac{q-1}{2}}=c^{\frac{q-1}{2}}$, 则由 (8.3) 可推出 $b=c$, 矛盾. 所以我们有 $b^{\frac{q-1}{2}}\neq c^{\frac{q-1}{2}}$. 由于 $\eta(b)=b^{\frac{q-1}{2}}=\pm 1$, $\eta(c)=c^{\frac{q-1}{2}}=\pm 1$, 不失一般性, 我们设 $\eta(b)=-1$ 且 $\eta(c)=1$. 由 (8.3) 得到 $bc^{-1}=(a+1)(a-1)^{-1}$, 从而

$$\begin{aligned}\eta(a^2-1) &= \eta(a+1)\eta(a-1)=\eta(a+1)\eta((a-1)^{-1})\\ &= \eta((a+1)(a-1)^{-1})=\eta(bc^{-1})\\ &= \eta(b)\eta(c^{-1})=\eta(b)\eta(c)=-1.\end{aligned}$$

反之, 设 $\eta(a^2-1)\neq 1$, 则有 $a^2-1=0$ 或 $\eta(a^2-1)=-1$. 若 $a^2-1=0$, 则 $a=\pm 1$, 从而存在 $c\in\mathbb{F}_q^*$ 使得 $a=-c^{\frac{q-1}{2}}$, 故 $f(c)=c^{\frac{q+1}{2}}+ac=0=f(0)$, 所以 f 不是单射. 若 $\eta(a^2-1)=-1$, 令 $b=(a+1)(a-1)^{-1}$, 则有 $\eta(b)=-1$, 即 $b^{\frac{q-1}{2}}=-1$, 所以

$$f(b)=b^{\frac{q+1}{2}}+ab=-b+ab=b(a-1)=a+1=f(1).$$

由于 $b\neq 1$, 所以 f 不是单射. □

对于 $\alpha\in\mathbb{F}_q^*$, 若存在 $\beta\in\mathbb{F}_q^*$ 使得 $\alpha=\beta^2$, 则称 α 为 $\mathbb{F}_q$ 中的非零平方元. 容易验证对任意 $\alpha\in\mathbb{F}_q^*$, α 为 $\mathbb{F}_q$ 中的非零平方元当且仅当 $\eta(\alpha)=1$, 而 α 为 $\mathbb{F}_q$ 中的非平方元当且仅当 $\eta(\alpha)=-1$. 进一步地, 若 q 为奇素数幂, 则 $\mathbb{F}_q$ 中的非零平方元和非平方元各有 $\frac{q-1}{2}$ 个, 而若 q 为 2 的方幂, 则 $\mathbb{F}_q^*$ 中每个元素都是非零平方元. 注意到在定理 6.2 中, $f(0)=0$, 若 x 为 $\mathbb{F}_q$ 中的非零平方元, 则 $f(x)=(1+a)x$, 而若 x 为 $\mathbb{F}_q$ 中的非平方元, 则 $f(x)=(-1+a)x$, 由此也可以得到定理的证明. 另外, 若 $\eta(a^2-1)=1$, 则存在 $b\in\mathbb{F}_q^*$ 使得 $a^2-1=b^2$. 令 $c=\frac{a+1}{b}$, 则 $c\in\mathbb{F}_q^*$ 且 $c^2=\frac{a+1}{a-1}\neq 1$, 故

$$a=\frac{(a+1)+(a-1)}{(a+1)-(a-1)}=\frac{\frac{a+1}{a-1}+1}{\frac{a+1}{a-1}-1}=\frac{c^2+1}{c^2-1}.$$

反之, 若存在 $c \in \mathbb{F}_q^*$ 且 $c^2 \neq 1$, 令 $a = \frac{c^2+1}{c^2-1}$, 则 $a^2 - 1 = \frac{4c^2}{(c^2-1)^2} = (\frac{2c}{c^2-1})^2$ 为 $\mathbb{F}_q$ 中的非零平方元, 故 $\eta(a^2-1) = 1$. 这样我们便证明了对于 $a \in \mathbb{F}_q$, $\eta(a^2-1) = 1$ 当且仅当存在 $c \in \mathbb{F}_q^* \setminus \{\pm 1\}$ 使得 $a = \frac{c^2+1}{c^2-1}$.

为了证明判定置换多项式的 Hermite 准则, 我们先证明如下引理.

引理 6.3: 设 $a_0, a_1, \ldots, a_{q-1} \in \mathbb{F}_q$ (这 q 个元素不一定互不相同), 则 q 个元素 $a_0, a_1, \ldots, a_{q-1}$ 互不相同当且仅当

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0, & \text{若 } 0 \leq t \leq q-2, \\ -1, & \text{若 } t = q-1, \end{cases}$$

其中的求和运算是 $\mathbb{F}_q$ 中的运算并且对任意 $c \in \mathbb{F}_q$ 有 $c^0 = 1$ (包括 c 为 $\mathbb{F}_q$ 中的零元).

证明: 对任意固定的 $0 \leq i \leq q-1$, 定义多项式

$$g_i(x) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j = 1 - (a_i^{q-1} + a_i^{q-2}x + \cdots + a_i x^{q-2} + x^{q-1}).$$

则有

$$g_i(a_i) = 1 - \sum_{j=0}^{q-1} a_i^{q-1} = 1 - q a_i^{q-1} = 1,$$

而对 $b \in \mathbb{F}_q \setminus \{a_i\}$,

$$g_i(b) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} b^j,$$

进一步地, 若 $a_i = 0$, 则有 $g_i(b) = 1 - b^{q-1} = 1 - 1 = 0$, 若 $a_i \neq 0$, 则

$$\sum_{j=0}^{q-1} a_i^{q-1-j} b^j = \sum_{j=0}^{q-1} a_i^{q-1} (a_i^{-1}b)^j = \sum_{j=0}^{q-1} (a_i^{-1}b)^j = \frac{1-(a_i^{-1}b)^q}{1-a_i^{-1}b} = \frac{1-a_i^{-1}b}{1-a_i^{-1}b} = 1,$$

所以这时我们依然有 $g_i(b) = 0$, 即我们得到对任意 $b \in \mathbb{F}_q$ 有

$$g_i(b) = \begin{cases} 1, & \text{若 } b = a_i, \\ 0, & \text{若 } b \neq a_i. \end{cases}$$

令

$$g(x) = \sum_{i=0}^{q-1} g_i(x) = \sum_{i=0}^{q-1} \left(1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j\right) = -\sum_{j=0}^{q-1} \left(\sum_{i=0}^{q-1} a_i^{q-1-j}\right) x^j,$$

若 $a_0, a_1, \ldots, a_{q-1}$ 互不相同, 即映射 $c \mapsto g(c)$ 把 $\mathbb{F}_q$ 中每个元素都映成 1, 又 $\deg(g) < q$, 由多项式表示的唯一性得到 $g(x) = 1$. 反之若 $a_0, a_1, \ldots, a_{q-1}$ 中有相同的元素, 则一定存在 $b \in \mathbb{F}_q$ 使得 $b \neq a_k$, $0 \leq k \leq q-1$, 从而 $g(b) = 0$, 故 $g(x) \neq 1$. 这表明 $a_0, a_1, \ldots, a_{q-1}$ 互不相同当且仅当 $g(x) = 1$, 而多项式 $g(x) = 1$ 当且仅当

$$-\sum_{i=0}^{q-1} a_i^{q-1-j} = \begin{cases} 1, & \text{若 } j = 0, \\ 0, & \text{若 } 1 \leq j \leq q-1, \end{cases}$$

这便证明了引理. □

对于 $f(x)\in\mathbb{F}_q[x]$, 显然 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\{f(c)\mid c\in\mathbb{F}_q\}=\mathbb{F}_q$, 由引理 6.3, 这又等价于

$$\sum_{c\in\mathbb{F}_q} f(c)^t=\begin{cases} 0, & \text{若 } 0\le t\le q-2,\\ -1, & \text{若 } t=q-1,\end{cases}$$

这就是判定置换多项式的 Hermite 准则. 注意到由多项式的表示形式 (6.2), 对任意 $1\le t\le q-2$, $f(x)^t$ 的表示式中 $1-(x-c)^{q-1}$ 前面的系数为 $f(c)^t$, 由此我们有下面的表述. 这里对任意多项式 $g(x)\in\mathbb{F}_q[x]$, 我们用 $g(x)\,(\mathrm{mod}\ x^q-x)$ 表示与 $g(x)$ 模 x^q-x 同余的那个唯一的次数 $<q$ 的多项式.

定理 6.4: (Hermite 准则) 设 $p=\mathrm{char}\mathbb{F}_q$, $f(x)\in\mathbb{F}_q[x]$, 则 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当下面两个条件成立:

(i) $f(x)$ 在 $\mathbb{F}_q$ 中恰有一个根.

(ii) 对任意 $1\le t\le q-2$ 且 $p\nmid t$, $f(x)^t\,(\mathrm{mod}\ x^q-x)$ 的次数 $\le q-2$.

证明: 由 (6.2) 显然有

$$f(x)^t\,(\mathrm{mod}\ x^q-x)=\sum_{c\in\mathbb{F}_q} f(c)^t\left(1-(x-c)^{q-1}\right),$$

故 $f(x)^t\,(\mathrm{mod}\ x^q-x)$ 中 x^{q-1} 的系数为 $-\sum_{c\in\mathbb{F}_q} f(c)^t$.

设 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式, 则由定理 6.1 知 $f(x)=0$ 在 $\mathbb{F}_q$ 中有唯一根, 故 (i) 成立. 进一步地, 由于 $\{f(c)\mid c\in\mathbb{F}_q\}=\mathbb{F}_q$, 由引理 6.3 知对任意 $1\le t\le q-2$, 有 $\sum_{c\in\mathbb{F}_q} f(c)^t=0$, 即 $f(x)^t\,(\mathrm{mod}\ x^q-x)$ 中 x^{q-1} 的系数为 0, 所以 $f(x)^t\,(\mathrm{mod}\ x^q-x)$ 的次数 $\le q-2$.

反之设多项式 $f(x)$ 满足条件 (i) 和 (ii), 由条件 (i) 得到

$$\sum_{c\in\mathbb{F}_q} f(c)^{q-1}=q-1=-1.$$

条件 (ii) 告诉我们, 对任意 $1\le t\le q-2$ 且 $p\nmid t$, 有 $\sum_{c\in\mathbb{F}_q} f(c)^t=0$. 而对于 $1\le t\le q-2$, 若 $p\mid t$, 不妨设 $t=p^js$, 其中 $j\ge 1$, $p\nmid s$, 则有

$$\sum_{c\in\mathbb{F}_q} f(c)^t=\sum_{c\in\mathbb{F}_q} f(c)^{p^js}=\left(\sum_{c\in\mathbb{F}_q} f(c)^s\right)^{p^j}=0^{p^j}=0,$$

又显然有 $\sum_{c\in\mathbb{F}_q} f(c)^0=q=0$, 这样我们便证明了

$$\sum_{c\in\mathbb{F}_q} f(c)^t=\begin{cases} 0, & \text{若 } 0\le t\le q-2,\\ -1, & \text{若 } t=q-1,\end{cases}$$

从而由引理 6.3 知 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式. □

推论 6.5: 设正整数 $d>1$ 且 $d\mid(q-1)$, 则不存在 $\mathbb{F}_q$ 上的 d 次置换多项式.

证明: 设多项式 $f(x)\in\mathbb{F}_q[x]$ 且 $\deg f(x)=d$, 则显然 $\deg(f(x)^{\frac{q-1}{d}})=q-1$. 又 $1\le\frac{q-1}{d}<q-1$ 且 $p\nmid\frac{q-1}{d}$, 其中 $p=\mathrm{char}\mathbb{F}_q$, 由定理 6.4 知 $f(x)$ 不是 $\mathbb{F}_q$ 上的置换多项式. □

由定理 6.4 的证明可以看出其条件 (ii) 中没有 $p\nmid t$ 的限制依然成立, 而它的条件 (i) 也可以用另外的条件来代替, 我们有如下结论, 其证明请读者自己给出.

定理 6.6: 设 $p=\mathrm{char}\mathbb{F}_q$, $f(x)\in\mathbb{F}_q[x]$, 则 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当下面两个条件成立:

(i) 多项式 $f(x)^{q-1}\pmod{x^q-x}$ 的次数为 $q-1$.

(ii) 对任意 $1\le t\le q-2$ 且 $p\nmid t$, $f(x)^t\pmod{x^q-x}$ 的次数 $\le q-2$.

□

定理 6.7: 设正整数 r 和 s 满足 $\gcd(r,q-1)=1$, $s\mid(q-1)$, 设 $g(x)\in\mathbb{F}_q[x]$ 且 $g(x^s)$ 在 $\mathbb{F}_q$ 中无非零根, 则 $f(x)=x^rg(x^s)^{\frac{q-1}{s}}$ 是 $\mathbb{F}_q$ 上的置换多项式.

证明: 显然 $f(x)$ 在 $\mathbb{F}_q$ 中只有一个根 0, 即定理 6.4 中条件 (i) 成立. 进一步地, 对任意 $1\le t\le q-2$, 我们有 $f(x)^t=x^{rt}g(x^s)^{\frac{q-1}{s}t}$. 容易验证对任意正整数 k 和 ℓ, 若 $k\equiv\ell\pmod{q-1}$, 则有 $x^k\equiv x^\ell\pmod{x^q-x}$. 下面我们分两种情形来讨论。

若 $s\nmid t$, 显然 $f(x)^t$ 的每一项的 x 的幂次为 $rt+sm$, 其中 m 为非负整数. 由已知条件易知 $\gcd(r,s)=1$, 故 $s\nmid(rt+sm)$, 从而 $(q-1)\nmid(rt+sm)$, 故 $f(x)^t\pmod{x^q-x}$ 中不会出现 x 的幂次为 $q-1$ 的项, 所以其次数 $\le q-2$.

若 $s\mid t$, 则 $f(x)^t=x^{rt}(g(x^s)^{q-1})^{\frac{t}{s}}$. 令 $h(x)=x^{rt}$, 则有 $f(0)^t=0=h(0)$, 而对任意 $c\in\mathbb{F}_q^*$, 由于 $g(x^s)$ 在 $\mathbb{F}_q$ 中无非零根, 所以 $g(c^s)\ne0$, 从而 $g(c^s)^{q-1}=1$, 故 $f(c)^t=c^{rt}(g(c^s)^{q-1})^{\frac{t}{s}}=c^{rt}=h(c)$, 这表明 $f(x)^t$ 和 $h(x)$ 给出的是 $\mathbb{F}_q$ 上的同一个映射, 所以 $f(x)^t\equiv x^{rt}\pmod{x^q-x}$. 由于 $(q-1)\nmid t$, 又 $\gcd(r,q-1)=1$, 所以 $(q-1)\nmid rt$, 类似地也得到 $f(x)^t\pmod{x^q-x}$ 的次数 $\le q-2$. 故两种情形下定理 6.4 的条件 (ii) 都成立, 从而由 Hermite 准则知 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式. □

设 $f(x)\in\mathbb{F}_q[x]$, 自然 $f(x)$ 也可以看成是 $\mathbb{F}_q$ 的扩域 $\mathbb{F}_{q^r}$ 上的多项式. 若 $f(x)$ 不是 $\mathbb{F}_q$ 上的置换多项式, 则 f 在 $\mathbb{F}_q$ 上不是单射, 自然 f 在 $\mathbb{F}_{q^r}$ 上也不是单射, 从而 $f(x)$ 不是 $\mathbb{F}_{q^r}$ 上的置换多项式. 那么反之如何? 或者若 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式, 那么它是否还是 $\mathbb{F}_{q^r}$ 上的置换多项式? 下面的例子表明这通常来说是不成立的.

例 6.2: 设 q 为奇素数幂, 定理 6.2 给出对于多项式 $f(x)=x^{\frac{q+1}{2}}+ax\in\mathbb{F}_q[x]$, $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 a^2-1 为 $\mathbb{F}_q$ 中的非零平方元. 设 $r>1$, 下面我们考察多项式 $f(x)$ 在扩域 $\mathbb{F}_{q^r}$ 上的情况.

若 $a=0$, 则 $f(x)=x^{\frac{q+1}{2}}$, 由例 6.1 (b) 得知 $f(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式当且仅当 $\gcd(\frac{q+1}{2},q^r-1)=1$. 如此得到在很多情形下 $f(x)$ 不是 $\mathbb{F}_{q^r}$ 上的置换多项式, 比如 r 为偶数或者 r 为奇数但是 $q\equiv3\pmod4$ 等情形.

下面设 $a \neq 0$, 若 r 为偶数, 则由于 $f(x)$ 的次数 $d = \frac{q+1}{2}$ 满足 $d > 1$ 且 $d \mid (q^r - 1)$, 由推论 6.5 知 $f(x)$ 不是 $\mathbb{F}_{q^r}$ 上的置换多项式. 若 r 为奇数, 令 $m = \frac{q-1}{2}$, 则 $m + 1 = \frac{q+1}{2}$, 从而 $f(x) = x^{m+1} + ax$. 又显然有 $q^r \equiv -1 \equiv m \pmod{m+1}$, 故存在正整数 k 使得 $q^r = k(m+1)+m$, 由 $r > 1$ 容易得到 $k > 1$. 注意到

$$k(m+1) = q^r - m \equiv q - m = m + 1 \pmod{q},$$

又 $\gcd(q, m+1) = 1$, 由此我们得到 $k \equiv 1 \pmod{q}$. 显然有 $1 < k + m - 1 \leq q^r - 2$, 下面我们考察 $f(x)^{k+m-1} \pmod{x^{q^r} - x}$ 的次数. 由二项式定理有

$$\begin{aligned} f(x)^{k+m-1} &= (x^{m+1} + ax)^{k+m-1} = \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} (x^{m+1})^{k+m-1-j} (ax)^j \\ &= \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} a^j x^{q^r + m^2 - m - 1 - jm}. \end{aligned}$$

若 $j \geq m$, 则对应项 x 的幂次为 $q^r + m^2 - m - 1 - jm \leq q^r - 2$. 若 $0 \leq j \leq m-2$, 则一方面有

$$q^r + m^2 - m - 1 - jm \geq q^r + m^2 - m - 1 - (m-2)m = q^r + m - 1 \geq q^r,$$

另一方面有

$$q^r + m^2 - m - 1 - jm \leq q^r + m^2 - m - 1 = q^r + \left(\frac{q-1}{2}\right)^2 - \frac{q-1}{2} - 1 \leq 2q^r - 3,$$

所以 $1 \leq q^r + m^2 - m - 1 - jm \pmod{q^r - 1} \leq q^r - 2$. 这表明在 $j \geq m$ 和 $0 \leq j \leq m-2$ 时, 都有 $x^{q^r + m^2 - m - 1 - jm} \pmod{x^{q^r} - x}$ 的次数 $\leq q^r - 2$. 对于剩下的一项 $j = m-1$, 我们有 $q^r + m^2 - m - 1 - jm = q^r - 1$, 而这一项的系数 $\binom{k+m-1}{m-1} a^{m-1}$ 在 $\mathbb{F}_{q^r}$ 中非零 (自己证明), 从而 $f(x)^{k+m-1} \pmod{x^{q^r} - x}$ 的次数为 $q^r - 1$, 由定理 6.4 得到多项式 $f(x)$ 不是 $\mathbb{F}_{q^r}$ 上的置换多项式 (注意到前面已指出定理 6.4 条件 (ii) 中 $p \nmid t$ 的限制并不必要). 这便证出, 对任意 $a \in \mathbb{F}_q^*$ 和任意 $r > 1$, 多项式 $f(x) = x^{\frac{q+1}{2}} + ax$ 不是 $\mathbb{F}_{q^r}$ 上的置换多项式. □

例 6.2 表明 $\mathbb{F}_q$ 上的置换多项式不一定还是 $\mathbb{F}_q$ 的扩域上的置换多项式, 所以提到置换多项式, 我们一定要强调是哪个域上的. 例 6.2 还显示 $\mathbb{F}_q$ 上的置换多项式同时还是 $\mathbb{F}_q$ 的任意扩域上的置换多项式应该是很少的, 事实上, 这样的多项式我们可以完全给出, 见如下定理.

定理 6.8: 设 $f(x) \in \mathbb{F}_q[x]$, 则对任意 $r \geq 1$, $f(x)$ 是每一个 $\mathbb{F}_{q^r}$ 上的置换多项式当且仅当 $f(x) = ax^{p^t} + b$, 其中 $a, b \in \mathbb{F}_q$, $a \neq 0$, $p = \mathrm{char}\mathbb{F}_q$, t 为非负整数.

证明: 对任意 $r \geq 1$, 由于 $\gcd(p^t, q^r - 1) = 1$, 由例 6.1 知 $h(x) = x^{p^t}$ 是 $\mathbb{F}_{q^r}$ 上的置换多项式, 又 $g(x) = ax + b$ 也是 $\mathbb{F}_{q^r}$ 上的置换多项式, 所以 $f(x) = g(h(x))$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式.

反之, 设 $f(x)$ 是每一个 $\mathbb{F}_{q^r}$ 上的置换多项式, 则首先 $f(x)$ 是 $\mathbb{F}_q$ 上的置换多项式, 故对任意 $c \in \mathbb{F}_q$, $f(x) = c$ 在 $\mathbb{F}_q$ 中有唯一根 d_c (依赖于给定的 c), 从而 $f(x) - c = (x - d_c)^{k_c} g_c(x)$, 其中 k_c 为正整数, $g_c(x) \in \mathbb{F}_q[x]$. 若 $g_c(x)$ 不是非零常数, 则 $g_c(x)$ 在 $\mathbb{F}_q[x]$ 中的每个不可约因式的次数都 ≥ 2. 取 $g_c(x)$ 在 $\mathbb{F}_q[x]$ 中的一个不可约因式 $g_{c1}(x)$, 设 $\deg(g_{c1}(x)) = e \geq 2$, 则 $g_{c1}(x)$ 在域 $\mathbb{F}_{q^e}$ 中有根. 故方程 $f(x) = c$ 在 $\mathbb{F}_{q^e}$ 中除了根 d_c 之外还有其它的根, 与 $f(x)$ 是 $\mathbb{F}_{q^e}$ 上的

置换多项式矛盾, 所以 $g_c(x)$ 为非零常数 a_c, 即

$$f(x)-c=a_c(x-d_c)^{k_c}. \tag{6.4}$$

注意到从前面看多项式 $g_c(x)$ 和正整数 k_c 都与 c 的选取有关, 但式 (6.4) 告诉我们 a_c 是 $f(x)$ 的首项系数, k_c 是 $f(x)$ 的次数, 所以实际上它们均与 c 的选取无关. 下面记 $a_c=a$, $k_c=k$. 由于式 (6.4) 对 $\mathbb{F}_q$ 中的任意元素 c 都成立, 特别地, 取 $c=0$ 和 $c=1$, 我们得到 $f(x)=a(x-d_0)^k=1+a(x-d_1)^k$, 即 $a(x-d_0)^k-a(x-d_1)^k=1$. 用 $x+d_1$ 代替 x 得到 $a(x+d_1-d_0)^k=ax^k+1$, 从而 $a(d_1-d_0)^k=1$, 故 $d_1-d_0\neq 0$. 又对 $1\leq j\leq k-1$ 有 $\binom{k}{j}a(d_1-d_0)^j=0$, 由此得到对每个 $1\leq j\leq k-1$ 有 $p\mid\binom{k}{j}$. 由于 k 为正整数, 所以存在非负整数 t 使得 $p^t\leq k<p^{t+1}$. 若 $k\neq p^t$, 则 $1\leq p^t\leq k-1$, 又容易验证 $p\nmid\binom{k}{p^t}$, 矛盾, 从而 $k=p^t$, 由此得到 $f(x)-c=a(x-d_c)^{p^t}$. 特别地, 令 $b=f(0)$, 则 $f(x)=b$ 的唯一根 $d_b=0$, 故 $f(x)=ax^{p^t}+b$. □

由定理 6.8, 可以立得如下推论.

推论 6.9: 对任意 $r\geq 1$, 在每个域 $\mathbb{F}_{q^r}$ 上都是置换多项式的规范多项式一定为 x^{p^t}, 其中 $p=\mathrm{char}\mathbb{F}_q$, t 为非负整数. 进一步地, 若多项式 $f(x)\in\mathbb{F}_q[x]$ 的规范形不是 x^{p^t}, 则一定有 $\mathbb{F}_q$ 的无穷多个扩域 $\mathbb{F}_{q^s}$ 使得 $f(x)$ 不是 $\mathbb{F}_{q^s}$ 上的置换多项式. □

6.2 Dickson 多项式与线性化多项式的置换性质

域 $\mathbb{F}_q$ 上的置换多项式共有 $q!$ 个, 每一个都可以由 Lagrange 插值公式 (6.1) 或式 (6.2) 给出, 所以构造一个一般的置换多项式并不太困难. 一般地, 我们只对具有简洁代数表示或者具有其它特别性质的置换多项式感兴趣, 而这些其它的特别性质来源于在数学的其它领域或者工程上的应用, 通常来说, 构造这样的置换多项式就比较困难. 本节我们来讨论两类具有特别形式的多项式的置换性质.

设 n 为正整数, 则 x^n+y^n 是整数环 $\mathbb{Z}$ 上的以 x 和 y 为未定元的二元对称多项式, 所以它可以用二元初等对称多项式 $\sigma_1=x+y$, $\sigma_2=xy$ 的多项式表出, 即存在二元多项式 $D_n(x,y)$ 使得 $x^n+y^n=D_n(\sigma_1,\sigma_2)$. 对于 $n\geq 2$, 由

$$x^n+y^n=(x+y)(x^{n-1}+y^{n-1})-xy(x^{n-2}+y^{n-2})$$

得到 $D_n(\sigma_1,\sigma_2)=\sigma_1D_{n-1}(\sigma_1,\sigma_2)-\sigma_2D_{n-2}(\sigma_1,\sigma_2)$, 或写为

$$D_n(x,y)=xD_{n-1}(x,y)-yD_{n-2}(x,y), \tag{6.4}$$

又显然 $D_0(x,y)=2$, $D_1(x,y)=x$, 这便给出 $D_n(x,y)$ 的递推关系和初始条件, 由此可以对任意正整数 n 得到多项式 $D_n(x,y)$. 例如 $D_2(x,y)=x^2-2y$, $D_3(x,y)=x^3-3xy$, $D_4(x,y)=x^4-4x^2y+2y^2$ 等等. 由递推关系 (6.4) 和初始条件容易看出 $D_n(x,y)$ 也是整系数多项式, 即 $D_n(x,y)\in\mathbb{Z}[x,y]$.

利用如上的递推关系 (6.4) 和初始条件我们可以给出多项式 $D_n(x,y)$ 的精确表达式. 设 $D_n(x,y)$ 的生成函数为

$$f(t)=\sum_{n=0}^{\infty}D_n(x,y)t^n,$$

则有

$$\begin{aligned}
f(t) &= 2+xt+\sum_{n=2}^{\infty}D_n(x,y)t^n\\
&= 2+xt+\sum_{n=2}^{\infty}(xD_{n-1}(x,y)-yD_{n-2}(x,y))t^n\\
&= 2+xt+xt\sum_{n=2}^{\infty}D_{n-1}(x,y)t^{n-1}-yt^2\sum_{n=2}^{\infty}D_{n-2}(x,y)t^{n-2}\\
&= 2+xt+xt(f(t)-2)-yt^2f(t)=2-xt+(xt-yt^2)f(t),
\end{aligned}$$

故

$$\begin{aligned}
f(t) &= \frac{2-xt}{1-xt+yt^2}=(2-xt)\frac{1}{1-(xt-yt^2)}=(2-xt)\sum_{k\geq 0}(xt-yt^2)^k\\
&= (2-xt)\sum_{k\geq 0}\sum_{i=0}^{k}\binom{k}{i}(xt)^{k-i}(-yt^2)^i\\
&= (2-xt)\sum_{k\geq 0}\sum_{i=0}^{k}(-1)^i\binom{k}{i}x^{k-i}y^it^{k+i}\\
&= (2-xt)\sum_{n\geq 0}\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^i\binom{n-i}{i}x^{n-2i}y^it^n\\
&= \sum_{n\geq 0}\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^i2\binom{n-i}{i}x^{n-2i}y^it^n-\sum_{n\geq 0}\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^i\binom{n-i}{i}x^{n+1-2i}y^it^{n+1}\\
&= \sum_{n\geq 0}\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^i2\binom{n-i}{i}x^{n-2i}y^it^n-\sum_{n\geq 1}\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^i\binom{n-1-i}{i}x^{n-2i}y^it^n\\
&= 2+\sum_{n\geq 1}\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^i\left[2\binom{n-i}{i}-\binom{n-1-i}{i}\right]x^{n-2i}y^it^n\\
&= 2+\sum_{n\geq 1}\left(\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^i\frac{n}{n-i}\binom{n-i}{i}x^{n-2i}y^i\right)t^n,
\end{aligned}$$

从而对任意 $n\geq 1$, 我们有

$$D_n(x,y)=\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^i\frac{n}{n-i}\binom{n-i}{i}x^{n-2i}y^i.$$

对任意整数 $n \geq 0$ 和 $a \in \mathbb{F}_q$, 称多项式

$$D_n(x,a) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i \frac{n}{n-i} \binom{n-i}{i} a^i x^{n-2i} \in \mathbb{F}_q[x]$$

为第 n 个具有参数 a 的 Dickson 多项式, 其中定义 $D_0(x,a) = 2$. 容易计算出 $D_1(x,a) = x$, 由递推关系 (6.4) 我们得到对 $n \geq 2$ 有 $D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a)$, 由此容易得到对任意 $n \geq 1$, Dickson 多项式 $D_n(x,a)$ 首一且次数为 n. 对开始的几个 n, 容易算出 $D_2(x,a) = x^2 - 2a$, $D_3(x,a) = x^3 - 3ax$, $D_4(x,a) = x^4 - 4ax^2 + 2a^2$ 等等.

设 R 是一个交换环, 注意到 $D_n(x,y)$ 的系数为整数, 所以对于 $a \in R$, $D_n(x,a)$ 就是环 R 上的多项式. 特别地, 若把 $D_n(x,a)$ 看成是复数域 $\mathbb{C}$ 上的多项式, 则它与 Chebyshev 多项式 $T_n(x) = \cos(n \arccos x)$ 有关. 事实上, 由 Dickson 多项式的定义, 对任意复数 x_1, x_2 我们有 $D_n(x_1 + x_2, x_1x_2) = x_1^n + x_2^n$. 令 $x_1 = e^{i\theta}$, $x_2 = e^{-i\theta}$, 则有 $x_1 + x_2 = 2\cos\theta$, $x_1x_2 = 1$, 从而

$$D_n(2\cos\theta, 1) = e^{in\theta} + e^{-in\theta} = 2\cos n\theta,$$

故 $D_n(2x,1) = 2\cos(n \arccos x) = 2T_n(x)$. 进一步地, 设 F 是任意域, 则在 F 的有理分式域 $F(y)$ 上有

$$D_n\left(y + \frac{a}{y}, a\right) = y^n + \frac{a^n}{y^n}.$$

对于 $a, b \in F$ 且 $b \neq 0$, 我们有

$$D_n(x, ab^2) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i \frac{n}{n-i} \binom{n-i}{i} a^i b^n (b^{-1}x)^{n-2i} = b^n D_n(b^{-1}x, a).$$

若 a 为 F 中的非零平方元, 即存在 $b \in F^*$ 使得 $a = b^2$, 则有 $D_n(x,a) = b^n D_n(b^{-1}x, 1)$. 若 a 为 F 中的非平方元, 设 c 为 F 中一个固定的非平方元, 则存在 $b \in F^*$ 使得 $a = b^2c$, 从而 $D_n(x,a) = b^n D_n(b^{-1}x, c)$. 这表明对任意 $a \in F^*$, 域 F 上的 Dickson 多项式 $D_n(x,a)$ 可用 $D_n(x,1)$ 或者 $D_n(x,c)$ 来表示, 若 $F = \mathbb{C}$, 则存在非零复数 b 使得 $a = b^2$, 从而

$$D_n(x,a) = b^n D_n(b^{-1}x, 1) = b^n D_n(2(2b)^{-1}x, 1) = 2b^n T_n((2b)^{-1}x).$$

下面继续讨论有限域 $\mathbb{F}_q$ 上的 Dickson 多项式 $D_n(x,a)$, 若 $a = 0$, 则显然 $D_n(x,0) = x^n$, 例 6.1 (b) 已经给出 $D_n(x,0)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(n, q-1) = 1$. 当 $a \neq 0$ 时, 则有 $a = b^2$ 或者 b^2c, 其中 $b \in \mathbb{F}_q^*$, c 为 $\mathbb{F}_q$ 中一个固定的非平方元, 从而 $D_n(x,a) = b^n D_n(b^{-1}x, 1)$ 或者 $b^n D_n(b^{-1}x, c)$, 由此看出 $D_n(x,a)$ 是否为 $\mathbb{F}_q$ 上的置换多项式并不依赖于 a, 我们有如下定理.

定理 6.10: 设 $a \in \mathbb{F}_q^*$, 则 Dickson 多项式 $D_n(x,a)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(n, q^2 - 1) = 1$.

证明: 对任意 $b \in \mathbb{F}_q$, $y^2 - by + a$ 在 $\mathbb{F}_{q^2}$ 中有根 β, 由于 $a \neq 0$, 所以 $\beta \neq 0$, 又由 $\beta^2 - b\beta + a = 0$

得到 $b=\beta+\frac{a}{\beta}$, 从而

$$D_n(b,a)=D_n\left(\beta+\frac{a}{\beta},a\right)=\beta^n+\frac{a^n}{\beta^n}.$$

先证充分性, 设 $\gcd(n,q^2-1)=1$. 设 $b,c\in\mathbb{F}_q$ 满足 $D_n(b,a)=D_n(c,a)$, 设 $\beta,\gamma\in\mathbb{F}_{q^2}$ 分别是 y^2-by+a 和 y^2-cy+a 的根, 则有

$$\beta^n+\frac{a^n}{\beta^n}=\gamma^n+\frac{a^n}{\gamma^n},$$

故 $(\beta^n-\gamma^n)((\beta\gamma)^n-a^n)=0$, 由此得到 $\beta^n=\gamma^n$ 或者 $(\beta\gamma)^n=a^n$. 由 $\gcd(n,q^2-1)=1$ 知 x^n 为 $\mathbb{F}_{q^2}$ 上的置换多项式, 从而 $\beta=\gamma$ 或者 $\beta=\frac{a}{\gamma}$, 这便得出 $b=c$, 所以 $D_n(x,a)$ 是 $\mathbb{F}_q$ 上的置换多项式.

再证必要性, 用反证法, 设 $d=\gcd(n,q^2-1)>1$. 若 d 为偶数, 则 n 为偶数且 q 为奇数, 这时对于 $c\in\mathbb{F}_q^*$, 我们有 $c\neq -c$, 但是 $D_n(x,a)$ 中每一项 x 的幂次都是偶数, 所以 $D_n(c,a)=D_n(-c,a)$, 从而 $D_n(x,a)$ 不是 $\mathbb{F}_q$ 上的置换多项式. 若 d 为奇数, 则 d 有素因子 $r\geq 3$, 从而 $r\mid n$ 且 $r\mid(q^2-1)=(q+1)(q-1)$, 由 r 为素数我们可以得到 $r\mid n$ 且 $r\mid(q-1)$ 或者 $r\mid n$ 且 $r\mid(q+1)$.

若 $r\mid n$ 且 $r\mid(q-1)$. 注意到方程 $x^r=1$ 在 $\mathbb{F}_q$ 中有 $\gcd(r,q-1)=r$ 个根, 由于 $r\geq 3$, 所以存在 $b\in\mathbb{F}_q$ 使得 $b^r=1$ 但是 $b\neq 1$, $b\neq a$ (若 $a^r\neq 1$ 则显然 $b\neq a$), 从而 $b+\frac{a}{b}\neq 1+a$. 又

$$D_n\left(b+\frac{a}{b},a\right)=b^n+\frac{a^n}{b^n}=1+a^n=D_n(1+a,a),$$

所以 $D_n(x,a)$ 不是 $\mathbb{F}_q$ 上的置换多项式.

若 $r\mid n$ 且 $r\mid(q+1)$. 由于 $a\in\mathbb{F}_q^*$, 所以 $x^{q+1}=\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x)=a$ 在 $\mathbb{F}_{q^2}^*$ 中有 $\frac{q^2-1}{q-1}=q+1$ 个根, 设 $\gamma\in\mathbb{F}_{q^2}^*$ 满足 $\gamma^{q+1}=a$. 又 $r\mid(q^2-1)$, 故 $x^r=1$ 在 $\mathbb{F}_{q^2}$ 中有 r 个根, 所以存在 $\beta\in\mathbb{F}_{q^2}$ 使得 $\beta^r=1$ 但是 $\beta\neq 1$, $\beta\neq a\gamma^{-2}$, 从而 $\gamma+\frac{a}{\gamma}\neq\beta\gamma+\frac{a}{\beta\gamma}$. 又由 $\gamma+\frac{a}{\gamma}=\gamma+\gamma^q=\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\gamma)\in\mathbb{F}_q$, $\beta\gamma+\frac{a}{\beta\gamma}=\beta\gamma+(\beta\gamma)^q=\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta\gamma)\in\mathbb{F}_q$, 和

$$D_n\left(\gamma+\frac{a}{\gamma},a\right)=\gamma^n+\frac{a^n}{\gamma^n}=(\beta\gamma)^n+\frac{a^n}{(\beta\gamma)^n}=D_n\left(\beta\gamma+\frac{a}{\beta\gamma},a\right)$$

得到 $D_n(x,a)$ 不是 $\mathbb{F}_q$ 上的置换多项式. □

Dickson 多项式在置换多项式的讨论中非常重要, Schur 在 1922 年提出如下猜想: 把整系数多项式 $f(x)$ 的系数模素数 p 后看成是 $\mathbb{F}_p$ 上的多项式, 若存在无穷多个素数 p 使得 $f(x)$ 是 $\mathbb{F}_p$ 上的置换多项式, 则 $f(x)$ 一定为二项式 ax^n+b 和 Dickson 多项式的合成. Schur 本人证明了 $\deg(f)$ 为素数的情形, 1970 年 Fried 证明了 Schur 猜想.

例 6.1 (c) 给出了一个 p-多项式为置换多项式的充要条件, 下面我们考察一般的线性化多项式. 设

$$L(x)=\sum_{i=0}^{r-1}\alpha_i x^{q^i}\in\mathbb{F}_{q^r}[x]$$

为 $\mathbb{F}_{q^r}$ 上的一个 q-多项式, 把 $\mathbb{F}_{q^r}$ 看作是 $\mathbb{F}_q$ 上的线性空间, 则 $L:\gamma\mapsto L(\gamma)$ 是 $\mathbb{F}_{q^r}$ 上的线性变换, 类似于例 6.1 (c), $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式当且仅当 $L(x)$ 在 $\mathbb{F}_{q^r}$ 中只有零根. 这个结论在判断一个具体给定的 q-多项式是否为置换多项式时不太好用, 下面我们给出利用给定 q-多项式的系数来判定其是否为置换多项式的结论.

依然利用 L 为 $\mathbb{F}_{q^r}$ 上的线性变换这个性质, 由线性代数可知变换 L 为双射当且仅当 $\mathbb{F}_{q^r}$ 的一组基在 L 下的像仍为 $\mathbb{F}_{q^r}$ 的一组基. 设 $\{\beta_1,\beta_2,\ldots,\beta_r\}$ 是 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基, 记矩阵

$$B=\begin{pmatrix}\beta_1 & \beta_2 & \cdots & \beta_{r-1} & \beta_r\\ \beta_1^q & \beta_2^q & \cdots & \beta_{r-1}^q & \beta_r^q\\ \vdots & \vdots & & \vdots & \vdots\\ \beta_1^{q^{r-2}} & \beta_2^{q^{r-2}} & \cdots & \beta_{r-1}^{q^{r-2}} & \beta_r^{q^{r-2}}\\ \beta_1^{q^{r-1}} & \beta_2^{q^{r-1}} & \cdots & \beta_{r-1}^{q^{r-1}} & \beta_r^{q^{r-1}}\end{pmatrix},$$

由推论 3.9 得到行列式 $\det(B)\neq 0$. 令 $\gamma_j=L(\beta_j)$, $1\leq j\leq r$, 并记

$$C=\begin{pmatrix}\gamma_1 & \gamma_2 & \cdots & \gamma_{r-1} & \gamma_r\\ \gamma_1^q & \gamma_2^q & \cdots & \gamma_{r-1}^q & \gamma_r^q\\ \vdots & \vdots & & \vdots & \vdots\\ \gamma_1^{q^{r-2}} & \gamma_2^{q^{r-2}} & \cdots & \gamma_{r-1}^{q^{r-2}} & \gamma_r^{q^{r-2}}\\ \gamma_1^{q^{r-1}} & \gamma_2^{q^{r-1}} & \cdots & \gamma_{r-1}^{q^{r-1}} & \gamma_r^{q^{r-1}}\end{pmatrix}$$

和

$$A(L)=\begin{pmatrix}\alpha_0 & \alpha_1 & \cdots & \alpha_{r-2} & \alpha_{r-1}\\ \alpha_{r-1}^q & \alpha_0^q & \cdots & \alpha_{r-3}^q & \alpha_{r-2}^q\\ \vdots & \vdots & & \vdots & \vdots\\ \alpha_2^{q^{r-2}} & \alpha_3^{q^{r-2}} & \cdots & \alpha_0^{q^{r-2}} & \alpha_1^{q^{r-2}}\\ \alpha_1^{q^{r-1}} & \alpha_2^{q^{r-1}} & \cdots & \alpha_{r-1}^{q^{r-1}} & \alpha_0^{q^{r-1}}\end{pmatrix},\tag{6.5}$$

则有 $C=A(L)B$, 从而 $\det(C)=\det(A(L))\det(B)$. 这样我们得到 $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式当且仅当 $\{\gamma_1,\gamma_2,\ldots,\gamma_r\}$ 是 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基, 由推论 3.9 得知这也当且仅当 $\det(C)\neq 0$, 而后者显然等价于 $\det(A(L))\neq 0$, 由此我们证明了如下定理.

定理 6.11: 设 $L(x)=\sum_{i=0}^{r-1}\alpha_i x^{q^i}\in\mathbb{F}_{q^r}[x]$ 为 $\mathbb{F}_{q^r}$ 上的一个 q-多项式, 则 $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式当且仅当 $\det(A(L))\neq 0$, 其中矩阵 $A(L)$ 由式 (6.5) 给出. □

注意到实际上定理 6.11 是习题 4.27 的一个推论. 进一步地容易验证 $(\det(A(L)))^q=\det(A(L))$ (为什么?), 所以虽然 $A(L)$ 是 $\mathbb{F}_{q^r}$ 上的矩阵, 但其行列式却在 $\mathbb{F}_q$ 中.

设 $L(x)\in\mathbb{F}_{q^r}[x]$ 为 $\mathbb{F}_{q^r}$ 上的一个 q-多项式, 取定 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基 $\{\omega_1,\omega_2,\ldots,\omega_r\}$, 对任意 $x\in\mathbb{F}_{q^r}$, $L(x)$ 可被 $\{\omega_1,\omega_2,\ldots,\omega_r\}$ 唯一线性表出, 设

$$L(x)=L_1(x)\omega_1+L_2(x)\omega_2+\cdots+L_r(x)\omega_r,$$

其中 $L_i(x) \in \mathbb{F}_q$, $1 \le i \le r$. 由 L 为 $\mathbb{F}_{q^r}$ 上的线性变换容易得到 $L_i : x \mapsto L_i(x)$ 为 $\mathbb{F}_{q^r}$ 到 $\mathbb{F}_q$ 的线性映射, 由定理 3.5 知存在 $\theta_i \in \mathbb{F}_{q^r}$ 使得 $L_i(x) = \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\theta_i x)$, 从而存在 $\theta_1, \theta_2, \ldots, \theta_r \in \mathbb{F}_{q^r}$ 使得

$$L(x) = \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\theta_1 x)\omega_1 + \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\theta_2 x)\omega_2 + \cdots + \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\theta_r x)\omega_r. \tag{6.6}$$

反之, 设 $\theta_1, \theta_2, \ldots, \theta_r$ 为 $\mathbb{F}_{q^r}$ 中的任意 r 个元素, 由 (6.6) 式给出的多项式 $L(x)$ 为

$$L(x) = \sum_{j=0}^{r-1} \left(\sum_{i=1}^{r} \theta_i^{q^j} \omega_i \right) x^{q^j},$$

它显然为 $\mathbb{F}_{q^r}$ 上的 q-多项式. 这样我们得到 $L(x) \in \mathbb{F}_{q^r}[x]$ 为 $\mathbb{F}_{q^r}$ 上的 q-多项式当且仅当 $L(x)$ 形如式 (6.6).

定理 6.12: 设 $\{\omega_1, \omega_2, \ldots, \omega_r\}$ 为 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基, $L(x)$ 是由 (6.6) 给出的 $\mathbb{F}_{q^r}$ 上的 q-多项式, 则 $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式当且仅当 $\{\theta_1, \theta_2, \ldots, \theta_r\}$ 为 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基.

证明: 设 $W = \langle \theta_1, \theta_2, \ldots, \theta_r \rangle$ 是 $\mathbb{F}_{q^r}$ 的由 $\theta_1, \theta_2, \ldots, \theta_r$ 生成的子空间, 定义

$$W^{\perp} = \{x \in \mathbb{F}_{q^r} \mid \text{对所有 } \theta \in W \text{ 有 } \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\theta x) = 0\}.$$

注意到 $(x, y) \mapsto \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(xy)$ 是 $\mathbb{F}_{q^r}$ 上的非退化对称双线性函数, 所以 $W^{\perp}$ 是 $\mathbb{F}_{q^r}$ 的子空间且 $\dim_{\mathbb{F}_q} W^{\perp} = r - \dim_{\mathbb{F}_q} W$. 由 (6.6) 易知 $\beta \in \mathbb{F}_{q^r}$ 满足 $L(\beta) = 0$ 当且仅当对每个 i 都有 $\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\theta_i \beta) = 0$, $1 \le i \le r$, 而后者等价于对所有 $\theta \in W$ 有 $\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\theta\beta) = 0$, 即等价于 $\beta \in W^{\perp}$. 由此我们得到 $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式当且仅当 $L(x)$ 在 $\mathbb{F}_{q^r}$ 中只有零根, 即当且仅当 $W^{\perp} = \{0\}$, 这等价于 $\dim_{\mathbb{F}_q} W = r$, 即 $\theta_1, \theta_2, \ldots, \theta_r$ 在 $\mathbb{F}_q$ 上线性无关, 也等价于 $\{\theta_1, \theta_2, \ldots, \theta_r\}$ 为 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基. □

由第 3.2 节我们知道 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的基共有 $(q^r - 1)(q^r - q) \cdots (q^r - q^{r-1})$ 个, 我们有下面的推论.

推论 6.13: 域 $\mathbb{F}_{q^r}$ 上置换 q-多项式共有 $(q^r - 1)(q^r - q) \cdots (q^r - q^{r-1})$ 个. □

与定理 6.12 对偶地, 我们有如下定理.

定理 6.14: 设 $\{\theta_1, \theta_2, \ldots, \theta_r\}$ 为 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基, $L(x)$ 是由 (6.6) 给出的 $\mathbb{F}_{q^r}$ 上的 q-多项式, 则 $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式当且仅当 $\{\omega_1, \omega_2, \ldots, \omega_r\}$ 为 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基.

证明: 充分性由定理 6.12 立得. 反之, 因为对任意 $x \in \mathbb{F}_{q^r}$ 和每个 i 都有 $\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\theta_i x) \in \mathbb{F}_q$, $1 \le i \le r$, 由式 (6.6) 可得 $L(\mathbb{F}_{q^r}) \subseteq \langle \omega_1, \omega_2, \ldots, \omega_r \rangle$. 若 $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式, 则有 $\mathbb{F}_{q^r} = L(\mathbb{F}_{q^r})$, 由此得到 $\mathbb{F}_{q^r} = \langle \omega_1, \omega_2, \ldots, \omega_r \rangle$, 从而 $\{\omega_1, \omega_2, \ldots, \omega_r\}$ 为 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基. □

设 α 是 $\mathbb{F}_{q^r}$ 的一个本原元素, 则 $\{1, \alpha, \ldots, \alpha^{r-1}\}$ 是 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基. 任取 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基 $\{\alpha_0, \alpha_1, \ldots, \alpha_{r-1}\}$, 由定理 6.14, 我们得到 $\mathbb{F}_{q^r}$ 上的置换 q-多项式

$$L(x) = \sum_{i=0}^{r-1} \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha^i x)\alpha_i = \sum_{i=0}^{r-1} \left(\sum_{j=0}^{r-1} (\alpha^i x)^{q^j} \right) \alpha_i = \sum_{j=0}^{r-1} \left(\sum_{i=0}^{r-1} \alpha_i \alpha^{iq^j} \right) x^{q^j}.$$

显然不同的基 $\{\alpha_0,\alpha_1,\ldots,\alpha_{r-1}\}$ 给出的置换 q-多项式 $L(x)$ 也不同 (为什么?), 由于 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的基的个数与 $\mathbb{F}_{q^r}$ 上的置换 q-多项式的个数都是 $(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})$, 我们有如下推论.

推论 6.15: 设 α 是 $\mathbb{F}_{q^r}$ 的一个本原元素, 则当 $\{\alpha_0,\alpha_1,\ldots,\alpha_{r-1}\}$ 跑遍 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的所有基时,

$$L(x)=\sum_{j=0}^{r-1}\left(\sum_{i=0}^{r-1}\alpha_i\alpha^{iq^j}\right)x^{q^j}$$

给出所有的 $\mathbb{F}_{q^r}$ 上的置换 q-多项式. □

注意到在推论 6.15 中取 $\alpha\in\mathbb{F}_{q^r}$ 使得 α 在 $\mathbb{F}_q$ 上的次数为 r 即可, 这时 $\{1,\alpha,\ldots,\alpha^{r-1}\}$ 仍为 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基. 再任取某个 $\beta\in\mathbb{F}_{q^r}^*$, 则 $\{\beta,\alpha\beta,\ldots,\alpha^{r-1}\beta\}$ 也是 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的一组基, 所以当 $\{\alpha_0,\alpha_1,\ldots,\alpha_{r-1}\}$ 跑遍 $\mathbb{F}_{q^r}$ 在 $\mathbb{F}_q$ 上的所有基时,

$$L(x)=\sum_{i=0}^{r-1}\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha^i\beta x)\alpha_i=\sum_{j=0}^{r-1}\beta^{q^j}\left(\sum_{i=0}^{r-1}\alpha_i\alpha^{iq^j}\right)x^{q^j}$$

也给出了所有的 $\mathbb{F}_{q^r}$ 上的置换 q-多项式.

设 $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的 q-多项式, 前面我们已经讨论了 $L(x)$ 在 $\mathbb{F}_{q^r}$ 上的置换性质, 下面考察多项式 $\frac{L(x)}{x}$. 对任意 $x\in\mathbb{F}_{q^r}^*$, 用 $\overline{x}$ 表示商群 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 中的元素 $x\mathbb{F}_q^*$. 对于 $x_1,x_2\in\mathbb{F}_{q^r}^*$, 若 $\overline{x_1}=\overline{x_2}$, 则存在 $c\in\mathbb{F}_q^*$ 使得 $x_1=cx_2$, 由 L 的线性性质有

$$\frac{L(x_1)}{x_1}=\frac{L(cx_2)}{cx_2}=\frac{cL(x_2)}{cx_2}=\frac{L(x_2)}{x_2},$$

从而若对任意 $x\in\mathbb{F}_{q^r}^*$, 均有 $L(x)\in\mathbb{F}_{q^r}^*$ (即 $L(x)$ 在 $\mathbb{F}_{q^r}$ 中只有零根), 则 $\overline{x}\mapsto\overline{\left(\frac{L(x)}{x}\right)}$ 是 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的变换. 进一步地, 若这个变换是 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换, 则称 $\frac{L(x)}{x}$ 为 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式. 显然这等价于对任意 $\beta\in\mathbb{F}_{q^r}^*$, 存在 $\gamma\in\mathbb{F}_{q^r}^*$ 使得 $\overline{\left(\frac{L(\gamma)}{\gamma}\right)}=\overline{\beta}$, 从而 $\frac{L(x)}{x}$ 为 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式当且仅当对任意 $\beta\in\mathbb{F}_{q^r}^*$, 存在 $\gamma\in\mathbb{F}_{q^r}^*$ 和 $c\in\mathbb{F}_q^*$ 使得 $L(\gamma)=c\beta\gamma$.

注意到若 $\frac{L(x)}{x}$ 为 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式, 则对任意 $x\in\mathbb{F}_{q^r}^*$ 有 $L(x)\in\mathbb{F}_{q^r}^*$, 这表明 $L(x)$ 在 $\mathbb{F}_{q^r}$ 中只有零根, 所以 $L(x)$ 一定为 $\mathbb{F}_{q^r}$ 上的置换多项式. 进一步地, 若 $L(x)$ 为单项式, 即存在整数 k 使得 $L(x)=\alpha_kx^{q^k}$, 其中 $\alpha_k\in\mathbb{F}_{q^r}^*$, 则 $\frac{L(x)}{x}=\alpha_kx^{q^k-1}$. 由于商群 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 为 $\frac{q^r-1}{q-1}$ 阶循环群, $\overline{x}\mapsto\overline{x^{q^k-1}}=\overline{x}^{q^k-1}$ 是 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 的自同态, 类似于例 6.1 (b), 我们有 $\frac{L(x)}{x}=\alpha_kx^{q^k-1}$ 为 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式当且仅当 $\gcd(q^k-1,\frac{q^r-1}{q-1})=1$.

引理 6.16: 设 $L(x)=\sum_{i=0}^{r-1}\alpha_ix^{q^i}$ 是 $\mathbb{F}_{q^r}$ 上的 q-多项式, 矩阵 $A(L)$ 由式 (6.5) 给出, 若 $\frac{L(x)}{x}$ 为 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式, 则对任意 m, $1\le m\le r-1$, 有

(i) 矩阵 $A(L)$ 的任意 m 阶主子式均为 0.

(ii) 设 $r>1$, $0\le i_1,i_2,\ldots,i_m\le r-1$, 若 $i_1+i_2+\cdots+i_m\equiv 0\,(\mathrm{mod}\ r)$, 则 $\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_m}=0$.

证明: (i) 令

$$D(x)=\begin{vmatrix} \alpha_0+x & \alpha_1 & \cdots & \alpha_{r-2} & \alpha_{r-1} \\ \alpha_{r-1}^q & (\alpha_0+x)^q & \cdots & \alpha_{r-3}^q & \alpha_{r-2}^q \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_2^{q^{r-2}} & \alpha_3^{q^{r-2}} & \cdots & (\alpha_0+x)^{q^{r-2}} & \alpha_1^{q^{r-2}} \\ \alpha_1^{q^{r-1}} & \alpha_2^{q^{r-1}} & \cdots & \alpha_{r-1}^{q^{r-1}} & (\alpha_0+x)^{q^{r-1}} \end{vmatrix},$$

则 $D(x)$ 为 $\mathbb{F}_{q^r}$ 上的多项式, 次数为 $1+q+\cdots+q^{r-1}=\frac{q^r-1}{q-1}$ 且 $D(0)=\det(A(L))$. 由于 $\frac{L(x)}{x}$ 为 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式, 故对任意 $\beta\in\mathbb{F}_{q^r}^*$, 存在 $\gamma\in\mathbb{F}_{q^r}^*$ 和 $c\in\mathbb{F}_q^*$ 使得 $L(\gamma)=-c\beta\gamma$, 从而 γ 为 $\mathbb{F}_{q^r}$ 上的 q-多项式

$$L(x)+c\beta x=(\alpha_0+c\beta)x+\alpha_1x^q+\cdots+\alpha_{r-1}x^{q^{r-1}}$$

在 $\mathbb{F}_{q^r}$ 中的非 0 根, 所以 $L(x)+c\beta x$ 不是 $\mathbb{F}_{q^r}$ 上的置换多项式, 由定理 6.11 得到 $D(c\beta)=0$. 由此我们证出对任意 $\beta\in\mathbb{F}_{q^r}^*$, 有

$$\prod_{c\in\mathbb{F}_q^*}D(c\beta)=0,$$

即 β 为多项式 $\prod_{c\in\mathbb{F}_q^*}D(cx)$ 的根, 又 $\deg\prod_{c\in\mathbb{F}_q^*}D(cx)=q^r-1$, 这便得到多项式 $\prod_{c\in\mathbb{F}_q^*}D(cx)$ 的所有根恰为 $\mathbb{F}_{q^r}$ 中的非零元, 这也是多项式 $x^{q^r-1}-1$ 的所有根. 从而存在 $\delta\in\mathbb{F}_{q^r}^*$ 使得

$$\prod_{c\in\mathbb{F}_q^*}D(cx)=\delta(x^{q^r-1}-1).$$

上式中取 $x=0$ 得到 $D(0)^{q-1}=-\delta$, 由 $D(0)\in\mathbb{F}_q^*$ 得到 $\delta=-1$, 所以我们有

$$\prod_{c\in\mathbb{F}_q^*}D(cx)=-x^{q^r-1}+1. \tag{6.7}$$

对任意 m, $1\le m\le r-1$, 任取 $i_1,i_2,\ldots,i_m$ 满足 $0\le i_1<i_2<\cdots<i_m\le r-1$, 记矩阵 $A(L)$ 中以 $i_1,i_2,\ldots,i_m$ 为行指标和列指标做成的主子矩阵为 $A(L)(i_1,i_2,\ldots,i_m)$, 则 $A(L)$ 的任一 m 阶主子式就是某个 $A(L)(i_1,i_2,\ldots,i_m)$ 的行列式. 令

$$\{0,1,\ldots,r-1\}\setminus\{i_1,i_2,\ldots,i_m\}=\{j_1,j_2,\ldots,j_s\},$$

其中 $s=r-m$ 且 $0\le j_1<j_2<\cdots<j_s\le r-1$. 由于

$$D(cx)=\begin{vmatrix} \alpha_0+cx & \alpha_1 & \cdots & \alpha_{r-2} & \alpha_{r-1} \\ \alpha_{r-1}^q & \alpha_0^q+cx^q & \cdots & \alpha_{r-3}^q & \alpha_{r-2}^q \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_2^{q^{r-2}} & \alpha_3^{q^{r-2}} & \cdots & \alpha_0^{q^{r-2}}+cx^{q^{r-2}} & \alpha_1^{q^{r-2}} \\ \alpha_1^{q^{r-1}} & \alpha_2^{q^{r-1}} & \cdots & \alpha_{r-1}^{q^{r-1}} & \alpha_0^{q^{r-1}}+cx^{q^{r-1}} \end{vmatrix},$$

完全展开可得 $D(cx)$ 中 $x^{q^{j_1}+q^{j_2}+\cdots+q^{j_s}}$ 的系数为 $c^s\det(A(L)(i_1,i_2,\ldots,i_m))$. 注意到整数 $(q-1)(q^{j_1}+q^{j_2}+\cdots+q^{j_s})$ 用 q-进制表示是唯一的, 我们有 $\prod_{c\in\mathbb{F}_q^*}D(cx)$ 中 $x^{(q-1)(q^{j_1}+q^{j_2}+\cdots+q^{j_s})}$

的系数为

$$\begin{aligned}\prod_{c\in\mathbb{F}_q^*} c^s \det(A(L)(i_1,i_2,\ldots,i_m)) &= (\det(A(L)(i_1,i_2,\ldots,i_m)))^{q-1}\left(\prod_{c\in\mathbb{F}_q^*} c\right)^s\\ &= (-1)^s(\det(A(L)(i_1,i_2,\ldots,i_m)))^{q-1}.\end{aligned}$$

由于 $1\le(q-1)(q^{j_1}+q^{j_2}+\cdots+q^{j_s})<(q-1)(1+q+\cdots+q^{r-1})=q^r-1$, 比较 (6.7) 式两边的系数我们得到 $\det(A(L)(i_1,i_2,\ldots,i_m))=0$.

(ii) 设 $r>1$, 记 $A(L)=(\beta_{ij})_{0\le i,j\le r-1}$, 则 $\beta_{ij}=\alpha_{j-i}^{q^i}$, 其中 α_{j-i} 的下标 $j-i$ 是模 r 意义下的, 由此我们得到 $\beta_{ij}=0$ 当且仅当 $\alpha_{j-i}=0$. 由前面已证明的 (i), 对于 $1\le m\le r-1$, $A(L)$ 的任一 m 阶主子式为 0, 特别地, 取 $m=1$, 我们有 $\alpha_0=0$.

下面对 m 作归纳, $m=1$ 的情形显然. 设 $m>1$ 且结论对 $<m$ 成立, 记 $j_0=0$, $j_1=i_1$, $j_2=i_1+i_2$, …, $j_{m-1}=i_1+\cdots+i_{m-1}$, 若 $j_0,j_1,\ldots,j_{m-1}$ 中有相同的, 则存在 ℓ,t 使得 $1\le\ell<t\le m-1$ 且 $i_\ell+\cdots+i_t\equiv 0\,(\mathrm{mod}\ r)$, 由归纳假设 $\alpha_{i_\ell}\cdots\alpha_{i_t}=0$, 从而 $\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_m}=0$. 下面设 $j_0,j_1,\ldots,j_{m-1}$ 互不相同, 若 $\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_m}\ne 0$. 由于 $\beta_{j_0j_1}=0$ 当且仅当 $\alpha_{j_1-j_0}=\alpha_{i_1}=0$, 故 $\beta_{j_0j_1}\ne 0$, 类似地, 由于 $\alpha_{i_2},\ldots,\alpha_{i_{m-1}},\alpha_{i_m}$ 均不为零, 再注意到 $j_0-j_{m-1}=-(i_1+\cdots+i_{m-1})\equiv i_m\,(\mathrm{mod}\ r)$, 我们有 $\beta_{j_1j_2},\ldots,\beta_{j_{m-2}j_{m-1}},\beta_{j_{m-1}j_0}$ 均不为 0. 对任意 $0\le k\le m-2$, 由

$$\det(A(L)(j_k,j_{k+1}))=\begin{vmatrix}0 & \beta_{j_kj_{k+1}}\\ \beta_{j_{k+1}j_k} & 0\end{vmatrix}=-\beta_{j_kj_{k+1}}\beta_{j_{k+1}j_k}=0$$

得到 $\beta_{j_{k+1}j_k}=0$, 即 $\beta_{j_1j_0}=\beta_{j_2j_1}=\cdots=\beta_{j_{m-1}j_{m-2}}=0$. 进一步地, 由

$$\det(A(L)(j_0,j_1,j_2))=\begin{vmatrix}0 & \beta_{j_0j_1} & \beta_{j_0j_2}\\ 0 & 0 & \beta_{j_1j_2}\\ \beta_{j_2j_0} & 0 & 0\end{vmatrix}=\beta_{j_0j_1}\beta_{j_1j_2}\beta_{j_2j_0}=0$$

得到 $\beta_{j_2j_0}=0$, 类似地, 有 $\beta_{j_3j_1}=\cdots=\beta_{j_{m-1}j_{m-3}}=0$. 以此类推, 一直到由 $A(L)$ 的 $m-1$ 阶主子式 $\det(A(L)(\beta_0,\beta_1,\ldots,\beta_{m-2}))$ 和 $\det(A(L)(\beta_1,\beta_2,\ldots,\beta_{m-1}))$ 均为 0 得到 $\beta_{j_{m-2}j_0}=\beta_{j_{m-1}j_1}=0$. 最后, 由 $A(L)$ 的 m 阶主子式

$$\begin{aligned}\det(A(L)(j_0,j_1,\ldots,j_{m-1})) &= \begin{vmatrix}0 & \beta_{j_0j_1} & * & \cdots & * & *\\ 0 & 0 & \beta_{j_1j_2} & \cdots & * & *\\ 0 & 0 & 0 & \cdots & * & *\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 0 & \beta_{j_{m-2}j_{m-1}}\\ \beta_{j_{m-1}j_0} & 0 & 0 & \cdots & 0 & 0\end{vmatrix}\\ &= \beta_{j_0j_1}\beta_{j_1j_2}\cdots\beta_{j_{m-2}j_{m-1}}\beta_{j_{m-1}j_0}=0\end{aligned}$$

就得到矛盾. □

定理 6.17: 设 $L(x)$ 是 $\mathbb{F}_{q^r}$ 上的 q-多项式, 则 $\frac{L(x)}{x}$ 为 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式当且仅当 $\gcd(r, q-1) = 1$ 且 $L(x) = \alpha x^{q^k}$, 其中 $\alpha \in \mathbb{F}_{q^r}^*$, 整数 k 满足 $0 \le k \le r-1$ 且 $\gcd(k, r) = 1$.

证明: 设 $\gcd(r, q-1) = 1$ 且 $L(x) = \alpha x^{q^k}$, 其中 $\alpha \in \mathbb{F}_{q^r}^*$, 整数 k 满足 $0 \le k \le r-1$ 且 $\gcd(k, r) = 1$, 则有 $\frac{L(x)}{x} = \alpha x^{q^k-1}$. 由 $\gcd(k, r) = 1$ 我们有 $\gcd(q^k-1, q^r-1) = q-1$, 又

$$\begin{aligned} \gcd\left(q^k-1, \tfrac{q^r-1}{q-1}\right) &= \gcd\left(\gcd(q^k-1, q^r-1), \tfrac{q^r-1}{q-1}\right) \\ &= \gcd\left(q-1, \tfrac{q^r-1}{q-1}\right) = \gcd(q-1, r) = 1, \end{aligned} \tag{6.8}$$

所以 $\frac{L(x)}{x}$ 为 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式.

反之, 设 $L(x) = \sum_{i=0}^{r-1} \alpha_i x^{q^i} \in \mathbb{F}_{q^r}[x]$ 且 $\frac{L(x)}{x}$ 为 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式, 若 $r = 1$, 则有 $\gcd(r, q-1) = 1$ 且 $L(x) = \alpha_0 x$, 结论显然成立. 下面设 $r > 1$, 由于 $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式, 故显然有 $L(x) \ne 0$. 设 $L(x)$ 的某个系数 $\alpha_k \ne 0$, 其中 $0 \le k \le r-1$, 则必有 $\gcd(k, r) = 1$. 事实上, 若 $d = \gcd(k, r) > 1$, 令 $\ell = \frac{r}{d}$, 则有 $1 \le \ell \le r-1$ 且 $\ell k = \frac{k}{d} r \equiv 0 \pmod r$, 由引理 6.16 (ii) 我们有 $\alpha_k^\ell = 0$, 与 $\alpha_k \ne 0$ 矛盾. 进一步地, 对任意 $0 \le i \le r-1$ 但是 $i \ne k$, 由 $\gcd(k, r) = 1$ 可知存在 j 满足 $0 \le j \le r-2$ 且 $i \equiv -jk \pmod r$, 从而 $i + jk \equiv 0 \pmod r$, 继续由引理 6.16 (ii) 我们有 $\alpha_i \alpha_k^j = 0$, 故 $\alpha_i = 0$. 记 $\alpha_k = \alpha$, 则有 $\alpha \in \mathbb{F}_{q^r}^*$ 且 $L(x) = \alpha x^{q^k}$, 其中 $\gcd(k, r) = 1$. 由于 $\frac{L(x)}{x} = \alpha x^{q^k-1}$ 是 $\mathbb{F}_{q^r}^*/\mathbb{F}_q^*$ 上的置换多项式, 所以 $\gcd(q^k-1, \frac{q^r-1}{q-1}) = 1$, 再利用式 (6.8) 就有 $\gcd(r, q-1) = 1$. □

特别地, 在定理 6.17 中取 $q = 2$, 则商群 $\mathbb{F}_{2^r}^*/\mathbb{F}_2^*$ 就是 $\mathbb{F}_{2^r}^*$. 设 $r > 1$, $L(x) = \sum_{i=0}^{r-1} \alpha_i x^{2^i}$ 是 $\mathbb{F}_{2^r}$ 上的 2-多项式且 $\frac{L(x)}{x} = \sum_{i=0}^{r-1} \alpha_i x^{2^i-1}$ 是 $\mathbb{F}_{2^r}^*$ 上的置换多项式, 若我们再要求 $\frac{L(x)}{x}$ 在 $x = 0$ 处的取值为 0, 即我们要求 $\alpha_0 = 0$, 则 $\frac{L(x)}{x}$ 就是 $\mathbb{F}_{2^r}$ 上的置换多项式. 由此我们有下面定理.

定理 6.18: (Payne 定理) 设 $r > 1$, $L(x) = \sum_{i=1}^{r-1} \alpha_i x^{2^i}$ 是 $\mathbb{F}_{2^r}$ 上的 2-多项式, 则 $\frac{L(x)}{x} = \sum_{i=1}^{r-1} \alpha_i x^{2^i-1}$ 为 $\mathbb{F}_{2^r}$ 上的置换多项式当且仅当 $L(x) = \alpha x^{2^k}$, 其中 $\alpha \in \mathbb{F}_{2^r}^*$, 整数 k 满足 $1 \le k \le r-1$ 且 $\gcd(k, r) = 1$. □

6.3 AGW 准则

Akbary, Ghioca 和 Wang 在 2011 年证明了如下被称之为 AGW 准则的结论, 它可以给出之前很多有限域上置换多项式构造方法的统一解释, 还可以给出众多新的构造, 本节的内容来源于 Akbary, Ghioca 和 Wang 的论文.

定理 6.19: (AGW 准则) 设 A, S, $\overline{S}$ 为有限集合满足 $|S| = |\overline{S}|$, 映射 $f: A \to A$, $\overline{f}: S \to \overline{S}$, $\lambda: A \to S$ 和 $\overline{\lambda}: A \to \overline{S}$ 满足 $\overline{\lambda} \circ f = \overline{f} \circ \lambda$, 若映射 λ 和 $\overline{\lambda}$ 都是满射, 则 f 是集合 A 上的置换当且仅当 $\overline{f}$ 是双射且对任意 $s \in S$, f 在 $\lambda^{-1}(s)$ 上的限制 $f|_{\lambda^{-1}(s)}$ 是单射, 其中 $\lambda^{-1}(s) = \{a \in A \mid \lambda(a) = s\}$.

证明: 设 f 是集合 A 上的置换, 即为 A 到自身的双射, 则显然对任意 $s \in S$, $f|_{\lambda^{-1}(s)}: \lambda^{-1}(s) \to$

A 为单射. 进一步地, 由于 f 和 $\overline{\lambda}$ 都是满射, 故 $\overline{f}\circ\lambda=\overline{\lambda}\circ f$ 为满射, 由此得到 $\overline{f}\colon S\to\overline{S}$ 为满射, 又因为 $|S|=|\overline{S}|$, 所以 $\overline{f}$ 是双射.

反之, 设 $\overline{f}$ 是双射且对任意 $s\in S$, $f|_{\lambda^{-1}(s)}$ 是单射. 若 $a_1,a_2\in A$ 满足 $f(a_1)=f(a_2)$, 则有 $\overline{\lambda}(f(a_1))=\overline{\lambda}(f(a_2))$, 从而 $\overline{f}(\lambda(a_1))=\overline{f}(\lambda(a_2))$, 由 $\overline{f}$ 是双射得到 $\lambda(a_1)=\lambda(a_2)$. 记 $\lambda(a_1)=s\in S$, 则有 $a_1,a_2\in\lambda^{-1}(s)$. 由 $f|_{\lambda^{-1}(s)}$ 是单射, 又 $f(a_1)=f(a_2)$, 我们得到 $a_1=a_2$. 这样我们证出 $f\colon A\to A$ 为单射, 由 A 有限就得到 f 为 A 上的置换. □

设 d 和 r 是正整数且 $d\mid(q-1)$, 则方程 $x^d=1$ 在 $\mathbb{F}_q$ 中有 d 个根, 令 μ_d 为 $x^d=1$ 在 $\mathbb{F}_q$ 中的这 d 个根构成的集合. 设 α 为 $\mathbb{F}_q$ 的一个本原元素, 则显然有 $\mu_d=\langle\alpha^{\frac{q-1}{d}}\rangle$. 设 $g(x)\in\mathbb{F}_q[x]$ 且 $g(x^{\frac{q-1}{d}})$ 在 $\mathbb{F}_q$ 中无非零根. 令 $A=\mathbb{F}_q^*$, $S=\overline{S}=\mu_d$, $f(x)=x^rg(x^{\frac{q-1}{d}})$, $\overline{f}(x)=x^rg(x)^{\frac{q-1}{d}}$, $\lambda(x)=\overline{\lambda}(x)=x^{\frac{q-1}{d}}$, 则容易验证 f 为 A 上的变换, $\overline{f}$ 为 μ_d 上的变换, $\lambda=\overline{\lambda}$ 为 A 到 μ_d 的满射且 $\overline{\lambda}\circ f=\overline{f}\circ\lambda$, 由 AGW 准则我们得到 f 是 $\mathbb{F}_q^*$ 上的置换当且仅当 $\overline{f}$ 是双射且对任意 $s\in\mu_d$, $f|_{\lambda^{-1}(s)}$ 是单射. 设 $s=\alpha^{i\frac{q-1}{d}}$, 其中 $0\le i\le d-1$, 则容易得到 $\lambda^{-1}(s)=\alpha^i\langle\alpha^d\rangle$, 故 $f|_{\lambda^{-1}(s)}(x)=x^rg(s)$, 所以 $f|_{\lambda^{-1}(s)}$ 为单射当且仅当 $x\mapsto x^r$ 在 $\lambda^{-1}(s)$ 上为单射, 这也等价于 $x\mapsto x^r$ 在循环群 $\langle\alpha^d\rangle$ 上为单射. 由于 $x\mapsto x^r$ 为群 $\langle\alpha^d\rangle$ 的自同态, 而群 $\langle\alpha^d\rangle$ 的阶为 $\frac{q-1}{d}$, 所以 $x\mapsto x^r$ 为循环群 $\langle\alpha^d\rangle$ 上的单射当且仅当 $\gcd(r,\frac{q-1}{d})=1$. 又显然 $f(0)=0$, 所以 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 f 为 $\mathbb{F}_q^*$ 上的置换, 这样我们便有如下定理.

定理 6.20: 设 r 和 d 是正整数且 $d\mid(q-1)$, μ_d 为 $x^d=1$ 的 d 个根构成的集合 (一定为 $\mathbb{F}_q$ 的子集), 设 $g(x)\in\mathbb{F}_q[x]$, 则 $f(x)=x^rg(x^{\frac{q-1}{d}})$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(r,\frac{q-1}{d})=1$ 且 $\overline{f}(x)=x^rg(x)^{\frac{q-1}{d}}$ 是 μ_d 上的置换. □

定理 6.20 的重要性在于把判断一个给定的多项式是否为置换多项式转化为判断另一个多项式是否为更小的集合上的置换. 例如若 q 为奇素数幂, $d=2$, 则 $\mu_d=\{1,-1\}$, 故 $\overline{f}(x)$ 是 μ_d 上的置换当且仅当 $\overline{f}(1)\overline{f}(-1)=-1$, 即 $(-1)^r(g(1)g(-1))^{\frac{q-1}{2}}=-1$, 由此我们得到 $f(x)=x^rg(x^{\frac{q-1}{2}})$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(r,\frac{q-1}{2})=1$ 且 $(g(1)g(-1))^{\frac{q-1}{2}}=(-1)^{r+1}$. 注意到在定理 6.20 的叙述中我们并没有要求 $g(x^{\frac{q-1}{d}})$ 在 $\mathbb{F}_q$ 中无非零根, 这是因为不论多项式 $g(x)$ 如何, 我们都有 $f(0)=0$, 若 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式, 则对于 $\beta\neq0$ 必有 $f(\beta)\neq0$, 而这等价于 $g(\beta^{\frac{q-1}{d}})\neq0$, 即等价于 $g(x^{\frac{q-1}{d}})$ 在 $\mathbb{F}_q$ 中无非零根, 所以从逻辑上来说, 我们在定理的叙述中完全可以不加"$g(x^{\frac{q-1}{d}})$ 在 $\mathbb{F}_q$ 中无非零根" 这个条件. 另外由定理 6.20 也容易给出定理 6.7 的证明.

定理 6.21: 设多项式 $h(x),k(x),B(x)\in\mathbb{F}_q[x]$ 和集合 $T\subseteq\mathbb{F}_q$ 满足

(i) $h(0)\neq0$, $k(0)=0$.

(ii) $0\in T$, $h(B(\mathbb{F}_q))\subseteq T$.

(iii) 对任意 $a\in T$ 和 $x\in\mathbb{F}_q$ 有 $B(ax)=k(a)B(x)$.

则 $f(x)=xh(B(x))$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\overline{f}(x)=xk(h(x))$ 限制到 $B(\mathbb{F}_q)$ 上为 $B(\mathbb{F}_q)$ 的置换.

证明: 在定理 6.19 中令 $A = \mathbb{F}_q$, $S = \overline{S} = B(\mathbb{F}_q)$, $\lambda = \overline{\lambda} = B$. 由于对任意 $x \in \mathbb{F}_q$ 有 $h(B(x)) \in T$, 再由条件 (iii) 有

$$B(f(x)) = B(xh(B(x))) = k(h(B(x)))B(x) = \overline{f}(B(x)),$$

即 $\overline{\lambda} \circ f = \overline{f} \circ \lambda$, 故由定理 6.19 得到 $f(x) = xh(B(x))$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\overline{f}(x) = xk(h(x))$ 限制到 $B(\mathbb{F}_q)$ 上为 $B(\mathbb{F}_q)$ 的置换且对任意 $s \in B(\mathbb{F}_q)$, $f|_{B^{-1}(s)}$ 为单射. 由于 $f|_{B^{-1}(s)}(x) = h(s)x$, 所以 $f|_{B^{-1}(s)}$ 为单射当且仅当 $h(s) \neq 0$. 下面我们证明若 $\overline{f}(x)$ 限制到 $B(\mathbb{F}_q)$ 上为 $B(\mathbb{F}_q)$ 的置换, 则对任意 $s \in B(\mathbb{F}_q)$, 有 $h(s) \neq 0$. 事实上, 若 $h(s) = 0$, 由条件 (i) 可得 $s \neq 0$. 由条件 (i), (ii) 和 (iii) 得到

$$B(0) = B(0 \cdot x) = k(0)B(x) = 0 \cdot B(x) = 0,$$

故 $0 \in B(\mathbb{F}_q)$. 但是 $\overline{f}(s) = sk(h(s)) = sk(0) = 0 = \overline{f}(0)$, 与 $\overline{f}(x)$ 限制到 $B(\mathbb{F}_q)$ 上为 $B(\mathbb{F}_q)$ 的置换矛盾. 这样我们便证明了若 $\overline{f}(x)$ 限制到 $B(\mathbb{F}_q)$ 上为 $B(\mathbb{F}_q)$ 的置换, 则对任意 $s \in B(\mathbb{F}_q)$, 一定有 $f|_{B^{-1}(s)}$ 为单射, 定理证毕. □

注意到在 AGW 准则中对集合 S 和 $\overline{S}$ 的结构没有任何限制, 我们把寻找大集合 A 上的置换转化为判断另一个映射为小集合间的双射. 然而用 AGW 准则证明定理 6.20 时, 我们用到的集合 A 是一个群, 而映射 λ 和 $\overline{\lambda}$ 都是群同态, 这时 S 和 $\overline{S}$ 都是同态像, 这个做法可以推广为如下定理, 其中 $\mathrm{End}(G)$ 表示群 G 的所有自同态构成的集合, 对于 $\psi \in \mathrm{End}(G)$, 令 $\mathrm{Im}\psi = \psi(G)$ 为同态 ψ 的像.

定理 6.22: 设 G 为有限群, 运算写为加法, 单位元记为 0 (群 G 不一定交换), 设 $\varphi, \psi, \overline{\psi} \in \mathrm{End}(G)$ 满足 $\overline{\psi} \circ \varphi = \varphi \circ \psi$ 和 $|\mathrm{Im}\psi| = |\mathrm{Im}\overline{\psi}|$, 设 $g : G \to G$ 为 G 上的任一变换, 定义 $f : G \to G$ 和 $\overline{f} : G \to G$ 为对任意 $x \in G$ 有 $f(x) = \varphi(x) + g(\psi(x))$ 和 $\overline{f}(x) = \varphi(x) + \overline{\psi}(g(x))$, 则有

(i) f 是 G 上的置换当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 且 $\overline{f}$ 在 $\mathrm{Im}\psi$ 上的限制 $\overline{f}|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 到 $\mathrm{Im}\overline{\psi}$ 的双射.

(ii) f 是 G 上的置换当且仅当 φ 在 $\ker(\psi)$ 上的限制 $\varphi|_{\ker(\psi)}$ 是 $\ker(\psi)$ 到 $\ker(\overline{\psi})$ 的双射且 $\overline{f}$ 在 $\mathrm{Im}\psi$ 上的限制 $\overline{f}|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 到 $\mathrm{Im}\overline{\psi}$ 的双射.

(iii) 若 g 满足 $(\overline{\psi} \circ g)|_{\mathrm{Im}\psi} = 0$, 即对任意 $x \in \mathrm{Im}\psi$ 有 $\overline{\psi}(g(x)) = 0$, 则 f 是 G 上的置换当且仅当 φ 是 G 的自同构.

(iv) 若 $\varphi \circ \psi = 0$ 且 $g|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 上的置换, 则 f 是 G 上的置换当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 且 $\overline{\psi}|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 到 $\mathrm{Im}\overline{\psi}$ 的双射.

证明: (i) 在 AGW 准则中取 $A = G$, $S = \mathrm{Im}\psi$, $\overline{S} = \mathrm{Im}\overline{\psi}$, $\lambda = \psi$, $\overline{\lambda} = \overline{\psi}$, 则有 $|S| = |\overline{S}|$, λ 和 $\overline{\lambda}$ 都是满射, 又

$$\overline{\lambda} \circ f = \overline{\psi} \circ (\varphi + g \circ \psi) = \overline{\psi} \circ \varphi + \overline{\psi} \circ g \circ \psi = \varphi \circ \psi + \overline{\psi} \circ g \circ \psi = (\varphi + \overline{\psi} \circ g) \circ \psi = \overline{f} \circ \lambda,$$

由此可得到 $\overline{f}(\lambda(G)) \subseteq \overline{\lambda}(G)$, 即 $\overline{f}(\mathrm{Im}\psi) \subseteq \mathrm{Im}\overline{\psi}$. 由定理 6.19 我们有 f 是 G 上的置换当且仅当对任意 $s \in \mathrm{Im}\psi$, $f|_{\psi^{-1}(s)}$ 为单射且 $\overline{f} : \mathrm{Im}\psi \to \mathrm{Im}\overline{\psi}$ 为双射. 后面这个条件即 $\overline{f}|_{\mathrm{Im}\psi}$ 是

$\mathrm{Im}\psi$ 到 $\mathrm{Im}\overline{\psi}$ 的双射, 下面看第一个条件. 对于任意 $s \in \mathrm{Im}\psi$ 和 $\alpha, \beta \in \psi^{-1}(s)$, 若 $f(\alpha) = f(\beta)$, 则有 $\varphi(\alpha) + g(s) = \varphi(\beta) + g(s)$, 这等价于 $\varphi(\alpha - \beta) = \varphi(\alpha) - \varphi(\beta) = 0$, 即 $\alpha - \beta \in \ker(\varphi)$. 又显然 $\psi(\alpha) = \psi(\beta) = s$, 所以 $\alpha - \beta \in \ker(\psi)$, 这样我们便证出若 $f(\alpha) = f(\beta)$, 则有 $\alpha - \beta \in \ker(\varphi) \cap \ker(\psi)$, 从而由 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 可推出 $f|_{\psi^{-1}(s)}$ 为单射. 另一方面, 若存在 $\gamma \in \ker(\varphi) \cap \ker(\psi)$ 且 $\gamma \neq 0$, 则 $f(\gamma) = \varphi(\gamma) + g(\psi(\gamma)) = g(0) = f(0)$, 又 $0, \gamma \in \ker(\psi) = \psi^{-1}(0)$, 这与 $f|_{\psi^{-1}(0)}$ 为单射矛盾. 故对任意 $s \in \mathrm{Im}\psi$, 我们有 $f|_{\psi^{-1}(s)}$ 为单射当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{0\}$.

(ii) 对于任意 $\gamma \in \ker(\psi)$, 我们有 $(\overline{\psi} \circ \varphi)(\gamma) = (\varphi \circ \psi)(\gamma) = \varphi(0) = 0$, 所以 $\varphi(\gamma) \in \ker(\overline{\psi})$, 即 $\varphi(\ker(\psi)) \subseteq \ker(\overline{\psi})$, 这表明 $\varphi|_{\ker(\psi)}$ 是 $\ker(\psi)$ 到 $\ker(\overline{\psi})$ 的映射. 由群同态基本定理我们有 $|G| = |\ker(\psi)||\mathrm{Im}\psi| = |\ker(\overline{\psi})||\mathrm{Im}\overline{\psi}|$, 所以由 $|\mathrm{Im}\psi| = |\mathrm{Im}\overline{\psi}|$ 我们有 $|\ker(\psi)| = |\ker(\overline{\psi})|$, 故 $\varphi|_{\ker(\psi)}$ 是双射当且仅当 $\varphi|_{\ker(\psi)}$ 是单射. 对任意 $s \in \mathrm{Im}\psi$, 选取 $a \in G$ 使得 $\psi(a) = s$, 则由 ψ 为群同态易知 $\psi^{-1}(s) = a + \ker(\psi)$. 故对任意 $x \in \psi^{-1}(s)$, 存在 $y \in \ker(\psi)$ 使得 $x = a + y$, 从而在 $\psi^{-1}(s)$ 上有 $f(x) = \varphi(a + y) + g(s) = \varphi(a) + \varphi(y) + g(s)$, 所以 $f|_{\psi^{-1}(s)}$ 为单射当且仅当 $\varphi|_{\ker(\psi)}$ 是单射, 由 (i) 便得到 f 是 G 上的置换当且仅当 $\varphi|_{\ker(\psi)}$ 是 $\ker(\psi)$ 到 $\ker(\overline{\psi})$ 的双射且 $\overline{f}|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 到 $\mathrm{Im}\overline{\psi}$ 的双射.

(iii) 由于 $\overline{f} = \varphi + \overline{\psi} \circ g$, 所以若 $(\overline{\psi} \circ g)|_{\mathrm{Im}\psi} = 0$, 则有 $\overline{f}|_{\mathrm{Im}\psi} = \varphi|_{\mathrm{Im}\psi}$, 故由 (ii) 我们有 f 是 G 上的置换当且仅当 $\varphi|_{\ker(\psi)} : \ker(\psi) \to \ker(\overline{\psi})$ 和 $\varphi|_{\mathrm{Im}\psi} : \mathrm{Im}\psi \to \mathrm{Im}\overline{\psi}$ 都是双射. 在定理 6.19 中取 $A = G$, $S = \mathrm{Im}\psi$, $\overline{S} = \mathrm{Im}\overline{\psi}$, $f' = \varphi$, $\overline{f'} = \varphi|_S$, $\lambda = \psi$, $\overline{\lambda} = \overline{\psi}$, 则有 $|S| = |\overline{S}|$, λ 和$\overline{\lambda}$ 都是满射且 $\overline{\psi} \circ f' = \overline{f'} \circ \psi$, 由定理 6.19 得到 $f' = \varphi$ 是 G 上的置换当且仅当 $\overline{f'} = \varphi|_{\mathrm{Im}\psi}$ 为双射且对任意 $s \in \mathrm{Im}\psi$, $\varphi|_{\psi^{-1}(s)}$ 为单射. 由于 ψ 为群同态且 $\psi^{-1}(0) = \ker(\psi)$, 所以 $\psi^{-1}(s)$ 是 G 的关于其子群 $\ker(\psi)$ 的一个左陪集, 从而 $\varphi|_{\psi^{-1}(s)}$ 为单射当且仅当 $\varphi|_{\ker(\psi)}$ 是单射, 后者也当且仅当 $\varphi|_{\ker(\psi)}$ 是双射. 这样我们就证出 f 是 G 上的置换当且仅当 $f' = \varphi$ 是 G 上的置换, 由 φ 为群 G 的自同态, 所以 f 是 G 上的置换当且仅当 φ 是群 G 的自同构.

(iv) 由于 $\varphi \circ \psi = 0$, 所以 $\overline{f}|_{\mathrm{Im}\psi} = (\overline{\psi} \circ g)|_{\mathrm{Im}\psi}$, 由 (i) 得到 f 是 G 上的置换当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 且 $(\overline{\psi} \circ g)|_{\mathrm{Im}\psi} : \mathrm{Im}\psi \to \mathrm{Im}\overline{\psi}$ 是双射. 又 $g|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 上的置换, 所以 $(\overline{\psi} \circ g)|_{\mathrm{Im}\psi} : \mathrm{Im}\psi \to \mathrm{Im}\overline{\psi}$ 是双射当且仅当 $\overline{\psi}|_{\mathrm{Im}\psi} : \mathrm{Im}\psi \to \mathrm{Im}\overline{\psi}$ 是双射. □

设 G 为域 $\mathbb{F}_q$ 的乘法群 $\mathbb{F}_q^*$. 由于 $\mathbb{F}_q^*$ 为 $q-1$ 阶循环群, 所以 $\mathbb{F}_q^*$ 的每个自同态一定形如 $x \mapsto x^s$, 其中 s 为正整数 (事实上可要求 $1 \leq s \leq q-1$). 设 r, s 为正整数, 在定理 6.22 中取 $\varphi, \psi, \overline{\psi} \in \mathrm{End}(G)$ 为 $\varphi(x) = x^r$, $\psi(x) = \overline{\psi}(x) = x^s$, 则有 $\overline{\psi} \circ \varphi = \varphi \circ \psi$ 和 $|\mathrm{Im}\psi| = |\mathrm{Im}\overline{\psi}|$. 由于 $\ker(\varphi) = \{x \in \mathbb{F}_q^* \mid x^r = 1\}$ 和 $\ker(\psi) = \{x \in \mathbb{F}_q^* \mid x^s = 1\}$, 所以 $\ker(\varphi) \cap \ker(\psi) = \{x \in \mathbb{F}_q^* \mid x^{\gcd(r,s)} = 1\}$, 从而 $\ker(\varphi) \cap \ker(\psi) = \{1\}$ 当且仅当 $\gcd(\gcd(r,s), q-1) = \gcd(r, s, q-1) = 1$. 设 $g(x) \in \mathbb{F}_q[x]$ 且 $g(x)$ 在 $\mathbb{F}_q$ 中无非零根, 由定理 6.22 我们得到 $f(x) = x^r g(x^s)$ 为 $\mathbb{F}_q^*$ 上的置换当且仅当 $\gcd(r, s, q-1) = 1$ 且 $\overline{f}(x) = x^r g(x)^s$ 为 $\mathrm{Im}\psi = (\mathbb{F}_q^*)^s$ 上的置换. 显然 $f(0) = 0$, 我们有如下推论.

推论 6.23: 设 r, s 为正整数, $g(x) \in \mathbb{F}_q[x]$, 则 $f(x) = x^r g(x^s)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(r, s, q-1) = 1$ 且 $\overline{f}(x) = x^r g(x)^s$ 限制到 $(\mathbb{F}_q^*)^s$ 上为 $(\mathbb{F}_q^*)^s$ 的置换. □

注意到在推论 6.23 的叙述中我们依然没有要求 $g(x)$ 在 $\mathbb{F}_q$ 中无非零根. 进一步地, 若 $s \mid (q-1)$, 则 $\gcd(r, s, q-1) = \gcd(r, s)$ 且 $(\mathbb{F}_q^*)^s$ 为 $\mathbb{F}_q^*$ 的 $\frac{q-1}{s}$ 阶子群, 也是 $\mathbb{F}_q$ 中方程 $x^{\frac{q-1}{s}} = 1$ 的所有 $\frac{q-1}{s}$ 个根构成的集合, 即 $(\mathbb{F}_q^*)^s = \mu_{\frac{q-1}{s}}$. 这里取 $d = \frac{q-1}{s}$ 就得到定理 6.20.

设多项式 $f(x) \in \mathbb{F}_q[x]$ 满足 $f(0) = 0$, 不妨令

$$f(x) = a_0 x^n + a_1 x^{n_1} + \cdots + a_{t-1} x^{n_{t-1}} + a_t x^{n_t},$$

其中 $a_0, a_1, \ldots, a_{t-1}, a_t \in \mathbb{F}_q^*$, $n > n_1 > \cdots > n_{t-1} > n_t \geq 1$. 设 $s = \gcd(n - n_t, n_1 - n_t, \cdots, n_{t-1} - n_t, q-1)$, 令 $n_i - n_t = e_i s$ 和 $q - 1 = \ell s$, 其中 $0 \leq i \leq t-1$, $n_0 = n$, 而正整数 $\ell = \frac{q-1}{s}$ 称为多项式的指数. 这时我们有 $\gcd(e_0, e_1, \cdots, e_{t-1}, \ell) = 1$ 且

$$f(x) = x^{n_t}(a_0 x^{e_0 s} + a_1 x^{e_1 s} + \cdots + a_{t-1} x^{e_{t-1} s} + a_t) = x^r g(x^s),$$

其中 $r = n_t$, $g(x) = a_0 x^{e_0} + a_1 x^{e_1} + \cdots + a_{t-1} x^{e_{t-1}} + a_t \in \mathbb{F}_q[x]$. 故任一常数项为 0 的多项式均可以表示为 $f(x) = x^r g(x^s)$ 的形式, 其中 r, s 为正整数满足 $s \mid (q-1)$ 且 $g(x) \in \mathbb{F}_q[x]$. 这表明定理 6.20 的结论可以适用于任意的多项式, 注意到若 $s = 1$, 即多项式 $f(x)$ 的指数 (定理 6.20 中的 d) 为 $q-1$, 则定理 6.20 是平凡的.

下面我们继续考察形如 $x^r g(x^s)$ 的多项式, 其中 r, s 为正整数且 $s \mid (q-1)$, 令 $d = \frac{q-1}{s}$. 由前面的记号, 定理 6.22 (iii) 中的条件 $(\overline{\psi} \circ g)|_{\mathrm{Im}\psi} = 0$ 即为对任意 $x \in \mu_d$ 有 $g(x)^s = 1$, 则由定理 6.22 (iii) 得到 $x^r g(x^s)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 φ 是 $\mathbb{F}_q^*$ 的自同构, 即当且仅当 $\gcd(r, q-1) = 1$ (此结论也容易由定理 6.20 得到, 因这时 $\overline{f}|_{\mu_d}(x) = x^r$). 由于 $(\varphi \circ \psi)(x) = x^{rs}$, 所以定理 6.22 (iv) 中的条件 $\varphi \circ \psi = 0$ 等价于 $(q-1) \mid rs$, 下面取 $r = d = \frac{q-1}{s}$ 且假设 $g|_{\mu_d}$ 为 μ_d 上的置换, 则由定理 6.22 (iv) 得到 $x^d g(x^s)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{1\}$ 且 x^s 是 μ_d 上的置换. 由推论 6.23 之前的讨论我们有 $\ker(\varphi) \cap \ker(\psi) = \{1\}$ 当且仅当 $\gcd(d, s) = 1$, 又 μ_d 为 d 阶循环群, 所以 x^s 是 μ_d 上的置换依然等价于 $\gcd(d, s) = 1$. 我们把如上事实叙述成如下推论.

推论 6.24: 设 r, s 为正整数且 $s \mid (q-1)$, 令 $d = \frac{q-1}{s}$, $g(x) \in \mathbb{F}_q[x]$, 则有

(i) 设对任意 $x \in \mu_d$ 有 $g(x)^s = 1$, 则 $f(x) = x^r g(x^s)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(r, q-1) = 1$.

(ii) 设 $g|_{\mu_d}$ 为 μ_d 上的置换, 则 $f(x) = x^d g(x^s)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(d, s) = 1$.

□

设 q 为素数幂, n 为正整数, 在有限域 $\mathbb{F}_{q^n}$ 上利用推论 6.24 (ii), 其中取 $d = q-1$, 则 $s = \frac{q^n-1}{q-1}$. 由于 $\mu_{q-1} = \mathbb{F}_q^*$ 且 $\gcd(q-1, \frac{q^n-1}{q-1}) = \gcd(n, q-1)$, 我们有如下推论.

推论 6.25: 设 q 为素数幂, n 为正整数, $g(x) \in \mathbb{F}_{q^n}[x]$ 为 $\mathbb{F}_q^*$ 上的置换, 则 $f(x) = x^{q-1} g(x^{\frac{q^n-1}{q-1}})$ 为 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\gcd(n, q-1) = 1$. □

设 q 为素数 p 的方幂, n 为正整数, 在 AGW 准则 (定理 6.19) 中令 A 为 $\mathbb{F}_{q^n}$ 的加法群. 由于 $\mathbb{F}_{q^n}$ 的特征为 p, 容易验证加法群 $\mathbb{F}_{q^n}$ 的每个自同态一定为某个 $\mathbb{F}_{q^n}$ 上的 p-多项式 (为什么?). 当然 q-多项式也是 p-多项式, 但若把 $\mathbb{F}_{q^n}$ 看作为 $\mathbb{F}_q$ 上的线性空间, 则 $\mathbb{F}_{q^n}$ 上的 q-多项式是 $\mathbb{F}_{q^n}$ 上的线性变换, 而 $\mathbb{F}_{q^n}$ 上的 p-多项式就不一定保持 $\mathbb{F}_q$ 中的数乘, 故不一定是 $\mathbb{F}_{q^n}$ 上的线性变换. 下面我们依然用 ker 和 Im 表示加法群 $\mathbb{F}_{q^n}$ 的自同态的核和像, 类似于定理 6.22, 我们有如下定理 (比定理 6.22 多加了一个满足一定条件的多项式 $h(x)$), 其证明也类似于定理 6.22 的证明, 故略去.

定理 6.26: 设 p 为素数, q 为 p 的方幂, n 为正整数, 设 $g(x), \varphi(x), \psi(x), \overline{\psi}(x), h(x) \in \mathbb{F}_{q^n}[x]$ 满足 $\varphi(x)$ 和 $\psi(x)$ 是 p-多项式, $\overline{\psi}(x)$ 是 q-多项式, $\overline{\psi} \circ \varphi = \varphi \circ \psi$, $|\mathrm{Im}\psi| = |\mathrm{Im}\overline{\psi}|$ 以及 $h(\psi(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q^*$, 令 $f(x) = h(\psi(x))\varphi(x) + g(\psi(x))$ 和 $\overline{f}(x) = h(x)\varphi(x) + \overline{\psi}(g(x))$, 则有

(i) $f(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 且 $\overline{f}$ 在 $\mathrm{Im}\psi$ 上的限制 $\overline{f}|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 到 $\mathrm{Im}\overline{\psi}$ 的双射.

(ii) 若 g 满足 $(\overline{\psi} \circ g)|_{\mathrm{Im}\psi} = 0$, 即对任意 $x \in \mathrm{Im}\psi$ 有 $\overline{\psi}(g(x)) = 0$, 则 $f(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 且 $h(x)\varphi(x)$ 在 $\mathrm{Im}\psi$ 上的限制是 $\mathrm{Im}\psi$ 到 $\mathrm{Im}\overline{\psi}$ 的双射.

(iii) 若 $\varphi \circ \psi = 0$ 且 $g|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 上的置换, 则 $f(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 且 $\overline{\psi}|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 到 $\mathrm{Im}\overline{\psi}$ 的双射.

□

例 6.3: 设 p 为奇素数, 正整数 n 为偶数且 $p \nmid n$. 设 α 为 $\mathbb{F}_{p^n}$ 的一个本原元素, 由 n 为偶数得到 $\frac{p^n-1}{p-1}$ 为偶数, 令 $\epsilon = \alpha^{\frac{p^n-1}{2(p-1)}}$, 则有 $\epsilon^{p-1} = \alpha^{\frac{p^n-1}{2}} = -1$. 令 $\varphi(x) = \epsilon \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x)$, $\psi(x) = x - x^p$, $\overline{\psi}(x) = x + x^p$, 则 $\varphi(x)$, $\psi(x)$ 和 $\overline{\psi}(x)$ 都是 $\mathbb{F}_{p^n}$ 上的 p- 多项式且容易验证 $\overline{\psi} \circ \varphi = \varphi \circ \psi = 0$. 由于 $\ker(\psi) = \{x \in \mathbb{F}_{p^n} \mid x^p = x\} = \mathbb{F}_p$, 故 $|\ker(\psi)| = p$. 由 n 为偶数得到 $\mathbb{F}_{p^2}$ 为 $\mathbb{F}_{p^n}$ 的子域, 从而 $\overline{\psi}(x) = x + x^p = \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x)$, 故 $\overline{\psi}(x) = 0$ 在 $\mathbb{F}_{p^2}$ 中, 从而也在 $\mathbb{F}_{p^n}$ 中有 p 个根, 所以 $|\ker(\overline{\psi})| = p = |\ker(\psi)|$, 这样我们便证出 $|\mathrm{Im}\psi| = |\mathrm{Im}\overline{\psi}| = p^{n-1}$. 又对于任意 $c \in \ker(\varphi) \cap \ker(\psi)$, 有 $c \in \mathbb{F}_p$ 且 $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(c) = 0$, 即 $nc = 0$, 再由 $p \nmid n$ 得到 $c = 0$, 故 $\ker(\varphi) \cap \ker(\psi) = \{0\}$. 设 $g(x), h(x) \in \mathbb{F}_{p^n}[x]$ 且对任意 $x \in \mathbb{F}_{p^n}$ 有 $h(x - x^p) \subseteq \mathbb{F}_p^*$, 则由定理 6.26 (i) 得到 $f(x) = \epsilon \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x)h(x - x^p) + g(x - x^p)$ 是 $\mathbb{F}_{p^n}$ 上的置换多项式当且仅当 $\overline{f}(x) = \epsilon \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x)h(x) + g(x) + g(x)^p$ 诱导出一个 $\mathrm{Im}\psi = \{x - x^p \mid x \in \mathbb{F}_{p^n}\}$ 到 $\mathrm{Im}\overline{\psi} = \{x + x^p \mid x \in \mathbb{F}_{p^n}\}$ 的双射. 进一步地, 对任意 $x \in \mathbb{F}_{p^n}$, 我们有 $(\varphi \circ \psi)(x) = \epsilon \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x - x^p) = 0$, 所以 $\overline{f}|_{\mathrm{Im}\psi}(x) = g(x) + g(x)^p$, 由此我们得到 $f(x) = \epsilon \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x)h(x - x^p) + g(x - x^p)$ 是 $\mathbb{F}_{p^n}$ 上的置换多项式当且仅当 $g(x) + g(x)^p$ 给出一个 $\mathrm{Im}\psi = \{x - x^p \mid x \in \mathbb{F}_{p^n}\}$ 到 $\mathrm{Im}\overline{\psi} = \{x + x^p \mid x \in \mathbb{F}_{p^n}\}$ 的双射. □

下面我们假设 φ 和 ψ 都是 $\mathbb{F}_q$ 上的 q-多项式, 由第 4.4 节我们知道这时有 $\varphi \circ \psi = \psi \circ \varphi$, 取 $\overline{\psi} = \psi$, 由定理 6.26 (i) 我们有如下定理.

定理 6.27: 设 q 为素数幂, n 为正整数, $\varphi(x)$ 和 $\psi(x)$ 为 $\mathbb{F}_q$ 上的 q-多项式 (φ 和 ψ 看成是加法群 $\mathbb{F}_{q^n}$ 的自同态), 设 $g(x), h(x) \in \mathbb{F}_{q^n}[x]$ 满足 $h(\psi(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q^*$, 令 $f(x) = h(\psi(x))\varphi(x) + g(\psi(x))$ 和 $\overline{f}(x) = h(x)\varphi(x) + \psi(g(x))$, 则 $f(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 且 $\overline{f}$ 在 $\mathrm{Im}\psi$ 上的限制 $\overline{f}|_{\mathrm{Im}\psi}$ 是 $\mathrm{Im}\psi$ 上的置换. □

特别地, 在定理 6.27 中取 $\psi(x) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = x^{q^{n-1}} + \cdots + x^q + x$, 则 $\mathrm{Im}\psi = \psi(\mathbb{F}_{q^n}) = \mathbb{F}_q$, 我们有如下定理.

定理 6.28: 设 $\varphi(x)$ 为 $\mathbb{F}_q$ 上的 q-多项式, 设 $g(x), h(x) \in \mathbb{F}_{q^n}[x]$ 满足 $h(\mathbb{F}_q) \subseteq \mathbb{F}_q^*$, 令 $f(x) = h(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))\varphi(x) + g(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$ 和 $\overline{f}(x) = h(x)\varphi(x) + \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g(x))$, 则 $f(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 且 $\overline{f}(x)$ 是 $\mathbb{F}_q$ 上的置换多项式. □

设 $\varphi(x)$ 为 $\mathbb{F}_q$ 上的 q-多项式, 若 $\varphi(x)$ 为 $\mathbb{F}_{q^n}$ 上的置换多项式, 则 $\varphi(x) = 0$ 在 $\mathbb{F}_{q^n}$ 中只有零根, 即 $\ker(\varphi) = \{0\}$. 在定理 6.28 中令 $h(x) = 1$, $g(x) = \gamma\overline{g}(x)$, 其中 $\overline{g}(x) \in \mathbb{F}_q[x]$, $\gamma \in \mathbb{F}_{q^n}$, 则有 $f(x) = \varphi(x) + \gamma\overline{g}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$, $\overline{f}(x) = \varphi(x) + \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma\overline{g}(x))$. 令 $\varphi(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, 其中 $a_i \in \mathbb{F}_q$, $0 \le i \le n-1$, 则 $\varphi(x)$ 在 $\mathbb{F}_q$ 上等于 $\left(\sum_{i=0}^{n-1} a_i\right) x$. 由 $\overline{g}(x) \in \mathbb{F}_q[x]$, 所以对任意 $x \in \mathbb{F}_q$, 有 $\overline{g}(x) \in \mathbb{F}_q$, 故在 $\mathbb{F}_q$ 上有 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma\overline{g}(x)) = \overline{g}(x)\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma)$. 由定理 6.28 我们有如下推论, 其中我们把 $\overline{g}$ 记成 g.

推论 6.29: (Marcos) 设 $\varphi(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_q[x]$ 为 $\mathbb{F}_{q^n}$ 上的置换 q-多项式, $g(x) \in \mathbb{F}_q[x]$, $\gamma \in \mathbb{F}_{q^n}$ 且 $a = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma)$, 令 $f(x) = \varphi(x) + \gamma g(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$ 和 $\overline{f}(x) = \left(\sum_{i=0}^{n-1} a_i\right) x + ag(x)$, 则 $f(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\overline{f}(x)$ 是 $\mathbb{F}_q$ 上的置换多项式. □

在定理 6.27 中取 $\psi(x) = x^q - x$, 则显然 $\ker(\psi) = \mathbb{F}_q$ 而 $\mathrm{Im}\psi = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^n}\} = \ker(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q})$. 令 $\varphi(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, 其中 $a_i \in \mathbb{F}_q$, $0 \le i \le n-1$, 则 $\ker(\varphi) \cap \ker(\psi) = \{0\}$ 等价于 $\varphi(x)$ 在 $\mathbb{F}_q$ 中只有零根, 这也等价于 $\varphi(x)$ 为 $\mathbb{F}_q$ 上的置换多项式. 在 $\mathbb{F}_q$ 上 $\varphi(x) = \left(\sum_{i=0}^{n-1} a_i\right) x$, 所以 $\varphi(x)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\varphi(1) = \sum_{i=0}^{n-1} a_i \ne 0$, 由此我们有如下定理.

定理 6.30: 设 $\varphi(x)$ 为 $\mathbb{F}_q$ 上的 q-多项式, 设 $g(x), h(x) \in \mathbb{F}_{q^n}[x]$ 满足对任意 $x \in \mathbb{F}_{q^n}$ 有 $h(x^q - x) \subseteq \mathbb{F}_q^*$, 令 $f(x) = h(x^q - x)\varphi(x) + g(x^q - x)$ 和 $\overline{f}(x) = h(x)\varphi(x) + g(x)^q - g(x)$, 则 $f(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\varphi(1) \ne 0$ 且 $\overline{f}(x)$ 是 $S = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^n}\}$ 上的置换. □

例 6.4: (a) 设 $a, b \in \mathbb{F}_q$ 且 $a \ne \pm b$, k 为正偶数, $n = 2$. 在定理 6.30 中令 $\varphi(x) = ax^q + bx$, $g(x) = x^k$, $h(x) = 1$. 则显然 $\varphi(1) = a + b \ne 0$, $\overline{f}(x) = \varphi(x) + x^{qk} - x^k$, $S = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^2}\}$. 对任意 $\alpha \in \mathbb{F}_{q^2}$, 由于 k 为偶数, 我们有 $(\alpha^q - \alpha)^{qk} - (\alpha^q - \alpha)^k = (\alpha^{q^2} - \alpha^q)^k - (\alpha^q - \alpha)^k = (\alpha - \alpha^q)^k - (\alpha^q - \alpha)^k = 0$, 故

$$\overline{f}(\alpha^q - \alpha) = \varphi(\alpha^q - \alpha) + (\alpha^q - \alpha)^{qk} - (\alpha^q - \alpha)^k = \varphi(\alpha^q - \alpha) = \varphi(\alpha)^q - \varphi(\alpha) \in S.$$

由于 $\mathbb{F}_{q^2}$ 上的 q-多项式 $\varphi(x)$ 对应的矩阵 $A(\varphi)$ 的行列式 $\det(A(\varphi)) = b^2 - a^2 \ne 0$, 所以 $\varphi(x)$ 是 $\mathbb{F}_{q^2}$ 上的置换多项式, 又 $\overline{f}(x)$ 限制到 S 上为 $\varphi(x)$, 故 $\overline{f}(x)$ 是 S 上的置换, 由定理 6.30 我们

得到多项式 $f(x)=\varphi(x)+g(x^q-x)=ax^q+bx+(x^q-x)^k$ 为 $\mathbb{F}_{q^2}$ 上的置换多项式.

(b) 设 q 为奇素数幂, $a\in\mathbb{F}_q^*$, k 为奇数且 $\gcd(k,q-1)=1$, $n=2$. 在定理 6.30 中令 $\varphi(x)=a\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x)=ax^q+ax$, $g(x)=x^k$, $h(x)=1$. 则显然 $\varphi(1)=a+a=2a\neq 0$, $\overline{f}(x)=\varphi(x)+x^{qk}-x^k$, $S=\{\alpha^q-\alpha\mid\alpha\in\mathbb{F}_{q^2}\}$. 对任意 $\alpha\in\mathbb{F}_{q^2}$, 由于 $\varphi(\alpha^q-\alpha)=0$, 我们有

$$\overline{f}(\alpha^q-\alpha)=(\alpha^q-\alpha)^{qk}-(\alpha^q-\alpha)^k=((\alpha^q-\alpha)^k)^q-(\alpha^q-\alpha)^k\in S.$$

设 γ 为 $\mathbb{F}_{q^2}$ 的一个本原元素, 令 $\epsilon=\gamma^{\frac{q+1}{2}}$, 则有 $\epsilon^q=-\epsilon$, 故 $\epsilon\notin\mathbb{F}_q$, 这表明 $\{1,\epsilon\}$ 构成 $\mathbb{F}_{q^2}$ 在 $\mathbb{F}_q$ 上的一组基. 任取 $\alpha_1,\alpha_2\in\mathbb{F}_{q^2}$, 则存在 $c_1,d_1,c_2,d_2\in\mathbb{F}_q$ 使得 $\alpha_1=c_1+d_1\epsilon$, $\alpha_2=c_2+d_2\epsilon$. 容易计算得到 $\alpha_1^q-\alpha_1=-2d_1\epsilon$, 故 $\overline{f}(\alpha_1^q-\alpha_1)=2(2d_1\epsilon)^k$. 若对 $\alpha_1^q-\alpha_1,\alpha_2^q-\alpha_2\in S$ 有 $\overline{f}(\alpha_1^q-\alpha_1)=\overline{f}(\alpha_2^q-\alpha_2)$, 则有 $2(2d_1\epsilon)^k=2(2d_2\epsilon)^k$, 从而 $d_1^k=d_2^k$, 由 $\gcd(k,q-1)=1$ 可得 $d_1=d_2$, 所以 $\alpha_1^q-\alpha_1=\alpha_2^q-\alpha_2$, 这表明 $\overline{f}(x)$ 是 S 上的单射, 从而也是 S 上的双射. 由定理 6.30 我们得到 $f(x)=ax^q+ax+(x^q-x)^k$ 为 $\mathbb{F}_{q^2}$ 上的置换多项式. □

在定理 6.26 中令 $\varphi(x)=\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$, $\psi(x)=\overline{\psi}(x)=x^q-x$, 我们有如下定理.

定理 6.31: 设 p 为素数, q 为 p 的方幂, n 为正整数, $S=\{\alpha^q-\alpha\mid\alpha\in\mathbb{F}_{q^n}\}$, 设 $g(x),h(x)\in\mathbb{F}_{q^n}[x]$ 满足 $g(x)$ 限制到 S 上为 S 的置换且 $h(S)\subseteq\mathbb{F}_q^*$, 则 $f(x)=h(x^q-x)\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)+g(x^q-x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $p\nmid n$.

证明: 在定理 6.26 中令 $\varphi(x)=\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$, $\psi(x)=\overline{\psi}(x)=x^q-x$, 则有 $S=\mathrm{Im}\psi$ 且 $\varphi\circ\psi=0$. 由定理 6.26 (iii) 有 $f(x)=h(x^q-x)\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)+g(x^q-x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\ker(\varphi)\cap\ker(\psi)=\{0\}$ 且 $\psi|_S$ 是 S 上的双射.

由于 $\ker(\psi)=\mathbb{F}_q$, 设 $c\in\ker(\varphi)\cap\ker(\psi)$, 则有 $c\in\mathbb{F}_q$ 且 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c)=nc=0$, 故当且仅当 $p\nmid n$, 由此可推出 $c=0$, 即 $\ker(\varphi)\cap\ker(\psi)=\{0\}$ 当且仅当 $p\nmid n$. 进一步地, $S=\ker(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q})$ 是 $\mathbb{F}_q$ 上的 $(n-1)$-维线性空间, $\psi|_S$ 是 S 上的线性变换, 考察 $\ker(\psi|_S)$. 设 $s\in S$ 且 $s\in\ker(\psi|_S)$, 则 $s\in\mathbb{F}_q$, 从而 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(s)=ns$. 又存在 $\alpha\in\mathbb{F}_{q^n}$ 使得 $s=\alpha^q-\alpha$, 所以 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(s)=0$, 故 $ns=0$, 当 $p\nmid n$ 时可推出 $s=0$. 所以 $\psi|_S$ 是 S 上的双射等价于 $\ker(\psi|_S)=\{0\}$, 而后者也等价于 $p\nmid n$. 这样我们便证出 $\ker(\varphi)\cap\ker(\psi)=\{0\}$ 且 $\psi|_S$ 是 S 上的双射当且仅当 $p\nmid n$. □

6.4 习题

6.1 设 $f(x)\in\mathbb{F}_q[x]$, 证明 $f(x)$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当二元多项式 $f(x,y)=\frac{f(x)-f(y)}{x-y}\in\mathbb{F}_q[x,y]$ 没有使得 $a\neq b$ 的解 $(a,b)\in\mathbb{F}_q^2$.

6.2 设 p 为素数, q 为 p 的方幂, $a_0,a_1,\ldots,a_{q-1}\in\mathbb{F}_q$ 满足对所有 $1\leq t\leq q-2$, $\sum_{i=0}^{q-1}a_i^t=0$ 成立.

(a). 若 $\sum_{i=0}^{q-1}a_i^{q-1}\neq 0$, 证明 $a_0,a_1,\ldots,a_{q-1}$ 互不相同..

(b). 若 $\sum_{i=0}^{q-1} a_i^{q-1} = 0$, 证明 $a_0, a_1, \ldots, a_{q-1}$ 中每个元素在序列 $a_0, a_1, \ldots, a_{q-1}$ 中出现 p 的倍数次.

6.3 设 F 为任意域, A 为 F^* 的 k 阶子群, 对于 $a_1, a_2, \ldots, a_k \in A$, 证明 $a_1, a_2, \ldots, a_k$ 互不相同当且仅当对所有 $1 \le t \le k-1$ 有 $\sum_{i=1}^{k} a_i^t = 0$.

6.4 设 $q-1 = mk$, 其中 m, k 为正整数, 证明 x^{m+1} 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(m+1, k) = 1$.

6.5 设 $p = \mathrm{char}\mathbb{F}_q$, $a \in \mathbb{F}_q$, $i > j$, 证明 $x^{p^i} - ax^{p^j}$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 a 不是 $\mathbb{F}_q^*$ 中元素的 $p^i - p^j$ 次幂.

6.6 若 q 为奇素数, 证明定理 6.4 (Hermite 准则) 中条件 (ii) 中的 t 可限制为 $1 \le t \le \frac{q-1}{2}$. 举例说明此限制对 $q = p^r$ 并不成立, 其中 $r > 1$.

6.7 证明定理 6.6.

6.8 列出有限域上所有的 3 次和 4 次规范置换多项式.

6.9 确定所有 $\mathbb{F}_7$ 上形如 $x^r(x^3 - a)^2$ 的置换多项式, 其中 r 为正整数, $a \in \mathbb{F}_7$.

6.10 设 $q \equiv \pm 2 \pmod 5$, 证明对任意 $a \in \mathbb{F}_q$, $5x^5 + 5ax^3 + a^2x$ 是 $\mathbb{F}_q$ 上的置换多项式.

6.11 对于素数 p 和任意正整数 m, 用 $v_p(m)$ 表示能整除 m 的 p 的最高次幂的指数, 例如 $v_2(24) = 3$, $v_3(24) = 1$, $v_5(24) = 0$ 等等, 称 $v_p(m)$ 为 m 的 p-adic 阶, 证明

(a).

$$v_p(m!) = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor = \frac{m-s}{p-1},$$

其中 $\lfloor x \rfloor$ 表示不超过 x 的最大整数, s 是把 m 写成 p 进制表示时的各数位的和, 即若 $m = s_0 + s_1 p + \cdots + a_{k-1}p^{k-1}$, 这里 $0 \le s_j \le p-1$, $0 \le j \le k-1$, 则 $s = \sum_{j=0}^{k-1} s_j$.

(b). 设 p 为奇素数, $q = p^r$, $m = \frac{q-1}{2}$, $k \equiv 1 \pmod q$, 则有

$$p \nmid \binom{k+m-1}{m-1},$$

并由此完成例 6.2 的证明.

(c). 设 t 为非负整数, $p^t < k < p^{t+1}$, 则 $p \nmid \binom{k}{p^t}$.

6.12 证明对任意 $m, n \ge 0$ 有 $D_m(D_n(x, y), y^n) = D_{mn}(x, y)$, 特别地, 对于 $a \in \mathbb{F}_q$ 有 $D_{mn}(x, a) = D_m(D_n(x, a), a^n)$, 故对于所有以 a 为参数的 Dickson 多项式构成的集合 $\mathcal{D}(a) = \{D_n(x, a) \mid n \ge 0\}$, $\mathcal{D}(a)$ 在合成下封闭当且仅当 $a = 0$ 或者 $a = 1$.

6.13 设 a 为非零整数, 证明存在无穷多个素数 p 使得 Dickson 多项式 $D_n(x, a)$ 模 p 后为 $\mathbb{F}_p$ 上的置换多项式当且仅当 $\gcd(n, 6) = 1$.

6.14 对于 $a \in \mathbb{F}_q$, 称 $D_n(a,x) \in \mathbb{F}_q[x]$ 为第 n 个具有参数 a 的反 Dickson 多项式, 其中 $D_0(a,x)=2$, 证明

(a). 若 n 为奇数, 则 $D_n(0,x)=0$, 而若 $n=2k$ 为偶数, 则 $D_n(a,x)=2(-x)^k$. 若 $a\in\mathbb{F}_q^*$, 则 $D_n(a,x)=a^nD_n(1,a^{-2}x)$, 所以对于 $a\in\mathbb{F}_q^*$, $D_n(a,x)$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 $D_n(1,x)$ 是 $\mathbb{F}_q$ 上的置换多项式.

(b). 设正整数 k,e 满足 $\gcd(k,2e)=1$, 令 $n=2^k+1$, 证明 $D_n(1,x)$ 为 $\mathbb{F}_{2^e}$ 上的置换多项式.

(c). 多项式 $f(x)\in\mathbb{F}_q[x]$ 称为在 $\mathbb{F}_q$ 上是几乎完美非线性 (APN) 函数若对任意 $a\in\mathbb{F}_q^*$ 和 $b\in\mathbb{F}_q$, 方程 $f(x+a)-f(x)=b$ 在 $\mathbb{F}_q$ 中有至多 2 个解. 设 p 为素数, e 为正整数, $q=p^e$, 证明若 $p=2$ 或者 $p\geq 3$ 且 n 为奇数时由 x^n 是 $\mathbb{F}_{q^2}$ 上的 APN 函数可推出 $D_n(1,x)$ 为 $\mathbb{F}_q$ 上的置换多项式, 又可推出 x^n 是 $\mathbb{F}_q$ 上的 APN 函数.

6.15 设 $L(x)=\sum_{i=0}^{r-1}a_ix^{q^i}\in\mathbb{F}_q[x]$ 为 $\mathbb{F}_q$ 上的 q-多项式, $l(x)=\sum_{i=0}^{r-1}a_ix^i$ 为 $L(x)$ 的常规 q-相伴多项式, 证明 $L(x)$ 为 $\mathbb{F}_{q^r}$ 上的置换多项式当且仅当 $\gcd(l(x),x^r-1)=1$.

6.16 证明 $f(x)=x^{2^{m+1}}+x^3+x$ 是 $\mathbb{F}_{2^{2m+1}}$ 上的置换多项式.

6.17 利用定理 6.20 证明定理 6.7.

6.18 设 p 为素数, $q=p^m$, 证明域 $\mathbb{F}_q$ 的乘法群 $\mathbb{F}_q^*$ 的每个自同态一定形如 $x\mapsto x^s$, 其中整数 s 满足 $1\leq s\leq q-1$, 而 $\mathbb{F}_q$ 的加法群的每个自同态的多项式表示一定为某个 p-多项式 $\sum_{i=0}^{m-1}a_ix^{p^i}\in\mathbb{F}_q[x]$.

6.19 设 r 和 d 是正整数且 $d\mid(q-1)$, $g(x)\in\mathbb{F}_q[x]$, 设 γ 为 $\mathbb{F}_q$ 的一个本原元素, $\zeta=\gamma^{\frac{q-1}{d}}$, 证明 $f(x)=x^rg(x^{\frac{q-1}{d}})$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(r,\frac{q-1}{d})=1$ 且 $\{\log_\gamma(f(\zeta^i))+ir \pmod d \mid i\in\mathbb{Z}_d\}=\mathbb{Z}_d$, 并由此给出所有 $\mathbb{F}_q$ 上形如 $x^rg(x^{\frac{q-1}{2}})$ 且次数小于 q 的置换多项式.

6.20 设 r 和 d 是正整数且 $d\mid(q-1)$, $g(x)\in\mathbb{F}_q[x]$ 满足存在正整数 n 使得对所有 $x\in\mu_d$ 有 $g(x)^{\frac{q-1}{d}}=x^n$, 证明 $f(x)=x^rg(x^{\frac{q-1}{d}})$ 是 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(r+n,d)=\gcd(r,\frac{q-1}{d})=1$.

6.21 设 e 为正整数, $q=2^e$, 证明 $f(x)=x+x^{q-1}+x^{\frac{q(q-1)}{2}}$ 是 $\mathbb{F}_{q^2}$ 上的置换多项式当且仅当 $e\not\equiv 0 \pmod 3$.

6.22 证明定理 6.26.

6.23 设 n 为正整数, $\varphi(x)\in\mathbb{F}_q[x]$ 是 $\mathbb{F}_q$ 上的 q-多项式, $g(x),h(x)\in\mathbb{F}_{q^n}[x]$ 且 $h(\mathbb{F}_q)\subseteq\mathbb{F}_q^*$, 则有

(a). $f(x)=h(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))\varphi(x)+g(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))^q-g(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$ 为 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $\ker(\varphi)\cap\ker(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q})=\{0\}$ 且 $h(x)\varphi(x)$ 为 $\mathbb{F}_q$ 上的置换.

(b). 设 $g(x)$ 在 $\mathbb{F}_q$ 上的限制为 $\mathbb{F}_q$ 上的置换, 则 $f(x)=h(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))(x^q-x)+g(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$ 为 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $p\nmid n$, 其中 $p=\mathrm{char}\mathbb{F}_{q^n}$.

6.24 设 n 为正整数, $L_1(x),L_2(x),L_3(x)\in\mathbb{F}_q[x]$ 是 $\mathbb{F}_q$ 上的 q-多项式, $g(x)\in\mathbb{F}_{q^n}[x]$ 满足 $g(L_3(\mathbb{F}_{q^n}))\subseteq\mathbb{F}_q$. 对任意 $y\in L_3(\mathbb{F}_{q^n})$, 定义 $\mathbb{F}_q$ 上的 q-多项式 $F_y(x)=L_1(x)+L_2(x)g(y)$, 证明 $f(x)=L_1(x)+L_2(x)g(L_3(x))$ 为 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当对任意 $y\in L_3(\mathbb{F}_{q^n})$, $\ker(F_y)\cap\ker(L_3)=\{0\}$ 且 $\overline{f}(x)=L_1(x)+L_2(x)g(x)$ 为 $L_3(\mathbb{F}_{q^n})$ 上的置换. (注: 在其中令 $L_2(x)=x$, $L_3(x)=\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$, 则得到 Coulter, Henderson 和 Matthews 的结论.)

6.25 设 A 为有限域, S, $\overline{S}$ 为有限集合满足 $|S|=|\overline{S}|$, 映射 $\lambda:A\to S$ 和 $\overline{\lambda}:A\to\overline{S}$ 都是满射且 $\overline{\lambda}$ 保持加法, 即对任意 $x,y\in A$ 有 $\overline{\lambda}(x+y)=\overline{\lambda}(x)+\overline{\lambda}(y)$, 设 $g:S\to A$ 和 $f:A\to A$ 满足 $\overline{\lambda}(f+g\circ\lambda)=f\circ\lambda$ 和对任意 $x\in A$ 有 $\overline{\lambda}(g(\lambda(x)))=0$, 证明 $f(x)+g(\lambda(x))$ 是集合 A 上的置换当且仅当 f 是集合 A 上的置换.

6.26 设 $p=\mathrm{char}\mathbb{F}_q$, $L(x)\in\mathbb{F}_q[x]$ 为 p-多项式, $h(x)\in\mathbb{F}_{q^n}[x]$ 满足 $h(\mathbb{F}_{q^n})\subseteq\mathbb{F}_q$, 证明对任意 $\delta\in\mathbb{F}_{q^n}$, $f(x)=h(x^q-x+\delta)+L(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $L(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式.

6.27 设 $p=\mathrm{char}\mathbb{F}_q$ 为奇素数, 整数 $t\geq 0$, $k>0$, $n=2k$, 设 $L(x)\in\mathbb{F}_{q^k}[x]$ 为 p-多项式, $\delta\in\mathbb{F}_{q^k}$, $\alpha,\beta\in\mathbb{F}_{q^n}$ 满足 $\alpha^{q^k}=-\alpha$ 和 $\beta^{q^k}=-\beta$, 证明 $f(x)=\alpha(x^{q^k}+x+\delta)^t+\beta\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)+L(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式当且仅当 $L(x)$ 是 $\mathbb{F}_{q^n}$ 上的置换多项式.

6.28 设 k 为正整数, q 是素数 p 的方幂, 证明

(a). 若 k 为偶数或者 k 为奇数且 $p=2$, $a,b\in\mathbb{F}_{q^2}$, 证明 $f(x)=ax^q+bx+(x^q-x)^k$ 为 $\mathbb{F}_{q^2}$ 上的置换多项式当且仅当 $b-a^q\in\mathbb{F}_q^*$ 且 $a+b\neq 0$.

(b). 若 k 和 p 都是奇数, $a\in\mathbb{F}_{q^2}^*$ 且 $a+a^q\neq 0$, 则 $f(x)=ax^q+a^qx+(x^q-x)^k$ 为 $\mathbb{F}_{q^2}$ 上的置换多项式当且仅当 $\gcd(k,q-1)=1$.

6.29 设 p 是奇素数, e 为正整数, $q=p^e$, 多项式 $f(x)\in\mathbb{F}_q[x]$ 称为是平面函数若对任意 $a\in\mathbb{F}_q^*$, $f(x+a)-f(x)$ 都是 $\mathbb{F}_q$ 上的置换多项式.

(a). 设 n 为正整数, 证明 x^n 为 $\mathbb{F}_q$ 上的平面函数当且仅当 $(x+1)^n-x^n$ 是 $\mathbb{F}_q$ 上的置换多项式.

(b). (Dembowski-Ostrom 定理) 设 $i\geq 0$, 证明 x^{1+p^i} 为 $\mathbb{F}_q$ 上的平面函数当且仅当 $v_2(i)\geq v_2(e)$.

第七章　有限域上多项式的根

本章我们讨论有关有限域上多项式的根 (或零点, 解) 的问题, 包括根的个数, 求根算法等. 假设多项式 $f(x)$ 没有重根, 即满足 $\gcd(f(x), f'(x)) = 1$. 实际上, 若 $f(x)$ 有重根, 则 $f(x)/\gcd(f(x), f'(x))$ 与 $f(x)$ 有相同的根且没有重根.

7.1　多项式在扩域中的根

显然有限域上的一元多项式在扩域中一定有根, 且根的个数等于它的次数, 本节我们讨论如何求出这些根. 首先考察 q-多项式.

设 $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i} \in \mathbb{F}_{q^m}[x]$ 是域 $\mathbb{F}_{q^m}$ 上的 q-多项式并设 $L(x)$ 的全部根都在 $\mathbb{F}_{q^m}$ 的扩域 $\mathbb{F}_{q^s}$ 中. 把 $\mathbb{F}_{q^s}$ 看成 $\mathbb{F}_q$ 上的 s-维线性空间, 由第 4.4 节我们知道 $L(x)$ 的所有根构成的集合 $U = \{\alpha \in \mathbb{F}_{q^s} \mid L(\alpha) = 0\}$ 是 $\mathbb{F}_{q^s}$ 的子空间, 即 U 是 $\mathbb{F}_q$ 上的 n-维线性空间.

设 $\{\beta_1, \beta_2, \ldots, \beta_s\}$ 是 $\mathbb{F}_{q^s}$ 在 $\mathbb{F}_q$ 上的一组基, 则任意 $\beta \in \mathbb{F}_{q^s}$ 可以唯一地表成 $\beta = \sum_{i=1}^{s} c_i\beta_i$, 其中 $c_i \in \mathbb{F}_q$, $1 \le i \le s$. 由于 $L : \beta \mapsto L(\beta)$ 是 $\mathbb{F}_{q^s}$ 上的 $\mathbb{F}_q$-线性变换, 设 L 在基 $\{\beta_1, \beta_2, \ldots, \beta_s\}$ 下的矩阵为 A, 即对每个 j, $1 \le j \le s$, 设 $L(\beta_j) = \sum_{i=1}^{s} a_{ij}\beta_i$, 则 $A = (a_{ij})_{1\le i,j\le s}$, 或简写为

$$(L(\beta_1), L(\beta_2), \cdots, L(\beta_s)) = (\beta_1, \beta_2, \cdots, \beta_s)A.$$

对任意 $\beta \in \mathbb{F}_{q^s}$, 若 β 在基 $\{\beta_1, \beta_2, \ldots, \beta_s\}$ 下的坐标为 $(c_1, c_2, \ldots, c_s)^T$, 则 $L(\beta)$ 在基 $\{\beta_1, \beta_2, \ldots, \beta_s\}$ 下的坐标为 $A(c_1, c_2, \ldots, c_s)^T$. 所以 β 为 $L(x)$ 的根当且仅当

$$A(c_1, c_2, \ldots, c_s)^T = 0,$$

即 β 在基 $\{\beta_1, \beta_2, \ldots, \beta_s\}$ 下的坐标为 $\mathbb{F}_q$ 上的齐次线性方程组 $AX = 0$ 的解. 解这个齐次线性方程组, 我们就可以得到 $L(x)$ 的根的坐标, 从而得到 $L(x)$ 的所有根.

例 7.1: 设 α 是 $\mathbb{F}_3$ 上本原多项式 x^2+x-1 的一个根, 求 $\mathbb{F}_{3^2}$ 上线性化多项式 $L(x) = x^9 - x^3 - \alpha x$ 在 $\mathbb{F}_{3^2}$ 的扩域中的根. $L(x)$ 的根都在 $\mathbb{F}_{3^4}$ 中 (为什么?), 取 $\mathbb{F}_3$ 上的一个 4 次本原多项式 $x^4 + x^3 + x^2 - x - 1$, ζ 是它的一个根, 则 $\{1, \zeta, \zeta^2, \zeta^3\}$ 构成 $\mathbb{F}_{3^4}$ 在 $\mathbb{F}_3$ 上的一组基. 由于 ζ 为 $\mathbb{F}_{3^4}$ 的本原元素, $\alpha \in \mathbb{F}_{3^4}$, 设 $\alpha = \zeta^k$, 又 $\mathrm{ord}(\zeta) = 80$, $\mathrm{ord}(\alpha) = 8$, 故 $\gcd(80, k) = 10$, 所以

$k=10,30,50$ 或者 70. 容易验证 $\zeta^{20}+\zeta^{10}-1=0$, 所以我们可取 $\alpha=\zeta^{10}$ (当然也可取 $\alpha=\zeta^{30}$, 它与 ζ^{10} 在 $\mathbb{F}_3$ 上共轭). 计算得出 $L(1)=-\alpha=1-\zeta-\zeta^2+\zeta^3$, $L(\zeta)=\zeta^9-\zeta^3-\alpha\zeta=-\zeta-\zeta^2-\zeta^3$, $L(\zeta^2)=-1+\zeta^3$, 和 $L(\zeta^3)=1-\zeta^3$, 所以 L 在基 $\{1,\zeta,\zeta^2,\zeta^3\}$ 下的矩阵为

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

解齐次线性方程组 $AX=0$, 可以求出它的一个基础解系为 $(1,-1,1,0)^T$ 和 $(-1,1,0,1)^T$, 故 $AX=0$ 的全部解为 $(c_1-c_2,-c_1+c_2,c_1,c_2)^T$, 所以 $L(x)$ 在 $\mathbb{F}_{3^2}$ 的扩域中的全部根为 $(c_1-c_2)+(-c_1+c_2)\zeta+c_1\zeta^2+c_2\zeta^3$, 其中 $c_1,c_2\in\mathbb{F}_3$. 或者我们可以具体写出 $L(x)$ 的 9 个根为 $\theta_1=0$, $\theta_2=-1+\zeta+\zeta^3$, $\theta_3=1-\zeta-\zeta^3$, $\theta_4=1-\zeta+\zeta^2$, $\theta_5=\zeta^2+\zeta^3$, $\theta_6=-1+\zeta+\zeta^2-\zeta^3$, $\theta_7=-1+\zeta-\zeta^2$, $\theta_8=1-\zeta-\zeta^2+\zeta^3$, 和 $\theta_9=-\zeta^2-\zeta^3$. □

类似的方法也可以求仿射 q-多项式在扩域中的根, 设 $A(x)=L(x)-\alpha\in\mathbb{F}_{q^m}[x]$ 是 $\mathbb{F}_{q^m}$ 上的一个仿射 q-多项式, 即 $L(x)$ 是 $\mathbb{F}_{q^m}$ 上的一个 q-多项式, $\alpha\in\mathbb{F}_{q^m}$. 与之前一样, 设 $A(x)$ 的全部根都在 $\mathbb{F}_{q^m}$ 的扩域 $\mathbb{F}_{q^s}$ 中, $\{\beta_1,\beta_2,\dots,\beta_s\}$ 是 $\mathbb{F}_{q^s}$ 在 $\mathbb{F}_q$ 上的一组基且 $\mathbb{F}_{q^m}$ 上的线性变换 L 在基 $\{\beta_1,\beta_2,\dots,\beta_s\}$ 下的矩阵为 A, 再设 $\alpha\in\mathbb{F}_{q^m}$ 在基 $\{\beta_1,\beta_2,\dots,\beta_s\}$ 下的坐标为 $\mathbf{b}=(b_1,b_2,\dots,b_s)^T$. 对于 $\beta\in\mathbb{F}_{q^s}$, 设 β 在基 $\{\beta_1,\beta_2,\dots,\beta_s\}$ 下的坐标为 $(c_1,c_2,\dots,c_s)^T$, 则 β 是 $A(x)$ 的根当且仅当

$$A(c_1,c_2,\dots,c_s)^T=\mathbf{b},$$

即 β 在基 $\{\beta_1,\beta_2,\dots,\beta_s\}$ 下的坐标为 $\mathbb{F}_q$ 上的线性方程组 $AX=\mathbf{b}$ 的解. 解这个线性方程组, 可以得到 $A(x)$ 的根的坐标, 从而得到 $A(x)$ 的所有根.

如上讨论表明求仿射 q-多项式的根可以转化为求解线性方程组, 而利用 Gauss 消去法我们很容易解线性方程组. 对于域 $\mathbb{F}_{q^m}$ 上的任意多项式 $f(x)$, 我们可以首先找到 $\mathbb{F}_{q^m}$ 上的一个非零仿射 q-多项式 $A(x)$ 使得 $f(x)\mid A(x)$ (这样的 $A(x)$ 称为 $f(x)$ 的仿射 q-倍式), 然后用如上方法求出 $A(x)$ 的全部根, 最后把求出的 $A(x)$ 的根带入 $f(x)$ 来检查它们哪些是 $f(x)$ 的根. 由于 $f(x)$ 的根一定是 $A(x)$ 的根, 这样就可以求出 $f(x)$ 的所有根.

下面需要解决的问题就是如何找到 $f(x)$ 的仿射 q-倍式. 设 $\deg f(x)=n$, 对于 $0\le i\le n-1$, 求出唯一的多项式 $r_i(x)\in\mathbb{F}_{q^m}[x]$ 满足 $x^{q^i}\equiv r_i(x)\pmod{f(x)}$ 且 $\deg r_i(x)<n$ (可利用 4.3 节求不可约多项式的阶那部分给出的方法). 确定不全为零的元素 $\alpha_0,\alpha_1,\dots,\alpha_{n-1}\in\mathbb{F}_{q^m}$ 使得 $\sum_{i=0}^{n-1}\alpha_i r_i(x)=\alpha\in\mathbb{F}_{q^m}$. 事实上, 设 $\sum_{i=0}^{n-1}\alpha_i r_i(x)=\sum_{j=0}^{n-1}\delta_j x^j$, 其中每个 δ_j 都是 $\alpha_0,\alpha_1,\dots,\alpha_{n-1}$ 的系数在 $\mathbb{F}_{q^m}$ 中的线性组合, $0\le j\le n-1$. 令 $\delta_1=\delta_2=\cdots=\delta_{n-1}=0$, 这是一个以 $\alpha_0,\alpha_1,\dots,\alpha_{n-1}$ 为未知量的域 $\mathbb{F}_{q^m}$ 上的齐次线性方程组, 有 $n-1$ 个方程, 所以它一定有非零解, 取出它的一组非零解 $\alpha_0,\alpha_1,\dots,\alpha_{n-1}\in\mathbb{F}_{q^m}$, 则 $\sum_{i=0}^{n-1}\alpha_i r_i(x)=\alpha\in\mathbb{F}_{q^m}$. 令

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

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

即 $A(x)$ 是 $f(x)$ 的一个仿射 q-倍式.

注意到类似地, 我们也可以找到 $\mathbb{F}_{q^m}$ 上的一个 q-多项式 $L(x)$ 使得 $f(x)\mid L(x)$, 同样利用解齐次线性方程组求出 $L(x)$ 的所有根, 试验可以从中得到 $f(x)$ 的所有根. 但是如上面讨论的那样, n 次多项式 $f(x)$ 的仿射 q-倍式 $A(x)$ 的次数 $\le q^{n-1}$, 它的根 $\le q^{n-1}$ 个, 而求出的能被 $f(x)$ 整除的 q-多项式 $L(x)$ 的次数 $\le q^n$ (参见 §4.4), 根的个数扩大了, 从中找出 $f(x)$ 的根的范围也就扩大了.

例 7.2: 设 θ 是 $\mathbb{F}_2$ 上不可约多项式 x^2+x+1 的一个根, $f(x)=x^4+\theta^2x^3+\theta x^2+x+\theta\in\mathbb{F}_{2^2}[x]$, 我们求 $f(x)$ 在 $\mathbb{F}_{2^6}$ 中的根. 先确定 $f(x)$ 的仿射 q-倍式 $A(x)$, 这里 $q=2$. 计算 x, x^2, x^4, $x^8\,(\mathrm{mod}\ f(x))$ 得到 $r_0(x)=x$, $r_1(x)=x^2$, $r_2(x)=\theta^2x^3+\theta x^2+x+\theta$, $r_3(x)=\theta x^3+\theta x^2+x+\theta$. 所以

$$\sum_{i=0}^{3}\alpha_i r_i(x)=(\theta^2\alpha_2+\theta\alpha_3)x^3+(\alpha_1+\theta\alpha_2+\theta\alpha_3)x^2+(\alpha_0+\alpha_2+\alpha_3)x+(\theta\alpha_2+\theta\alpha_3).$$

解齐次线性方程组

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

可得到它的一组非零解为 $\alpha_0=\theta$, $\alpha_1=\theta^2$, $\alpha_2=\theta^2$, $\alpha_3=1$, 由此可求出 $\alpha=\theta\alpha_2+\theta\alpha_3=\theta^2$, 从而我们得到 $f(x)$ 的仿射 q-倍式为 $A(x)=L(x)+\theta^2$, 其中 $L(x)=x^8+\theta^2x^4+\theta^2x^2+\theta x$.

下面求 $A(x)$ 在 $\mathbb{F}_{2^6}$ 中的根. 取 $\mathbb{F}_2$ 上的一个 6 次本原多项式 x^6+x+1, 设 ζ 是它的一个根, 则 $\{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5\}$ 构成 $\mathbb{F}_{2^6}$ 在 $\mathbb{F}_2$ 上的一组基. 由于 $\mathrm{ord}(\zeta)=63$, 所以 $\mathrm{ord}(\zeta^{21})=3$, 又 $\mathbb{F}_2$ 扩域中的任意 3 阶元一定是 x^2+x+1 的根, 我们可取 $\theta=\zeta^{21}$. 容易算出 $\mathbb{F}_{2^6}$ 上的线性变换 L 在基 $\{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5\}$ 下的矩阵为

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

而 θ^2 在基 $\{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5\}$ 下的坐标为 $\mathbf{b}=(0,1,0,1,1,1)^T$. 解线性方程组 $AX=\mathbf{b}$, 可得其全部解为

$$(1,0,0,0,0,0)^T+c_1(0,1,1,1,0,0)^T+c_2(1,1,1,0,1,0)^T+c_3(1,1,0,0,0,1)^T,$$

其中 $c_1, c_2, c_3 \in \mathbb{F}_2$. 从而仿射 2-多项式 $A(x)$ 在 $\mathbb{F}_{2^6}$ 中的 8 个根为 $\eta_1 = 1$, $\eta_2 = \zeta + \zeta^2 + \zeta^4$, $\eta_3 = \zeta + \zeta^5$, $\eta_4 = 1 + \zeta^2 + \zeta^4 + \zeta^5$, $\eta_5 = 1 + \zeta + \zeta^2 + \zeta^3$, $\eta_6 = \zeta^3 + \zeta^4$, $\eta_7 = \zeta^2 + \zeta^3 + \zeta^5$, 和 $\eta_8 = 1 + \zeta + \zeta^3 + \zeta^4 + \zeta^5 = \theta$. 对 $1 \le j \le 8$, 通过计算 $f(\eta_j)$, 我们可得 $f(x)$ 在 $\mathbb{F}_{2^6}$ 中的 4 个根为 η_2, η_5, η_6 和 η_8. □

注意到给定 $\mathbb{F}_{q^m}$ 上的 n 次多项式 $f(x)$, 要求它在 $\mathbb{F}_{q^m}$ 的扩域中的所有根, 困难之处是我们并不知道 $f(x)$ 的根在哪个扩域中, 也即我们需要找到 $f(x)$ 在 $\mathbb{F}_{q^m}$ 上的分裂域. 若 $f(x)$ 在 $\mathbb{F}_{q^m}$ 上不可约, 则我们知道 $f(x)$ 的根一定在 $\mathbb{F}_{q^m}$ 的 n 次扩域 $\mathbb{F}_{q^{mn}}$ 中. 但若 $f(x)$ 可约则没有什么太好的结果, 由分裂域的结果我们有一个估计, 即扩张次数 $\le n!$. 当然我们可以先给出 $f(x)$ 的完全分解, 对它的每个不可约因子我们可以得到其根所在的扩域, 最后这些扩域的复合就是包含 $f(x)$ 的全部根的域. 设 $f(x) = p_1(x)p_2(x)\cdots p_k(x)$ 为 $f(x)$ 在 $\mathbb{F}_{q^m}$ 上的标准分解式 (由于我们假设 $f(x)$ 无重根, 所以 $f(x)$ 无重因式), 其中 $p_1(x), p_2(x), \ldots, p_k(x)$ 是互不相同的不可约多项式, 其次数分别为 $n_1, n_2, \ldots, n_k$, 则有 $\sum_{i=1}^{k} n_i = n$. 对于每个 $1 \le i \le k$, $p_i(x)$ 的根在 $\mathbb{F}_{q^{mn_i}}$ 中, 所以 $f(x)$ 的所有根在 $\mathbb{F}_{q^{mt}}$ 中, 其中 $t = \mathrm{lcm}(n_1, n_2, \ldots, n_k)$. 例如例 7.2 中的多项式 $f(x)$ 在 $\mathbb{F}_{2^2}$ 上的完全分解为 $f(x) = (x + \theta)(x^3 + x^2 + 1)$, 所以 $f(x)$ 的所有根在 $\mathbb{F}_{2^2}$ 的 3 次扩域 $\mathbb{F}_{2^6}$ 中, 这就是我们在计算时取的域. 如果按照一般的估计, $f(x)$ 的根一定包含在 $\mathbb{F}_{2^2}$ 的 $4! = 24$ 次扩域中, 则需要在 $\mathbb{F}_{2^{48}}$ 中讨论, 计算会比较复杂.

7.2 解的个数

设 $f(x_1, x_2, \ldots, x_n)$ 是 $\mathbb{F}_q$ 上的一个 n 元多项式, $f(x_1, x_2, \ldots, x_n)$ 在 $\mathbb{F}_q$ 上的一个解 (或零点) 指的是 $\mathbb{F}_q$ 上的一个 n 元有序数组 $(c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$ 使得 $f(c_1, c_2, \ldots, c_n) = 0$. 给定 $\mathbb{F}_q$ 上的一个多项式, 我们自然会问它在 $\mathbb{F}_q$ 上是否有解? 若有解, 解数是多少? 是否有好的解数表达式? 本节我们讨论一个多项式在 $\mathbb{F}_q$ 上的互不相同的解的个数问题, 下面用 $N_q(f)$ 表示多项式 $f(x_1, x_2, \ldots, x_n)$ 在 $\mathbb{F}_q$ 上 (或 $\mathbb{F}_q^n$ 中) 的解的个数.

首先看最简单的一元多项式的情形, 一元多项式的解也称为它的根. 设 $f(x)$ 是 $\mathbb{F}_q$ 上的多项式, 由于 $x^q - x$ 为 $\mathbb{F}_q$ 上所有首一一次因式的乘积, 所以 $\gcd(f(x), x^q - x)$ 就是 $\mathbb{F}_q$ 上整除 $f(x)$ 的那些首一一次因式的乘积, 由此得到 $f(x)$ 在 $\mathbb{F}_q$ 上的根就是多项式 $\gcd(f(x), x^q - x)$ 的全部根, 故 $f(x)$ 在 $\mathbb{F}_q$ 上的根的个数等于 $\gcd(f(x), x^q - x)$ 的次数.

下面我们给出一元多项式 $f(x)$ 在 $\mathbb{F}_q$ 上的根的个数的另一种求法, 首先很容易判断 0 是否为多项式 $f(x)$ 的根, 这只需要看 $f(x)$ 的常数项是否为零, 所以下面我们只考虑它的非零根. 显然 $f(x)$ 在 $\mathbb{F}_q$ 上的非零根就是 $\gcd(f(x), x^{q-1} - 1)$ 的根, 从而不失一般性可以假设 $\deg f(x) \le q-1$. 又因为对任意 $b \in \mathbb{F}_q^*$, 有 $b^{q-1} = 1$, 所以多项式 $f(x) = a_0 + a_1x + \cdots + a_{q-2}x^{q-2} + a_{q-1}x^{q-1}$ 在 $\mathbb{F}_q$ 上的非零根也就是多项式 $(a_0 + a_{q-1}) + a_1x + \cdots + a_{q-2}x^{q-2}$ 在 $\mathbb{F}_q$ 上的非零根, 这样我们可以假设 $\deg f(x) \le q - 2$.

设 $f(x)=a_0+a_1x+\cdots+a_{q-2}x^{q-2}\in\mathbb{F}_q[x]$, 定义与多项式 $f(x)$ 相关的 $(q-1)\times(q-1)$ 矩阵 $A(f)$ 为

$$A(f)=\begin{bmatrix} a_0 & a_1 & \cdots & a_{q-3} & a_{q-2} \\ a_1 & a_2 & \cdots & a_{q-2} & a_0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{q-2} & a_0 & \cdots & a_{q-4} & a_{q-3} \end{bmatrix}. \tag{7.1}$$

这是一个循环矩阵, 即从第二行开始, 它的每一行元素都是上一行元素循环左移一位 (最左边的元素移到最右边) 得到的.

定理 7.1: (König-Rados 定理) 设 $f(x)=a_0+a_1x+\cdots+a_{q-2}x^{q-2}\in\mathbb{F}_q[x]$, 则 $f(x)$ 在 $\mathbb{F}_q$ 上的非零根的个数等于 $q-1-r$, 其中 r 是式 (7.1) 定义的矩阵 $A(f)$ 的秩.

证明: 记 $\mathbb{F}_q^*=\{b_1,\ldots,b_{q-1}\}$, 构造 $q-1$ 阶 Vandermonde 矩阵为

$$B=\begin{bmatrix} 1 & 1 & \cdots & 1 \\ b_1 & b_2 & \cdots & b_{q-1} \\ b_1^2 & b_2^2 & \cdots & b_{q-1}^2 \\ \vdots & \vdots & & \vdots \\ b_1^{q-2} & b_2^{q-2} & \cdots & b_{q-1}^{q-2} \end{bmatrix}.$$

由于对任意 $b\in\mathbb{F}_q^*$ 有 $b^{q-1}=1$, 我们有

$$A(f)B=\begin{bmatrix} f(b_1) & f(b_2) & \cdots & f(b_{q-1}) \\ b_1^{-1}f(b_1) & b_2^{-1}f(b_2) & \cdots & b_{q-1}^{-1}f(b_{q-1}) \\ b_1^{-2}f(b_1) & b_2^{-2}f(b_2) & \cdots & b_{q-1}^{-2}f(b_{q-1}) \\ \vdots & \vdots & & \vdots \\ b_1^{-(q-2)}f(b_1) & b_2^{-(q-2)}f(b_2) & \cdots & b_{q-1}^{-(q-2)}f(b_{q-1}) \end{bmatrix}.$$

设 $f(x)$ 在 $\mathbb{F}_q$ 上的非零根的个数为 N 且 $f(x)$ 的非零根为 $b_{q-N},\ldots,b_{q-1}$, 则矩阵 $A(f)B$ 的后 N 列全为零, 从而 $\operatorname{rank}(A(f)B)\le q-1-N$. 另一方面, 矩阵 $A(f)B$ 的 $q-1-N$ 阶顺序主子式 (即前 $q-1-N$ 行和前 $q-1-N$ 列构成的子式) 等于

$$f(b_1)f(b_2)\cdots f(b_{q-1-N})\begin{vmatrix} 1 & 1 & \cdots & 1 \\ b_1^{-1} & b_2^{-1} & \cdots & b_{q-1-N}^{-1} \\ b_1^{-2} & b_2^{-2} & \cdots & b_{q-1-N}^{-2} \\ \vdots & \vdots & & \vdots \\ b_1^{-(q-2-N)} & b_2^{-(q-2-N)} & \cdots & b_{q-1-N}^{-(q-2-N)} \end{vmatrix},$$

上式出现的行列式是由互不相同的元素 $b_1^{-1},b_2^{-1},\ldots,b_{q-1-N}^{-1}$ 构成的 Vandermonde 行列式, 故这个 $q-1-N$ 阶顺序主子式非零, 所以 $\operatorname{rank}(A(f)B)=q-1-N$. 由于矩阵 B 的行列式非零, 所以 B 可逆, 从而 $r=\operatorname{rank}(A(f))=\operatorname{rank}(A(f)B)=q-1-N$, 故 $N=q-1-r$. □

例 7.3: 设 $f(x)=3+x-3x^2+2x^3\in\mathbb{F}_7[x]$, 则矩阵 $A(f)$ 为

$$A(f)=\begin{bmatrix} 3 & 1 & -3 & 2 & 0 & 0\\ 1 & -3 & 2 & 0 & 0 & 3\\ -3 & 2 & 0 & 0 & 3 & 1\\ 2 & 0 & 0 & 3 & 1 & -3\\ 0 & 0 & 3 & 1 & -3 & 2\\ 0 & 3 & 1 & -3 & 2 & 0 \end{bmatrix}.$$

容易算出 $\operatorname{rank}(A(f))=6$, 所以由 König-Rados 定理得 $f(x)$ 在 $\mathbb{F}_7$ 上无非零根, 又显然 0 不是 $f(x)$ 的根, 从而 $f(x)$ 在 $\mathbb{F}_7$ 上没有根. 再注意到 $f(x)$ 的次数为 3, 这就得到 $f(x)$ 在 $\mathbb{F}_7$ 上不可约. □

下面我们来看一般的 n 元多项式, 1935 年 E. Artin 猜测了如下定理, 几乎同时就被 C. Chevalley 所证明.

定理 7.2: (Chevalley 定理) 设 $f(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q[x_1,x_2,\ldots,x_n]$ 满足 $n>d=\deg f$ (这里 $\deg f$ 表示 n 元多项式 $f(x_1,x_2,\ldots,x_n)$ 的次数) 且 $f(0,0,\ldots,0)=0$, 则 $f(x_1,x_2,\ldots,x_n)$ 在 $\mathbb{F}_q^n$ 中有至少 2 个解.

注意到多项式 $f(x_1,x_2,\ldots,x_n)$ 有解 $(0,0,\ldots,0)$ 当且仅当 $f(x_1,x_2,\ldots,x_n)$ 的常数项为 0. 设 $f(x_1,x_2,\ldots,x_n)$ 的常数项为 0, 解 $(0,0,\ldots,0)$ 称为 $f(x_1,x_2,\ldots,x_n)$ 的零解或平凡解. Chevalley 定理说的是次数小于未定元个数且常数项为 0 的多项式一定有非零解. 为了证明 Chevalley 定理, 我们需要如下引理.

引理 7.3: 设 $f(x_1,x_2,\ldots,x_n)$ 是 $\mathbb{F}_q$ 上的一个 n 元多项式且其每个未定元的次数都小于 q, 若对任意 $(a_1,a_2,\ldots,a_n)\in\mathbb{F}_q^n$ 都有 $f(a_1,a_2,\ldots,a_n)=0$, 则 $f(x_1,x_2,\ldots,x_n)$ 为零多项式.

证明: 我们对 n 做归纳. 若 $n=1$, 则 $f(x)$ 是 $\mathbb{F}_q$ 上的一个次数小于 q 的多项式, 但是 $\mathbb{F}_q$ 中每个元素都是它的根, 即 $f(x)$ 在 $\mathbb{F}_q$ 上的根的个数大于它的次数, 从而 $f(x)=0$.

假设结论对 $n-1$ 成立, 下面考察 n 元多项式 $f(x_1,x_2,\ldots,x_n)$, 并记

$$f(x_1,\ldots,x_{n-1},x_n)=\sum_{i=0}^{q-1}g_i(x_1,\ldots,x_{n-1})x_n^i.$$

对任意给定的 $a_1,\ldots,a_{n-1}\in\mathbb{F}_q$, $g(x_n)=\sum_{i=0}^{q-1}g_i(a_1,\ldots,a_{n-1})x_n^i$ 是 $\mathbb{F}_q$ 上以 x_n 为未定元的一元多项式, 其次数小于 q 但是在 $\mathbb{F}_q$ 上有 q 个根, 故 $g(x_n)$ 为零多项式, 所以对任意 $0\le i\le q-1$, 有 $g_i(a_1,\ldots,a_{n-1})=0$. 由归纳假设每个 $n-1$ 元多项式 $g_i(x_1,\ldots,x_{n-1})$ 都是零多项式, 从而 $f(x_1,x_2,\ldots,x_n)$ 也是零多项式. □

注意到 $f(x)=x^q-x$ 是一个非零多项式, 其根为 $\mathbb{F}_q$ 中所有元素, 所以引理对于每个未定元的次数小于 q 的假设是至关重要的. 如果一个多项式每个未定元的次数都小于 q, 则称其为约化的. 而两个 n 元多项式 $f(x_1,x_2,\ldots,x_n)$ 和 $g(x_1,x_2,\ldots,x_n)$ 称为是等价的若对所有的 $(a_1,a_2,\ldots,a_n)\in\mathbb{F}_q^n$, 均有 $f(a_1,a_2,\ldots,a_n)=g(a_1,a_2,\ldots,a_n)$, 并记为 $f\sim g$. 容易验证 $\sim$ 是

$\mathbb{F}_q$ 上的 n 元多项式集合 $\mathbb{F}_q[x_1,x_2,\ldots,x_n]$ 上的一个等价关系.

引理 7.4: 任意多项式 $f(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q[x_1,\ldots,x_n]$ 均等价于约化多项式.

证明: 首先考虑一元的情形. 注意到 $x^q\sim x$, 若对正整数 $m>0$ 且 ℓ 为最小正整数满足 $x^m\sim x^\ell$, 则一定有 $\ell<q$. 事实上, 若 $\ell\geq q$, 则做带余除法有 $\ell=sq+r$, 其中 $0\leq r<q$ 且 $s>0$. 从而 $x^\ell=(x^q)^sx^r\sim x^{s+r}$, 但是 $s+r<sq+r=\ell$, 这与 ℓ 的最小性矛盾.

在任意 n 元的情形, 考察单项式 $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$, 对每个 x_k, $1\leq k\leq n$, 由上面的证明存在非负整数 $j_k<q$ 使得 $x_k^{i_k}\sim x_k^{j_k}$, 从而 $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\sim x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}$, 由此可直接推出结论. □

下面我们用反证法来证明定理 7.2. 若 $(0,0,\ldots,0)$ 是 $f(x_1,x_2,\ldots,x_n)=0$ 的唯一解, 则多项式 $1-f(x_1,x_2,\ldots,x_n)^{q-1}$ 满足对任意 $(a_1,a_2,\ldots,a_n)\in\mathbb{F}_q^n$,

$$1-f(a_1,a_2,\ldots,a_n)^{q-1}=\begin{cases}1, & \text{若 } (a_1,a_2,\ldots,a_n)=(0,0,\ldots,0),\\ 0, & \text{若 } (a_1,a_2,\ldots,a_n)\neq(0,0,\ldots,0),\end{cases}\tag{7.2}$$

而显然多项式 $(1-x_1^{q-1})(1-x_2^{q-1})\cdots(1-x_n^{q-1})$ 也具有 (7.2) 式同样的性质. 设 $g(x_1,x_2,\ldots,x_n)$ 是与多项式 $1-f(x_1,x_2,\ldots,x_n)^{q-1}$ 等价的约化多项式, 则 $g(x_1,x_2,\ldots,x_n)-(1-x_1^{q-1})(1-x_2^{q-1})\cdots(1-x_n^{q-1})$ 的每个未定元的次数都小于 q 且在 $\mathbb{F}_q^n$ 上取值为 0, 由引理 7.3,我们有 $g(x_1,x_2,\ldots,x_n)=(1-x_1^{q-1})(1-x_2^{q-1})\cdots(1-x_n^{q-1})$, 这便给出 $\deg g=n(q-1)$. 另一方面, 显然 $\deg g\leq\deg(1-f^{q-1})=d(q-1)$, 由此可推出 $n\leq d$, 与已知条件矛盾. 所以 $f(x_1,x_2,\ldots,x_n)$ 的解数大于 1.

下面我们给出另一个证明, 由此可以推广定理 7.2 的结论, 此证明基于下面这个引理.

引理 7.5: 设 $i_1,i_2,\ldots,i_n$ 为非负整数, 则除非每个 i_j 均非零且被 $q-1$ 整除, $1\leq j\leq n$, 我们有

$$\sum_{c_1,c_2\ldots,c_n\in\mathbb{F}_q}c_1^{i_1}c_2^{i_2}\cdots c_n^{i_n}=\begin{cases}(-1)^n, & \text{若对每个 } 1\leq j\leq n, \text{ 都有 } i_j\neq0 \text{ 且 } (q-1)\mid i_j,\\ 0, & \text{其它,}\end{cases}$$

其中的运算是 $\mathbb{F}_q$ 中的运算且定义 $0^0=1$.

证明: 首先假设 $n=1$. 若 $i=0$, 则 $\sum_{c\in\mathbb{F}_q}c^0=q=0$. 设 $i\neq0$, 并设 ξ 是 $\mathbb{F}_q$ 的一个本原元素, 若 $(q-1)\nmid i$, 则

$$\sum_{c\in\mathbb{F}_q}c^i=\sum_{k=0}^{q-2}\xi^{ki}=\frac{\xi^{(q-1)i}-1}{\xi^i-1}=0.$$

若 $(q-1)\mid i$, 则 $\sum_{c\in\mathbb{F}_q}c^i=q-1=-1$. 一般地, 由

$$\sum_{c_1,c_2,\ldots,c_n\in\mathbb{F}_q}c_1^{i_1}c_2^{i_2}\cdots c_n^{i_n}=\left(\sum_{c_1\in\mathbb{F}_q}c_1^{i_1}\right)\left(\sum_{c_2\in\mathbb{F}_q}c_2^{i_2}\right)\cdots\left(\sum_{c_n\in\mathbb{F}_q}c_n^{i_n}\right)$$

我们可以立即得到结论. □

前面我们用 $N_q(f)$ 来记 $f(x_1,x_2,\ldots,x_n)$ 在 $\mathbb{F}_q^n$ 中的解数, 设 $p=\mathrm{char}\mathbb{F}_q$. 对于 $(c_1,c_2,\ldots,c_n)\in\mathbb{F}_q^n$, 若 $f(c_1,c_2,\ldots,c_n)=0$, 则 $1-f(c_1,c_2,\ldots,c_n)^{q-1}=1$, 而若 $f(c_1,c_2,\ldots,c_n)\neq0$, 则

$1-f(c_1,c_2,\ldots,c_n)^{q-1}=0$, 从而

$$\sum_{(c_1,c_2,\ldots,c_n)\in\mathbb{F}_q^n}\big(1-f(c_1,c_2,\ldots,c_n)^{q-1}\big)=N_q(f)\cdot 1.$$

设 $a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ 是在 $1-f(x_1,x_2,\ldots,x_n)^{q-1}$ 中出现的一项, 因为 $\deg(1-f^{q-1})=d(q-1)<n(q-1)$, 则一定存在某个 j 使得 $i_j<q-1$, 由引理 7.5, 我们有

$$\sum_{c_1,c_2\ldots,c_n\in\mathbb{F}_q}a_{i_1i_2\cdots i_n}c_1^{i_1}c_2^{i_2}\cdots c_n^{i_n}=a_{i_1i_2\cdots i_n}\sum_{c_1,c_2\ldots,c_n\in\mathbb{F}_q}c_1^{i_1}c_2^{i_2}\cdots c_n^{i_n}=0.$$

由于 $1-f(x_1,x_2,\ldots,x_n)^{q-1}$ 是这些项 $a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ 的和, 故

$$N_q(f)\cdot 1=\sum_{(c_1,c_2,\ldots,c_n)\in\mathbb{F}_q^n}\big(1-f(c_1,c_2,\ldots,c_n)^{q-1}\big)=0,$$

这便得到 $p\mid N_q(f)$. 由此我们证明了如下定理.

定理 7.6: (Warning 定理) 设 $\mathrm{char}\mathbb{F}_q=p$, $f(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q[x_1,x_2,\ldots,x_n]$ 且其次数小于 n, 则 $p\mid N_q(f)$. □

对于定理 7.2 来说, 由于 $f(x_1,x_2,\ldots,x_n)$ 已经有零解, 故 $N_f>0$, 所以 $N_f\geq p\geq 2$, 这便给出 Chevalley 定理的另一个证明.

例 7.4: (a) 设 n 为正整数, $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ 是 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的一组基, 令

$$f(x_1,x_2,\ldots,x_n)=\prod_{j=0}^{n-1}(\alpha_1^{q^j}x_1+\alpha_2^{q^j}x_2+\cdots+\alpha_n^{q^j}x_n).$$

则因为对任意 $1\leq i\leq n$, 有 $\alpha_i^{q^n}=\alpha_i$, 我们容易得到 $f(x_1,x_2,\ldots,x_n)^q=f(x_1^q,x_2^q,\ldots,x_n^q)$, 从而 $f(x_1,x_2,\ldots,x_n)$ 是 $\mathbb{F}_q$ 上的多项式. 对任意 $(c_1,c_2,\ldots,c_n)\in\mathbb{F}_q^n$, 令 $\gamma=\sum_{i=1}^n c_i\alpha_i$, 则有

$$f(c_1,c_2,\ldots,c_n)=\prod_{j=0}^{n-1}(\alpha_1^{q^j}c_1+\alpha_2^{q^j}c_2+\cdots+\alpha_n^{q^j}c_n)=\prod_{j=0}^{n-1}(\alpha_1c_1+\alpha_2c_2+\cdots+\alpha_nc_n)^{q^j}=\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma).$$

所以 $(c_1,c_2,\ldots,c_n)$ 为 $f(x_1,x_2,\ldots,x_n)$ 在 $\mathbb{F}_q$ 上的解当且仅当 $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma)=0$, 后面这个条件等价于 $\gamma=0$, 即 $(c_1,c_2,\ldots,c_n)=(0,0,\ldots,0)$, 所以多项式 $f(x_1,x_2,\ldots,x_n)$ 无非零解. 这表明定理 7.2 中的条件 $\deg(f)<n$ 是必须的.

(b) 设 α 是 $\mathbb{F}_2$ 上不可约多项式 x^2+x+1 的一个根, 考虑 $\mathbb{F}_4$ 上的多项式

$$f(x_1,x_2,\ldots,x_n)=x_1^3+x_2^3+\cdots+x_n^3+\alpha.$$

显然对于任意 $c\in\mathbb{F}_4$, 有 $c^3=0$ 或 1, 即对任意 $(c_1,c_2,\ldots,c_n)\in\mathbb{F}_4^n$, 有 $c_1^3+c_2^3+\cdots+c_n^3\in\mathbb{F}_2$, 而 $\alpha\notin\mathbb{F}_2$, 所以 $f(x_1,x_2,\ldots,x_n)$ 在 $\mathbb{F}_4$ 上无解. 这表明定理 7.2 中假设多项式的常数项为零 (或者多项式存在解) 的条件也是必须的. □

熟知一元多项式的解数一定不超过它的次数, 下面我们把此结果推广到多元多项式的情形, 即给出 $N_q(f)$ 的上界.

定理 7.7: 设 n 为正整数, 非零多项式 $f(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q[x_1,x_2,\ldots,x_n]$ 且 $\deg(f)=d$, 则 $N_q(f)\leq dq^{n-1}$.

证明: 若 $n=1$, 结论显然成立. 若 $d=0$, 则 $f(x_1,x_2,\ldots,x_n)$ 为 $\mathbb{F}_q$ 中的非零元素, 故 $f(x_1,x_2,\ldots,x_n)$ 无解, 结论成立. 若 $d=1$, 则

$$f(x_1,x_2,\ldots,x_n)=a_1x_1+a_2x_2+\cdots+a_nx_n+b,$$

其中 $a_1,a_2,\ldots,a_n,b\in\mathbb{F}_q$ 且 $a_1,a_2,\ldots,a_n$ 不全为零. 不妨设 $a_1\neq 0$, 则对于任意给定的 $c_2,\ldots,c_n\in\mathbb{F}_q$, 令 $c_1=-a_1^{-1}(a_2c_2+\cdots+a_nc_n+b)$, 则 $(c_1,c_2,\ldots,c_n)$ 就是 $f(x_1,x_2,\ldots,x_n)$ 在 $\mathbb{F}_q$ 上的解. 反之 $f(x_1,x_2,\ldots,x_n)$ 在 $\mathbb{F}_q$ 上的任一解 $(c_1,c_2,\ldots,c_n)$ 一定满足 $c_1=-a_1^{-1}(a_2c_2+\cdots+a_nc_n+b)$. 由此得到 $N_q(f)=q^{n-1}$, 结论成立.

下面我们对 d 和 n 做双重归纳. 设 $n>1$ 且 $d>1$, 假设结论对未定元个数不超过 n 且次数小于 d 的非零多项式以及未定元个数至多为 $n-1$ 且次数不超过 d 的非零多项式成立, 我们来看 n 元 d 次非零多项式的情形. 设 $f(x_1,x_2,\ldots,x_n)$ 为 $\mathbb{F}_q$ 上的一个 n 元 d 次非零多项式, 分下面两种情形来证明.

(i) 若 $f(x_1,x_2,\ldots,x_n)$ 被某个 x_1-c 整除, 其中 $c\in\mathbb{F}_q$, 即存在非零多项式 $g(x_1,x_2,\ldots,x_n)$ 使得

$$f(x_1,x_2,\ldots,x_n)=(x_1-c)g(x_1,x_2,\ldots,x_n).$$

由于 $g(x_1,x_2,\ldots,x_n)$ 的未定元个数不超过 n 且次数为 $d-1$, 由归纳假设 $N_q(g)\leq(d-1)q^{n-1}$, 又 x_1-c 在 $\mathbb{F}_q^n$ 中的解数为 q^{n-1} ($x_1=c$, $x_2,\ldots,x_n$ 任取), 所以 $N_q(f)=q^{n-1}+N_q(g)\leq dq^{n-1}$.

(ii) 对每个 $c\in\mathbb{F}_q$, $f(x_1,x_2,\ldots,x_n)$ 都不能被多项式 x_1-c 整除, 从而 $f(c,x_2,\ldots,x_n)$ 是 $n-1$ 元非零多项式且次数至多为 d, 由归纳假设, $f(c,x_2,\ldots,x_n)$ 在 $\mathbb{F}_q^n$ 中的解的个数 $\leq dq^{n-2}$. 因为 c 有 q 种取法, 所以 $N_q(f)\leq q\cdot dq^{n-2}=dq^{n-1}$.

综合上面两种情形, 我们得到结论对 n 元 d 次非零多项式成立. 由归纳法原理, 结论对任意 $n\geq 1$ 和 $d\geq 0$ 成立. □

注意到 $\mathbb{F}_q^n$ 中共有 q^n 个元素, 所以定理 7.7 只有在 $d\leq q$ 时才有意义. 当 $d\leq q$ 时, 定理 7.7 中的上界是可以达到的. 例如任取 $\mathbb{F}_q$ 中 d 个互不相同的元素 $c_1,c_2,\ldots,c_d$, 令 $f(x_1,x_2,\ldots,x_n)=(x_1-c_1)(x_1-c_2)\cdots(x_1-c_d)$, 则有 $\deg(f)=d$. 若 $f(x_1,x_2,\ldots,x_n)=0$, 则 $x_1=c_1$, $c_2,\ldots,$ 或者 c_d, 即 x_1 有 d 种取法, 而 $x_2,\ldots,x_n$ 可任取, 所以 $N_q(f)=dq^{n-1}$.

多项式 $f(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q[x_1,x_2,\ldots,x_n]$ 称为是齐次的如果它的每一项的次数都相同, 所以次数大于 0 的齐次多项式一定有零解, 下面我们考察齐次多项式的非零解的个数.

定理 7.8: 设 $f(x_1,x_2,\ldots,x_n)$ 为 $\mathbb{F}_q$ 上的齐次多项式且 $\deg(f)=d\geq 1$, 则 $f(x_1,x_2,\ldots,x_n)$ 在 $\mathbb{F}_q^n$ 中有至多 $d(q^{n-1}-1)$ 个非零解.

证明: 若 $n=1$, 则 $f(x)=ax^d$, 这时 $f(x)$ 无非零解, 结论成立. 若 $d=1$, 则 $f(x_1,x_2,\ldots,x_n)=a_1x_1+a_2x_2+\cdots+a_nx_n$, 其中 $a_1,a_2,\ldots,a_n$ 不全为零, 所以 $f(x_1,x_2,\ldots,x_n)$ 在 $\mathbb{F}_q^n$ 中非零解的个数为 $q^{n-1}-1$, 结论成立.

下面我们对 d 和 n 做双重归纳. 设 $n>1$ 且 $d>1$, 假设结论对未定元个数不超过 n 且次

数小于 d 的非常数齐次多项式以及未定元个数至多为 $n-1$ 且次数不超过 d 的非常数齐次多项式成立, 我们来看 n 元 d 次非常数齐次多项式的情形. 设 $f(x_1,x_2,\dots,x_n)$ 为 $\mathbb{F}_q$ 上的一个 n 元 d 次齐次多项式, 分下面两种情形来证明.

(i) $f(x_1,x_2,\dots,x_n)$ 被 x_1 整除, 即存在非常数齐次多项式 $g(x_1,x_2,\dots,x_n)$ 使得

$$f(x_1,x_2,\dots,x_n)=x_1g(x_1,x_2,\dots,x_n).$$

由于 $g(x_1,x_2,\dots,x_n)$ 的未定元个数不超过 n 且次数为 $d-1$, 由归纳假设 $g(x_1,x_2,\dots,x_n)$ 的非零解个数 $\leq (d-1)(q^{n-1}-1)$, 而多项式 x_1 在 $\mathbb{F}_q^n$ 中的非零解显然为 $(0,c_2,\dots,c_n)$, 其中 $c_2,\dots,c_n\in\mathbb{F}_q$ 且不全为零, 故 x_1 在 $\mathbb{F}_q^n$ 中的非零解个数为 $q^{n-1}-1$, 所以 $f(x_1,x_2,\dots,x_n)$ 在 $\mathbb{F}_q^n$ 中的非零解个数 $\leq (q^{n-1}-1)+(d-1)(q^{n-1}-1)=d(q^{n-1}-1)$.

(ii) $f(x_1,x_2,\dots,x_n)$ 不能被 x_1 整除, 从而 $f(x_1,x_2,\dots,x_n)$ 的某些系数非零的项中不出现未定元 x_1. 所以对每个 $c\in\mathbb{F}_q^*$, $f(c,x_2,\dots,x_n)$ 是一个 $n-1$ 元 d 次多项式, 由定理 7.7, $f(c,x_2,\dots,x_n)$ 在 $\mathbb{F}_q$ 上解的个数 $\leq dq^{n-2}$. 故 $f(x_1,x_2,\dots,x_n)$ 在 $\mathbb{F}_q$ 上有至多 $d(q-1)q^{n-2}$ 个非零解 $(c_1,c_2,\dots,c_n)$ 满足 $c_1\neq 0$. 进一步地, $f(0,x_2,\dots,x_n)$ 是一个未定元个数小于 n 的 d 次齐次多项式, 由归纳假设, $f(0,x_2,\dots,x_n)$ 在 $\mathbb{F}_q$ 上有至多 $d(q^{n-2}-1)$ 个非零解, 即 $f(x_1,x_2,\dots,x_n)$ 在 $\mathbb{F}_q$ 上有至多 $d(q^{n-2}-1)$ 个非零解 $(c_1,c_2,\dots,c_n)$ 满足 $c_1=0$. 合起来我们就得到 $f(x_1,x_2,\dots,x_n)$ 在 $\mathbb{F}_q$ 上的非零解个数 $\leq d(q-1)q^{n-2}+d(q^{n-2}-1)=d(q^{n-1}-1)$.

综合上面两种情形, 我们得到结论对 n 元 d 次非零多项式成立. 由归纳法原理, 结论对任意 $n\geq 1$ 和 $d\geq 1$ 成立. □

下面我们整体上来讨论 n 元多项式解数, 即讨论解数的平均值 (期望) 以及与平均值的平均偏差 (方差) 问题. 设 d 为正整数, 用 $\Omega_{d,n}(q)$ 来表示 $\mathbb{F}_q$ 上所有次数不超过 d 的 n 元多项式构成的集合 (显然 $\Omega_{d,n}(q)$ 是 $\mathbb{F}_q$ 上的一个线性空间), 这样的多项式的每一项形如 $a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$, 其中 $a_{i_1i_2\cdots i_n}\in\mathbb{F}_q$, $i_1,i_2,\dots,i_n$ 为非负整数且 $i_1+i_2+\cdots+i_n\leq d$. 用 $\omega_n(d)$ 表示这样的有序数组 $(i_1,i_2,\dots,i_n)$ 的个数, 即

$$\omega_n(d)=\sharp\{(i_1,i_2,\dots,i_n)\mid i_1,i_2,\dots,i_n \text{ 为非负整数且 } i_1+i_2+\cdots+i_n\leq d\},$$

自然我们可以具体求出 $\omega_n(d)=\sum_{j=0}^{d}\binom{n+j-1}{n-1}=\binom{n+d}{n}$, 但是下面我们并不需要它的具体值. 注意到显然有 $|\Omega_{d,n}(q)|=q^{\omega_n(d)}$, 下面我们依然用 $N_q(f)$ 表示 $\mathbb{F}_q$ 上的多项式 $f(x_1,x_2,\dots,x_n)$ 在 $\mathbb{F}_q^n$ 中的解数.

定理 7.9: 设 n 和 d 为正整数, 则次数不超过 d 的 $\mathbb{F}_q$ 上 n 元多项式在 $\mathbb{F}_q^n$ 中的解数平均值为 q^{n-1}, 而解数与平均值的平均偏差为 $q^{n-1}-q^{n-2}$, 即我们有

$$\frac{1}{|\Omega_{d,n}(q)|}\sum_{f(x_1,x_2,\dots,x_n)\in\Omega_{d,n}(q)}N_q(f)=q^{n-1} \tag{7.3}$$

和

$$\frac{1}{|\Omega_{d,n}(q)|}\sum_{f(x_1,x_2,\dots,x_n)\in\Omega_{d,n}(q)}\big(N_q(f)-q^{n-1}\big)^2=q^{n-1}-q^{n-2}. \tag{7.4}$$

证明: 对于 $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$, 记 $\mathbf{c} = (c_1, c_2, \ldots, c_n)$, 我们有

$$\sum_{f\in\Omega_{d,n}(q)} N_q(f) = \sum_{f\in\Omega_{d,n}(q)} \sum_{\mathbf{c}\in\mathbb{F}_q^n,\, f(\mathbf{c})=0} 1 = \sum_{\mathbf{c}\in\mathbb{F}_q^n} \sum_{f\in\Omega_{d,n}(q),\, f(\mathbf{c})=0} 1.$$

对于给定的 $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$, 满足 $f(\mathbf{c}) = 0$ 的 $f \in \Omega_{d,n}(q)$ 的个数为 $q^{\omega_n(d)-1}$. 事实上, 若

$$f(x_1, x_2, \ldots, x_n) = \sum a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \in \Omega_{d,n}(q) \tag{7.5}$$

满足 $f(\mathbf{c}) = 0$, 则代入 $x_1 = c_1, x_2 = c_2, \ldots, x_n = c_n$ 到 (7.5), 式 (7.5) 成为一个以系数 $a_{i_1 i_2 \cdots i_n}$ 为未知量的齐次线性方程, 此线性方程有 $\omega_n(d)$ 个未知量且 $a_{00\cdots0}$ 的系数为 1, 故此方程在 $\mathbb{F}_q$ 上有 $q^{\omega_n(d)-1}$ 个解. 所以我们有

$$\sum_{f\in\Omega_{d,n}(q)} N_q(f) = \sum_{\mathbf{c}\in\mathbb{F}_q^n} \sum_{f\in\Omega_{d,n}(q),\, f(\mathbf{c})=0} 1 = \sum_{\mathbf{c}\in\mathbb{F}_q^n} q^{\omega_n(d)-1} = q^n q^{\omega_n(d)-1} = |\Omega_{d,n}(q)| q^{n-1},$$

由此给出 (7.3) 的证明. 进一步地,

$$\begin{aligned}
\sum_{f\in\Omega_{d,n}(q)} N_q(f)^2 &= \sum_{f\in\Omega_{d,n}(q)} \left(\sum_{\mathbf{c}\in\mathbb{F}_q^n,\, f(\mathbf{c})=0} 1 \right)^2 \\
&= \sum_{f\in\Omega_{d,n}(q)} \sum_{\mathbf{b}\in\mathbb{F}_q^n,\, f(\mathbf{b})=0} \sum_{\mathbf{c}\in\mathbb{F}_q^n,\, f(\mathbf{c})=0} 1 \\
&= \sum_{\mathbf{b},\mathbf{c}\in\mathbb{F}_q^n} \sum_{f\in\Omega_{d,n}(q),\, f(\mathbf{b})=f(\mathbf{c})=0} 1.
\end{aligned}$$

类似地, 我们容易证明对于任意 $\mathbf{b}, \mathbf{c} \in \mathbb{F}_q^n$, 满若 $f(\mathbf{b}) = f(\mathbf{c}) = 0$ 的 $f \in \Omega_{d,n}(q)$ 的个数为

$$\begin{cases} q^{\omega_n(d)-1}, & \text{若 } \mathbf{b} = \mathbf{c}, \\ q^{\omega_n(d)-2}, & \text{若 } \mathbf{b} \neq \mathbf{c}. \end{cases}$$

所以

$$\sum_{f\in\Omega_{d,n}(q)} N_q(f)^2 = q^n q^{\omega_n(d)-1} + q^n(q^n - 1) q^{\omega_n(d)-2} = |\Omega_{d,n}(q)|(q^{2n-2} + q^{n-1} - q^{n-2}),$$

再利用 (7.3) 得

$$\begin{aligned}
\sum_{f\in\Omega_{d,n}(q)} (N_q(f) - q^{n-1})^2 &= \sum_{f\in\Omega_{d,n}(q)} N_q(f)^2 - 2q^{n-1} \sum_{f\in\Omega_{d,n}(q)} N_q(f) + q^{2n-2} \sum_{f\in\Omega_{d,n}(q)} 1 \\
&= |\Omega_{d,n}(q)|((q^{2n-2} + q^{n-1} - q^{n-2}) - 2q^{n-1}q^{n-1} + q^{2n-2}) \\
&= |\Omega_{d,n}(q)|(q^{n-1} - q^{n-2}),
\end{aligned}$$

由此证明了等式 (7.4). □

注意到定理 7.9 告诉我们 $(N_q(f) - q^{n-1})^2$ 的平均值为 $q^{n-1} - q^{n-2}$, 所以有理由预计 $|N_q(f) - q^{n-1}|$ 的数量级为 $q^{(n-1)/2}$, 这在很多情形下是正确的.

上面给出一个多项式在有限域上解的个数的一些上下界, 下面我们讨论一组多项式的公共解 (即一个多项式方程组的解) 的个数. 设 $f_1(x_1, x_2, \ldots, x_n)$, $f_2(x_1, x_2, \ldots, x_n)$,

$\ldots, f_m(x_1, x_2, \ldots, x_n)$ 是 $\mathbb{F}_q$ 上的多项式, 所谓 $f_1, f_2, \ldots, f_m$ 在 $\mathbb{F}_q$ 上的公共解即有序数组 $(c_1, c_2, \ldots, c_m) \in \mathbb{F}_q^n$ 满足对所有 $1 \leq i \leq m$, 都有 $f_i(c_1, c_2, \ldots, c_n) = 0$. 用 $N_q(f_1, f_2, \ldots, f_m)$ 表示多项式 $f_1, f_2, \ldots, f_m$ 在 $\mathbb{F}_q$ 上的公共解的个数.

若 $\sum_{i=1}^m \deg(f_i) < n$, 令多项式

$$F(x_1, x_2, \ldots, x_n) = (1 - f_1(x_1, \ldots, x_n)^{q-1})(1 - f_2(x_1, \ldots, x_n)^{q-1}) \cdots (1 - f_m(x_1, \ldots, x_n)^{q-1}),$$

则 $\deg(F) = (q-1)\sum_{i=1}^m \deg(f_i) < n(q-1)$. 所以 $F(x_1, x_2, \ldots, x_n)$ 的每一项 $a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ 中一定有一个 j 满足 $0 \leq i_j < q-1$, 从而类似于定理 7.6 的证明, 我们有

$$\sum_{(c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n} F(c_1, c_2, \ldots, c_n) = 0.$$

又 $F(x_1, x_2, \ldots, x_n)$ 在 $f_1, f_2, \ldots, f_m$ 的公共解上取值为 1, 而在 $\mathbb{F}_q^n$ 的其它元素处取值为 0, 从而

$$\sum_{(c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n} F(c_1, c_2, \ldots, c_n) = N_q(f_1, f_2, \ldots, f_m) \cdot 1.$$

这便得到 $p \mid N_q(f_1, f_2, \ldots, f_m)$, 其中 $p = \mathrm{char}\mathbb{F}_q$.

定理 7.10: 设 $p = \mathrm{char}\mathbb{F}_q$, $f_1, f_2, \ldots, f_m \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ 且 $\sum_{i=1}^m \deg(f_i) < n$, 则 $p \mid N_q(f_1, f_2, \ldots, f_m)$. □

推论 7.11: 设 $f_1, f_2, \ldots, f_m \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$, 每个多项式 f_i 的常数项均为 0, $1 \leq i \leq m$, 且满足 $\sum_{i=1}^m \deg(f_i) < n$, 则 $f_1, f_2, \ldots, f_m$ 在 $\mathbb{F}_q$ 上有非零公共解. □

设 $d = \sum_{i=1}^m \deg(f_i)$, 若 $d < n$, 定理 7.10 告诉我们 $N_q(f_1, f_2, \ldots, f_m)$ 可被域 $\mathbb{F}_q$ 的特征整除. 下面我们可以进一步地证明若 $N_q(f_1, f_2, \ldots, f_m) > 0$, 则有 $N_q(f_1, f_2, \ldots, f_m) \geq q^{n-d}$, 这需要一些更精细的讨论以及有限域上仿射几何中的一些计数.

$\mathbb{F}_q^n$ 是 $\mathbb{F}_q$ 上的 n 维线性空间, 它的 k-维子空间的基是 $\mathbb{F}_q^n$ 中 k 个线性无关的向量组成的向量组, 显然 $\mathbb{F}_q^n$ 中 k 个线性无关的有序向量组成的向量组的个数是 $(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})$, 而每个 k-维子空间中 k 个线性无关的有序向量组成的向量组的个数是 $(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})$, 所以 $\mathbb{F}_q^n$ 的 k-维子空间的个数为

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} = \prod_{i=0}^{k-1} \frac{q^n-q^i}{q^k-q^i},$$

记如上这个式子为 $\begin{bmatrix} n \\ k \end{bmatrix}_q$, 称其为 Gauss 系数, 它有着与二项式系数 $\binom{n}{k}$ 类似的性质. 设 U 是 $\mathbb{F}_q^n$ 的一个 k-维子空间, U 的一个陪集 (或平移) $\alpha + U = \{\alpha + \gamma \mid \gamma \in U\}$ 称为一个 k-维仿射线性集. 注意到 $\mathbb{F}_q^n$ 的 k-维子空间的个数为 $\begin{bmatrix} n \\ k \end{bmatrix}_q$, 而对于一个固定的 k-维子空间 U, $\alpha + U = \beta + U$ 当且仅当 $\alpha - \beta \in U$. 由于 U 中有 q^k 个元素, 所以由 U 出发构造出的 k-维仿射线性集有 q^{n-k} 个, 又由不同的 k-维子空间出发构造出的 k-维仿射线性集显然彼此不同, 从而 $\mathbb{F}_q^n$ 的 k-维仿射线性集的个数为 $q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}_q$. $\mathbb{F}_q^n$ 的两个仿射线性集称为是平行的, 如果它们是同一个线性子空间的平移. 一般地, $\mathbb{F}_q^n$ 的 0-维仿射线性集 (即一个向量) 称为仿射点, 1-维仿射线性集称为仿射直

线, 2-维仿射线性集称为仿射平面, $(n-1)$-维仿射线性集称为仿射超平面, 而 n-维仿射线性集就是 $\mathbb{F}_q^n$ 本身. $\mathbb{F}_q^n$ 及其所有的仿射线性集在集合包含关系下得到的结构称为 $\mathbb{F}_q$ 上的 n-维仿射几何.

设 W 是 $\mathbb{F}_q^n$ 的一个给定的 t-维子空间, 则 $\mathbb{F}_q^n$ 的包含 W 的 k-维子空间集合与商空间 $\mathbb{F}_q^n/W$ 的所有 $(k-t)$-维子空间集合之间有一个一一对应 (类似于群的第一同构定理), 所以 $\mathbb{F}_q^n$ 的包含 W 的 k-维子空间个数为 $\begin{bmatrix} n-t \\ k-t \end{bmatrix}_q$. 进一步地, 设 $\alpha+W$ 是 $\mathbb{F}_q^n$ 的一个给定的 t-维仿射线性集, 若 $\beta+U$ 是包含 $\alpha+W$ 的一个 k-维仿射线性集, 即 $\alpha+W\subseteq\beta+U$, 则 $\alpha\in\beta+U$, 从而 $\beta+U=\alpha+U$. 再由 $\alpha+W\subseteq\alpha+U$ 得知 $W\subseteq U$, 即 U 为包含 t-维子空间 W 的 k-维子空间. 反之, 对任意包含 W 的 k-维子空间 U, 一定有 $\alpha+W\subseteq\alpha+U$, 从而 $\mathbb{F}_q^n$ 的包含 $\alpha+W$ 的 k-维仿射线性集的个数即 $\mathbb{F}_q^n$ 的包含 W 的 k-维子空间的个数, 依然为 $\begin{bmatrix} n-t \\ k-t \end{bmatrix}_q$.

下面我们把 $\mathbb{F}_q^n$ 中的元素都看成是列向量的形式. 由线性代数得知, $\mathbb{F}_q^n$ 的每个 k-维子空间都是 $\mathbb{F}_q$ 上一个齐次线性方程组的解空间, 即对于 $\mathbb{F}_q^n$ 的任意 k-维子空间 U, 存在 $\mathbb{F}_q$ 上的秩为 $n-k$ 的 $(n-k)\times n$ 矩阵 A, 使得齐次线性方程组 $AX=0$ 的解空间恰为 U. 进一步地, 任给 $\mathbb{F}_q^n$ 的一个给定的 k-维仿射线性集 $\alpha+U$, 设 U 为齐次线性方程组 $AX=0$ 的解空间, 令 $A\alpha=\beta\in\mathbb{F}_q^{n-k}$, 则 $\alpha+U$ 就是线性方程组 $AX=\beta$ 的解集.

下面我们继续讨论多项式解的问题, 设 $f_i(x_1,x_2,\ldots,x_n)$, $1\le i\le m$, 是 $\mathbb{F}_q$ 上的 n 元多项式, 用 V 表示 $f_1,f_2,\ldots,f_m$ 在 $\mathbb{F}_q$ 上的公共解构成的集合, 所以 $V\subseteq\mathbb{F}_q^n$ 且 $N_q(f_1,f_2,\ldots,f_m)=|V|$. 对于 $\mathbb{F}_q$ 上的一个 n 阶可逆矩阵 M, $\alpha\mapsto M\alpha$ 是 $\mathbb{F}_q^n$ 上的可逆线性变换. 做未定元的可逆线性替换 $(y_1,y_2,\cdots,y_n)^T=M(x_1,x_2,\cdots,x_n)^T$, 或者 $(x_1,x_2,\cdots,x_n)^T=M^{-1}(y_1,y_2,\cdots,y_n)^T$, 则对每个 $1\le i\le m$, 多项式 $f_i(x_1,x_2,\ldots,x_n)$ 可以变为多项式 $F_i(y_1,y_2,\ldots,y_n)$. 我们有 $\deg(F_i)=\deg(f_i)$ (为什么? 请给出理由), 且对于 $(c_1,c_2,\ldots,c_n)^T\in V$, 令 $(b_1,b_2,\cdots,b_n)^T=M(c_1,c_2,\cdots,c_n)^T$, 则有 $F_i(b_1,b_2,\ldots,b_n)=0$, 即 $(b_1,b_2,\ldots,b_n)^T$ 为 $F_1,F_2,\ldots,F_m$ 在 $\mathbb{F}_q$ 上的公共解. 由 M 的可逆性知上面的推导可以反推, 由此得到 $N_q(F_1,F_2,\ldots,F_m)=N_q(f_1,f_2,\ldots,f_m)$.

引理 7.12: 设 $p=\mathrm{char}\mathbb{F}_q$, $f_1,f_2,\ldots,f_m\in\mathbb{F}_q[x_1,x_2,\ldots,x_n]$ 且 $d=\sum_{i=1}^m\deg(f_i)<n$, 设 V 为 $f_1,f_2,\ldots,f_m$ 在 $\mathbb{F}_q$ 上的公共解构成的集合, 则对 $\mathbb{F}_q^n$ 的任意两个平行的 d-维仿射线性集 W_1 和 W_2, 有 $|W_1\cap V|\equiv|W_2\cap V|\pmod p$.

证明: 若 $W_1=W_2$, 则结论是平凡的, 下面假设 $W_1\ne W_2$, 同时不失一般性我们可以假设 W_1 是一个 d-维线性子空间 (即零向量为陪集代表元), 则 W_2 就是 W_1 的一个平移. 我们知道 W_1 是齐次线性方程组 $AX=0$ 的解空间, 其中 A 为 $\mathbb{F}_q$ 上的一个秩为 $n-d$ 的 $(n-d)\times n$ 矩阵, 而 W_2 就是线性方程组 $AX=\beta$ 的解集, 其中 $\beta\in\mathbb{F}_q^{n-d}$ 且 $\beta\ne0$. 以矩阵 A 为基础再添加一个 $d\times n$ 矩阵 $\overline{A}$ 可得到 $\mathbb{F}_q$ 上的一个 n 阶可逆矩阵 $M_1=\begin{pmatrix} A \\ \overline{A} \end{pmatrix}$. 由于 $\beta\ne0$, 存在 $\mathbb{F}_q$ 上的一个秩为 $n-d$ 的 $(n-d)\times n$ 矩阵 B 使得 $B\beta=(1,0,\ldots,0)^T\in\mathbb{F}_q^{n-d}$, 同样在 B 的基础上添加 d 行可得到 $\mathbb{F}_q$ 上的一个 n 阶可逆矩阵 M_2. 令 $M=M_2M_1$, 做未定元的可逆线性替

换 $(y_1, y_2, \cdots, y_n)^T = M(x_1, x_2, \cdots, x_n)^T$, 在此可逆线性替换下, 设 W_1 变成 W_1', W_2 变成 W_2', 且对每个 $1 \le i \le m$, $f_i(x_1, x_2, \ldots, x_n)$ 变成 $F_i(y_1, y_2, \ldots, y_n)$, 用 V' 表示 $F_1, F_2, \ldots, F_m$ 在 $\mathbb{F}_q$ 上的公共解构成的集合, 则对 $(y_1, y_2, \cdots, y_n) \in W_1'$ 有 $(y_1, y_2, \ldots, y_{n-d}) = (0, 0, \ldots, 0)$, 而对 $(y_1, y_2, \cdots, y_n) \in W_2'$ 有 $(y_1, y_2, \ldots, y_{n-d}) = (1, 0, \ldots, 0)$, 类似于上面的讨论还有 $\deg(F_i) = \deg(f_i)$, $1 \le i \le m$, 且 $|W_1' \cap V'| = |W_1 \cap V|$, $|W_2' \cap V'| = |W_2 \cap V|$, 所以不失一般性我们可以假设

$$\begin{aligned} W_1 &= \{(c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n \mid c_1 = c_2 = \cdots = c_{n-d} = 0\}, \\ W_2 &= \{(c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n \mid c_1 = 1,\ c_2 = \cdots = c_{n-d} = 0\}. \end{aligned}$$

定义多项式 $G(x_1, x_2, \ldots, x_n) = -(1 + x_1 + \cdots + x_1^{q-2})(1 - x_2^{q-1}) \cdots (1 - x_{n-d}^{q-1})$, 则 $G(x_1, x_2, \ldots, x_n)$ 的次数为 $(q-2) + (n-d-1)(q-1) = (n-d)(q-1) - 1$ 且在 W_1 上的取值为 -1, 在 W_2 上的取值为 1, 而在 $\mathbb{F}_q^n$ 中的其它元素上的取值为 0. 令

$$H(x_1, x_2, \ldots, x_n) = G(x_1, x_2, \ldots, x_n)(1 - f_1^{q-1})(1 - f_2^{q-1}) \cdots (1 - f_m^{q-1}),$$

由于 $V = \{(c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n \mid f_i(c_1, c_2, \ldots, c_n) = 0,\ 1 \le i \le m\}$, 所以 $H(x_1, x_2, \ldots, x_n)$ 在 $W_1 \cap V$ 上的取值为 -1, 在 $W_2 \cap V$ 上的取值为 1, 而在 $\mathbb{F}_q^n$ 中的其它元素上的取值为 0, 所以

$$\sum_{c_1, c_2, \ldots, c_n \in \mathbb{F}_q} H(c_1, c_2, \ldots, c_n) = (|W_2 \cap V| - |W_1 \cap V|) \cdot 1.$$

由于

$$\deg(H) = \deg(G) + (q-1)\sum_{i=1}^{m} \deg(f_i) = (n-d)(q-1) - 1 + d(q-1) = n(q-1) - 1 < n(q-1),$$

类似于前面的讨论我们有

$$\sum_{c_1, c_2, \ldots, c_n \in \mathbb{F}_q} H(c_1, c_2, \ldots, c_n) = 0,$$

从而 $p \mid (|W_2 \cap V| - |W_1 \cap V|)$, 即 $|W_1 \cap V| \equiv |W_2 \cap V| \pmod{p}$. □

定理 7.13: 设 $f_1, f_2, \ldots, f_m \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ 且 $d = \sum_{i=1}^{m} \deg(f_i) < n$, 若 $N_q(f_1, f_2, \ldots, f_m) > 0$, 则 $N_q(f_1, f_2, \ldots, f_m) \ge q^{n-d}$.

证明: 我们依然设 $p = \mathrm{char}\mathbb{F}_q$ 且 V 为 $f_1, f_2, \ldots, f_m$ 在 $\mathbb{F}_q$ 上的公共解构成的集合. 若存在 $\mathbb{F}_q^n$ 的一个 d-维仿射线性集 W_1 使得 $|W_1 \cap V| \not\equiv 0 \pmod{p}$, 则由引理 7.12 知对每个与 W_1 平行的 d-维仿射线性集 W_2 有 $|W_2 \cap V| \not\equiv 0 \pmod{p}$, 从而 $|W_2 \cap V| \ge 1$. 由于与 W_1 平行的 d-维仿射线性集有 q^{n-d} 个, 而这些平行的 d-维仿射线性集是 $\mathbb{F}_q^n$ 的一个划分, 所以

$$N_q(f_1, f_2, \ldots, f_m) = |V| = \sum_{W} |W \cap V| \ge q^{n-d},$$

其中和式下标 W 跑遍所有与 W_1 平行的 d-维仿射线性集 (当然包括 W_1).

下面设对 $\mathbb{F}_q^n$ 的所有 d-维仿射线性集 W 均有 $|W \cap V| \equiv 0 \pmod{p}$. 由于 V 非空, 所以一定存在正整数 k 满足 $1 \le k \le d$ 且使得对 $\mathbb{F}_q^n$ 的所有 k-维仿射线性集 U 均有 $|U \cap V| \equiv 0 \pmod{p}$ 但是存在一个 $(k-1)$-维仿射线性集 S 使得 $|S \cap V| \not\equiv 0 \pmod{p}$. 考虑所有包含 S 的 k-维仿射

线性集 T, 这样的 k- 维仿射线性集有 $\begin{bmatrix} n \\ k \end{bmatrix}_q - \begin{bmatrix} k \\ 1 \end{bmatrix}_q = \begin{bmatrix} n \\ 1 \end{bmatrix}_q - \begin{bmatrix} k \\ 1 \end{bmatrix}_q$ 个且其中任意两个的交为 S. 事实上, 对任意两个包含 S 的 k-维仿射线性集 T_1 和 T_2, 记 $S = \delta + P$, 其中 P 为一个 $(k-1)$-维子空间, 由 $T_1, T_2 \supseteq S$ 得到存在两个 k-维子空间 Q_1 和 Q_2 使得 $T_1 = \delta + Q_1$, $T_2 = \delta + Q_2$ 且 $Q_1, Q_2 \supseteq P$. 由于 $Q_1 \cap Q_2 \supseteq P$, $Q_1 \neq Q_2$ 且维数均为 k, 所以 $Q_1 \cap Q_2$ 的维数小于 k, 故 $Q_1 \cap Q_2 = P$, 从而 $T_1 \cap T_2 = \alpha + (Q_1 \cap Q_2) = \alpha + P = S$. 对每一个包含 S 的 k-维仿射线性集 T, 设 $T \backslash S$ 为集合的差, 即 $T \backslash S = \{\gamma \in T \mid \gamma \notin S\}$, 由于

$$|(T \backslash S) \cap V| = |T \cap V| - |S \cap V| \equiv -|S \cap V| \not\equiv 0 \,(\mathrm{mod}\ p),$$

所以 $|(T \backslash S) \cap V| \geq 1$. 注意到 S 和所有这些 $T \backslash S$ 构成了 $\mathbb{F}_q^n$ 的一个划分, 所以

$$N_q(f_1, f_2, \ldots, f_m) = |V| = |S \cap V| + \sum_T |(T \backslash S) \cap V| \geq 1 + \frac{q^{n-k+1} - 1}{q - 1} > q^{n-k} \geq q^{n-d},$$

其中和式下标 V 跑遍所有包含 S 的 k-维仿射线性集. □

当然如上结论对单个多项式也成立, 所以我们有如下推论.

推论 7.14: 设 $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ 满足 $d = \deg(f) < n$ 且 $f(x_1, x_2, \ldots, x_n)$ 在 $\mathbb{F}_q$ 上有解, 则 $N_q(f) \geq q^{n-d}$. □

类似于例 7.4 (a), 设 n 和 d 为正整数且 $d < n$, $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ 是 $\mathbb{F}_{q^d}$ 在 $\mathbb{F}_q$ 上的一组基, 令

$$f(x_1, x_2, \ldots, x_n) = \prod_{j=0}^{d-1} (\alpha_1^{q^j} x_1 + \alpha_2^{q^j} x_2 + \cdots + \alpha_d^{q^j} x_d).$$

则容易验证 $f(x_1, x_2, \ldots, x_n)$ 依然是 $\mathbb{F}_q$ 上的多项式且 $(c_1, c_2, \ldots, c_n)$ 为 $f(x_1, x_2, \ldots, x_n)$ 在 $\mathbb{F}_q$ 上的解当且仅当 $c_1 = \cdots = c_d = 0$. 由于 $c_{d+1}, \ldots, c_n$ 可以在 $\mathbb{F}_q$ 中任意选取, 所以多项式 $f(x_1, x_2, \ldots, x_n)$ 在 $\mathbb{F}_q$ 上恰有 q^{n-d} 个解, 这表明推论 7.14 中的下界可以达到.

设 $f(x_1, x_2, \ldots, x_n)$ 为 $\mathbb{F}_q$ 上的 d 次齐次多项式且 $1 \leq d < n$, 由于 $f(x_1, x_2, \ldots, x_n)$ 有零解, 所以一定有 $N_q(f) \geq q^{n-d}$, 再加上定理 7.8, 我们有如下定理.

定理 7.15: 设 $f(x_1, x_2, \ldots, x_n)$ 为 $\mathbb{F}_q$ 上的 d 次齐次多项式且 $1 \leq d < n$, 则 $q^{n-d} \leq N_q(f) \leq d(q^{n-1} - 1) + 1$. □

本节的最后我们给出一族多项式的公共解的个数可以由单个多项式的解数表示. 设 $f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$, 定义 $\mathbb{F}_q$ 上的 $n+m$ 元多项式 $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ 为

$$F(x_1, \ldots, x_n, y_1, \ldots, y_m) = f_1(x_1, \ldots, x_n) y_1 + f_2(x_1, \ldots, x_n) y_2 + \cdots + f_m(x_1, \ldots, x_n) y_m.$$

对每个 $(c_1, \ldots, c_n) \in V$, $d_1, \ldots, d_m$ 在 $\mathbb{F}_q$ 中任取可得 $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ 在 $\mathbb{F}_q$ 上的 q^m 个解 $(c_1, \ldots, c_n, d_1, \ldots, d_m)$. 对任意 $(c_1, \ldots, c_n) \notin V$, 必有某个 j, $1 \leq j \leq m$, 使得 $f_j(c_1, \ldots, c_n) \neq 0$, 所以 $d_1, \ldots, d_{j-1}, d_{j+1}, \ldots, d_m$ 在 $\mathbb{F}_q$ 中任取且令

$$d_j = -f_j(c_1, \ldots, c_n)^{-1} \sum_{k \neq j} f_k(c_1, \ldots, c_n) d_k$$

可得 $F(x_1,\ldots,x_n,y_1,\ldots,y_m)$ 在 $\mathbb{F}_q$ 上的 q^{m-1} 个解 $(c_1,\ldots,c_n,d_1,\ldots,d_m)$. 所以

$$N_q(F)=N_q(f_1,f_2,\ldots,f_m)\cdot q^m+(q^n-N_q(f_1,f_2,\ldots,f_m))\cdot q^{m-1},$$

由此可推出

$$N_q(f_1,f_2,\ldots,f_m)=\frac{1}{q^m-q^{m-1}}(N_q(F)-q^{n+m-1}).$$

7.3 求根算法

给定多项式 $f(x)\in\mathbb{F}_q[x]$, 本节我们讨论如何求 $f(x)$ 在 $\mathbb{F}_q$ 中的根. 先看最简单的情形, 即 $\deg f(x)=2$ 的情形. 我们已经在第 3 章的 3.1 节给出了特征为 2 的域上的 2 次多项式的求根方法, 所以本节我们首先来讨论特征为奇素数的域上的 2 次多项式的求根问题.

设 q 为奇素数幂, $f(x)=Ax^2+Bx+C$, 其中 $A,B,C\in\mathbb{F}_q$ 且 $A\neq 0$. 对 $f(x)$ 做配方可得 $f(x)=A\left((x+\frac{B}{2A})^2-\frac{B^2-4AC}{4A^2}\right)$, 故我们只需讨论首一且一次项系数为 0 的二次多项式 x^2-a, 其中 $a\in\mathbb{F}_q$. 显然多项式 x^2-a 在 $\mathbb{F}_q$ 中有根当且仅当存在 $b\in\mathbb{F}_q$ 使得 $a=b^2$, 满足这个条件的元素 a 称为 $\mathbb{F}_q$ 中的平方元. 一般地, 我们容易得到 $\mathbb{F}_q$ 上的二次多项式 $f(x)=Ax^2+Bx+C$ 在 $\mathbb{F}_q$ 中有根当且仅当 B^2-4AC 为 $\mathbb{F}_q$ 中的平方元. 定义 $\Delta=B^2-4AC$ 并称其为多项式 $f(x)$ 的根的判别式, 从而 $\mathbb{F}_q$ 上的二次多项式在 $\mathbb{F}_q$ 中有根当且仅当其根的判别式为 $\mathbb{F}_q$ 中的平方元. 下面我们首先讨论一般有限域上平方元的问题.

设 q 为任意素数幂, 定义 $\mathbb{F}_q^2=\{a^2\mid a\in\mathbb{F}_q\}$ 和 $\mathbb{F}_q^{*2}=\{a^2\mid a\in\mathbb{F}_q^*\}$, $\mathbb{F}_q^2$ 中的元素称为 $\mathbb{F}_q$ 中的平方元, $\mathbb{F}_q^{*2}$ 中的元素称为 $\mathbb{F}_q$ 中的非零平方元, 显然 $\mathbb{F}_q^2=\mathbb{F}_q^{*2}\cup\{0\}$. 我们知道 $\mathbb{F}_q^*$ 为 $q-1$ 阶循环群, 对任意 $a,b\in\mathbb{F}_q^*$, 由于 $a^2(b^2)^{-1}=(ab^{-1})^2$, 所以 $\mathbb{F}_q^{*2}$ 是 $\mathbb{F}_q^*$ 的乘法子群. 设 α 是 $\mathbb{F}_q$ 的一个本原元素, 则容易验证 $\mathbb{F}_q^{*2}$ 是由 α^2 生成的子群, 由于 $\mathrm{ord}(\alpha^2)=\frac{q-1}{\gcd(2,q-1)}$, 我们得到子群 $\mathbb{F}_q^{*2}$ 的阶为 $\frac{q-1}{\gcd(2,q-1)}$. 特别地, 若 q 为 2 的方幂, 即 $\gcd(2,q-1)=1$, 这时我们有 $\mathbb{F}_q^{*2}=\mathbb{F}_q^{*2}$ 和 $\mathbb{F}_q^2=\mathbb{F}_q$, 所以特征为 2 的有限域中每个元素都是平方元. 实际上, 若 $q=2^m$, 则对任意 $a\in\mathbb{F}_q$, 我们有 $a=a^{2^m}=(a^{2^{m-1}})^2$. 若 q 为奇素数幂, 则 $\gcd(2,q-1)=2$, 故 $\mathbb{F}_q^{*2}$ 的阶为 $\frac{q-1}{2}$, 所以在特征为奇素数的有限域 $\mathbb{F}_q$ 中, 有 $\frac{q-1}{2}$ 个非零平方元, 也有 $\frac{q-1}{2}$ 个非平方元.

设 q 为奇素数幂, 如何判断 $\mathbb{F}_q^*$ 中的元素为非零平方元? 给定 $a\in\mathbb{F}_q^*$, 若 $a\in\mathbb{F}_q^{*2}$, 则存在 $b\in\mathbb{F}_q^*$ 使得 $a=b^2$, 故 $a^{\frac{q-1}{2}}=b^{q-1}=1$. 由于 $\mathbb{F}_q^{*2}$ 中的 $\frac{q-1}{2}$ 个元素都是多项式 $x^{\frac{q-1}{2}}-1$ 的根而多项式 $x^{\frac{q-1}{2}}-1$ 在 $\mathbb{F}_q$ 中的根至多有 $\frac{q-1}{2}$ 个, 从而 $\mathbb{F}_q^{*2}$ 中的元素就是多项式 $x^{\frac{q-1}{2}}-1$ 的所有根. 这样我们就证明了 a 为非零平方元当且仅当 a 是多项式 $x^{\frac{q-1}{2}}-1$ 的根, 也当且仅当 $a^{\frac{q-1}{2}}=1$. 对任意 $a\in\mathbb{F}_q^*$, 因为 $a^{q-1}=1$, 所以 $a^{\frac{q-1}{2}}=\pm 1$, 由此我们得到 a 为 $\mathbb{F}_q$ 中非平方元当且仅当 $a^{\frac{q-1}{2}}=-1$. 容易验证 -1 为 $\mathbb{F}_q$ 中的平方元当且仅当 $q\equiv 1\pmod 4$, 而 -1 为 $\mathbb{F}_q$ 中的非平方元当且仅当 $q\equiv 3\pmod 4$.

例 7.5: 设 q 为奇素数幂, 考察元素 $2\in\mathbb{F}_q$ 何时为平方元. 注意到由于 q 与 8 互素, 所以在 $\mathbb{F}_q$ 的某个扩域中存在 8 阶元素 γ, 即 $\gamma^8=1$. 由于 $\gamma^4=-1$, 即 $\gamma^4+1=0$, 两边同时乘以 γ^{-2} 得

$\gamma^2+\gamma^{-2}=0$, 从而 $2=(\gamma+\gamma^{-1})^2$.

由于 $(\gamma+\gamma^{-1})^q=\gamma^q+\gamma^{-q}$, 所以当 $q\equiv 1,7\,(\mathrm{mod}\ 8)$ 时, $(\gamma+\gamma^{-1})^q=\gamma+\gamma^{-1}$, 即 $(\gamma+\gamma^{-1})^{q-1}=1$. 类似地, 当 $q\equiv 3,5\,(\mathrm{mod}\ 8)$ 时, $(\gamma+\gamma^{-1})^q=-(\gamma+\gamma^{-1})$, 即 $(\gamma+\gamma^{-1})^{q-1}=-1$. 所以我们有

$$2^{\frac{q-1}{2}}=(\gamma+\gamma^{-1})^{q-1}=\begin{cases}1, & \text{若 } q\equiv 1,7\,(\mathrm{mod}\ 8),\\ -1, & \text{若 } q\equiv 3,5\,(\mathrm{mod}\ 8),\end{cases}$$

从而 2 为 $\mathbb{F}_q$ 中平方元当且仅当 $q\equiv 1,7\,(\mathrm{mod}\ 8)$, 而 2 为 $\mathbb{F}_q$ 中非平方元当且仅当 $q\equiv 3,5\,(\mathrm{mod}\ 8)$. □

若 $q=p$ 为奇素数, 则 $\mathbb{F}_p=\mathbb{Z}_p$, 即整数模素数 p 的剩余类环 (也是一个域), 其中的运算就是整数模 p 的运算, 这时关于域中平方元的讨论属于初等数论范围, 其中 $\mathbb{F}_p$ 中的平方元称为模 p 的二次剩余, 而 $\mathbb{F}_p$ 中的非平方元称为模 p 的二次非剩余. 上面的讨论告诉我们对于 $a\in\mathbb{F}_p^*$, a 为模 p 的二次剩余当且仅当 $a^{\frac{p-1}{2}}=1$, a 为模 p 的二次非剩余当且仅当 $a^{\frac{p-1}{2}}=-1$. 注意到直接计算 $a^{\frac{p-1}{2}}$ 需要很多乘法运算, 下面我们引进一个符号来帮助我们判断一个数是否为模 p 的二次剩余. 定义映射 $\left(\frac{\cdot}{p}\right)$ 如下:

$$\begin{array}{rcl}\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* & \to & \{1,-1\}\\ a & \mapsto & \left(\frac{a}{p}\right)=\begin{cases}1 & \text{若 } a \text{ 为模 } p \text{ 的二次剩余},\\ -1 & \text{否则}.\end{cases}\end{array}$$

映射 $\left(\frac{\cdot}{p}\right)$ 称为 Legendre 符号, 容易验证 Legendre 符号是一个群同态, 即保持群的乘法运算, 由定义我们还可以得到

$$\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}.$$

上面的 Legendre 符号可以自然地推广到对任意正整数 a 的情形, 若 $p\mid a$, 则定义 $\left(\frac{a}{p}\right)=0$, 对于 $p\nmid a$, 则定义 $\left(\frac{a}{p}\right)=\left(\frac{a\,(\mathrm{mod}\,p)}{p}\right)$. 著名的 Gauss 二次互反律告诉我们对任意两个不同的奇素数 p 和 r, 有

$$\left(\frac{r}{p}\right)\left(\frac{p}{r}\right)=(-1)^{\frac{(p-1)(r-1)}{4}},$$

这个结论可帮助我们来计算 Legendre 符号. 例如,

$$\left(\frac{3}{67}\right)=\left(\frac{67}{3}\right)(-1)^{33}=\left(\frac{67\ (\mathrm{mod}\ 3)}{3}\right)(-1)=\left(\frac{1}{3}\right)(-1)=-1,$$

所以 3 为模 67 的二次非剩余. 类似地, 我们可以得到 $\left(\frac{11}{67}\right)=-1$, 从而 $\left(\frac{33}{67}\right)=\left(\frac{3}{67}\right)\left(\frac{11}{67}\right)=(-1)(-1)=1$, 即 33 是模 67 的平方剩余.

设 q 为奇素数幂, a 为 $\mathbb{F}_q$ 中的平方元, 下面我们来具体求多项式 x^2-a 在 $\mathbb{F}_q$ 中的根, x^2-a 在 $\mathbb{F}_q$ 中的根也称为 a 的平方根. 显然 0 的平方根依然为 0. 若 $a\neq 0$, 则 a 有两个互不相同的平方根 $\pm b$, 其中 $b^2=a$. 那么如何求出元素 b? 如果 q 比较小, 我们自然可以用穷搜索的办法, 即对每个 $\alpha\in\mathbb{F}_q$, 我们来计算 α^2, 如果对某个 α, $\alpha^2=a$, 我们就找到这样的元素 b 了.

但是如果 q 很大, 我们需要计算大量的平方, 穷搜索这个方法就不适合了, 因为随机地选取 $\mathbb{F}_q^*$ 中的元素来计算, 我们得到正确结果的概率为 $\frac{2}{q-1}$.

对于一般的情形, 我们有如下求平方根方法. 下面总是假设 q 为奇素数幂且 $a^{\frac{q-1}{2}}=1$, 我们分为如下几种不同的情形:

(1). 若 $q\equiv 3\,(\mathrm{mod}\ 4)$. 令 $b=a^{\frac{q+1}{4}}$, 则

$$b^2=a^{\frac{q+1}{2}}=a\cdot a^{\frac{q-1}{2}}=a\cdot 1=a.$$

所以 a 的平方根为 $\pm a^{\frac{q+1}{4}}$.

(2). 若 $q\equiv 5\,(\mathrm{mod}\ 8)$. 注意到 $a^{\frac{q-1}{2}}=1$ 且 $4\mid(q-1)$, 所以 $a^{\frac{q-1}{4}}=1$ 或者 $a^{\frac{q-1}{4}}=-1$.

(2-1). 若 $a^{\frac{q-1}{4}}=1$, 令 $b=a^{\frac{q+3}{8}}$, 则

$$b^2=a^{\frac{q+3}{4}}=a\cdot a^{\frac{q-1}{4}}=a.$$

所以 a 的平方根为 $\pm a^{\frac{q+3}{8}}$.

(2-2). 若 $a^{\frac{q-1}{4}}=-1$, 注意到由例 7.5 知这时 2 为非平方元, 故 $2^{\frac{q-1}{2}}=-1$. 令 $b=(2a)(4a)^{\frac{q-5}{8}}$, 则

$$b^2=2^2a^2\cdot 2^{\frac{q-5}{2}}a^{\frac{q-5}{4}}=2^{\frac{q-1}{2}}a\cdot a^{\frac{q-1}{4}}=a.$$

所以 a 的平方根为 $\pm 2a(4a)^{\frac{q-5}{8}}$.

(3). 若 $q\equiv 1\,(\mathrm{mod}\ 8)$. 记 $q-1=2^e\ell$, 其中 $e\geq 3$ 且 ℓ 为奇数. 令 G 为 $\mathbb{F}_q^*$ 的 2^e 阶子群, 则 G 为循环群, 取 G 的一个生成元 c. 找到一个偶数 k 满足 $0\leq k<2^e$ 且 $a^\ell c^k=1$. 令 $b=a^{\frac{\ell+1}{2}}c^{\frac{k}{2}}$, 则有 $b^2=a^{\ell+1}c^k=a\cdot a^\ell c^k=a$, 即 a 的平方根为 $\pm a^{\frac{\ell+1}{2}}c^{\frac{k}{2}}$.

如何取群 G 的一个生成元, 即 $\mathbb{F}_q^*$ 中一个阶为 2^e 的元素? 事实上, 容易验证若 β 为 $\mathbb{F}_q$ 中的一个非平方元, 即 β 为 $\mathbb{F}_q$ 的本原元素的奇数次幂, 则 β^ℓ 的阶为 2^e, 我们令 $c=\beta^\ell$ 即可 (注意到随机在 $\mathbb{F}_q^*$ 中选取一个元素, 它是非平方元的概率为 $\frac{1}{2}$, 所以我们还是比较容易得到 $\mathbb{F}_q$ 中的非平方元的). 由此我们有如下算法来求 a 的平方根.

算法 7.1:

- 输入: 奇素数幂 q 满足 $q\equiv 1\,(\mathrm{mod}\ 8)$, $a\in\mathbb{F}_q^*$ 为平方元, 令 $q-1=2^e\ell$, 其中 $e\geq 3$ 且 ℓ 为奇数.
- 输出 $b\in\mathbb{F}_q$ 使得 $b^2=a$.

(i) 随机选取 $\beta\in\mathbb{F}_q^*$.

(ii) 验证是否有 $\beta^{\frac{q-1}{2}}=-1$, 否则返回步骤 (i).

(iii) 计算 $c=\beta^\ell$.

(iv) 找到偶数 k 满足 $0\leq k<2^e$ 且 $a^\ell c^k=1$.

(v) 输出 $b=\pm a^{\frac{\ell+1}{2}}c^{\frac{k}{2}}$.

注释: 这是一个概率算法, 即在算法的某些步骤的操作时不确定, 有有限种选择, 这些选择有的正确, 有的错误, 但是出错的概率的界关于输入长度是一个常数. 接下来我们来看看如何进行步骤 (iv). 令 $r = a^{\frac{\ell+1}{2}}$, $j = \frac{k}{2}$, $b = rc^j$, 步骤 (iv) 即寻找 j 满足 $0 \le j < 2^{e-1}$ 和 $b^2 = a$. 把 j 用二进制表示为

$$j = j_0 + j_1 \cdot 2 + j_2 \cdot 2^2 + \cdots + j_{e-2} \cdot 2^{e-2},$$

其中 $j_0, j_1, \ldots, j_{e-2} = 0$ 或 1. 另外由于 c 的阶为 2^e, 所以 $c^{2^{e-1}} = -1$.

(iv).1 设 $s_0 = a^{-1}r^2 (= a^\ell)$. 注意到 $s_0^{2^{e-1}} = (a^\ell)^{2^{e-1}} = a^{\frac{q-1}{2}} = 1$, 所以 $s_0^{2^{e-2}} = 1$ 或者 -1. 若 $s_0^{2^{e-2}} = 1$, 则令 $j_0 = 0$, 否则令 $j_0 = 1$.

(iv).2 设 $s_1 = s_0(c^{j_0})^2 = a^{-1}(rc^{j_0})^2$. 则 $s_1^{2^{e-2}} = s_0^{2^{e-2}}(c^{2^{e-1}})^{j_0} = 1$, 所以 $s_1^{2^{e-3}} = 1$ 或者 -1. 若 $s_1^{2^{e-3}} = 1$, 则令 $j_1 = 0$, 否则令 $j_1 = 1$.

(iv).3 类似地, 设 $s_2 = s_1(c^{j_1 \cdot 2})^2 = a^{-1}(rc^{j_0 + j_1 \cdot 2})^2$, s_2 是一个 2^{e-3} 次单位根. 继续这个过程, 假设我们已经找到 $j_0, j_1, \ldots, j_{k-1}$ 使得

$$s_k = s_{k-1}(c^{j_{k-1} \cdot 2^{k-1}})^2 = a^{-1}(rc^{j_0 + j_1 2 + \cdots + j_{k-1}2^{k-1}})^2$$

是一个 2^{e-k-1} 次单位根, 则当 $s_k^{2^{e-k-2}} = 1$ 时令 $j_k = 0$, 否则令 $j_k = 1$. 最后当 $k = e-2$ 时我们得到 $s_{e-1} = s_{e-2}(c^{j_{e-2}2^{e-2}})^2 = a^{-1}(rc^{j_0 + j_1 2 + \cdots + j_{e-2}2^{e-2}})^2$ 是一个 $2^{e-(e-1)-1} = 1$ 次单位根, 即 $s_{e-1} = 1$. 所以 $b = rc^{j_0 + j_1 2 + \cdots + j_{e-2}2^{e-2}}$ 满足 $b^2 = a$.

设 $q = p^m$, 其中 p 为奇素数, 显然有若 $q \equiv 3 \pmod 4$, 则必有 $p \equiv 3 \pmod 4$ 且 m 为奇数, 而若 $q \equiv 5 \pmod 8$, 则必有 $p \equiv 5 \pmod 8$ 且 m 为奇数. 这两种情形我们都有确定的求平方元素的平方根的方法, 而当 $q \equiv 1 \pmod 8$ 时, 还没有找到这样的确定算法.

例 7.6: 求多项式 $x^2 - 186$ 在域 $\mathbb{F}_{401}$ 中的根. 这时 $q = 401$ 为素数, $q - 1 = 400 = 2^4 \cdot 25$. 选取模 401 的一个二次非剩余 $\beta = 3$, 所以 $c = 3^{25} = 268$, $r = 186^{13} = 103$ 且 $a^{-1} = 186^{-1} = 235$. $s_0 = a^{-1}r^2$, 则 s_0 是一个 8 次单位根, 直接计算得到 $s_0^4 = -1$, 所以 $j_0 = 1$. 接下来 $s_1 = a^{-1}(rc^1)^2$ 是一个 4 次单位根, 计算得到 $s_1^2 = 1$, 所以令 $j_1 = 0$. 现在 $s_2 = a^{-1}(rc^{1+0\cdot 2})^2 (= s_1)$ 是一个 2 次单位根, 由 $s_2 = -1$ 得到 $j_2 = 1$. 所以 $\pm rc^5 = \pm 304$ 就是所求的根. □

下面我们讨论求任意 $\mathbb{F}_q$ 上的多项式在 $\mathbb{F}_q$ 中的根的算法. 设 $f(x) \in \mathbb{F}_q[x]$, 我们已经知道 $f(x)$ 在 $\mathbb{F}_q$ 中的互不相同的根恰为 $\gcd(f(x), x^q - x)$ 的所有根, 所以我们可以假设 $f(x)$ 在 $\mathbb{F}_q$ 上可以写成互不相同的首一一次多项式的乘积 (当然我们不知道这个具体的乘积是什么).

1. 设 $q = p$ 为素数且 $f(x) \in \mathbb{F}_p[x]$ 可分解为 $f(x) = \prod_{i=1}^n (x - c_i)$, 其中 $c_1, c_2, \ldots, c_n$ 为 $\mathbb{F}_p$ 中互不相同的元素 (开始时我们不知道这些 c_i 是什么, $1 \le i \le n$). 若 p 很小, 则我们可以用穷搜索的方法求 $f(x)$ 的根, 即只需要对每个 $c \in \mathbb{F}_p$, 计算 $f(c)$, 找到那些 c_i 使得 $f(c_i) = 0$. 但是如果 p 很大, 就不能简单地用穷搜索方法了, 因为这需要求很多的函数值, 这时我们可以用下面的方法. 下面设 p 为奇素数 ($p = 2$ 很小), 对于 $b \in \mathbb{F}_p$, 我们有 $f(x-b) = \prod_{i=1}^n (x - (b + c_i))$. 注意到 $f(x-b)$ 整除 $x^p - x = x(x^{\frac{p-1}{2}} + 1)(x^{\frac{p-1}{2}} - 1)$. 若 $x \mid f(x-b)$, 则 $f(-b) = 0$, 我们可以得到

$f(x)$ 的一个根 $-b$. 若 $x \nmid f(x-b)$, 则 $f(x-b)$ 与 x 互素, 所以 $f(x-b) \mid (x^{\frac{p-1}{2}}+1)(x^{\frac{p-1}{2}}-1)$, 从而

$$f(x-b) = \gcd(f(x-b), x^{\frac{p-1}{2}}+1) \cdot \gcd(f(x-b), x^{\frac{p-1}{2}}-1). \tag{7.6}$$

我们接下来计算 $x^{\frac{p-1}{2}} \pmod{f(x-b)}$, 若 $x^{\frac{p-1}{2}} \not\equiv \pm 1 \pmod{f(x-b)}$, 则式 (7.6) 给出 $f(x-b)$ 的一个非平凡分解, 再用 $x+b$ 代换 x 就得到 $f(x)$ 的一个非平凡分解. 但是若 $x^{\frac{p-1}{2}} \equiv \pm 1 \pmod{f(x-b)}$, 则我们需要再换一个 $b \in \mathbb{F}_p$ 施行同样的做法. 所以, 可能需要选择多次 b, 我们找到 $f(x)$ 的一个根或者得到 $f(x)$ 的非平凡分解. 对 $f(x)$ 的每个次数大于 1 的非平凡因式继续这一过程, 最后我们可以得到 $f(x)$ 的全部根. 需要注意的是如果我们利用某个 $b \in \mathbb{F}_p$ 得到了 $f(x)$ 的非平凡因式, 再对这些因式进一步分解时就要利用不为 b 的 $\mathbb{F}_p$ 中的元素. 当然这个求根算法依然是概率算法, 施行时与我们随机选取的 $b \in \mathbb{F}_p$ 有关.

例 7.7: 求出多项式 $f(x) = x^6 - 7x^5 + 3x^4 - 7x^3 + 4x^2 - x - 2 \in \mathbb{F}_{17}[x]$ 在 $\mathbb{F}_{17}$ 中的所有根. 先计算 $g(x) = \gcd(f(x), x^{17} - x)$ 我们得到 $g(x) = x^4 + 6x^3 - 5x^2 + 7x - 2$, 所以只需求出 $g(x)$ 的根. 先选取 $b = 0$, 直接计算得到 $x^{\frac{p-1}{2}} = x^8 \equiv 1 \pmod{g(x)}$, 故我们需要选取其它的 b. 接下来选取 $b = 1$, 则 $g(x-1) = x^4 + 2x^3 - 3x - 2$ 且 $x^8 \equiv -4x^3 - 7x^2 + 8x - 5 \pmod{g(x-1)}$, 所以 $b = 1$ 给出了 $g(x-1)$ 的非平凡分解. 由 Euclid 算法得到

$$\gcd(g(x-1), x^8+1) = \gcd(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 4) = x^2 - 7x + 4$$

和

$$\gcd(g(x-1), x^8-1) = \gcd(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 6) = x^2 - 8x + 8,$$

所以由 (7.6) 得到 $g(x-1) = (x^2 - 7x + 4)(x^2 - 8x + 8)$, 用 $x+1$ 代替 x 得到

$$g(x) = (x^2 - 5x - 2)(x^2 - 6x + 1).$$

设 $g_1(x) = x^2 - 5x - 2$, 为分解 $g_1(x)$, 我们试验 $b = 2$. 则有 $g_1(x-2) = x^2 + 8x - 5$ 且 $x^8 \equiv -8x + 2 \pmod{g_1(x-2)}$. 进一步地, 直接计算得到

$$\gcd(g_1(x-2), x^8+1) = \gcd(x^2 + 8x - 5, -8x + 3) = x + 6,$$

再通过长除得到 $g_1(x-2) = (x+6)(x+2)$, 所以 $g_1(x) = (x+8)(x+4)$. 再来看 $g_2(x) = x^2 - 6x + 1$, 依然试验 $b = 2$, 我们可以得到 $g_2(x-2) = x^2 + 7x = x(x+7)$, 故 $g_2(x) = (x+2)(x+9)$. 把这些分解综合起来得到 $g(x) = (x+8)(x+4)(x+2)(x+9)$, 所以 $g(x)$ 在 $\mathbb{F}_{17}$ 中的根, 也是 $f(x)$ 在 $\mathbb{F}_{17}$ 中的根为 $9, 13, 15$ 和 8. □

2. 设 $q = p^m$, 其中 p 是一个小素数. 自然我们只需考虑形如 $f(x) = \prod_{i=1}^{n}(x - \gamma_i)$ 的多项式, 其中 $\gamma_1, \gamma_2, \ldots, \gamma_n$ 是 $\mathbb{F}_q$ 中互不相同的元素. 定义

$$S(x) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = \sum_{j=0}^{m-1} x^{p^j}.$$

由第 3 章第 3.1 节得知, 对任意 $c \in \mathbb{F}_p$, 多项式 $S(x) - c$ 在 $\mathbb{F}_q$ 中有 p^{m-1} 个根, 又显然对不同

的 $c_1, c_2 \in \mathbb{F}_p$, $S(x)-c_1$ 和 $S(x)-c_2$ 在 $\mathbb{F}_q$ 中的根互不相同, 所以我们得到

$$x^q - x = \prod_{c\in\mathbb{F}_p} (S(x)-c). \tag{7.7}$$

由于 $f(x) \mid (x^q-x)$, 所以 $\prod_{c\in\mathbb{F}_p}(S(x)-c) \equiv 0 \pmod{f(x)}$, 由此我们得到

$$f(x) = \prod_{c\in\mathbb{F}_p} \gcd(f(x), S(x)-c). \tag{7.8}$$

这需要计算 p 个最大公因式, 因为 p 很小, 所以这个方法是可行的.

但是如果存在某个 $c \in \mathbb{F}_p$ 使得 $S(x) \equiv c \pmod{f(x)}$, 则 (7.8) 式给出的分解是平凡的, 这时可以利用另外的与 $S(x)$ 有关的辅助多项式. 设 β 是 $\mathbb{F}_q$ 在 $\mathbb{F}_p$ 上的一个定义元素, 即使得 $\{1, \beta, \ldots, \beta^{m-1}\}$ 是 $\mathbb{F}_q$ 在 $\mathbb{F}_p$ 上的一组基 (实际上 $\mathbb{F}_q$ 中任一在 $\mathbb{F}_p$ 上次数为 m 的元素都可以取为 β, 比如本原元素). 对每个 $0 \le j \le m-1$, 在 (7.7) 中用 $\beta^j x$ 代换 x 得到

$$(\beta^j)^q x^q - \beta^j x = \prod_{c\in\mathbb{F}_p} (S(\beta^j x) - c).$$

由于 $(\beta^j)^q = \beta^j$, 我们有$x^q - x = \beta^{-j} \prod_{c\in\mathbb{F}_p}(S(\beta^j x)-c)$, 由此得到式 (7.8) 的如下推广, 即

$$f(x) = \prod_{c\in\mathbb{F}_p} \gcd(f(x), S(\beta^j x) - c), \tag{7.9}$$

其中 $0 \le j \le m-1$. 可以证明, 若 $n = \deg(f) \ge 2$, 则至少存在一个 j 使得式 (7.9) 的分解是不平凡的, 其中 $0 \le j \le m-1$. 事实上, 如果对每一个 j, 式 (7.9) 的分解都是平凡的, 即存在 $c_j \in \mathbb{F}_p$ 使得 $S(\beta^j x) \equiv c_j \pmod{f(x)}$. 因为 γ_1, γ_2 是 $f(x)$ 在 $\mathbb{F}_q$ 中的互异根, 故对所有 $0 \le j \le m-1$, 我们有 $S(\beta^j\gamma_1) = S(\beta^j\gamma_2) = c_j$, 即 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta^j\gamma_1) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta^j\gamma_2) = c_j$. 由迹映射的线性性质得到 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}((\gamma_1-\gamma_2)\beta^j) = 0$, 又 $\{1, \beta, \ldots, \beta^{m-1}\}$ 是 $\mathbb{F}_q$ 在 $\mathbb{F}_p$ 上的一组基, 所以对所有 $\alpha \in \mathbb{F}_q$ 有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}((\gamma_1-\gamma_2)\alpha) = 0$. 由于 $\gamma_1 - \gamma_2 \ne 0$, 当 α 跑遍 $\mathbb{F}_q$ 时, $(\gamma_1-\gamma_2)\alpha$ 也跑遍 $\mathbb{F}_q$, 所以对所有 $\alpha \in \mathbb{F}_q$ 有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = 0$, 与迹映射为满射矛盾. 当我们利用式 (7.9) 给出 $f(x)$ 的非平凡分解后, 再利用其它的 j 对 $f(x)$ 的非平凡因式做类似于 (7.9) 的分解, 上面的讨论也表明 $f(x)$ 的所有根都可以通过选取合适的 j 利用式 (7.9) 得到, 即利用所有的 $0 \le j \le m-1$, 式 (7.9) 可以把 $f(x)$ 的所有根分离出来.

例 7.8: 设 $\mathbb{F}_{64} = \mathbb{F}_2(\beta)$, 其中 β 是 $\mathbb{F}_2$ 上不可约多项式 x^6+x+1 的一个根, 设

$$f(x) = x^4 + (\beta^5+\beta^4+\beta^3+\beta^2)x^3 + (\beta^5+\beta^4+\beta^2+\beta+1)x^2 + (\beta^4+\beta^3+\beta)x + (\beta^3+\beta) \in \mathbb{F}_{64}[x],$$

求 $f(x)$ 在 $\mathbb{F}_{64}$ 中的根. 通过计算 $x^{2^k} \pmod{f(x)}$, $0 \le k \le 6$, 我们可以得到 $f(x) \mid (x^{64}-x)$, 所以 $f(x)$ 在 $\mathbb{F}_{64}$ 中有 4 个互异根.

设 $S(x) = x + x^2 + x^4 + x^8 + x^{16} + x^{32}$, 故

$$S(x) \equiv (\beta^5+\beta^3+\beta^2+\beta+1)x^3 + \beta^5 x^2 + (\beta^3+\beta^2)x + (\beta^3+\beta^2+1) \pmod{f(x)},$$

由 Euclid 算法得到

$$\gcd(f(x), S(x)) = x^3 + (\beta^4+\beta^3+\beta^2)x^2 + (\beta^5+\beta^2+1)x + (\beta^3+\beta^2) = g(x),$$

和

$$\gcd(f(x), S(x)-1) = x+\beta^5,$$

所以 (7.8) 给出

$$f(x) = g(x)(x+\beta^5).$$

下面再求 $g(x)$ 在 $\mathbb{F}_{64}$ 中的根, 注意到显然 $\{1, \beta, \beta^2, \ldots, \beta^5\}$ 是 $\mathbb{F}_{64}$ 在 $\mathbb{F}_2$ 上的一组基, 我们在式 (7.9) 中取 $j=1$. 我们有

$$\begin{aligned} S(\beta x) &= \beta x + \beta^2 x^2 + \beta^4 x^4 + \beta^8 x^8 + \beta^{16} x^{16} + \beta^{32} x^{32} \\ &= \beta x + \beta^2 x^2 + \beta^4 x^4 + (\beta^3+\beta^2) x^8 + (\beta^4+\beta+1) x^{16} + (\beta^3+1) x^{32} \\ &\equiv (\beta^2+1)x^3 + (\beta^3+\beta+1)x^2 + (\beta^5+\beta^4+\beta^3+\beta^2+\beta+1)x + (\beta^4+\beta^2+\beta) \pmod{f(x)}. \end{aligned}$$

因为 $g(x) \mid f(x)$, 如上同余式对模 $g(x)$ 也对, 继续进行下去, 我们有 $S(\beta x) \equiv (\beta^5+\beta^2)x^2 + \beta^3 x + (\beta^5+\beta^3+\beta) \pmod{g(x)}$, 由此可得到

$$\gcd(g(x), S(\beta x)) = x^2 + (\beta^3+1)x + (\beta^4+\beta^3+\beta^2+\beta) = h(x),$$

和

$$\gcd(g(x), S(\beta x)-1) = x + (\beta^4+\beta^2+1),$$

故在式 (7.9) 中取 $j=1$ 得到

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

最后求 $h(x)$ 在 $\mathbb{F}_{64}$ 中的根, 在 (7.9) 中取 $j=2$. 类似的计算给出

$$S(\beta^2 x) \equiv (\beta^5+\beta^2+1)x + (\beta^5+\beta^3+\beta^2) \pmod{h(x)},$$

从而我们得到

$$\gcd(h(x), S(\beta^2 x)) = x + (\beta+1),$$

和

$$\gcd(h(x), S(\beta^2 x)-1) = x + (\beta^3+\beta),$$

即在 (7.9) 中取 $j=2$ 得到

$$h(x) = (x+\beta+1)(x+\beta^3+\beta).$$

综合上面的分解, 我们有

$$f(x) = (x+\beta+1)(x+\beta^3+\beta)(x+\beta^4+\beta^2+1)(x+\beta^5),$$

所以 $f(x)$ 在 $\mathbb{F}_{64}$ 中的根为 $\beta+1$, $\beta^3+\beta$, $\beta^4+\beta^2+1$ 和 β^5. □

3. $q=p^m$, 其中 p 是一个大素数. 我们依然设 $f(x) \in \mathbb{F}_q[x]$ 形如 $f(x) = \prod_{i=1}^{n}(x-\gamma_i)$, 其中 $\gamma_1, \gamma_2, \ldots, \gamma_n$ 是 $\mathbb{F}_q$ 中互不相同的元素, 但是我们已知的是 $f(x)$ 的标准表达式 $f(x) = \sum_{=0}^{n} \alpha_j x^j$, 其中 $\alpha_j \in \mathbb{F}_q$, $0 \le j \le n$, $\alpha_n = 1$. 为找到 $f(x)$ 在 $\mathbb{F}_q$ 中的根, 我们可以先找到 $f(x)$ 在 $\mathbb{F}_q$ 上的非平凡因式, 为了不处理平凡的情形, 我们还可以假设 $n \ge 2$.

对于 $0 \le k \le m-1$, 定义

$$f_k(x) = \sum_{j=0}^{n} \alpha_j^{p^k} x^j, \tag{7.10}$$

则显然 $f_0(x) = f(x)$, 且每个 $f_k(x)$ 都是 $\mathbb{F}_q$ 上的首一多项式. 进一步地, 对每个 $0 \le k \le m-1$ 和 $1 \le i \le n$ 有

$$f_k(\gamma_i^{p^k}) = \sum_{j=0}^{n} \alpha_j^{p^k} \left(\gamma_i^{p^k}\right)^j = \left(\sum_{=0}^{n} \alpha_j \gamma_i^j\right)^{p^k} = 0,$$

所以 $f_k(x)$ 的根为 $\gamma_1^{p^k}, \gamma_2^{p^k}, \ldots, \gamma_n^{p^k}$, 故 $f_k(x) = \prod_{i=1}^{n}(x - \gamma_i^{p^k})$, $0 \le k \le m-1$. 对于每个 $1 \le i \le n$, 设 γ_i 在 $\mathbb{F}_p$ 上的极小多项式为 $F_i(x)$, 其次数 d_i 就是满足 $\gamma_i^{p^{d_i}} = \gamma_i$ 的最小正整数, 由第 2.3 节得知 $d_i \mid m$ 和 $F_i(x) = \prod_{t=0}^{d_i-1}(x - \gamma_i^{p^t})$, 所以

$$\prod_{k=0}^{m-1}(x - \gamma_i^{p^k}) = F_i(x)^{\frac{m}{d_i}}.$$

设 $F(x) = \prod_{k=0}^{m-1} f_k(x)$, 则有

$$F(x) = \prod_{k=0}^{m-1}\prod_{i=1}^{n}(x - \gamma_i^{p^k}) = \prod_{i=1}^{n}\left(\prod_{k=0}^{m-1}(x - \gamma_i^{p^k})\right) = \prod_{i=1}^{n} F_i(x)^{\frac{m}{d_i}},$$

所以 $F(x)$ 是 $\mathbb{F}_p$ 上的多项式且被 $\mathbb{F}_p$ 上的不可约多项式 $F_i(x)$ 整除, $1 \le i \le n$. 注意到有可能出现 $1 \le i_1 \ne i_2 \le n$ 但是 $F_{i_1}(x) = F_{i_2}(x)$ 的情形 (即 γ_{i_1} 与 γ_{i_2} 在 $\mathbb{F}_p$ 上共轭), 设在 $F_1(x), F_2(x), \ldots, F_n(x)$ 中有 r 个互不相同, 不失一般性设 $F_1(x), F_2(x), \ldots, F_r(x)$ 互不相同, 则 $F(x)$ 在 $\mathbb{F}_p$ 上的标准分解式一定形为

$$F(x) = G_1(x)G_2(x)\cdots G_r(x),$$

其中 $G_t(x)$ 为 $F_t(x)$ 的方幂. 注意到因为我们不知道 $f(x)$ 的根 γ_i, 所以也不知道 $\mathbb{F}_p$ 上的不可约多项式 $F_i(x)$, 但是我们可以求出每个 $f_k(x)$, $0 \le k \le m-1$, 所以有这 m 个多项式的乘积 $F(x)$, 我们可以利用多项式分解的 Berlekamp 算法 (或者利用下节我们对 Berlekamp 算法的修正) 给出 $F(x)$ 在 $\mathbb{F}_p$ 上的标准分解. 注意到 $f(x) = f_0(x)$ 整除 $F(x)$, 所以由 $F(x) = G_1(x)G_2(x)\cdots G_r(x)$ 得到

$$f(x) = \prod_{t=1}^{r} \gcd(f(x), G_t(x)). \tag{7.11}$$

由于对每一个 $1 \le t \le r$, $f(x)$ 与 $G_t(x)$ 有公共根 γ_t, 所以 $\gcd(f(x), G_t(x)) \ne 1$, 从而若 $r \ge 2$, 式 (7.11) 一定给出 $f(x)$ 的一个非平凡分解. 当然, 若 $r = 1$, 则有 $F_1(x) = F_2(x) = \cdots = F_n(x)$, 故 $F(x) = G_1(x) = F_1(x)^{\frac{mn}{d_1}}$, 这时 (7.11) 的分解是平凡的. 另外 (7.11) 需要做 r 次计算最大公因式, 由于 $r \le n = \deg f(x)$, 所以利用 (7.11), 我们最多只需施行 n 次计算最大公因式. 特别地, 若 $r = n$, 由于 $G_1(x), G_2(x), \ldots, G_n(x)$ 两两互素, (7.11) 给出的是 $f(x)$ 在 $\mathbb{F}_q$ 上分解为一次因式乘积的完全分解.

下面我们进一步考察 (7.11) 给出 $f(x)$ 的平凡分解的情形, 这时 $F(x)$ 是 $\mathbb{F}_p$ 上一个不可约多项式的方幂, 故 $f(x)$ 在 $\mathbb{F}_q$ 中的所有根在 $\mathbb{F}_p$ 上是互相共轭的, 所以 $f(x)$ 在 $\mathbb{F}_q$ 上根的个数 $n \le m$ 且对 $f(x)$ 的根适当排序可设 $\gamma_i = \gamma_1^{p^{b_i}}$, $1 \le i \le n$ 且 $0 = b_1 < b_2 < \cdots < b_n < m$. 记 $b_{n+1} = m$, 则 $\gamma_1^{p^{b_{n+1}}} = \gamma_1^{p^{b_1}}$. 设 $d = \min_{1\le i\le n}(b_{i+1} - b_i)$, 则由 $m = b_{n+1} - b_1 = \sum_{i=1}^{n}(b_{i+1} - b_i) \ge nd$ 得到 $d \le \frac{m}{n}$. 这需要讨论如下两种情形:

情形 (I). 存在某个 i 使得 $b_{i+1} - b_i > d$, $1 \le i \le n$, 显然这时有 $d < \frac{m}{n}$ 且 $f(x)$ 的根集 $\{\gamma_1^{p^{b_1}}, \gamma_1^{p^{b_2}}, \ldots, \gamma_1^{p^{b_n}}\}$ 与 $f_d(x)$ 的根集 $\{\gamma_1^{p^{b_1+d}}, \gamma_1^{p^{b_2+d}}, \ldots, \gamma_1^{p^{b_n+d}}\}$ 不相同. 另一方面, 还存在某个 j 使得 $b_{j+1} - b_j = d$, $1 \le j \le n$, 所以这两个根集有公共元素, 即 $f(x)$ 与 $f_d(x)$ 有公共根, 故 $\gcd(f(x), f_d(x))$ 既不为 $f(x)$ 也不为 1, 从而 $\gcd(f(x), f_d(x))$ 就是 $f(x)$ 的一个非平凡因式.

情形 (II). 对所有的 i 均有 $b_{i+1} - b_i = d$, $1 \le i \le n$, 则 $f(x)$ 与 $f_d(x)$ 有相同的根且对每个 $1 \le k < d$, $f(x)$ 与 $f_k(x)$ 无公共根, 所以 $f(x) = f_d(x)$ 且 $\gcd(f(x), f_k(x)) = 1$, $1 \le k < d$. 由 $f(x) = f_d(x)$ 知对每个 j 有 $\alpha_j^{p^d} = \alpha_j$, 故 $\alpha_j \in \mathbb{F}_{p^d}$, $0 \le j \le n$, 所以 $f(x) \in \mathbb{F}_{p^d}[x]$. 此时又显然有 $d = \frac{m}{n}$, 故 $n \mid m$ 且对每个 $1 \le i \le n$ 有 $b_i = d(i-1)$, 由此得到 $\gamma_i = \gamma_1^{p^{d(i-1)}}$, $1 \le i \le n$. 所以这 n 个元素 γ_i 恰为 γ_1 在域 $\mathbb{F}_{p^d}$ 上的所有共轭元, 故 $f(x)$ 是 γ_1 在 $\mathbb{F}_{p^d}$ 上的极小多项式.

注意到在情形 (I) 我们并不知道 d 的具体值, 我们只知道 $d < \frac{m}{n}$. 故对 $1 \le k < \frac{m}{n}$, 计算 $\gcd(f(x), f_k(x))$, 总有某个 k 使得 $\gcd(f(x), f_k(x))$ 为 $f(x)$ 的非平凡因式. 而对情形 (II), 有 $n \mid m$, 设 $d = \frac{m}{n}$, 对于 $1 \le k < d$ 有 $\gcd(f(x), f_k(x)) = 1$, 且 $f(x) = f_d(x) \in \mathbb{F}_{p^d}[x]$ 在 $\mathbb{F}_{p^d}$ 上不可约. 设 β 是 $\mathbb{F}_q$ 在 $\mathbb{F}_{p^d}$ 上的一个定义元素, 则 $\mathbb{F}_{p^d}(\beta) = \mathbb{F}_q = \mathbb{F}_{p^m}$, 故 β 在 $\mathbb{F}_{p^d}$ 上的次数为 $\frac{m}{d} = n$, 从而对每个 $1 \le j \le n-1$, 有 $\beta^j \notin \mathbb{F}_{p^d}$. 若 $f(x)$ 的系数中存在某个 $\alpha_{j_0} \ne 0$, 其中 $1 \le j_0 \le n-1$, 定义多项式 $\bar{f}(x) = \beta^{-n} f(\beta x)$, 则 $\bar{f}(x)$ 是 $\mathbb{F}_q$ 上的首一多项式. 由于 $\alpha_{j_0} \in \mathbb{F}_{p^d}^*$, 所以 $\bar{f}(x)$ 中 x^{j_0} 的系数 $\beta^{-n+j_0}\alpha_{j_0} \notin \mathbb{F}_{p^d}$. 这样对 $\bar{f}(x)$ 施行上面的讨论不会出现情形 (II), 故我们可得到 $\bar{f}(x)$ 的非平凡因式, 利用 $f(x) = \beta^n \bar{f}(\beta^{-1}x)$ 就可以得到 $f(x)$ 的非平凡因式. 接下来我们还需要讨论情形 (II) 且对所有 $1 \le j \le n-1$, $f(x)$ 的系数 $\alpha_j = 0$ 的情况, 这时 $f(x) = x^n + \alpha_0$ 为 $\mathbb{F}_{p^d}$ 上的一个二项式. 显然此时 $p \nmid n$, 因为若否, 则 $f(x) = (x^{\frac{n}{p}} + \alpha_0^{p^{d-1}})^p$, 与 $f(x)$ 在 $\mathbb{F}_{p^d}$ 上不可约矛盾. 定义多项式 $\bar{f}(x) = \beta^{-n} f(\beta x + 1)$, 则 $\bar{f}(x)$ 是 $\mathbb{F}_q$ 上的首一多项式且 x^{n-1} 的系数为 $n\beta^{-1} \notin \mathbb{F}_{p^d}$. 对 $\bar{f}(x)$ 施行上面的讨论不会出现情形 (II), 我们可得到 $\bar{f}(x)$ 的非平凡因式, 再利用 $f(x) = \beta^n \bar{f}(\beta^{-1}(x-1))$ 从 $\bar{f}(x)$ 的非平凡因式就可以得到 $f(x)$ 的非平凡因式.

综合上面的讨论, 我们可以得到如下的求根算法. 给定首一多项式 $f(x) \in \mathbb{F}_q[x]$ 满足 $f(x) \mid (x^q - x)$, 首先对每个 $0 \le k \le m-1$, 根据 (7.10) 计算 $f_k(x)$, 把这 m 个 $f_k(x)$ 做乘积得到多项式 $F(x) \in \mathbb{F}_p[x]$. 利用多项式分解算法在 $\mathbb{F}_p$ 上分解 $F(x)$ 求得 $F(x)$ 在 $\mathbb{F}_p$ 上的标准分解式, 若 $F(x)$ 在 $\mathbb{F}_p$ 上互不相同的首一不可约因式多于一个, 则 (7.11) 可以给出 $f(x)$ 的非平凡分解. 若 $F(x)$ 为 $\mathbb{F}_p$ 上一个不可约多项式的方幂, 则计算 $\gcd(f(x), f_k(x))$ 以便求出 $f(x)$ 的非平凡因式, 其中 $1 \le k < \frac{m}{n}$. 若对所有 $1 \le k < \frac{m}{n}$, 均有 $\gcd(f(x), f_k(x)) = 1$, 令 $d = \frac{m}{n}$ (这

时一定有 $n \mid m$), 找到 $\mathbb{F}_q$ 在 $\mathbb{F}_{p^d}$ 上的一个定义元素 (或 n 次元素) β, 若 $f(x)$ 不是二项式, 则定义 $\bar{f}(x) = \beta^{-n} f(\beta x)$, 而若 $f(x)$ 为二项式, 则定义 $\bar{f}(x) = \beta^{-n} f(\beta x + 1)$. 对于 $1 \leq k < d$, 计算 $\gcd(\bar{f}(x), \bar{f}_k(x))$ 就可以得到 $\bar{f}(x)$ 的非平凡因式 (其中 $\bar{f}_k(x)$ 的定义与 (7.10) 类似, 就是将 $\bar{f}(x)$ 的各项系数做 p^k 次乘方后得到的多项式), 从而得到 $f(x)$ 的非平凡因式. 继续对 $f(x)$ 的次数 ≥ 2 的非平凡因式施行同样的过程最后可以把 $f(x)$ 分解为一次因式的乘积, 得到 $f(x)$ 在 $\mathbb{F}_q$ 中的根.

7.4 有限域上多项式的分解

上一节中我们给出了求多项式根的一些算法, 多数情形下需要我们先进行多项式的因式分解. 在第 4.2 节我们给出了在有限域 $\mathbb{F}_q$ 上分解多项式的 Berlekamp 算法, 这需要我们计算 q 个最大公因式, 但是当 q 很大 (比多项式的次数大得多) 时这并不是有效的. 本节我们来讨论这时如何来有效地应用 Berlekamp 算法.

设 $f(x) \in \mathbb{F}_q[x]$ 首一且 $\deg f(x) = n$, 设 $h(x)$ 为一个 f-约化多项式, 即满足 $h(x)^q \equiv h(x) \pmod{f(x)}$ 且满足 $0 < \deg h(x) < n$ 的多项式 $h(x) \in \mathbb{F}_q[x]$ (第 4.2 节我们已经证明若 $f(x)$ 的互不相同的首一不可约因式个数大于 1, 则 f-约化多项式一定存在并且也给出了求 f-约化多项式的有效方法), 则 $f(x) = \prod_{s \in \mathbb{F}_q} \gcd(f(x), h(x) - s)$ 是 $f(x)$ 在 $\mathbb{F}_q$ 上的一个非平凡分解. 利用如上算法分解 $f(x)$, 名义上需要对每个 $s \in \mathbb{F}_q$, 都要计算 $\gcd(f(x), h(x) - s)$, 但实际上当 q 很大时, 会出现大量的 $s \in \mathbb{F}_q$ 使得 $\gcd(f(x), h(x) - s) = 1$. 事实上, 若 $f(x)$ 在 $\mathbb{F}_q$ 上有 k 个互不相同的首一不可约因式, 则至少有 $q - k$ 个 $s \in \mathbb{F}_q$ 满足 $\gcd(f(x), h(x) - s) = 1$. 显然对于这样的 s, 计算 $\gcd(f(x), h(x) - s)$ 是完全没有必要的. 这自然提出如下的问题, 我们能否事先找到这些 $c \in \mathbb{F}_q$, 使得 $\gcd(f(x), h(x) - c) \neq 1$? 如果可以, 我们只需计算这些 c 对应的最大公因式 $\gcd(f(x), h(x) - c)$ 即可, 而这样的 c 显然至多有 k 个.

注意到多项式 $f(x)$ 与 $h(x) - c$ 不互素当且仅当它们在 $\mathbb{F}_q$ 的扩域中有公共根, 由结式理论得知, 这也等价于 $f(x)$ 与 $h(x) - c$ 的结式 $R(f(x), h(x) - c) = 0$. 由此我们可以定义 $F(y) = R(f(x), h(x) - y)$, 由结式的定义我们可以算出 $F(y)$. 事实上, 设 $f(x) =$

$x^n + a_{n-1}x^{n-1} + \cdots + a_1 + a_0$, $h(x) = h_{n-1}x^{n-1} + \cdots + h_1 x + h_0$, 则

$$F(y) = \begin{vmatrix} 1 & a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 & a_0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & a_{n-1} & \cdots & & a_2 & a_1 & a_0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-1} & a_{n-2} & & & \cdots & a_1 & a_0 \\ h_{n-1} & h_{n-2} & h_{n-3} & \cdots & h_1 & h_0 - y & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & h_{n-1} & h_{n-1} & \cdots & h_2 & h_1 & h_0 - y & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & h_{n-1} & h_{n-2} & & & \cdots & h_1 & h_0 - y \end{vmatrix},$$

这是一个 $2n-1$ 阶行列式, 有 n 个元素 $h_0 - y$, 从而 $F(y)$ 是 $\mathbb{F}_q$ 上的次数 $\le n$ 的多项式. 所以对于 $c \in \mathbb{F}_q$, $\gcd(f(x), h(x) - c) \neq 1$ 当且仅当 $F(c) = 0$, 即 c 为多项式 $F(y)$ 在 $\mathbb{F}_q$ 中的根. 利用上一节中给出的多项式求根算法, 我们可以得到使得 $\gcd(f(x), h(x) - c) \neq 1$ 的那些 $c \in \mathbb{F}_q$.

当然我们可以计算这个行列式求出 $F(y)$. 我们还可以任取 $\mathbb{F}_q$ 中 $n+1$ 个互异元素 $c_0, c_1, \ldots, c_n$, 对每个 c_i, 计算出 $r_i = R(f(x), h(x) - c_i))$, $0 \le i \le n$, 再利用定理 1.12 的 Lagrange 插值公式求出次数 $\le n$ 的唯一多项式 $F(y)$ 满足 $F(c_i) = r_i$, $0 \le i \le n$. 这种做法还有一个好处, 如果我们能够恰好选取到 c_i 使得 $r_i = 0$, 则 c_i 自然就是 $F(y)$ 在 $\mathbb{F}_q$ 中的根.

下面我们给出另一个求出那些使得 $\gcd(f(x), h(x) - c) \neq 1$ 的 $c \in \mathbb{F}_q$ 的方法. 令 C 为满足这个条件的 $c \in \mathbb{F}_q$ 构成的集合, 即 $C = \{c \in \mathbb{F}_q \mid \gcd(f(x), h(x) - c) \neq 1\}$. 则显然有

$$f(x) = \prod_{c \in C} \gcd(f(x), h(x) - c), \tag{7.12}$$

从而 $f(x) \mid \prod_{c \in C}(h(x) - c)$. 定义多项式 $G(y) = \prod_{c \in C}(y - c)$, 则有 $f(x) \mid G(h(x))$, 多项式 $G(y)$ 可以被如下结论所刻画.

定理 7.16: 在所有满足 $f(x) \mid g(h(x))$ 的多项式 $g(y) \in \mathbb{F}_q[y]$ 中, 如上定义的 $G(y)$ 是唯一的次数最低的首一多项式.

证明: 用 S 表示所有满足 $f(x) \mid g(h(x))$ 的多项式 $g(y) \in \mathbb{F}_q[y]$ 构成的集合, 即 $S = \{g(y) \in \mathbb{F}_q[y] \mid f(x) \mid g(h(x))\}$, 则容易验证 S 是多项式环 $\mathbb{F}_q[y]$ 的一个理想, 从而为主理想. 设 $G_0(y)$ 为生成 S 的那个唯一的首一多项式, 即 S 中那个次数最低的首一多项式, 则有 $G_0(y) \mid G(y)$, 从而存在 C 的一个子集 C_1 使得 $G_0(y) = \prod_{c \in C_1}(y - c)$. 由于 $f(x) \mid G_0(h(x)) = \prod_{c \in C_1}(h(x) - c)$, 所以

$$f(x) = \prod_{c \in C_1} \gcd(f(x), h(x) - c). \tag{7.13}$$

比较 (7.12) 和 (7.13), 我们得到 $C_1 = C$, 从而 $G_0(y) = G(y)$. □

但是我们需要具体求出多项式 $G(y)$, 再求 $G(y)$ 在 $\mathbb{F}_q$ 中的根才能得到我们要找的 $c \in \mathbb{F}_q$.

设 $t=|C|$ 并记 $G(y)=\sum_{j=0}^{t}b_jy^j$, 其中 $b_j\in\mathbb{F}_q$ 且 $b_t=1$. 由 $f(x)\mid G(h(x))$ 我们有

$$\sum_{j=0}^{t}b_jh(x)^j\equiv 0\,(\mathrm{mod}\ f(x)). \tag{7.14}$$

由于 $b_t=1$, 所以 $h(x)^t\,(\mathrm{mod}\ f(x))$ 可被 $1,\ h(x),\ \ldots,\ h(x)^{t-1}\,(\mathrm{mod}\ f(x))$ 在 $\mathbb{F}_q$ 上线性表出. 再由 t 的最小性我们得到 $1,h(x),\ldots,h(x)^{t-1}\,(\mathrm{mod}\ f(x))$ 在 $\mathbb{F}_q$ 上线性无关, 而 $1,\ h(x),\ \ldots,\ h(x)^{t-1},\ h(x)^t\,(\mathrm{mod}\ f(x))$ 在 $\mathbb{F}_q$ 上线性相关. 由此我们可以得到下面求出 $G(y)$ 的方法, 首先计算 $1,h(x),h(x)^2,\ldots$ 模 $f(x)$ 的剩余类直至找到最小的正整数 t 使得 $1,\ h(x),\ \ldots,\ h(x)^{t-1},\ h(x)^t\,(\mathrm{mod}\ f(x))$ 在 $\mathbb{F}_q$ 上线性相关, 再写出 $h(x)^t\,(\mathrm{mod}\ f(x))$ 被 $1,h(x),\ldots,h(x)^{t-1}\,(\mathrm{mod}\ f(x))$ 线性表出的表达式 (由 t 的最小性知这个线性表出式存在且唯一), 不妨设

$$h(x)^t\equiv -b_0-b_1h(x)-\cdots-b_{t-1}h(x)^{t-1}\,(\mathrm{mod}\ f(x)),$$

则 $G(y)=y^t+b_{t-1}y^{t-1}+\cdots+b_1y+b_0$. 注意到由 (7.12) 一定有 $t\le k$, 其中 k 为 $f(x)$ 在 $\mathbb{F}_q$ 上互不相同的首一不可约因式的个数. 进一步地, 若 $t=k$, 由于对每个 $c\in C$, $\gcd(f(x),h(x)-c)$ 给出的是 $f(x)$ 的非平凡因式, 故分解式 $f(x)=\prod_{c\in C}\gcd(f(x),h(x)-c)$ 就把 $f(x)$ 分解为 k 个互素的非平凡因式的乘积, 若还有 $f(x)$ 无重因式, 则这就是 $f(x)$ 的标准分解式.

例 7.9: 在域 $\mathbb{F}_{23}$ 上分解 $f(x)=x^6-3x^5+5x^4-9x^3-5x^2+6x+7$. 由于 $\gcd(f(x),f'(x))=1$, 所以 $f(x)$ 在 $\mathbb{F}_{23}$ 上没有重因式, 利用 Berlekamp 算法我们得到 $f(x)$ 在 $\mathbb{F}_{23}$ 上有 3 个不同的首一不可约因式, 解对应的齐次方程组我们还可求出一个 f-约化多项式 $h(x)=x^3+2x^2+4x\in\mathbb{F}_{23}[x]$. 容易算出 $h(x)^2\equiv 7x^5+7x^4+2x^3-2x^2-6x-7\,(\mathrm{mod}\ f(x))$, 由此得到 $1,h(x),h(x)^2(\mathrm{mod}\ f(x))$ 在 $\mathbb{F}_{23}$ 上线性无关. 又 $h(x)^3\equiv -11x^5-11x^4-x^3-9x^2-5x-2\,(\mathrm{mod}\ f(x))$, 我们得到

$$h(x)^3\equiv 10-11h(x)+5h(x)^2\,(\mathrm{mod}\ f(x)),$$

所以 $G(y)=y^3-5y^2+11y-10$. 下面我们需要求 $G(y)$ 在 $\mathbb{F}_{23}$ 中的根, 现在 $q=23$ 为素数, 利用上节给出的求根算法, 我们计算得到 $y^{11}\equiv 2y^2+7y+2\,(\mathrm{mod}\ G(y))$, 进一步地, 我们可以计算出 $\gcd(G(y),y^{11}+1)=y+3$, $\gcd(G(y),y^{11}-1)=y^2-8y+12$, 所以 $G(y)=(y+3)(y^2-8y+12)=(y+3)(y-2)(y-6)$, 由此得到 $G(y)$ 在 $\mathbb{F}_{23}$ 中的根为 -3, 2 和 6. 从而

$$f(x)=\gcd(f(x),h(x)+3)\cdot\gcd(f(x),h(x)-2)\cdot\gcd(f(x),h(x)-6),$$

且上式的 3 个最大公因式均给出 $f(x)$ 的非平凡因式, 又 $f(x)$ 的互异首一不可约因式只有 3 个, 所以上式给出的一定是 $f(x)$ 的标准分解. 继续计算得到

$$\begin{aligned}\gcd(f(x),h(x)+3) &= x-4,\\ \gcd(f(x),h(x)-2) &= x^2-x-7,\\ \gcd(f(x),h(x)-6) &= x^3+2x^2+4x-6,\end{aligned}$$

最后我们得到 $f(x)$ 在 $\mathbb{F}_{23}$ 上的标准分解式为

$$f(x)=(x-4)(x^2-x+7)(x^3+2x^2+4x-6).$$

□

如上我们给出分解多项式的 Berlekamp 算法的一个修正使得它可以应用到 q 很大的有限域 $\mathbb{F}_q$ 上, 这可以应用到上节计算多项式根的情形 3, 那时 $q = p^m$, p 是一个大素数. 我们需要在素域 $\mathbb{F}_p$ 上分解多项式 $F(x)$, 由本节的修正, 就需要求出多项式 $R(f(x), h(x) - y)$ 或者 $G(y)$ 在 $\mathbb{F}_p$ 中的根, 这又转为上节计算多项式根的情形 1. 给出 $F(x)$ 在 $\mathbb{F}_p$ 上的标准分解式后, 利用上节给出的算法就可以进行下去了.

本节的最后我们给出另一种得到多项式部分分解的方法. 设首一多项式 $f(x) \in \mathbb{F}_q[x]$ 无重因式且 $\deg f(x) = n$, 对于任意正整数 i, 定义 $g_i(x)$ 为 $\mathbb{F}_q$ 上 $f(x)$ 的所有首一 i 次不可约因式的乘积, 若 $f(x)$ 在 $\mathbb{F}_q$ 上无 i 次不可约因式, 则定义 $g_i(x) = 1$, 由此我们有 $f(x)$ 的部分分解

$$f(x) = \prod_{i=1}^{n} g_i(x).$$

下面我们来计算这些多项式 $g_i(x)$. 对任意 $i \geq 0$, 递归地构造多项式 $r_i(x)$, $d_{i+1}(x)$ 和 $F_i(x)$ 如下: $r_0(x) = x$, $F_0(x) = f(x)$, 当 $i \geq 1$ 时定义

$$\begin{aligned} r_i(x) &\equiv r_{i-1}(x)^q \pmod{F_{i-1}(x)} \text{ 且 } \deg r_i(x) < \deg F_{i-1}(x), \\ d_i(x) &= \gcd(F_{i-1}(x), r_i(x) - x), \\ F_i(x) &= \tfrac{F_{i-1}(x)}{d_i(x)}, \end{aligned}$$

若有某个 i 使得 $d_i(x) = F_{i-1}(x)$, 则不需要继续计算了.

定理 7.17: 在如上递归构造下, 对任意 $i \geq 1$, 我们有 $g_i(x) = d_i(x)$.

证明: 由于 $F_i(x) \mid F_{i-1}(x)$, 对 i 做归纳容易得到对任意 $i \geq 1$, 有

$$r_i(x) \equiv x^{q^i} \pmod{F_{i-1}(x)}. \tag{7.15}$$

下面我们对 i 做归纳来证明对任意 $i \geq 1$, 有 $F_{i-1}(x) = \prod_{j \geq i} g_j(x)$ 且 $d_i(x) = g_i(x)$. 当 $i = 1$ 时, 显然有 $F_0(x) = f(x) = \prod_{j \geq 1} g_j(x)$. 进一步地, 由式 (7.15) 有

$$d_1(x) = \gcd(F_0(x), r_1(x) - x) = \gcd(f(x), x^q - x),$$

由于 $x^q - x = \prod_{s \in \mathbb{F}_q} (x - s)$, 所以 $d_1(x)$ 就是 $f(x)$ 的所有 $\mathbb{F}_q$ 上互不相同的首一一次因式的乘积, 从而 $d_1(x) = g_1(x)$. 假设结论对某个 $i \geq 1$ 成立, 我们来考察 $i + 1$ 的情形. 首先我们有

$$F_i(x) = \frac{F_{i-1}(x)}{d_i(x)} = \frac{\prod_{j \geq i} g_j(x)}{g_i(x)} = \prod_{j \geq i+1} g_j(x).$$

进一步地,

$$d_{i+1}(x) = \gcd(F_i(x), r_{i+1}(x) - x) = \gcd(F_i(x), x^{q^{i+1}} - x),$$

由于 $x^{q^{i+1}} - x$ 是 $\mathbb{F}_q$ 上所有次数整除 $i + 1$ 的首一不可约多项式的乘积, 所以 $d_{i+1}(x)$ 是 $\mathbb{F}_q$ 上所有次数整除 $i + 1$ 的 $F_i(x)$ 的首一不可约因式的乘积, 再由 $F_i(x) = \prod_{j \geq i+1} g_j(x)$ 得到 $d_{i+1}(x) = g_{i+1}(x)$, 从而结论对 $i + 1$ 成立. 由归纳法原理结论对任意 $i \geq 1$ 成立. □

在上面的的递归构造中, 我们需要计算 $r_i(x) \equiv r_{i-1}(x)^q \pmod{F_{i-1}(x)}$, 当然我们可以利用平方乘算法来计算方幂, 然而在分解多项式的 Berlekamp 算法中求出的矩阵 B 也

可以帮助我们来做这个运算. 事实上, Berlekamp 算法中的矩阵 B 满足 $(1, x^q, \cdots, x^{(n-1)q}) \equiv (1, x, \ldots, x^{n-1})B \pmod{f(x)}$, 即 B 为Frobenius 映射 $\alpha \mapsto \alpha^q \pmod{f(x)}$ 在基 $\{1, x, \ldots, x^{n-1}\}$ 下的矩阵. 设 $r_{i-1}(x) = \sum_{j=0}^{n-1} r_{i-1}^{(j)} x^j$, 则

$$r_{i-1}(x)^q = \sum_{j=0}^{n-1} r_{i-1}^{(j)} x^{jq} \equiv (1, x, \ldots, x^{n-1})B(r_{i-1}^{(0)}, r_{i-1}^{(1)}, \cdots, r_{i-1}^{(n-1)})^T \pmod{f(x)},$$

令

$$(s_i^{(0)}, s_i^{(1)}, \cdots, s_i^{(n-1)})^T = B(r_{i-1}^{(0)}, r_{i-1}^{(1)}, \cdots, r_{i-1}^{(n-1)})^T \text{ 和 } s_i(x) = \sum_{j=0}^{n-1} s_i^{(j)} x^j, \tag{7.16}$$

则有 $r_{i-1}(x)^q \equiv s_i(x) \pmod{f(x)}$. 又由于 $F_{i-1}(x) \mid F_0(x) = f(x)$, 所以 $r_{i-1}(x)^q \equiv s_i(x) \pmod{F_{i-1}(x)}$, 故 $r_i(x) \equiv s_i(x) \pmod{F_{i-1}(x)}$. 从而我们在求出矩阵 B 后, 就可以利用 (7.16) 从 $r_{i-1}(x)$ 求出 $r_i(x)$ 了.

例 7.10: 用如上给出的部分分解方法讨论多项式 $f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7$ 在域 $\mathbb{F}_{23}$ 上的分解. 首先可求出 Berlekamp 算法中的矩阵 B 为

$$B = \begin{pmatrix} 1 & 5 & -10 & 0 & 11 & -3 \\ 0 & 0 & 10 & 7 & 0 & 0 \\ 0 & -1 & 10 & 9 & -4 & -10 \\ 0 & 8 & 0 & -8 & 7 & 9 \\ 0 & -3 & 1 & 10 & 7 & 2 \\ 0 & -10 & -9 & -11 & 2 & -9 \end{pmatrix}.$$

由 $r_0(x) = x$ 和 $F_0(x) = f(x)$ 开始, 利用 (7.16) 求出 $s_1(x) = -10x^5 - 3x^4 + 8x^3 - x^2 + 5$, 模 $F_0(x)$ 得到 $r_1(x) = s_1(x)$, 所以可求出 $g_1(x) = d_1(x) = \gcd(F_0(x), r_1(x) - x) = x - 4$ 和 $F_1(x) = \frac{F_0(x)}{d_1(x)} = x^5 + x^4 + 9x^3 + 4x^2 + 11x + 4$.

接下来继续利用 (7.16) 可求出 $s_2(x) = 5x^5 - 8x^4 + 9x^3 - 10x^2 - 11$, 模 $F_1(x)$ 得到 $r_2(x) = 10x^4 + 10x^3 - 7x^2 - 9x - 8$, 由此计算出 $g_2(x) = d_2(x) = \gcd(F_1(x), r_2(x) - x) = x^2 - x - 7$ 和 $F_2(x) = x^3 + 2x^2 + 4x - 6$. 由定理 7.17 的证明知道 $F_2(x)$ 的每个不可约因式的次数都至少为 3, 所以这时 $F_2(x)$ 一定在 $\mathbb{F}_{23}$ 上不可约, 从而 $g_3(x) = F_2(x)$, 由此我们得到 $f(x)$ 的一个部分分解为

$$f(x) = (x - 4)(x^2 - x + 7)(x^3 + 2x^2 + 4x - 6).$$

又由 $\operatorname{rank}(B - I) = 3$ 知道 $f(x)$ 的互异首一不可约因式有 $6 - 3 = 3$ 个, 所以上式给出的也是 $f(x)$ 的标准分解式. □

7.5 二次型

有限域 $\mathbb{F}_q$ 上的一个 n 元二次型即 $\mathbb{F}_q$ 上的一个 n 元 2 次齐次多项式 (为方便起见, 我们也

称零多项式 0 为二次型), 即二次型 $f(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q[x_1,x_2,\ldots,x_n]$ 形如

$$f(x_1,x_2,\ldots,x_n)=\sum_{1\le i\le j\le n}b_{ij}x_ix_j,$$

其中 $b_{ij}\in\mathbb{F}_q$, $1\le i\le j\le n$. 对任意 $b\in\mathbb{F}_q$, 下面我们讨论方程 $f(x_1,x_2,\ldots,x_n)=b$ (或多项式 $f(x_1,x_2,\ldots,x_n)-b$) 在 $\mathbb{F}_q^n$ 中解的个数, 其中 $f(x_1,x_2,\ldots,x_n)$ 为 $\mathbb{F}_q$ 上的一个二次型, 用 $N_q(f(x_1,x_2,\ldots,x_n)=b)$ 来表示这个解数. 我们需要区分 q 为奇数或偶数这两种情形来讨论.

首先假设 q 为奇素数幂. 对 $1\le i\le n$, 令 $a_{ii}=b_{ii}$, 而对任意 $1\le i<j\le n$, 令 $a_{ij}=a_{ji}=\frac{1}{2}b_{ij}$, 则二次型 $f(x_1,x_2,\ldots,x_n)$ 可以表示为

$$f(x_1,x_2,\ldots,x_n)=\sum_{i,j=1}^{n}a_{ij}x_ix_j. \tag{7.17}$$

记 $A=(a_{ij})_{1\le i,j\le n}$, 并称 A 为二次型 $f(x_1,x_2,\ldots,x_n)$ 的系数矩阵. 显然二次型的系数矩阵是对称矩阵且每个二次型被它的系数矩阵唯一确定, 用 $\mathbf{x}$ 表示未定元 $x_1,x_2,\ldots,x_n$ 做成的列向量, 则二次型可由其系数矩阵表为 $f(x_1,x_2,\ldots,x_n)=\mathbf{x}^TA\mathbf{x}$. 定义二次型 f 的秩和行列式为它的系数矩阵 A 的秩和行列式, 分别记为 $\mathrm{rank}(f)$ 和 $\det(f)$, 秩为 n 的二次型称为非退化的二次型, 显然二次型 f 非退化当且仅当 $\det(f)\neq 0$.

设 $y_1,y_2,\ldots,y_n$ 为一组新的未定元, 设 $\mathbf{y}$ 为这些新未定元 $y_1,y_2,\ldots,y_n$ 做成的列向量, 设 C 是域 $\mathbb{F}_q$ 上的一个可逆矩阵, 称 $\mathbf{x}=C\mathbf{y}$ 为未定元的可逆线性替换. 对于 $\mathbb{F}_q$ 上的两个二次型 f 和 g, 若存在一个可逆线性替换把 f 变成 g, 则称二次型 f 与 g 等价, 并记为 $f\sim g$, 容易验证关系 $\sim$ 是 $\mathbb{F}_q$ 上二次型集合上的一个等价关系. 进一步地, 对于 $\mathbb{F}_q$ 上的两个 n 阶矩阵 A 和 B, 若存在 $\mathbb{F}_q$ 上的一个可逆矩阵 C 使得 $C^TAC=B$, 则称矩阵 A 与 B 合同. 设二次型 f 和 g 的系数矩阵分别为 A 和 B, 若二次型 f 与 g 等价, 可逆线性替换 $\mathbf{x}=C\mathbf{y}$ 把 f 变成 g, 则有 $g=(C\mathbf{y})^TA(C\mathbf{y})=\mathbf{y}^T(C^TAC)\mathbf{y}$, 由于 A 对称, 所以 C^TAC 仍为对称矩阵, 所以 g 的系数矩阵为 $B=C^TAC$, 从而 A 与 B 合同. 反之, 若矩阵 A 与 B 合同, 且可逆矩阵 C 满足 $C^TAC=B$, 则可逆线性替换 $\mathbf{x}=C\mathbf{y}$ 就把 f 变成 g, 从而 f 与 g 等价. 这样我们便证明了两个二次型等价当且仅当它们的系数矩阵合同, 从而若 $f\sim g$, 则 $\mathrm{rank}(f)=\mathrm{rank}(g)$, 且 $\det(f)$ 与 $\det(g)$ 相差一个 $\mathbb{F}_q$ 中非零平方元的倍数.

设二次型 f 与 g 等价且可逆线性替换 $\mathbf{x}=C\mathbf{y}$ 把 f 变成 g. 若 $(c_1,c_2,\ldots,c_n)\in\mathbb{F}_q^n$ 是方程 $f(x_1,x_2,\ldots,x_n)=b$ 的一个解, 令 $(d_1,d_2,\cdots,d_n)^T=C^{-1}(c_1,c_2,\cdots,c_n)^T$, 则容易验证 $(d_1,d_2,\ldots,d_n)$ 是方程 $g(x_1,x_2,\ldots,x_n)=b$ 的一个解, 反之亦然, 从而方程 $f(x_1,x_2,\ldots,x_n)=b$ 和 $g(x_1,x_2,\ldots,x_n)=b$ 在 $\mathbb{F}_q^n$ 中的解数相同, 即 $N_q(f(x_1,x_2,\ldots,x_n)=b)=N_q(g(x_1,x_2,\ldots,x_n)=b)$.

类似于线性代数中的讨论, 我们可以证明如下定理.

定理 7.18: 设 q 为奇素数幂, $f(x_1,x_2,\ldots,x_n)$ 为 $\mathbb{F}_q$ 上的二次型, 则 f 等价于一个只含有平方项的二次型 $g(x_1,x_2,\ldots,x_n)=a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2$. □

只含有平方项的二次型的系数矩阵是对角矩阵, 若 f 等价于一个只含有平方项的二次型, 则这个只含有平方项的二次型称为 f 的一个标准形. 另外定理 7.18 给出的标准形中的某些系数 a_i 有可能为 0, 又显然其中非零的 a_i 的个数等于 $\mathrm{rank}(f)$. 设 $\mathrm{rank}(f)=k$, 则 $f(x_1,x_2,\dots,x_n)\sim a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2$, 其中 $a_i\in\mathbb{F}_q^*$, $1\le i\le k$. 对任意 $b\in\mathbb{F}_q$, $N_q(f(x_1,x_2,\dots,x_n)=b)=N_q(a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2=b)$, 若 $k<n$, 则由于 $x_{k+1},\dots,x_n$ 可以任取, 我们有方程 $a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2=b$ 在 $\mathbb{F}_q^n$ 中的解的个数等于 $a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2=b$ 在 $\mathbb{F}_q^k$ 中的解的个数的 q^{n-k} 倍, 所以下面我们只考虑 $k=n$, 即 f 非退化的情形.

在 $\mathbb{F}_q$ 上定义两个整数值函数 η 和 υ 如下: 对任意 $b\in\mathbb{F}_q$, 定义 $\eta(b)=b^{\frac{q-1}{2}}$ 和 $\upsilon(b)=-1$ 若 $b\in\mathbb{F}_q^*$ 及 $\upsilon(0)=q-1$. 从而 $\eta(0)=0$, 若 b 为非零平方元则 $\eta(b)=1$ 而若 b 为非平方元则 $\eta(b)=-1$, 容易验证 η 保持乘法, 即 η 是群 $\mathbb{F}_q^*$ 到乘法群 $\{1,-1\}$ 的群同态且 $\sum_{b\in\mathbb{F}_q}\eta(b)=0$. 对函数 υ 我们有如下结论.

引理 7.19: 域 $\mathbb{F}_q$ 上的整数值函数 υ 满足

$$\sum_{c\in\mathbb{F}_q}\upsilon(c)=0$$

且对任意 $b\in\mathbb{F}_q$ 有

$$\sum_{c_1+\cdots+c_m=b}\upsilon(c_1)\cdots\upsilon(c_k)=\begin{cases}0, & \text{若 } 1\le k<m,\\ \upsilon(b)q^{m-1}, & \text{若 } k=m,\end{cases}\tag{7.18}$$

其中求和式跑遍所有满足 $c_1+\cdots+c_m=b$ 的 $c_1,\dots,c_m\in\mathbb{F}_q$.

证明: 等式 $\sum_{c\in\mathbb{F}_q}\upsilon(c)=0$ 由定义可显然得到. 下面证明式 (7.18), 若 $1\le k<m$, 我们有

$$\begin{aligned}\sum_{c_1+\cdots+c_m=b}\upsilon(c_1)\cdots\upsilon(c_k) &= \sum_{c_1,\dots,c_k\in\mathbb{F}_q}\upsilon(c_1)\cdots\upsilon(c_k)\sum_{c_{k+1}+\cdots+c_m=b-c_1-\cdots-c_k}1\\ &= q^{m-k-1}\sum_{c_1,\dots,c_k\in\mathbb{F}_q}\upsilon(c_1)\cdots\upsilon(c_k)\\ &= q^{m-k-1}\left(\sum_{c_1\in\mathbb{F}_q}\upsilon(c_1)\right)\cdots\left(\sum_{c_k\in\mathbb{F}_q}\upsilon(c_k)\right)=0.\end{aligned}$$

若 $k=m$, 我们对 m 做归纳, $m=1$ 是平凡的, 设结论对 $m\ge1$ 成立, 则对情形 $m+1$, 由前面已经证明的 $k<m$ 的结论, 我们有

$$\sum_{c_1+\cdots+c_m+c_{m+1}=b}\upsilon(c_1)\cdots\upsilon(c_m)\upsilon(c_{m+1})=\sum_{c_1+\cdots+c_m+c_{m+1}=b}\upsilon(c_1)\cdots\upsilon(c_m)[\upsilon(c_{m+1})+1],$$

其中 $c_1,\dots,c_m$ 可以任取, 而 $c_{m+1}=b-c_1-\cdots-c_m$, 所以若 $b\ne c_1+\cdots+c_m$, 则有 $\upsilon(c_{m+1})+1=0$, 而若 $b=c_1+\cdots+c_m$, 则有 $\upsilon(c_{m+1})+1=q$, 从而

$$\sum_{c_1+\cdots+c_m+c_{m+1}=b}\upsilon(c_1)\cdots\upsilon(c_m)\upsilon(c_{m+1})=q\sum_{c_1+\cdots+c_m=b}\upsilon(c_1)\cdots\upsilon(c_m),$$

再由归纳假设, 我们得到 $\sum_{c_1+\cdots+c_m+c_{m+1}=b}\upsilon(c_1)\cdots\upsilon(c_m)\upsilon(c_{m+1})=\upsilon(b)q^m$, 故结论对 $m+1$ 也成立. 由归纳法原理得到式 (7.18) 在 $k=m$ 时对任意正整数 m 成立. □

注意到上面定义的函数 η 只对奇特征的有限域才有 (因为需要 $2 \mid (q-1)$), 而函数 υ 的定义可以不区分 q 为奇数或者偶数, 所以引理 7.19 对任意的有限域都对.

设 q 为奇素数幂, 下面我们来计算 $N_q(a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2=b)$, 其中 $a_1,a_2,\ldots,a_n\in\mathbb{F}_q^*$, $b\in\mathbb{F}_q$. 若 $n=1$, 方程可写为 $ax^2=b$, 或写为 $x^2=a^{-1}b$. 若 $b=0$, 则方程有唯一解 $x=0$ (我们只考虑方程的互不相同的解, 不计重数), 若 $a^{-1}b$ 为非零平方元, 方程有 2 个解, 而若 $a^{-1}b$ 为非平方元, 方程无解, 把这 3 种情形综合起来可得到 $N_q(ax^2=b)=1+\eta(a^{-1}b)$. 由于 $\eta(a^{-1}b)=\eta(a^{-2}ab)=\eta(a^{-2})\eta(ab)=\eta(ab)$, 我们又有 $N_q(ax^2=b)=1+\eta(ab)$. 当 $n=2$ 时, 我们有如下结论.

引理 7.20: 设 q 为奇素数幂, $a_1,a_2\in\mathbb{F}_q^*$, $b\in\mathbb{F}_q$, 则 $N_q(a_1x_1^2+a_2x_2^2=b)=q+\upsilon(b)\eta(-a_1a_2)$.

证明: 把方程 $a_1x_1^2+a_2x_2^2=b$ 改写为 $x_1^2-ax_2^2=d$, 其中 $a=-a_1^{-1}a_2$, $d=a_1^{-1}b$. 注意到 $a=a_1^{-2}(-a_1a_2)$, 所以 $\eta(a)=\eta(-a_1a_2)$.

若 $\eta(-a_1a_2)=1$, 则 a 为 $\mathbb{F}_q$ 中非零平方元, 设 $a=s^2$, 其中 $s\in\mathbb{F}_q^*$, 则方程 $x_1^2-ax_2^2=d$ 可写为 $(x_1+sx_2)(x_1-sx_2)=d$, 对任意 $d_1,d_2\in\mathbb{F}_q$ 满足 $d_1d_2=d$, 方程组

$$\begin{cases} x_1 + sx_2 = d_1, \\ x_1 - sx_2 = d_2, \end{cases} \tag{7.19}$$

的解就给出方程 $x_1^2-ax_2^2=d$ 的解, 反之亦然. 由于线性方程组 (7.19) 的解唯一, 所以 $N_q(x_1^2-ax_2^2=d)$ 就等于满足 $d_1d_2=d$ 的有序对 $(d_1,d_2)\in\mathbb{F}_q^2$ 的个数. 当 $d=0$ 时, 若 $d_1=0$, 则 d_2 可以任取, 即 d_2 有 q 种取法, 若 $d_1\neq0$, 则 $d_2=0$, 即取法唯一, 所以满足 $d_1d_2=0$ 的 $(d_1,d_2)\in\mathbb{F}_q^2$ 的个数为 $q+(q-1)=2q-1$, 从而 $N_q(x_1^2-ax_2^2=0)=2q-1$. 当 $d\neq0$ 时, $d_1\neq0$, 故 d_1 有 $q-1$ 种取法, 而当 $d_1\in\mathbb{F}_q^*$ 给定后, $d_2=d_1^{-1}d$ 是被 d_1 唯一确定的, 所以满足 $d_1d_2=d$ 的 $(d_1,d_2)\in\mathbb{F}_q^2$ 的个数为 $q-1$, 即 $N_q(x_1^2-ax_2^2=d)=q-1$. 由于 $d=0$ 当且仅当 $b=0$, 把两种情形综合起来就有 $N_q(x_1^2-ax_2^2=d)=q+\upsilon(b)$.

若 $\eta(-a_1a_2)=-1$, 则 a 为 $\mathbb{F}_q$ 中非平方元, 从而 x^2-a 在 $\mathbb{F}_q$ 上不可约. 设 $\alpha\in\mathbb{F}_{q^2}$ 是 x^2-a 的一个根, 则有 $x^2-a=(x-\alpha)(x-\alpha^q)$, 从而 $x_1^2-ax_2^2=(x_1-\alpha x_2)(x_1-\alpha^qx_2)$. 对任意 $c_1,c_2\in\mathbb{F}_q$,

$$c_1^2-ac_2^2=(c_1-\alpha c_2)(c_1-\alpha^qc_2)=(c_1-\alpha c_2)(c_1-\alpha c_2)^q=(c_1-\alpha c_2)^{q+1},$$

令 $\gamma=c_1-\alpha c_2$, 所以方程 $x_1^2-ax_2^2=d$ 在 $\mathbb{F}_q^2$ 中的解 (c_1,c_2) 对应着 $x^{q+1}=d$ 在 $\mathbb{F}_{q^2}$ 中的解 $\gamma=c_1-\alpha c_2$, 由于 $1,\alpha$ 在 $\mathbb{F}_q$ 上线性无关, 这个对应是一一对应, 所以 $N_q(x_1^2-ax_2^2=d)$ 就是 $x^{q+1}=d$ 在 $\mathbb{F}_{q^2}$ 中的解的个数. 注意到对于 $\gamma\in\mathbb{F}_{q^2}$, $\gamma^{q+1}=\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\gamma)$, 由第 3.1 节我们知道 0 在 $\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ 下的原像为 0, 而对任意 $d\neq0$, d 在 $\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ 下的原像有 $\frac{q^2-1}{q-1}=q+1$ 个, 从而 $N_q(x_1^2-ax_2^2=0)=1$, 而对 $d\neq0$, $N_q(x_1^2-ax_2^2=d)=q+1$, 把两种情形综合起来就有 $N_q(x_1^2-ax_2^2=d)=q-\upsilon(d)=q-\upsilon(b)$.

综合 $\eta(-a_1a_2)=1$ 和 $\eta(-a_1a_2)=-1$ 这两种情形, 我们有 $N_q(a_1x_1^2+a_2x_2^2=b)=q+\upsilon(b)\eta(-a_1a_2)$. □

下面考虑一般的 n, 若 n 为偶数, 设 $m=\frac{n}{2}$, 则由引理 7.19 和 7.20 有

$$\begin{aligned}
& N_q(a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2=b)\\
= & \sum_{c_1+\cdots+c_m=b} N_q(a_1x_1^2+a_2x_2^2=c_1)\cdots N_q(a_{n-1}x_{n-1}^2+a_2x_2^2=c_m)\\
= & \sum_{c_1+\cdots+c_m=b} [q+\upsilon(c_1)\eta(-a_1a_2)]\cdots[q+\upsilon(c_m)\eta(-a_{n-1}a_n)]\\
= & q^{m-1}q^m+\eta((-1)^m a_1a_2\cdots a_n)\sum_{c_1+\cdots+c_m=b}\upsilon(c_1)\cdots\upsilon(c_m)\\
= & q^{n-1}+\upsilon(b)q^{\frac{n}{2}-1}\eta((-1)^{\frac{n}{2}}a_1a_2\cdots a_n).
\end{aligned}$$

若 n 为奇数, 利用未定元个数为偶数的结果, 我们有

$$\begin{aligned}
& N_q(a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2=b)\\
= & \sum_{c_1+c_2=b} N_q(a_1x_1^2=c_1)N_q(a_2x_2^2+\cdots+a_nx_n^2=c_2)\\
= & \sum_{c_1+c_2=b} [1+\eta(a_1c_1)][q^{n-2}+\upsilon(c_2)q^{\frac{n-1}{2}-1}\eta((-1)^{\frac{n-1}{2}}a_2\cdots a_n)]\\
= & q^{n-1}+q^{\frac{n-3}{2}}\eta((-1)^{\frac{n-1}{2}}a_1a_2\cdots a_n)\sum_{c_1+c_2=b}\eta(c_1)\upsilon(c_2).
\end{aligned}$$

注意到

$$\sum_{c_1+c_2=b}\eta(c_1)\upsilon(c_2)=\sum_{c\in\mathbb{F}_q}\eta(c)\upsilon(b-c)=\eta(b)(q-1)-\sum_{c\in\mathbb{F}_q,c\neq b}\eta(c)=q\eta(b)-\sum_{c\in\mathbb{F}_q}\eta(c)=q\eta(b),$$

所以

$$N_q(a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2=b)=q^{n-1}+q^{\frac{n-1}{2}}\eta((-1)^{\frac{n-1}{2}}ba_1a_2\cdots a_n).$$

注意到二次型 $a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2$ 的行列式为 $a_1a_2\cdots a_n$, 对于任意的非退化二次型 $f(x_1,x_2,\ldots,x_n)$, 若 $f(x_1,x_2,\ldots,x_n)\sim a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2$, 则 $\det(f)$ 与 $a_1a_2\cdots a_n$ 相差 $\mathbb{F}_q$ 中非零平方元的倍数, 从而 $\eta(a_1a_2\cdots a_n)=\eta(\det(f))$. 综合上面的讨论, 我们有如下定理.

定理 7.21: 设 q 为奇素数幂, $f(x_1,x_2,\ldots,x_n)$ 是 $\mathbb{F}_q$ 上的一个非退化二次型, 则对 $b\in\mathbb{F}_q$, 方程 $f(x_1,x_2,\ldots,x_n)=b$ 在 $\mathbb{F}_q^n$ 中的解的个数为

$$N_q(f(x_1,x_2,\ldots,x_n)=b)=\begin{cases} q^{n-1}+\upsilon(b)q^{\frac{n}{2}-1}\eta((-1)^{\frac{n}{2}}\det(f)), & \text{若 } n \text{ 为偶数},\\ q^{n-1}+q^{\frac{n-1}{2}}\eta((-1)^{\frac{n-1}{2}}b\det(f)), & \text{若 } n \text{ 为奇数}. \end{cases}$$

□

下面考察 q 为 2 的方幂的情形, 此时设二次型 $f(x_1,x_2,\ldots,x_n)$ 依然形如

$$f(x_1,x_2,\ldots,x_n)=\sum_{1\le i\le j\le n}b_{ij}x_ix_j,$$

其中 $b_{ij}\in\mathbb{F}_q$, $1\le i\le j\le n$. 这时在域 $\mathbb{F}_q$ 中有 $2=0$, 所以我们没办法把 f 用一个对称矩阵来表示, 也不能通过配方消去 f 的交叉项. 但是在域 $\mathbb{F}_q$ 中, 每个元素都是平方元, 对于任意 $a\in\mathbb{F}_q$, a 的唯一平方根为 $a^{\frac{q}{2}}$. 与前面一样我们可以定义未定元之间的可逆线性替换以及二次型等价的概念, 为了求方程 $f(x_1,x_2,\ldots,x_n)=b$ 在 $\mathbb{F}_q^n$ 中的解的个数, 我们要考察在可逆线性

替换下, $f(x_1,x_2,\ldots,x_n)$ 可以化成什么样的形式简单的二次型 (即 f 等价于什么样的形式简单的二次型)? 与前面一样, 我们依然讨论非退化二次型, 这里 $f(x_1,x_2,\ldots,x_n)$ 非退化指的是不存在可逆线性替换把 f 变成未定元个数少于 n 个的二次型 (因这时没有定义二次型的系数矩阵, 所以不能用前面的定义了).

引理 7.22: 设 $q=2^s$, $f(x_1,x_2,\ldots,x_n)$ 是 $\mathbb{F}_q$ 上一个非退化 n 元二次型, $n\geq 3$, 则 f 等价于 $x_1x_2+g(x_3,\ldots,x_n)$, 其中 $g(x_3,\ldots,x_n)$ 为 $\mathbb{F}_q$ 上一个非退化 $n-2$ 元二次型.

证明: 我们先证明 f 等价于一个 x_1^2 项系数为 0 的二次型. 设 $f(x_1,x_2,\ldots,x_n)=\sum_{1\leq i\leq j\leq n}b_{ij}x_ix_j$, 若存在某个 $b_{ii}=0$, 则交换未定元 x_1 和 x_i, 而其它未定元不动 (这自然是一个可逆线性替换), 就可使 x_1^2 的系数为 0. 若对所有 $1\leq i\leq n$, 都有 $b_{ii}\neq 0$, 则一定存在某个 $b_{ij}\neq 0$, 其中 $i<j$. 事实上, 若对所有 $1\leq i<j\leq n$ 均有 $b_{ij}=0$, 则

$$f(x_1,x_2,\ldots,x_n)=b_{11}x_1^2+b_{22}x_2^2+\cdots+b_{nn}x_n^2=(b_{11}^{\frac{q}{2}}x_1+b_{22}^{\frac{q}{2}}x_2+\cdots+b_{nn}^{\frac{q}{2}}x_n)^2=y_1^2,$$

这与 f 非退化矛盾. 由于我们可以交换未定元, 不失一般性, 我们假设 $b_{23}\neq 0$. 把 f 中包含 x_2 的项分离出来, 我们有

$$f(x_1,x_2,\ldots,x_n)=b_{22}x_2^2+x_2(b_{12}x_1+b_{23}x_3+\cdots+b_{2n}x_n)+g_1(x_1,x_3,\ldots,x_n),$$

令 $x_3=b_{23}^{-1}(b_{12}y_1+y_3+b_{24}y_4+\cdots+b_{2n}y_n)$, 且对 $i\neq 3$, 令 $x_i=y_i$, 则在此可逆线性替换下 $f(x_1,x_2,\ldots,x_n)$ 变成

$$f_1(y_1,y_2,\ldots,y_n)=b_{22}y_2^2+y_2y_3+g_2(y_1,y_3,\ldots,y_n).$$

设在二次型 g_2 中 y_1^2 的系数为 c_{11}, 则令 $y_2=(b_{22}^{-1}c_{11})^{\frac{q}{2}}z_1+z_2$, 且对 $i\neq 2$, 令 $y_i=z_i$, 则在此可逆线性替换下 $f_1(y_1,y_2,\ldots,y_n)$ 变成一个二次型, 其 z_1^2 的系数为 0.

现在设 $f(x_1,x_2,\ldots,x_n)=\sum_{1\leq i\leq j\leq n}b_{ij}x_ix_j$ 且 $b_{11}=0$, 因为 f 非退化, 一定存在某个 j 使得 $b_{1j}\neq 0$, $2\leq j\leq n$. 不妨设 $b_{12}\neq 0$, 则令 $x_2=b_{12}^{-1}(y_2+b_{13}y_3+\cdots+b_{1n}y_n)$, 且对 $i\neq 2$, 令 $x_i=y_i$, 则在此可逆线性替换下 $f(x_1,x_2,\ldots,x_n)$ 变成

$$f_2(y_1,y_2,\ldots,y_n)=y_1y_2+c_{22}y_2^2+c_{23}y_2y_3+\cdots+c_{2n}y_2y_n+g_3(y_3,\ldots,y_n).$$

令 $y_1=z_1+c_{22}z_2+\cdots+c_{2n}z_n$, 且对 $i\neq 1$, 令 $y_i=z_i$, 则在此可逆线性替换下 $f_2(y_1,y_2,\ldots,y_n)$ 变成 $z_1z_2+g(z_3,\ldots,z_n)$. 再由 f 非退化立得 g 非退化. □

由引理 7.22, 继续下去我们可以得到, 若 n 为奇数, 则非退化二次型 $f(x_1,x_2,\ldots,x_n)$ 等价于 $x_1x_2+x_3x_4+\cdots+x_{n-2}x_{n-1}+ax_n^2$, 其中 $a\in\mathbb{F}_q^*$, 令 $a^{-\frac{q}{2}}x_n$ 替换 x_n, 其它未定元不变, 我们可得 $f(x_1,x_2,\ldots,x_n)$ 等价于 $x_1x_2+x_3x_4+\cdots+x_{n-2}x_{n-1}+x_n^2$. 若 n 为偶数, 则非退化二次型 $f(x_1,x_2,\ldots,x_n)$ 等价于 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+g(x_{n-1},x_n)$, 其中 $g(x_{n-1},x_n)$ 非退化. 设 $g(x_{n-1},x_n)=bx_{n-1}^2+cx_{n-1}x_n+dx_n^2$, 由于 $g(x_{n-1},x_n)$ 非退化, 故 $c\neq 0$. 若 $b=0$, 则 $g(x_{n-1},x_n)=(cx_{n-1}+dx_n)x_n$, 则有 $g(x_{n-1},x_n)\sim x_{n-1}x_n$, 故 $f(x_1,x_2,\ldots,x_n)$ 等价于 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}x_n$. 若 $b\neq 0$, 用 $b^{-\frac{q}{2}}x_{n-1}$ 替换 x_{n-1}, $b^{\frac{q}{2}}c^{-1}x_n$ 替换 x_n, 则 $g(x_{n-1},x_n)$ 变成 $x_{n-1}^2+x_{n-1}x_n+ax_n^2$, 其中 $a=dbc^{-2}$. 进一

步地, 若 x^2+x+a 在 $\mathbb{F}_q$ 上可约, 则存在 $c_1,c_2\in\mathbb{F}_q$ 使得 $x^2+x+a=(x+c_1)(x+x_2)$, 从而 $x_{n-1}^2+x_{n-1}x_n+ax_n^2=(x_{n-1}+c_1x_n)(x_{n-1}+c_2x_n)$ 等价于 $x_{n-1}x_n$, 故这时依然有 $f(x_1,x_2,\dots,x_n)$ 等价于 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}x_n$. 若 x^2+x+a 在 $\mathbb{F}_q$ 上不可约, 即 x^2+x+a 在 $\mathbb{F}_q$ 上无根, 由定理 3.6 得这当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a)=1$. 这样我们证明了如下定理.

定理 7.23: 设 $q=2^s$, $f(x_1,x_2,\dots,x_n)$ 是 $\mathbb{F}_q$ 上一个非退化 n 元二次型. 若 n 为奇数, 则 $f(x_1,x_2,\dots,x_n)$ 等价于

$$x_1x_2+x_3x_4+\cdots+x_{n-2}x_{n-1}+x_n^2.$$

若 n 为偶数, 则 $f(x_1,x_2,\dots,x_n)$ 等价于

$$x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}x_n$$

或者

$$x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}^2+x_{n-1}x_n+ax_n^2,$$

其中 $a\in\mathbb{F}_q$ 满足 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a)=1$. □

我们依然利用 $\mathbb{F}_q$ 上的整数值函数 υ, 它的定义为 $\upsilon(0)=q-1$ 且对 $b\in\mathbb{F}_q^*$ 有 $\upsilon(b)=-1$, 这时引理 7.19 的结论依然成立, 类似于引理 7.20 的证明, 我们有如下结论.

引理 7.24: 设 $q=2^s$, $a\in\mathbb{F}_q$ 且 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a)=1$, 则对任意 $b\in\mathbb{F}_q$, 我们有方程 $x_1x_2=b$ 和 $x_1^2+x_1x_2+ax_2^2=b$ 在 $\mathbb{F}_q^2$ 中解的个数分别为 $N_q(x_1x_2=b)=q+\upsilon(b)$ 和 $N_q(x_1^2+x_1x_2+ax_2^2=b)=q-\upsilon(b)$. □

下面我们来求定理 7.23 中的三类非退化二次型对应的方程在 $\mathbb{F}_q^n$ 中的解数. 设 $b\in\mathbb{F}_q$, 首先考虑方程 $x_1x_2+x_3x_4+\cdots+x_{n-2}x_{n-1}+x_n^2=b$. 在此方程中, $x_1,x_2,\dots,x_{n-1}$ 可在 $\mathbb{F}_q$ 中任意选取, 当 $x_1,x_2,\dots,x_{n-1}$ 选定后, 由 $x_n^2=b+x_1x_2+x_3x_4+\cdots+x_{n-2}x_{n-1}$ 可确定唯一的 x_n 的值, 从而

$$N_q(x_1x_2+x_3x_4+\cdots+x_{n-2}x_{n-1}+x_n^2=b)=q^{n-1}.$$

上面是 n 为奇数的情形, 接下来考虑 n 为偶数的情形, 令 $m=\frac{n}{2}$. 对方程 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}x_n=b$, 我们有

$$\begin{aligned}
& N_q(x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}x_n=b)\\
=\ & \sum_{c_1+c_2+\cdots+c_m=b} N_q(x_1x_2=c_1)N_q(x_3x_4=c_2)\cdots N_q(x_{n-1}x_n=c_m)\\
=\ & \sum_{c_1+c_2+\cdots+c_m=b} [q+\upsilon(c_1)][q+\upsilon(c_2)]\cdots[q+\upsilon(c_m)]\\
=\ & q^{m-1}q^m+\sum_{c_1+c_2+\cdots+c_m=b}\upsilon(c_1)\upsilon(c_2)\cdots\upsilon(c_m)\\
=\ & q^{n-1}+\upsilon(b)q^{\frac{n}{2}-1}.
\end{aligned}$$

而对方程 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}^2+x_{n-1}x_n+ax_n^2=b$, 其中 $a\in\mathbb{F}_q$ 且 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a)=1$, 我们有

$$\begin{aligned}
& N_q(x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}^2+x_{n-1}x_n+ax_n^2=b)\\
= & \sum_{c_1+\cdots+c_{m-1}+c_m=b} N_q(x_1x_2=c_1)\cdots N_q(x_{n-3}x_{n-2}=c_{m-1})N_q(x_{n-1}^2+x_{n-1}x_n+ax_n^2=c_m)\\
= & \sum_{c_1+\cdots+c_{m-1}+c_m=b} [q+\upsilon(c_1)]\cdots[q+\upsilon(c_{m-1})][q-\upsilon(c_m)]\\
= & q^{m-1}q^m-\sum_{c_1+\cdots+c_{m-1}+c_m=b}\upsilon(c_1)\upsilon(c_2)\cdots\upsilon(c_m)\\
= & q^{n-1}-\upsilon(b)q^{\frac{n}{2}-1}.
\end{aligned}$$

注意到对于 $b\in\mathbb{F}_q$, 方程 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}x_n=b$ 和 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}^2+x_{n-1}x_n+ax_n^2=b$ 在 $\mathbb{F}_q^n$ 中的解数不同, 所以这两个非退化二次型 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}x_n$ 和 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}^2+x_{n-1}x_n+ax_n^2$ 不等价. 由定理 7.23, 当 q 和 n 都是偶数时, 对于 $\mathbb{F}_q$ 上的非退化 n 元二次型 $f(x_1,x_2,\ldots,x_n)$, 若 $f(x_1,x_2,\ldots,x_n)$ 等价于 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}x_n$, 则称 $f(x_1,x_2,\ldots,x_n)$ 为 I 型二次型, 而若 $f(x_1,x_2,\ldots,x_n)$ 等价于 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}^2+x_{n-1}x_n+ax_n^2$, 其中 $a\in\mathbb{F}_q$ 且 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a)=1$, 则称 $f(x_1,x_2,\ldots,x_n)$ 为 II 型二次型. 综合上面的讨论, 我们有如下定理.

定理 7.25: 设 q 为 2 的方幂, $f(x_1,x_2,\ldots,x_n)$ 是 $\mathbb{F}_q$ 上的一个非退化 n 元二次型, 则对 $b\in\mathbb{F}_q$, 当 n 为奇数时, 方程 $f(x_1,x_2,\ldots,x_n)=b$ 在 $\mathbb{F}_q^n$ 中解的个数为

$$N_q(f(x_1,x_2,\ldots,x_n)=b)=q^{n-1},$$

而当 n 为偶数时, 方程 $f(x_1,x_2,\ldots,x_n)=b$ 在 $\mathbb{F}_q^n$ 中解的个数为

$$N_q(f(x_1,x_2,\ldots,x_n)=b)=\begin{cases} q^{n-1}+\upsilon(b)q^{\frac{n}{2}-1}, & \text{若 } f \text{ 为 I 型二次型},\\ q^{n-1}-\upsilon(b)q^{\frac{n}{2}-1}, & \text{若 } f \text{ 为 II 型二次型}. \end{cases}$$

□

7.6 习题

7.1 计算下面线性化多项式在它们分裂域中的根.

(a) $L(x)=x^8+x^4+x^2+x\in\mathbb{F}_2[x]$.
(b) $L(x)=x^9+x\in\mathbb{F}_3[x]$.

7.2 首先确定下面多项式的仿射 q-倍式, 再求出它们在给定域中的根.

(a) $f(x)=x^7+x^6+x^3+x^2+1\in\mathbb{F}_2[x]$ 在 $\mathbb{F}_{32}$ 中的根.
(b) $f(x)=x^4+\theta x^3-x^2-(\theta+1)x-\theta\in\mathbb{F}_9[x]$ 在 $\mathbb{F}_{729}$ 中的根, 其中 θ 为 $\mathbb{F}_3$ 上不可约多项式 x^2-x-1 的一个根.

7.3 证明对任意非零多项式 $f(x) \in \mathbb{F}_{q^m}[x]$, 一定存在 $\mathbb{F}_{q^m}$ 上的非零 q- 多项式 $L(x)$ 使得 $f(x) \mid L(x)$.

7.4 确定下面多项式在给定域中根的个数.

(a) $f(x) = x^5 + 2x^4 + x^2 + 1$ 在 $\mathbb{F}_5$ 中.
(b) $f(x) = x^6 - 3x^5 - x^4 + x^3 - x$ 在 $\mathbb{F}_7$ 中.

7.5 设 $f(x_1, x_2, \ldots, x_n)$ 为 $\mathbb{F}_q$ 上的多项式且 $\deg(f) < n$, 设 $f(x_1, x_2, \ldots, x_n)$ 在 $\mathbb{F}_q$ 上的 N 个解为 $(c_{i1}, c_{i2}, \ldots, c_{in}) \in \mathbb{F}_q^n$, $1 \le i \le N$, 证明对所有 $j = 1, 2, \ldots, n$ 和 $k = 0, 1, \ldots, q-2$, 均有

$$\sum_{i=1}^{N} c_{ij}^k = 0,$$

其中定义 $0^0 = 1$.

7.6 设 $f(x_1, x_2, \ldots, x_n)$ 为 $\mathbb{F}_q$ 上的齐次多项式且 $\deg(f) = d \ge 1$, 若 $f(x_1, x_2, \ldots, x_n)$ 能被某个未定元 x_i 整除, 证明 $f(x_1, x_2, \ldots, x_n)$ 在 $\mathbb{F}_q$ 上有至多 $dq^{n-1} - (d-1)q^{n-2}$ 个解.

7.7 设 $f(x_1, x_2, \ldots, x_n)$ 为 $\mathbb{F}_q$ 上的多项式且 $\deg(f) = n$, 称 $f(x_1, x_2, \ldots, x_n)$ 为范数多项式若它在 $\mathbb{F}_q$ 上只有零解 (参见例 7.4 (a)).

(a) 在 $\mathbb{F}_2$ 上具体构造一个三元范数多项式.
(b) 设 $f(x_1, x_2, \ldots, x_n)$ 为范数多项式, 证明对任意满足 $\deg(g) < n$ 的多项式 $g(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$, 多项式 $f(x_1, x_2, \ldots, x_n) - g(x_1, x_2, \ldots, x_n)$ 在 $\mathbb{F}_q$ 上有解.

7.8 求出下面二次多项式在给定域中的根.

(a) $x^2 - 219$ 在 $\mathbb{F}_{383}$ 中.
(b) $x^2 - 431$ 在 $\mathbb{F}_{1409}$ 中.

7.9 设 q 为奇素数幂, a 为 $\mathbb{F}_q$ 中的非零平方元, $b \in \mathbb{F}_q$ 满足 $b^2 - 4a$ 为 $\mathbb{F}_q$ 中非平方元, 证明 $x^{\frac{q+1}{2}} \pmod{x^2 - bx + a}$ 为 a 的平方根.

7.10 设式 (7.6) 中的多项式 $f(x-b)$ 是二次的且具有常数项 $c \ne 0$, 证明 (7.6) 中的分解是非平凡的当且仅当 c 不是 $\mathbb{F}_p$ 中平方元.

7.11 求下面多项式在给定域中的根.

(a) $f(x) = x^5 - x^4 + 2x^3 + x^2 - x - 2$ 在 $\mathbb{F}_5$ 中.
(b) $f(x) = x^5 + 6x^4 + 2x^3 - 6x^2 - 5x + 5$ 在 $\mathbb{F}_{13}$ 中.
(c) $f(x) = x^3 + 8x^2 + 6x - 7$ 在 $\mathbb{F}_{19}$ 中.
(d) $f(x) = x^3 + (\beta^4 + \beta^3 + 1)x^2 + \beta^2 x + \beta^4 + \beta^3 + \beta + 1$ 在 $\mathbb{F}_{32}$ 中, 其中 β 是 $\mathbb{F}_2$ 上不可约多项式 $x^5 + x^2 + 1$ 的一个根.

7.12 设首一多项式 $f(x) \in \mathbb{F}_q[x]$ 无重因式且 $\deg f(x) = n$, 设 $f(x) = f_1(x) f_2(x) \cdots f_k(x)$ 为 $f(x)$ 的标准分解式且 $\deg f_i(x) = n_i$, $1 \le i \le n$, 令 $t = \operatorname{lcm}(n_1, n_2, \ldots, n_k)$.

(a) 证明 t 为满足 $x^{q^t} \equiv x \pmod{f(x)}$ 的最小正整数, 也是 $f(x)$ 在 $\mathbb{F}_q$ 上的分裂域关于 $\mathbb{F}_q$ 的次数.

(b) 定义 $T(x) \in \mathbb{F}_q[x]$ 为

$$T(x) = x + x^q + x^{q^2} + \cdots + x^{q^{t-1}} \ (= \mathrm{Tr}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(x)),$$

令 $T_i(x) \equiv T(x^i) \pmod{f(x)}, i \geq 1$. 证明若 $f(x)$ 在 $\mathbb{F}_q$ 上可约, 则在 $T_1(x), T_2(x), \ldots, T_{n-1}(x)$ 中一定存在一个 f-约化多项式.

7.13 确定多项式 $f(x) = x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$ 在 $\mathbb{F}_2$ 上的分裂域.

7.14 设矩阵 B 是在 Berlekamp 算法中得到的矩阵, 证明若 $f(x)$ 在 $\mathbb{F}_q$ 上不可约, 则 B 的特征多项式 $\det(xI - B)$ 为 $x^n - 1$. 进一步地, 设 $f(x)$ 无重因式且 $f(x) = f_1(x)f_2(x)\cdots f_k(x)$ 为 $f(x)$ 在 $\mathbb{F}_q$ 上的标准分解式满足 $\deg f_i(x) = n_i$, $1 \leq i \leq n$, 则 B 的特征多项式为 $(x^{n_1} - 1)(x^{n_2} - 1)\cdots(x^{n_k} - 1)$.

7.15 在所列的域上分解下面多项式.

(a) 在 $\mathbb{F}_{13}$ 上分解 $f(x) = x^4 + 3x^3 + 4x^2 + 2x - 1$.

(b) 在 $\mathbb{F}_{17}$ 上分解 $f(x) = x^5 + 3x^4 + 2x^3 - 6x^2 + 5$.

(c) 在 $\mathbb{F}_{19}$ 上分解 $f(x) = x^3 - 6x^2 - 8x - 8$.

7.16 先用第 7.4 节最后给出的方法在 $\mathbb{F}_{11}$ 上部分分解 $f(x) = x^7 - 2x^6 - 4x^4 + 3x^3 - 5x^2 + 3x + 5$, 再接下来给出该多项式的标准分解式.

7.17 把下面二次型在给定域上化为标准形.

(a) $x_1x_2 + 2x_1x_3 - x_2x_3 \in \mathbb{F}_5[x_1, x_2, x_3]$.

(b) $2x_1^2 - 5x_2^2 + 3x_3^2 + x_1x_2 - 4x_1x_3 - 3x_2x_3 \in \mathbb{F}_{11}[x_1, x_2, x_3]$.

7.18 证明定理 7.18.

7.19 设 q 为奇素数幂, $f(x_1, x_2, \ldots, x_n)$ 是 $\mathbb{F}_q$ 上的一个非退化 n 二次型, a 为 $\mathbb{F}_q$ 中一个给定的非平方元, 证明若 $\det(f)$ 为 $\mathbb{F}_q$ 中的非零平方元, 则 $f(x_1, x_2, \ldots, x_n)$ 等价于 $x_1^2 + x_2^2 + \cdots + x_n^2$, 而若 $\det(f)$ 为 $\mathbb{F}_q$ 中的非平方元, 则 $f(x_1, x_2, \ldots, x_n)$ 等价于 $x_1^2 + x_2^2 + \cdots + x_{n-1}^2 + ax_n^2$. (这两个二次型称为 $f(x_1, x_2, \ldots, x_n)$ 的规范形.)

7.20 确定下面方程在给定域上解的个数.

(a) $2x_1^2 - x_2^2 + x_3^2 - x_1x_2 - 2x_1x_3 = 2$ 在 $\mathbb{F}_5^3$ 中.

(b) $3x_1^2 + x_3^2 - 2x_1x_2 + x_1x_3 + 3x_2x_3 = 2$ 在 $\mathbb{F}_7^3$ 中.

(c) $x_1^2 - x_2^2 + 2x_3^2 - x_1x_4 - x_2x_3 + 2x_2x_4 = 0$ 在 $\mathbb{F}_5^4$ 中.

(d) $x_1^2 + x_3^2 + x_5^2 - x_1x_2 - x_2x_3 + x_2x_4 + x_4x_5 = -1$ 在 $\mathbb{F}_3^5$ 中.

(e) $x_1^2 + 2x_2^2 - 2x_3^2 - 2x_1x_2 + x_1x_3 + 2x_2x_3 = 1$ 在 $\mathbb{F}_{25}^3$ 中.

(f) $x_1^2 - x_2^2 - x_3^2 + x_1x_2 + 2x_2x_3 - x_1 + 2x_3 = 0$ 在 $\mathbb{F}_5^3$ 中.

(g) $x_2^2 - x_3^2 + x_4^2 - x_1x_2 - x_1x_3 + x_1x_4 + x_3x_4 + x_2 + x_4 = 1$ 在 $\mathbb{F}_3^4$ 中.

7.21 推广上面习题中的 (f) 和 (g), 设 q 为奇素数幂, $f(x_1,x_2,\ldots,x_n)$ 是 $\mathbb{F}_q$ 上的一个 n 元二次多项式, 讨论 $f(x_1,x_2,\ldots,x_n)$ 在 $\mathbb{F}_q^n$ 中解的个数.

7.22 设 $f(x_1,x_2,\ldots,x_n)$ 为 $\mathbb{F}_q$ 上的一个 n 元二次型, 证明若 $n\geq 3$, 则 $f(x_1,x_2,\ldots,x_n)=0$ 在 $\mathbb{F}_q^n$ 中一定有非零解, 并且此结论对 $n\leq 2$ 并不一定成立.

7.23 设 $f(x_1,x_2,\ldots,x_n)$ 为 $\mathbb{F}_q$ 上非零二次型, $b\in\mathbb{F}_q$, 证明若有条件 (i) q 为偶数或者 (ii) q 为奇数且 $\mathrm{rank}(f)\geq 2$, 则方程 $f(x_1,x_2,\ldots,x_n)=b$ 在 $\mathbb{F}_q^n$ 中一定有解.

7.24 确定下面方程在给定域上解的个数.

(a) $x_1^2+x_2^2+x_1x_2+x_1x_3=1$ 在 $\mathbb{F}_4^3$ 中.

(b) $x_1^2+x_2^2+x_1x_3+x_1x_4+x_2x_4+x_3x_4=1$ 在 $\mathbb{F}_8^4$ 中.

(c) $\theta^2x_2^2+\theta x_4^2+x_1x_2+x_1x_3+x_1x_4+x_2x_3=\theta$ 在 $\mathbb{F}_4^4$ 中, 其中 $\theta\in\mathbb{F}_4$ 为 x^2+x+1 的根.

(d) $(\theta^2+\theta)x_2^2+x_3^2+\theta x_4^2+\theta^2x_1x_2+\theta x_1x_4+\theta x_2x_3+(\theta+1)x_2x_4=0$ 在 $\mathbb{F}_8^4$ 中, 其中 $\theta\in\mathbb{F}_8$ 为 x^3+x^2+1 的根.

7.25 设 q 为奇素数幂, $f(x_1,x_2,\ldots,x_n)$ 是 $\mathbb{F}_q$ 上的一个非退化 n 二次型, 证明当 n 为偶数时, $f(x_1,x_2,\ldots,x_n)$ 等价于 $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+x_{n-1}^2+ax_n^2$, 对某个 $a\in\mathbb{F}_q^*$, 而当 n 为奇数时, $f(x_1,x_2,\ldots,x_n)$ 等价于 $x_1x_2+x_3x_4+\cdots+x_{n-2}x_{n-1}+ax_n^2$, 对某个 $a\in\mathbb{F}_q^*$. 并利用这时的二次型的等价形式求出对任意 $b\in\mathbb{F}_q$, 方程 $f(x_1,x_2,\ldots,x_n)=b$ 在 $\mathbb{F}_q^n$ 中的解数.

7.26 证明引理 7.24.

7.27 设 q 为奇素数幂, $a_0,b_0\in\mathbb{F}_q$, $a_1,a_2,\ldots,a_n\in\mathbb{F}_q^*$, $b_1,b_2,\ldots,b_n\in\mathbb{F}_q$ 且 $b_1,b_2,\ldots,b_n$ 不全为零, 求方程组

$$\begin{cases} a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = a_0, \\ b_1x_1 + b_2x_2 + \cdots + b_nx_n = b_0 \end{cases}$$

在 $\mathbb{F}_q^n$ 中解的个数.

第八章　指数和

8.1　有限交换群的特征

设 G 为 n 阶交换群, 其单位元记为 1_G, G 的一个特征 χ 是 G 到复数域乘法群 $\mathbb{C}^*$ 的一个群同态, 即映射 $\chi : G \to \mathbb{C}^*$ 满足对任意 $g_1, g_2 \in G$, 有 $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$. 注意到用表示论的语言来说, 这里的特征就是群 G 的一级 (复) 特征标, 特别地, 有限交换群的所有不可约 (复) 特征标都是一级的, 即这里讨论的特征. 由于群同态把单位元映成单位元, 所以对任意 $g \in G$, 有 $\chi(g)^n = \chi(g^n) = \chi(1_G) = 1$, 故 $\chi(g)$ 为 n 次单位根. 进一步地, 由 $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$ 可以得到 $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$, 其中符号 "$^-$" 表示复共轭. 定义 $\chi_0 : G \to \mathbb{C}^*$ 为对任意 $g \in G$ 有 $\chi_0(g) = 1$, 则显然 χ_0 为 G 的一个特征, 称其为 G 的主特征. 给定群 G 的一个特征 χ, 定义 $\overline{\chi} : G \to \mathbb{C}^*$ 为对任意 $g \in G$ 有 $\overline{\chi}(g) = \overline{\chi(g)}$, 容易验证 $\overline{\chi}$ 也是 G 的一个特征, 称其为特征 χ 的共轭.

用 $\widehat{G}$ 表示群 G 的所有特征构成的集合. 对于 $\chi, \psi \in \widehat{G}$, 定义 $\chi\psi : G \to \mathbb{C}^*$ 为对任意 $g \in G$ 有 $\chi\psi(g) = \chi(g)\psi(g)$, 则容易验证 $\chi\psi$ 为 G 的一个特征, 称为特征 χ 和 ψ 的乘积, 故特征的乘积为 $\widehat{G}$ 中的运算, 又容易证明 $\widehat{G}$ 在此运算下构成一个交换群, 其单位元为主特征 χ_0, 而元素 χ 的逆为它的共轭 $\overline{\chi}$, 群 $\widehat{G}$ 称为群 G 的特征群, 或称为 G 的对偶群.

例 8.1: 设 $G = \langle g \rangle$ 为由元素 g 生成的 n 阶循环群, $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$ (n 次本原单位根). 对于每个 $j \geq 0$, 定义 $\chi_j(g^k) = \zeta_n^{jk}$, $0 \leq k \leq n-1$, 则对任意 $0 \leq k_1, k_2 \leq n-1$ 有

$$\chi_j(g^{k_1}g^{k_2}) = \chi_j(g^{k_1+k_2}) = \zeta_n^{j(k_1+k_2)} = \zeta_n^{jk_1}\zeta_n^{jk_2} = \chi_j(g^{k_1})\chi_j(g^{k_2}),$$

故 $\chi_j \in \widehat{G}$. 进一步地, 对于 $j_1, j_2 \geq 0$, $\chi_{j_1} = \chi_{j_2}$ 当且仅当 $\chi_{j_1}(g) = \chi_{j_2}(g)$, 即当且仅当 $\zeta_n^{j_1} = \zeta_n^{j_2}$, 这也等价于 $j_1 \equiv j_2 \pmod{n}$, 这样我们便证明了 $\chi_{j_1} = \chi_{j_2}$ 当且仅当 $j_1 \equiv j_2 \pmod{n}$. 另外对每个 $j \geq 0$, 由 $\chi_j(g) = \zeta_n^j = \chi_1(g)^j = \chi_1^j(g)$ 可得到 $\chi_j = \chi_1^j$.

另一方面, 任取 $\chi \in \widehat{G}$, 则 $\chi(g)$ 为一个 n 次单位根, 从而存在某个 j 使得 $\chi(g) = \zeta_n^j$, 其中 $0 \leq j \leq n-1$. 由于 χ 为群同态, 所以对任意 $0 \leq k \leq n-1$ 有 $\chi(g^k) = \chi(g)^k = (\zeta_n^j)^k = \zeta_n^{jk}$, 故 $\chi = \chi_j$.

综合起来我们得到 $\widehat{G} = \{\chi_0, \chi_1, \ldots, \chi_{n-1}\}$, 又 $\chi_j = \chi_1^j$, 我们有 $\widehat{G} = \langle \chi_1 \rangle$, 故 $\widehat{G}$ 仍为 n 阶

循环群, 即有 $\widehat{G}\cong G$. □

设 G_1, G_2 为有限交换群, $G=G_1\times G_2$ (群的直积), 设 $\varphi\in\widehat{G_1}$, $\psi\in\widehat{G_2}$, 定义 $\varphi\times\psi$ 为

$$\begin{aligned}\varphi\times\psi:\ G=G_1\times G_2 &\to \mathbb{C}^*\\ g=(g_1,g_2) &\mapsto \varphi(g_1)\psi(g_2),\end{aligned}$$

则对任意 $g=(g_1,g_2),h=(h_1,h_2)\in G_1\times G_2$, 有

$$\begin{aligned}(\varphi\times\psi)(gh) &= (\varphi\times\psi)(g_1h_1,g_2h_2)=\varphi(g_1h_1)\psi(g_2h_2)\\ &= (\varphi(g_1)\varphi(h_1))(\psi(g_2)\psi(h_2))=(\varphi(g_1)\psi(g_2))\cdot(\varphi(h_1)\psi(h_2))\\ &= (\varphi\times\psi)(g_1,g_2)\cdot(\varphi\times\psi)(h_1,h_2)=(\varphi\times\psi)(g)\cdot(\varphi\times\psi)(h),\end{aligned}$$

所以 $\varphi\times\psi\in\widehat{G}$. 反之, 对任意 $\chi\in\widehat{G}$, 对任意 $g_1\in G_1$, 定义 $\varphi(g_1)=\chi(g_1,1_{G_2})$, 其中 1_{G_2} 为群 G_2 的单位元. 则容易验证 $\varphi\in\widehat{G_1}$, 记 $\varphi=\chi|_{G_1}$ 并称为 χ 在 G_1 上的限制. 类似地, 对任意 $g_2\in G_2$, 定义 $\psi(g_2)=\chi(1_{G_1},g_2)$, 其中 1_{G_1} 为群 G_1 的单位元, 则 $\psi\in\widehat{G_2}$, 记 $\psi=\chi|_{G_2}$ 并称为 χ 在 G_2 上的限制. 进一步地, 对任意 $(g_1,g_2)\in G$ 有

$$\chi(g_1,g_2)=\chi((g_1,1_{G_2})(1_{G_1},g_2))=\chi(g_1,1_{G_2})\chi(1_{G_1},g_2)=\chi|_{G_1}(g_1)\chi|_{G_2}(g_2)=(\chi|_{G_1}\times\chi|_{G_2})(g_1,g_2),$$

从而 $\chi=\chi|_{G_1}\times\chi|_{G_2}$.

引理 8.1: 设 G_1, G_2 为有限交换群, $G=G_1\times G_2$, 则 $\widehat{G_1}\times\widehat{G_2}\cong\widehat{G}$.

证明: 定义映射 $\pi:\widehat{G_1}\times\widehat{G_2}\to\widehat{G}$ 为 $\pi(\varphi,\psi)=\varphi\times\psi$, 其中 $\varphi\in\widehat{G_1}$, $\psi\in\widehat{G_2}$. 容易验证 π 为群同态, 我们考虑 π 的核 $\ker(\pi)$. 对于 $\varphi\in\widehat{G_1}$, $\psi\in\widehat{G_2}$, 若 $(\varphi,\psi)\in\ker(\pi)$, 则 $\varphi\times\psi$ 为 G 的主特征. 所以对任意 $g_1\in G_1$, $(\varphi\times\psi)(g_1,1_{G_2})=1$, 即 $\varphi(g_1)\psi(1_{G_2})=1$, 从而 $\varphi(g_1)=1$, 故 φ 为 G_1 的主特征. 同理可证明 ψ 为 G_2 的主特征, 这表明 (φ,ψ) 为群 $\widehat{G_1}\times\widehat{G_2}$ 的单位元, 所以 π 为单射. 又由上面的说明知道 π 也是满射, 故 π 为同构. □

设 G 为有限交换群, 则 G 同构于有限循环群的直积. 由引理 8.1 知群的直积的特征群同构于对应特征群的直积, 例 8.1 告诉我们循环群的特征群同构于自身, 由此我们有如下定理.

定理 8.2: 设 G 为有限交换群, 则 $\widehat{G}\cong G$. □

注意到由定理 8.2 显然有 $\widehat{\widehat{G}}\cong\widehat{G}\cong G$, 但在群 G 和 $\widehat{\widehat{G}}$ 之间有一个自然的同构. 对任意 $g\in G$, 定义 $\widehat{\widehat{g}}:\widehat{G}\to\mathbb{C}^*$ 为 $\widehat{\widehat{g}}(\chi)=\chi(g)$, 则容易验证 $\widehat{\widehat{g}}\in\widehat{\widehat{G}}$ 且 $g\mapsto\widehat{\widehat{g}}$ 是群 G 到 $\widehat{\widehat{G}}$ 的同构映射.

例 8.2: 设 $\mathbb{F}_q$ 为 q 元域, 则 $\mathbb{F}_q$ 带有两个群结构, 即它的加法群和乘法群, 分别记为 $\mathbb{F}_q$ 和 $\mathbb{F}_q^*$. 有限域 $\mathbb{F}_q$ 的乘法群 $\mathbb{F}_q^*$ 的特征称为域 $\mathbb{F}_q$ 的乘法特征, 由于 $\mathbb{F}_q^*$ 为 $q-1$ 阶循环群, 设 α 为 $\mathbb{F}_q$ 的一个本原元素, 由例 8.1 知 $\mathbb{F}_q$ 有 $q-1$ 个乘法特征, 分别为 $\chi_0,\chi_1,\ldots,\chi_{q-2}$, 其中 $\chi_j(\alpha^k)=\zeta_{q-1}^{kj}$, $0\le j,k\le q-2$. 若 q 为奇数, 记 $\eta=\chi_{\frac{q-1}{2}}$, 则对任意 $\beta=\alpha^k$ 有

$$\eta(\beta)=\eta(\alpha^k)=\zeta_{q-1}^{k\frac{q-1}{2}}=(-1)^k=\begin{cases}1, & \text{若 } k \text{ 为偶数}\\ -1, & \text{若 } k \text{ 为奇数}\end{cases}=\begin{cases}1, & \text{若 } \beta \text{ 为非零平方元,}\\ -1, & \text{若 } \beta \text{ 为非平方元.}\end{cases}$$

由于 $\eta^2=\chi_0$, 即 η 在群 $\widehat{\mathbb{F}_q^*}$ 中的阶为 2, 称 η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, 这个 η 就是我们在第 7.5 节定义的那个整数值函数. 群 $\widehat{\mathbb{F}_q^*}$ 中的 d 阶元素称为 $\mathbb{F}_q$ 的 d 阶乘法特征, 由于 $\widehat{\mathbb{F}_q^*}$ 为 $q-1$ 阶

循环群, χ_1 是它的一个生成元, 所以 $\mathbb{F}_q$ 的 d 阶乘法特征存在当且仅当 $d \mid (q-1)$ (例如 $\chi_1^{\frac{q-1}{d}}$ 就是 $\mathbb{F}_q$ 的一个 d 阶乘法特征). 进一步地, 对于 $q-1$ 的任意因子 d, $\widehat{\mathbb{F}_q^*}$ 中有 $\phi(d)$ 个 d 阶元素, 故 $\mathbb{F}_q$ 的 d 阶乘法特征恰有 $\phi(d)$ 个, 例如对于奇素数幂 q, $\mathbb{F}_q$ 的 2 阶乘法特征只有 1 个, 即上面定义的 η.

有限域 $\mathbb{F}_q$ 的加法群的特征称为 $\mathbb{F}_q$ 的加法特征, 下面我们来讨论 $\mathbb{F}_q$ 的加法特征. 设 $q = p^m$, 其中 p 为素数, 我们知道 $\mathbb{F}_q$ 的加法群即 m 个 p 阶循环群 $\mathbb{Z}_p$ 的直积, 其中 $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ 在加法下为由 1 生成的循环群. 由例 8.1 得到加法群 $\mathbb{Z}_p$ 的特征为 $\varphi_0, \varphi_1, \ldots, \varphi_{p-1}$, 其中 $\varphi_j(k) = \zeta_p^{kj}$, $0 \leq j, k \leq p-1$. 对 $\mathbb{F}_q$ 的任意加法特征 λ, 由引理 8.1 得到存在 $j_1, j_2, \ldots, j_m$ 使得 $\lambda = \varphi_{j_1} \times \varphi_{j_2} \times \cdots \times \varphi_{j_m}$, 其中 $0 \leq j_1, j_2, \ldots, j_m \leq p-1$. 故对任意 $(k_1, k_2, \ldots, k_m) \in \mathbb{F}_q$, 有

$$\lambda(k_1, k_2, \ldots, k_m) = \varphi_{j_1}(k_1)\varphi_{j_2}(k_2)\cdots\varphi_{j_m}(k_m) = \zeta_p^{j_1k_1 + j_2k_2 + \cdots + j_mk_m}.$$

记 $\mathbb{F}_q = \mathbb{Z}_p^m$, 且 $\mathbf{j} = (j_1, j_2, \ldots, j_m)$, $\mathbf{k} = (k_1, k_2, \ldots, k_m) \in \mathbb{Z}_p^m$ 为 $\mathbb{Z}_p$ 上的 m-维向量, 而对 $\lambda \in \widehat{\mathbb{F}_q}$, 若 $\lambda = \varphi_{j_1} \times \varphi_{j_2} \times \cdots \times \varphi_{j_m}$, 记这样的 λ 为 $\lambda_{\mathbf{j}}$. 对于 $\mathbf{j} = (j_1, j_2, \ldots, j_m)$, $\mathbf{k} = (k_1, k_2, \ldots, k_m) \in \mathbb{Z}_p^m$, 定义 $\mathbf{j}$ 和 $\mathbf{k}$ 在向量空间 $\mathbb{Z}_p^m$ 中的内积 $\mathbf{j} \cdot \mathbf{k}$ 为它们的对应分量乘积之和, 即

$$\mathbf{j} \cdot \mathbf{k} = j_1k_1 + j_2k_2 + \cdots + j_mk_m \in \mathbb{Z}_p.$$

由此我们得到 $\mathbb{F}_q$ 的 $q = p^m$ 个加法特征为 $\lambda_{\mathbf{j}}$, 其中 $\mathbf{j} \in \mathbb{Z}_p^m$, 且对任意 $\mathbf{k} \in \mathbb{F}_q$ 有 $\lambda_{\mathbf{j}}(\mathbf{k}) = \zeta_p^{\mathbf{j}\cdot\mathbf{k}}$. 显然 $\lambda_{\mathbf{0}}$ 为主特征.

有限域 $\mathbb{F}_q$ 的加法特征还有另一种表示形式. 对于 $a \in \mathbb{F}_q$, 定义 λ_a 为

$$\begin{array}{rccc} \lambda_a: & \mathbb{F}_q & \to & \mathbb{C}^* \\ & x & \mapsto & \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)}, \end{array}$$

(注意到 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)$ 的取值在 $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ 中, 因此这里方幂的含义是明确的) 则对任意 $x, y \in \mathbb{F}_q$ 有

$$\lambda_a(x+y) = \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a(x+y))} = \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax+ay)} = \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)}\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ay)} = \lambda_a(x)\lambda_a(y),$$

故 $\lambda_a \in \widehat{\mathbb{F}_q}$. 进一步地, 若 $a \neq b \in \mathbb{F}_q$, 则有 $a - b \neq 0$, 由迹映射为满射得知一定存在 $x \in \mathbb{F}_q$ 使得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}((a-b)x) \neq 0$, 从而 $\lambda_a(x) \neq \lambda_b(x)$, 即 $\lambda_a \neq \lambda_b$. 又因为 $\mathbb{F}_q$ 的加法特征共有 q 个, 所以 $\widehat{\mathbb{F}_q} = \{\lambda_a \mid a \in \mathbb{F}_q\}$, 即当 a 跑遍 $\mathbb{F}_q$ 中所有元素时, 我们就得到 $\mathbb{F}_q$ 的所有加法特征 λ_a. 显然 λ_0 为主特征, 又对任意 $a, x \in \mathbb{F}_q$, 有 $\lambda_a(x) = \lambda_1(ax)$, 从而 $\mathbb{F}_q$ 的每个加法特征都可以由 λ_1 表出, 我们称 λ_1 为 $\mathbb{F}_q$ 的典范加法特征.

有限域的加法特征和乘法特征在很多问题的讨论中有重要应用, 后面我们要定义的指数和, 包括 Gauss 和, Jacobi 和等都是利用它们构造出来的. 需要注意的是它们与有限域的特征完全是两码事. □

定理 8.3: 设 G 为有限交换群, $H \le G$, 则 H 的每个特征都可以扩充为 G 的特征, 即对任意 $\psi \in \widehat{H}$, 存在 $\chi \in \widehat{G}$ 使得对任意 $h \in H$ 有 $\chi(h) = \psi(h)$.

证明: 我们只需证明 H 为 G 的真子群的情形. 选取元素 $a \in G$ 但是 $a \notin H$, 令 $H_1 = \langle H, a\rangle$, 则 $H_1 \le G$ 且 $H \lneq H_1$. 在商群 G/H 中, $aH \ne H$, 设 aH 在群 G/H 中的阶为 m, 则 $m \ge 2$ 且 $a^m \in H$, 所以 H_1 中每个元素 g 一定形如 $g = a^j h$, 其中 $0 \le j < m$ 且 $h \in H$. 取定复数 $\omega \in \mathbb{C}$ 满足 $\psi(a^m) = \omega^m$ (注意这样的 ω 一定存在), 定义 $\psi_1 : H_1 \to \mathbb{C}^*$ 为 $\psi_1(g) = \psi_1(a^j h) = \omega^j \psi(h)$. 对任意 $g, g_1 \in H_1$, 设 $g = a^j h$, $g_1 = a^k h_1$, 其中 $0 \le j, k < m$ 且 $h, h_1 \in H$. 若 $j + k < m$, 则

$$\psi_1(gg_1) = \psi_1(a^{j+k} h h_1) = \omega^{j+k}\psi(hh_1) = \omega^j\omega^k\psi(h)\psi(h_1) = (\omega^j\psi(h))(\omega^k\psi(h_1)) = \psi_1(g)\psi_1(g_1),$$

若 $j + k \ge m$, 则有 $0 \le j + k - m < m$, 且

$$\psi_1(gg_1) = \psi_1(a^{j+k-m}a^m h h_1) = \omega^{j+k-m}\psi(a^m)\psi(h)\psi(h_1) = (\omega^j\psi(h))(\omega^k\psi(h_1)) = \psi_1(g)\psi_1(g_1),$$

这样我们便证出 $\psi_1 \in \widehat{H_1}$. 显然有 $\psi_1(h) = \psi(h)$, 即 ψ_1 是 ψ 在 H_1 上的扩充, 若 $H_1 = G$, 则令 $\chi = \psi_1$, 而若 $H_1 \lneq G$, 同样的过程可以扩充 ψ_1, 有限步后就可以得到 ψ 在 G 上的扩充. □

推论 8.4: 设 G 为有限交换群, $g_1, g_2 \in G$ 且 $g_1 \ne g_2$, 则存在 $\chi \in \widehat{G}$ 使得 $\chi(g_1) \ne \chi(g_2)$.

证明: 设 $g = g_1 g_2^{-1}$, $H = \langle g\rangle$. 由于 $g \ne 1_G$, 由例 8.1 知存在 $\psi \in \widehat{H}$ 使得 $\psi(g) \ne 1$ (例如定义 ψ 为 $\psi(g) = \zeta_m$, 其中 $m = |H|$). 则由定理 8.3 知存在 $\chi \in \widehat{G}$ 使得 $\chi(g) = \psi(g)$, 从而 $\chi(g_1 g_2^{-1}) \ne 1$, 即 $\chi(g_1) \ne \chi(g_2)$. □

子群 H 的主特征扩充成的 G 的特征称为 H 在 $\widehat{G}$ 中的零化特征, 下面我们就来讨论 H 在 $\widehat{G}$ 中的零化特征. 设 $H^\sharp \subseteq \widehat{G}$ 是 H 在 $\widehat{G}$ 中的所有零化特征构成的集合, 即

$$H^\sharp = \{\chi \in \widehat{G} \mid \text{对所有 } h \in H \text{ 有 } \chi(h) = 1\}.$$

定理 8.5: 设 G 为有限交换群, $H \le G$, $H^\sharp \subseteq \widehat{G}$ 是 H 在 $\widehat{G}$ 中的所有零化特征构成的集合, 则有 $H^\sharp \le \widehat{G}$ 且 $H^\sharp \cong \widehat{G/H}$.

证明: 显然 $H^\sharp$ 对特征的乘法和求逆封闭, 所以 $H^\sharp \le \widehat{G}$. 进一步地, 对任意 $\chi \in H^\sharp$, 定义商群 G/H 到 $\mathbb{C}^*$ 的映射 μ_χ 为 $\mu_\chi(gH) = \chi(g)$. 首先 μ_χ 是良定义的, 事实上, 若 $gH = g_1 H$, 则 $g^{-1}g_1 \in H$, 从而 $\chi(g^{-1}g_1) = 1$, 由此得到 $\chi(g) = \chi(g_1)$. 其次由

$$\mu_\chi(gHg_1H) = \mu_\chi(gg_1H) = \chi(gg_1) = \chi(g)\chi(g_1) = \mu_\chi(gH)\mu_\chi(g_1H)$$

有 $\mu_\chi \in \widehat{G/H}$.

定义 $\pi : H^\sharp \to \widehat{G/H}$ 为 $\pi(\chi) = \mu_\chi$, 则对任意 $\chi_1, \chi_2 \in H^\sharp$ 和 $gH \in G/H$ 有

$$\mu_{\chi_1\chi_2}(gH) = (\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) = \mu_{\chi_1}(gH)\mu_{\chi_2}(gH) = (\mu_{\chi_1}\mu_{\chi_2})(gH),$$

即 $\mu_{\chi_1\chi_2} = \mu_{\chi_1}\mu_{\chi_2}$, 故 π 为同态. 下面我们证明 π 为双射. 事实上, 若对 $\chi_1, \chi_2 \in H^\sharp$ 有 $\pi(\chi_1) = \pi(\chi_2)$, 则对任意 $g \in G$ 有 $\chi_1(g) = \mu_{\chi_1}(gH) = \mu_{\chi_2}(gH) = \chi_2(g)$, 从而 $\chi_1 = \chi_2$, 即 π 为单射. 另一方面, 对任意 $\mu \in \widehat{G/H}$, 定义 $\chi : G \to \mathbb{C}^*$ 为 $\chi(g) = \mu(gH)$, 则显然 $\chi \in \widehat{G}$, 又对任意 $h \in H$ 有 $\chi(h) = \mu(H) = 1$, 所以 $\chi \in H^\sharp$ 且 $\mu_\chi = \mu$, 即 π 为满射. 这样我们便证明了 π 为同构映射, 故 $H^\sharp \cong \widehat{G/H}$. □

注意到由于 $H^\sharp \cong \widehat{G/H}$ 所以 $|H^\sharp| = [G : H]$. 另外 $H^\sharp$ 中的元素是 G 的特征, 即 G 到 $\mathbb{C}^*$ 的群同态, 所以 $H^\sharp$ 和 $\widehat{H}$ 中的元素是不一样的, 当然 $H^\sharp$ 和 $\widehat{G/H}$ 中的元素也是不一样的. 我们常常称 $H^\sharp$ 为 H 在 G 中的对偶.

定理 8.6: 设 G 为有限交换群, $\chi \in \widehat{G}$ 且 $\chi \neq \chi_0$ (χ_0 为 G 的主特征), 则有 $\sum_{g\in G} \chi(g) = 0$.

证明: 因为 $\chi \neq \chi_0$, 所以存在 $h \in G$ 使得 $\chi(h) \neq 1$, 由

$$\chi(h)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(h)\chi(g) = \sum_{g\in G}\chi(hg) = \sum_{g\in G}\chi(g)$$

得到 $(\chi(h)-1)\sum_{g\in G}\chi(g) = 0$, 又 $\chi(h) - 1 \neq 0$, 所以 $\sum_{g\in G}\chi(g) = 0$. □

显然 $\sum_{g\in G}\chi_0(g) = |G| = n$, 类似地, 我们有如下定理.

定理 8.7: 设 G 为有限交换群, $g \in G$ 且 $g \neq 1_G$ (1_G 为 G 的单位元), 则有 $\sum_{\chi\in\widehat{G}} \chi(g) = 0$.

证明: 由于 $g \neq 1_G$, 由推论 8.4 知道存在 $\psi \in \widehat{G}$ 使得 $\psi(g) \neq \psi(1_G) = 1$, 由

$$\psi(g)\sum_{\chi\in\widehat{G}}\chi(g) = \sum_{\chi\in\widehat{G}}\psi(g)\chi(g) = \sum_{\chi\in\widehat{G}}(\psi\chi)(g) = \sum_{\chi\in\widehat{G}}\chi(g)$$

得到 $(\psi(g)-1)\sum_{\chi\in\widehat{G}}\chi(g) = 0$, 又 $\psi(g) - 1 \neq 0$, 所以 $\sum_{\chi\in\widehat{G}}\chi(g) = 0$. □

由定理 8.6, 我们有如下结论.

定理 8.8: (特征的第一正交关系) 设 G 为有限交换群, $\chi, \psi \in \widehat{G}$, 则有

$$\sum_{g\in G}\chi(g)\overline{\psi(g)} = \begin{cases} |G|, & \text{若 } \chi = \psi, \\ 0, & \text{若 } \chi \neq \psi, \end{cases}$$

或写为

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = \delta_{\chi,\psi},$$

其中的 $\delta_{\chi,\psi}$ 为 Kronecker δ-符号, 即当 $\chi = \psi$ 时 $\delta_{\chi,\psi} = 1$, 而当 $\chi \neq \psi$ 时 $\delta_{\chi,\psi} = 0$.

证明: 对任意 $g \in G$, 我们有 $\chi(g)\overline{\psi(g)} = \chi(g)\overline{\psi}(g) = (\chi\overline{\psi})(g)$, 又 $\chi\overline{\psi}$ 为 G 的主特征当且仅当 $\chi = \psi$, 由定理 8.6 我们立得定理的结论. □

显然 $\sum_{\chi\in\widehat{G}}\chi(1_G) = |\widehat{G}| = |G| = n$, 类似地, 由定理 8.7 我们有如下结论.

定理 8.9: (特征的第二正交关系) 设 G 为有限交换群, $g, h \in G$, 则有

$$\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi(h)} = \begin{cases} |G|, & \text{若 } g = h, \\ 0, & \text{若 } g \neq h, \end{cases}$$

或写为

$$\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi(h)} = \delta_{g,h},$$

其中的 $\delta_{g,h}$ 为 Kronecker δ-符号, 即当 $g = h$ 时 $\delta_{g,h} = 1$, 而当 $g \neq h$ 时 $\delta_{g,h} = 0$. □

设 $G = \{a_0, a_1, \ldots, a_{n-1}\}$, $\widehat{G} = \{\chi_0, \chi_1, \ldots, \chi_{n-1}\}$, 定义矩阵 $C = (c_{ij})_{0\le i,j\le n-1}$, 其中 $c_{ij} = \chi_j(a_i)$, 则由特征的第一正交关系有 $C^T\overline{C} = nI_n$, 其中 $\overline{C} = (\overline{c_{ij}})_{0\le i,j\le n-1}$ 称为复矩阵 C

的共轭. 定义 $A=\frac{1}{\sqrt{n}}C^T$, A^* 为矩阵 A 的共轭转置, 即 $A^*=\overline{A}^T$, 则有 $AA^*=I_n$, 从而 A 为酉矩阵. 前面构造的矩阵 C 称为群 G 的特征表, 注意到由 $C^T\overline{C}=nI_n$ 可得 $C\overline{C}^T=nI_n$, 具体写出就是特征的第二正交关系.

有限交换群 G 的特征理论常常用来得到 G 上方程的解的个数的表达式, 设 f 是 $G^m=G\times\cdots\times G$ (m 个 G) 到 G 的映射, 对 $g\in G$, 若 $(g_1,\ldots,g_m)\in G^m$ 满足 $f(g_1,\ldots,g_m)=g$, 则称 $(g_1,\ldots,g_m)$ 为方程 $f(x_1,\ldots,x_m)=g$ 在 G 上的一个解. 用 $N_G(f(x_1,\ldots,x_m)=g)$ 表示方程 $f(x_1,\ldots,x_m)=g$ 在 G 上的解的个数, 则由特征的第二正交关系有

$$\begin{aligned}
N_G(f(x_1,\ldots,x_m)=g) &= \sum_{g_1,\ldots,g_m\in G,\, f(g_1,\ldots,g_m)=g} 1=\sum_{g_1,\ldots,g_m\in G}\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(f(g_1,\ldots,g_m))\overline{\chi(g)}\\
&= \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\sum_{g_1,\ldots,g_m\in G}\chi(f(g_1,\ldots,g_m))\overline{\chi(g)}\\
&= \frac{1}{|G|}\left(|G|^m+\sum_{\chi\in\widehat{G},\chi\neq\chi_0}\sum_{g_1,\ldots,g_m\in G}\chi(f(g_1,\ldots,g_m))\overline{\chi(g)}\right)\\
&= |G|^{m-1}+\frac{1}{|G|}\sum_{\chi\in\widehat{G},\chi\neq\chi_0}\overline{\chi(g)}\sum_{g_1,\ldots,g_m\in G}\chi(f(g_1,\ldots,g_m)),
\end{aligned}$$

其中 $|G|^{m-1}$ 是 $N_G(f(x_1,\ldots,x_m)=g)$ 的主项 (m 是方程中包含的未知量的个数), 上式最后面的求和式 $\sum_{g_1,\ldots,g_m\in G}\chi(f(g_1,\ldots,g_m))$ 称为群 G 上的特征和, 计算和估计群 G 上的特征和是数论中的一个重要课题, 有很多深刻的结果.

利用域 $\mathbb{F}_q$ 的加法特征, 我们也可以给出置换多项式的一种判定方法.

定理 8.9: 设 $f(x)\in\mathbb{F}_q[x]$, 则 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式当且仅当对 $\mathbb{F}_q$ 的任意非主加法特征 λ 都有

$$\sum_{c\in\mathbb{F}_q}\lambda(f(c))=0.$$

证明: 设 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式, 则有 $\{f(c)\mid c\in\mathbb{F}_q\}=\mathbb{F}_q$, 从而对 $\mathbb{F}_q$ 的任意非主加法特征 λ 有

$$\sum_{c\in\mathbb{F}_q}\lambda(f(c))=\sum_{c\in\mathbb{F}_q}\lambda(c)=0.$$

反之, 对任意 $a\in\mathbb{F}_q$, 由前面的说明我们有方程 $f(x)=a$ 在 $\mathbb{F}_q$ 中根的个数为

$$\frac{1}{q}\sum_{c\in\mathbb{F}_q}\sum_{\lambda\in\widehat{\mathbb{F}_q}}\lambda(f(c))\overline{\lambda}(a).$$

用 λ_0 表示 $\mathbb{F}_q$ 的主加法特征, 则

$$\sum_{c\in\mathbb{F}_q}\sum_{\lambda\in\widehat{\mathbb{F}_q}}\lambda(f(c))\overline{\lambda}(a)=\sum_{\lambda\in\widehat{\mathbb{F}_q}}\overline{\lambda}(a)\sum_{c\in\mathbb{F}_q}\lambda(f(c))=q+\sum_{\lambda\in\widehat{\mathbb{F}_q},\,\lambda\neq\lambda_0}\overline{\lambda}(a)\sum_{c\in\mathbb{F}_q}\lambda(f(c))=q,$$

其中我们用到对任意 $\lambda\neq\lambda_0$, 都有 $\sum_{c\in\mathbb{F}_q}\lambda(f(c))=0$ 这个条件, 从而对任意 $a\in\mathbb{F}_q$, 方程 $f(x)=a$ 在 $\mathbb{F}_q$ 中的根恰有一个, 由定理 6.1 知 $f(x)$ 为 $\mathbb{F}_q$ 上的置换多项式. □

8.2 有限交换群上的离散 Fourier 变换

设 G 是 n 阶交换群, 所谓 G 上的一个复值函数就是一个 G 到复数域 $\mathbb{C}$ 的映射, 用 $L^2(G)$ 表示所有 G 上的复值函数构成的集合. 对任意 $f,g\in L^2(G)$ 和任意 $c\in\mathbb{C}$, 定义 $f+g: G\to\mathbb{C}$ 和 $cf: G\to\mathbb{C}$ 为 $(f+g)(a)=f(a)+g(x)$ 和 $(cf)(a)=cf(a)$, 其中 $a\in G$, 则显然有 $f+g, cf\in L^2(G)$, 分别称为 f 与 g 的和以及 f 被复数 c 的数乘, 容易验证 $L^2(G)$ 在如上定义的加法和数乘下构成复数域 $\mathbb{C}$ 上的一个线性空间, 其中的零元素为零函数 0, 即对任意 $a\in G$, 有 $0(a)=0$.

对每个 $a\in G$, 定义 $\delta_a: G\to\mathbb{C}$ 为 $\delta_a(s)=\delta_{a,s}$, 其中 s 为 G 中任意元素. 显然对任意 $f\in L^2(G)$ 有 $f=\sum_{a\in G}f(a)\delta_a$, 又若有 $\sum_{a\in G}c_a\delta_a=0$, 其中 $c_a\in\mathbb{C}$, 则对每个 $t\in G$, 有 $(\sum_{a\in G}c_a\delta_a)(t)=0$, 即 $c_t=0$, 故 $\{\delta_a\mid a\in G\}$ 构成 $L^2(G)$ 在 $\mathbb{C}$ 上的一组基, 从而 $\dim L^2(G)=n$.

定义 $\langle,\rangle: L^2(G)\times L^2(G)\to\mathbb{C}$ 为

$$\langle f,g\rangle=\frac{1}{n}\sum_{a\in G}f(a)\overline{g(a)},$$

其中 $f,g\in L^2(G)$, 则容易验证 $\langle,\rangle$ 是线性空间 $L^2(G)$ 上的一个内积, 这样 $L^2(G)$ 成为一个复内积空间, 或酉空间 (或 Hilbert 空间). 对任意 $f\in L^2(G)$, 显然 $\langle f,f\rangle$ 是一个非负实数, 定义 f 的长度 (或范数), 记为 $\|f\|$, 为 $\|f\|=\sqrt{\langle f,f\rangle}$. 显然由

$$\langle\sqrt{n}\delta_s,\sqrt{n}\delta_t\rangle=\frac{1}{n}\sum_{a\in G}\sqrt{n}\delta_s(a)\overline{\sqrt{n}\delta_t(a)}=\delta_{s,t}$$

得知 $\{\sqrt{n}\delta_a\mid a\in G\}$ 为 $L^2(G)$ 的一个标准正交基. 又由定理 8.8, 即特征的第一正交关系得到 $\widehat{G}$ 也构成 $L^2(G)$ 的一个标准正交基.

设 G 为 n 阶交换群, $\widehat{G}$ 为 G 的特征群, 类似地, 用 $L^2(\widehat{G})$ 表示所有 $\widehat{G}$ 上的复值函数构成的集合, 则 $L^2(\widehat{G})$ 也做成复数域 $\mathbb{C}$ 上的一个 n 维线性空间. 对于 $f\in L^2(G)$, 定义 $\hat{f}:\widehat{G}\to\mathbb{C}$ 为

$$\hat{f}(\chi)=\sum_{a\in G}f(a)\chi(a),\tag{8.1}$$

其中 χ 为 $\widehat{G}$ 中任意元素, 称 $\hat{f}$ 为 f 的 Fourier 变换, 显然 $\hat{f}\in L^2(\widehat{G})$. 我们知道 $\widehat{G}$ 构成 Hilbert 空间 $L^2(G)$ 的一个标准正交基, 所以任意 $f\in L^2(G)$ 可唯一表示为 $f=\sum_{\chi\in\widehat{G}}c_\chi\chi$ (这样的表示也称为一个三角和, 因为对任意 $a\in G$, $f(a)$ 写成了单位根的复系数线性组合, 其中的复系数 c_χ 也称为 Fourier 系数). 由标准正交基的性质显然有 $c_\chi=\langle f,\chi\rangle$, 从而由式 (8.1) 有

$$\hat{f}(\chi)=\sum_{a\in G}f(a)\chi(a)=\sum_{a\in G}f(a)\overline{\chi(a)}=n\langle f,\overline{\chi}\rangle=nc_{\overline{\chi}},$$

其中 $\overline{\chi}$ 为 χ 的共轭特征, 也是 χ 在群 $\widehat{G}$ 中的逆. 这样我们有

$$f=\frac{1}{n}\sum_{\chi\in\widehat{G}}\hat{f}(\chi)\overline{\chi},$$

由此我们得到如下定理.

定理 8.10: (Fourier 反变换) 设 G 为 n 阶交换群, $f \in L^2(G)$, $\hat{f}$ 为 f 的 Fourier 变换, 则对任意 $a \in G$ 有

$$f(a) = \frac{1}{n} \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\overline{\chi}(a). \tag{8.2}$$

□

例 8.3: 考察复值函数 $\delta_a \in L^2(G)$, 其中 $a \in G$, 我们有

$$\widehat{\delta_a}(\chi) = \sum_{x \in G} \delta_a(x)\chi(x) = \chi(a),$$

所以

$$\delta_a = \frac{1}{n} \sum_{\chi \in \widehat{G}} \chi(a)\overline{\chi} = \frac{1}{n} \sum_{\chi \in \widehat{G}} \overline{\chi(a)}\chi.$$

特别地, 若 $a = 1_G$, 则有 $\delta_{1_G} = \frac{1}{n}\sum_{\chi \in \widehat{G}} \chi$, 这便是定理 8.7. □

设 G 为 n 阶交换群, $f, g \in L^2(G)$, 则对任意 $\chi \in \widehat{G}$ 有

$$\widehat{f+g}(\chi) = \sum_{a \in G}(f+g)(a)\chi(a) = \sum_{a \in G}(f(a)+g(a))\chi(a) = \hat{f}(\chi) + \hat{g}(\chi) = (\hat{f}+\hat{g})(\chi),$$

即 $\widehat{f+g} = \hat{f} + \hat{g}$, 同理对任意 $c \in \mathbb{C}$ 和 $f \in L^2(G)$ 有 $\widehat{cf} = c\hat{f}$. 定义

$$\begin{array}{rccc} \mathcal{F}: & L^2(G) & \to & L^2(\widehat{G}) \\ & f & \mapsto & \hat{f}, \end{array}$$

所以 $\mathcal{F}$ 为线性空间 $L^2(G)$ 到 $L^2(\widehat{G})$ 的线性映射, 由定理 8.10 知 $\mathcal{F}$ 还是可逆线性映射. 我们称 $\mathcal{F}$ 为群 G 上的 Fourier 变换, 或离散 Fourier 变换.

对于 $f, g \in L^2(G)$, 定义 f 与 g 的卷积 $f * g$ 为对任意 $a \in G$,

$$(f * g)(a) = \sum_{b \in G} f(b)g(ab^{-1}),$$

所以 $f * g$ 仍为 G 上的复值函数. 进一步地, 对任意 $\chi \in \widehat{G}$ 有

$$\begin{aligned} \widehat{f*g}(\chi) &= \sum_{a \in G}(f*g)(a)\chi(a) = \sum_{a \in G}\sum_{b \in G} f(b)g(ab^{-1})\chi(a) \\ &= \sum_{b \in G} f(b) \sum_{s \in G} g(s)\chi(sb) = \sum_{b \in G} f(b)\chi(b) \sum_{s \in G} g(s)\chi(s) \\ &= \hat{f}(\chi)\hat{g}(\chi) = (\hat{f}\hat{g})(\chi), \end{aligned}$$

所以 $\widehat{f*g} = \hat{f}\hat{g}$, 即卷积的 Fourier 变换等于 Fourier 变换的乘积.

设 G 为有限交换群, 容易验证线性空间 $L^2(G)$ 在卷积下做成一个代数, 而线性空间 $L^2(\widehat{G})$ 在通常函数的乘积 (按点相乘) 下也构成一个代数, 前面的讨论表明 G 上的 Fourier 变换 $\mathcal{F}$ 是这两个代数之间的一个同构.

类似地可以在复线性空间 $L^2(\widehat{G})$ 上定义内积, 对于 $F,G\in L^2(\widehat{G})$, 定义

$$\langle F,G\rangle=\frac{1}{n}\sum_{\chi\in\widehat{G}}F(\chi)\overline{G(\chi)},$$

则 $L^2(\widehat{G})$ 在此内积下也成为一个 Hilbert 空间. 同样可以定义 $F\in L^2(\widehat{G})$ 的长度 (范数) 为 $\|F\|=\sqrt{\langle F,F\rangle}$.

定理 8.11: (Plancherel 公式) 设 G 为 n 阶交换群, $f,g\in L^2(G)$, 则 $\langle\hat{f},\hat{g}\rangle=n\langle f,g\rangle$.

证明: 直接计算得到

$$\begin{aligned}\langle\hat{f},\hat{g}\rangle &= \frac{1}{n}\sum_{\chi\in\widehat{G}}\hat{f}(\chi)\overline{\hat{g}(\chi)}=\frac{1}{n}\sum_{\chi\in\widehat{G}}\sum_{a\in G}f(a)\chi(a)\overline{\sum_{b\in G}g(b)\chi(b)}\\ &= \frac{1}{n}\sum_{a,b\in G}f(a)\overline{g(b)}\sum_{\chi\in\widehat{G}}\chi(a)\overline{\chi(b)}=\frac{1}{n}\sum_{a,b\in G}f(a)\overline{g(b)}\cdot n\delta_{a,b}\\ &= \sum_{a\in G}f(a)\overline{g(a)}=n\langle f,g\rangle,\end{aligned}$$

其中上面的运算用到了特征的第二正交关系. □

特别地, 在定理 8.11 中令 $g=f$, 我们有如下推论.

推论 8.12: (Parseval 恒等式) 设 G 为 n 阶交换群, $f\in L^2(G)$, 则有 $\|\hat{f}\|=\sqrt{n}\|f\|$. □

例 8.4: 设 G 为 n 阶交换群, $A\subseteq G$, 定义 A 的特征函数 $f_A\in L^2(G)$ 为

$$f_A(a)=\begin{cases}1, & \text{若 } a\in A,\\ 0, & \text{若 } a\notin A.\end{cases}$$

对 $A,B\subseteq G$, 容易计算出 $\langle f_A,f_B\rangle=\frac{1}{n}|A\cap B|$, 特别地有 $\|f_A\|=\frac{1}{\sqrt{n}}\sqrt{|A|}$, 从而 $\|\widehat{f_A}\|=\sqrt{|A|}$.

对于 $\chi\in\widehat{G}$, 记 $\chi(A)=\sum_{a\in A}\chi(a)$, 则有 $\widehat{f_A}(\chi)=\sum_{a\in A}\chi(a)=\chi(A)$. 特别地对于 G 的主特征 χ_0, 我们有 $\widehat{f_A}(\chi_0)=|A|$. 令

$$\Phi(A)=\max\{|\widehat{f_A}(\chi)|\mid\chi\in\widehat{G},\ \chi\neq\chi_0\},$$

显然由 $|\widehat{f_A}(\chi)|=|\chi(A)|\leq\sum_{a\in A}|\chi(a)|=|A|$ 可得 $\Phi(A)\leq|A|$. 进一步地, 假设 $|A|\leq\frac{n}{2}$, 由

$$|A|=\|\widehat{f_A}\|^2=\frac{1}{n}\sum_{\chi\in\widehat{G}}|\widehat{f_A}(\chi)|^2\leq\frac{1}{n}(|A|^2+(n-1)\Phi(A)^2)$$

可得 $(n-1)\Phi(A)^2\geq n|A|-|A|^2$, 即

$$\Phi(A)^2\geq\frac{(n-|A|)|A|}{n-1}\geq\frac{1}{2}|A|,$$

从而 $\Phi(A)\geq\sqrt{|A|/2}$. ($\Phi(A)$ 可以给出集合 A 的随机性的一些信息, $\Phi(A)$ 越小, 集合 A 看起来越随机.) □

例 8.5: 设 $\mathbb{F}_2$ 为 2 元域, $\mathbb{F}_2^n$ 为 $\mathbb{F}_2$ 上的 n-维向量空间, 其上的加法构成一个交换群, 即 n 个 2 阶循环群的直积. 设正整数 $m\geq2$, $\mathbb{Z}_m$ 为整数模 m 的剩余类环, 一个型为 $\{m,n\}$ 的广义布尔函数 f 是一个映射 $f:\ \mathbb{F}_2^n\to\mathbb{Z}_m$. 特别地, 若 $m=2$, 则 $\mathbb{Z}_2=\mathbb{F}_2$, 这样的函数 $f:\ \mathbb{F}_2^n\to\mathbb{F}_2$ 称

为 n 元布尔函数. 记 $\zeta_m = e^{\frac{2\pi i}{m}} \in \mathbb{C}$, 对于一个型为 $\{m,n\}$ 的广义布尔函数 f, 定义 f 的符号函数 $S_f : \mathbb{F}_2^n \to \mathbb{C}$ 为 $S_f(x) = \zeta_m^{f(x)}$, 其中 $x \in \mathbb{F}_2^n$, 故 S_f 是群 $\mathbb{F}_2^n$ 上的复值函数.

由例 8.2, 我们知道群 $\mathbb{F}_2^n$ 的每个特征形如 χ_a, 其中 $a \in \mathbb{F}_2^n$ 且 χ_a 定义为对 $x \in \mathbb{F}_2^n$ 有 $\chi_a(x) = (-1)^{a\cdot x}$. 对于一个型为 $\{m,n\}$ 的广义布尔函数 f, 定义 f 的 Walch 变换 $W_f : \mathbb{F}_2^n \to \mathbb{C}$ 为 $W_f(a) = \widehat{S_f}(\chi_a)$, 其中 $a \in \mathbb{F}_2^n$. 详细写出来, 对任意 $a \in \mathbb{F}_2^n$, 我们有

$$W_f(a) = \widehat{S_f}(\chi_a) = \sum_{x\in\mathbb{F}_2^n} S_f(x)\chi_a(x) = \sum_{x\in\mathbb{F}_2^n} \zeta_m^{f(x)}(-1)^{a\cdot x}.$$

由定理 8.10 我们可以得到 f 的 Walch 反变换为

$$\zeta_m^{f(x)} = \frac{1}{2^n}\sum_{a\in\mathbb{F}_2^n} W_f(a)(-1)^{a\cdot x}.$$

特别地, 当 $m = 2$ 时, 我们得到 n 元布尔函数 f 的 Walch 变换和 Walch 反变换分别为

$$W_f(a) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+a\cdot x}$$

和

$$(-1)^{f(x)} = \frac{1}{2^n}\sum_{a\in\mathbb{F}_2^n} W_f(a)(-1)^{a\cdot x}.$$

注意到对于布尔函数 f, f 的取值为 0 或 1, 所以我们有 $(-1)^{f(x)} = 1 - 2f(x)$, 故 f 的 Walch 反变换也可以写为

$$f(x) = \frac{1}{2} - \frac{1}{2^{n+1}}\sum_{a\in\mathbb{F}_2^n} W_f(a)(-1)^{a\cdot x}.$$

设 f 是一个型为 $\{m,n\}$ 的广义布尔函数, 其符号函数为 S_f, 容易计算出 S_f 在酉空间 $L^2(\mathbb{F}_2^n)$ 中的长度 $\|S_f\|$ 的平方为

$$\|S_f\|^2 = \langle S_f, S_f\rangle = \frac{1}{2^n}\sum_{a\in\mathbb{F}_2^n} |S_f(a)|^2 = \frac{1}{2^n}\sum_{a\in\mathbb{F}_2^n} |\zeta_m^{f(a)}|^2 = \frac{1}{2^n}\sum_{a\in\mathbb{F}_2^n} 1 = 1,$$

即 S_f 为 $L^2(\mathbb{F}_2^n)$ 中的单位向量. 由推论 8.12 得到 $\|W_f\|^2 = 2^n$, 从而

$$\sum_{a\in\mathbb{F}_2^n} |W_f(a)|^2 = 2^n\|W_f\|^2 = 2^{2n}.$$

令 $M = \max\{|W_f(a)| \mid a \in \mathbb{F}_2^n\}$, 由上式显然可得 $M \geq 2^{\frac{n}{2}}$ 且 $M = 2^{\frac{n}{2}}$ 当且仅当对每个 $a \in \mathbb{F}_2^n$ 都有 $|W_f(a)| = 2^{\frac{n}{2}}$, 满足此条件的函数称为广义 bent 函数, 而当 $m = 2$ 时这样的函数称为 bent 函数. 注意到当 $m = 2$ 时, 对任意 $a \in \mathbb{F}_2^n$, $W_f(a)$ 是整数, 从而由定义我们得到 n 元 bent 函数存在的必要条件是 n 为偶数. □

设 G 为有限交换群, $f \in L^2(G)$, 定义 f 的支撑集 $\mathrm{supp}(f)$ 为 $\mathrm{supp}(f) = \{a \in G \mid f(a) \neq 0\}$. 例如子集 $A \subseteq G$ 的特征函数 f_A 的支撑集就是 A. 同样可定义 $F \in L^2(\widehat{G})$ 的支撑集 $\mathrm{supp}(F)$ 为 $\mathrm{supp}(F) = \{\chi \in \widehat{G} \mid F(\chi) \neq 0\}$.

定理 8.13: (不确定性准则) 设 G 为有限交换群, $f \in L^2(G)$ 且 $f \neq 0$, 则

$$|\mathrm{supp}(f)| \cdot |\mathrm{supp}(\hat{f})| \geq |G|.$$

证明: 设 $|G|=n$. 对于 $f\in L^2(G)$, 定义 f 的 L_∞-范数 $\|f\|_\infty$ 为

$$\|f\|_\infty=\max\{|f(a)|\mid a\in G\},$$

故

$$\|f\|^2=\frac{1}{n}\sum_{a\in G}|f(a)|^2\le\frac{1}{n}\|f\|_\infty^2\cdot|\mathrm{supp}(f)|. \tag{8.3}$$

由定理 8.10 可得

$$\|f\|_\infty=\max_{a\in G}|f(a)|=\frac{1}{n}\max_{a\in G}\left|\sum_{\chi\in\widehat{G}}\hat{f}(\chi)\overline{\chi}(a)\right|\le\frac{1}{n}\max_{a\in G}\sum_{\chi\in\widehat{G}}|\hat{f}(\chi)||\overline{\chi}(a)|=\frac{1}{n}\sum_{\chi\in\widehat{G}}|\hat{f}(\chi)|,$$

所以由 Cauchy 不等式有

$$\|f\|_\infty^2\le\frac{1}{n^2}\left(\sum_{\chi\in\widehat{G}}|\hat{f}(\chi)|\right)^2\le\frac{1}{n^2}\left(\sum_{\chi\in\widehat{G}}|\hat{f}(\chi)|^2\cdot\sum_{\chi\in\mathrm{supp}(\hat{f})}1^2\right)=\frac{|\mathrm{supp}(\hat{f})|}{n^2}\sum_{\chi\in\widehat{G}}|\hat{f}(\chi)|^2.$$

由推论 8.12 有

$$\sum_{\chi\in\widehat{G}}|\hat{f}(\chi)|^2=n\|\hat{f}\|^2=n^2\|f\|^2,$$

代入上式得到

$$\|f\|_\infty^2\le\frac{|\mathrm{supp}(\hat{f})|}{n^2}\cdot(n^2\|f\|^2)=|\mathrm{supp}(\hat{f})|\cdot\|f\|^2,$$

上式代入 (8.3) 得到

$$\|f\|^2\le\frac{1}{n}(|\mathrm{supp}(\hat{f})|\cdot\|f\|^2)\cdot|\mathrm{supp}(f)|=\|f\|^2\cdot\left(\frac{1}{n}|\mathrm{supp}(f)|\cdot|\mathrm{supp}(\hat{f})|\right),$$

由 $f\neq0$ 得到 $\|f\|\neq0$, 从而由上式可得到 $|\mathrm{supp}(f)|\cdot|\mathrm{supp}(\hat{f})|\ge n$. □

例如, 设 G 为 n 阶交换群, $H\le G$, 考察 H 的特征函数 f_H, 如上我们已知 $|\mathrm{supp}(f_H)|=|H|$. 而对 $\chi\in\widehat{G}$,

$$\widehat{f_H}(\chi)=\sum_{a\in G}f_H(a)\chi(a)=\sum_{a\in H}\chi(a)=\begin{cases}|H|, & \text{若 }\chi\in H^\sharp,\\ 0, & \text{其它,}\end{cases}$$

所以 $|\mathrm{supp}(\widehat{f_H})|=|H^\sharp|=[G:H]$, 故 $|\mathrm{supp}(f_H)|\cdot|\mathrm{supp}(\widehat{f_H})|=|G|$, 此时定理 8.13 中的结论等号成立.

下面我们依然假设 H 是有限交换群 G 的子群, $f\in L^2(G)$, 定义 $f^\sharp:\ G/H\to\mathbb{C}$ 为

$$f^\sharp(gH)=\sum_{x\in gH}f(x)=\sum_{h\in H}f(gh).$$

由定理 8.5 的证明得知, 对任意 $\mu\in\widehat{G/H}$, 存在唯一的 $\chi\in H^\sharp$ 满足 $\chi(g)=\mu(gH)$. 所以

$$\widehat{f^\sharp}(\mu)=\sum_{gH\in G/H}f^\sharp(gH)\mu(gH)=\sum_{gH\in G/H}\sum_{h\in H}f(gh)\mu(gH)=\sum_{x\in G}f(x)\chi(x)=\hat{f}(\chi).$$

利用商群 G/H 上的 Fourier 反变换, 我们有

$$\sum_{h\in H} f(gh) = f^\sharp(gH) = \frac{1}{|G/H|}\sum_{\mu\in\widehat{G/H}} \widehat{f^\sharp}(\mu)\overline{\mu(gH)} = \frac{|H|}{|G|}\sum_{\chi\in H^\sharp}\hat{f}(\chi)\overline{\chi(g)},$$

由此我们证明了如下定理.

定理 8.14: (Poisson 求和公式) 设 G 为有限交换群, $H\le G$, $g\in G$, $f\in L^2(G)$, 则有

$$\frac{1}{|H|}\sum_{h\in H} f(gh) = \frac{1}{|G|}\sum_{\chi\in H^\sharp}\hat{f}(\chi)\overline{\chi(g)}.$$

□

在定理 8.14 中令 $g=1_G$, 群 G 的单位元, 则有如下推论.

推论 8.15: 设 G 为有限交换群, $H\le G$, $f\in L^2(G)$, 则有

$$\frac{1}{|H|}\sum_{h\in H} f(h) = \frac{1}{|G|}\sum_{\chi\in H^\sharp}\hat{f}(\chi).$$

□

注意到 $|H^\sharp| = |G|/|H|$, 所以定理 8.14 和推论 8.15 中的公式在 $|H|$ 较大时有效.

例 8.6: 设 $G=\mathbb{F}_2^n$, 即 $\mathbb{F}_2$ 上的 n-维线性空间, $H=C$ 是 $\mathbb{F}_2^n$ 的一个线性子空间 (也称为一个线性码), 只看其中的加法运算, 则 $\mathbb{F}_2^n$ 为阶为 2^n 的交换群, C 为 G 的子群. 我们知道 $\mathbb{F}_2^n$ 的特征形如 χ_a, 其中 $a\in\mathbb{F}_2^n$ 且对任意 $x\in\mathbb{F}_2^n$ 有 $\chi_a(x)=(-1)^{a\cdot x}$. 从而 $\chi_a\in C^\sharp$ 当且仅当对任意 $u\in C$ 有 $(-1)^{a\cdot u}=1$, 这也等价于在 $\mathbb{F}_2^n$ 中有 $a\cdot u=0$. 令 $C^\perp$ 表示对每个 $u\in C$ 都有 $a\cdot u=0$ 的元素 $a\in\mathbb{F}_2^n$ 构成的集合, 即

$$C^\perp = \{a\in\mathbb{F}_2^n \mid \text{对每个 } u\in C \text{ 都有 } a\cdot u=0\},$$

容易验证 $C^\perp$ 也是 $\mathbb{F}_2^n$ 的子空间且 $\dim C^\perp = n-\dim C$, 称 $C^\perp$ 为 C 的对偶.

设 $f\in L^2(\mathbb{F}_2^n)$, 由推论 8.15 我们有

$$\frac{1}{|C|}\sum_{u\in C} f(u) = 2^{-n}\sum_{a\in C^\perp}\hat{f}(\chi_a),$$

显然 $(C^\perp)^\perp = C$, 又 $|C^\perp| = 2^n/|C|$, 上式交换 C, $C^\perp$ 可以得到

$$\sum_{a\in C^\perp} f(a) = |C|^{-1}\sum_{u\in C}\hat{f}(\chi_u). \tag{8.4}$$

对任意 $v\in\mathbb{F}_2^n$, v 是 $\mathbb{F}_2$ 上的一个 n-维向量, 定义 v 的 Hamming 重量 $w_H(v)$ 为 v 中为 1 的分量个数, 对于给定的 $x,y\in C$, 定义 $f\in L^2(\mathbb{F}_2^n)$ 为

$$f(v) = x^{n-w_H(v)}y^{w_H(v)},$$

其中 $v\in\mathbb{F}_2^n$. 下面计算 $\hat{f}(\chi_u)$, 记 $u=(u_1,u_2,\cdots,u_n)$, 其中 $u_1,u_2,\ldots,u_n\in\mathbb{F}_2$, 对任意 $a\in\mathbb{F}_2^n$, 也记 $a=(a_1,a_2,\cdots,a_n)$, 其中 $a_1,a_2,\ldots,a_n\in\mathbb{F}_2$, 则有

$$\hat{f}(\chi_u) = \sum_{a\in\mathbb{F}_2^n} f(a)(-1)^{a\cdot u} = \prod_{i=1}^{n}\left(\sum_{a_i=0}^{1}(-1)^{a_iu_i}x^{1-a_i}y^{a_i}\right).$$

若 $u_i = 0$, 则有 $\sum_{a_i=0}^{1}(-1)^{a_i u_i}x^{1-a_i}y^{a_i} = x + y$, 而若 $u_i = 1$, 则有 $\sum_{a_i=0}^{1}(-1)^{a_i u_i}x^{1-a_i}y^{a_i} = x - y$, 从而 $\hat{f}(\chi_u) = (x+y)^{n-w_H(u)}(x-y)^{w_H(u)}$.

对于 $\mathbb{F}_2^n$ 的任一子空间 C, 定义 A_i 为 C 中 Hamming 重量为 i 的元素个数并定义 C 的重量计数多项式为

$$W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i,$$

由上面关于 f 的定义显然有 $W_C(x,y) = \sum_{v\in C} f(v)$. 由式 (8.4) 我们得到

$$W_{C^\perp}(x,y) = \frac{1}{|C|}\sum_{u\in C}\hat{f}(\chi_u) = \frac{1}{|C|}\sum_{u\in C}(x+y)^{n-w_H(u)}(x-y)^{w_H(u)} = \frac{1}{|C|}W_C(x+y,x-y).$$

上式称为 MacWilliam 恒等式, 它给出了二元线性码与其对偶码的重量计数多项式之间的联系, 是 MacWilliam 于 1963 年在她的博士论文中证明的, 著名编码学家 van Lint 称 MacWilliam 恒等式为编码理论中最基本结论之一. (对一般的 q 元线性码也有类似的 MacWilliam 恒等式) □

例 8.7: 设 Γ 为有限简单图, 其顶点集合为 $V(\Gamma) = \{v_1, v_2, \cdots, v_n\}$, 图 Γ 的邻接矩阵 A_Γ 为一个 n 阶方阵, 其 (i,j) 位置元素 a_{ij} 为

$$a_{ij} = \begin{cases} 1, & \text{若顶点 } v_i \text{ 与 } v_j \text{ 相邻,} \\ 0, & \text{其它.} \end{cases}$$

图 Γ 的特征值定义为它的邻接矩阵 A_Γ 的特征值, 由于矩阵 A_Γ 为实对称矩阵, 所以图 Γ 的特征值都是实数. 图的特征值及其重数的研究 (称图谱理论) 是图论中一个重要的研究领域, 在化学、统计力学、通信网络、信息科学等领域也有着重要的应用.

设 G 为一个有限群, A 是 G 的一个非空子集, 满足 $1_G \notin A$ 和 $A^{-1} = \{a^{-1} \mid a \in A\} = A$ (即 A 中每个元素的逆元仍在 A 中). 定义 G 由 A 生成的 Cayley 图为图 Γ, 其顶点集为 G 且两个顶点 x 和 y 相邻当且仅当 $x^{-1}y \in A$, G 由 A 生成的 Cayley 图记为 $\mathrm{Cay}(G,A)$. 下面我们来看有限交换群 G 的 Cayley 图的特征值.

设 G 为有限交换群, 取定 $f \in L^2(G)$, 定义 $L^2(G)$ 上的卷积变换 (或卷积算子) $\mathcal{C}_f$ 为

$$\begin{array}{rccc} \mathcal{C}_f: & L^2(G) & \to & L^2(G) \\ & g & \mapsto & f * g, \end{array}$$

容易验证 $\mathcal{C}_f$ 保持线性空间 $L^2(G)$ 的加法与数乘, 故 $\mathcal{C}_f$ 为 $L^2(G)$ 上的线性变换. 对任意 $\chi \in \widehat{G}$ 和任意 $a \in G$, 我们有

$$\begin{aligned} \mathcal{C}_f(\chi)(a) &= (f*\chi)(a) = \sum_{b\in G} f(b)\chi(ab^{-1}) = \sum_{b\in G} f(b)\chi(a)\overline{\chi(b)} \\ &= \chi(a)\sum_{b\in G} f(b)\overline{\chi(b)} = \chi(a)\sum_{b\in G} f(b)\overline{\chi}(b) \\ &= \hat{f}(\overline{\chi})\chi(a) = (\hat{f}(\overline{\chi})\cdot\chi)(a), \end{aligned}$$

所以 $\mathcal{C}_f(\chi)=\hat{f}(\overline{\chi})\cdot\chi$. 因为 $\chi\neq 0$, 故 $\hat{f}(\overline{\chi})$ 为线性变换 $\mathcal{C}_f$ 的特征值, χ 为对应的特征向量. 由于 $\widehat{G}$ 组成 $L^2(G)$ 的一个标准正交基, 所以卷积变换 $\mathcal{C}_f$ 的所有特征值恰为 $\hat{f}(\overline{\chi})$, 其中 $\chi\in\widehat{G}$. 因为当 χ 跑遍 $\widehat{G}$ 中所有元素时, $\overline{\chi}$ 也跑遍 $\widehat{G}$ 中所有元素, 所以卷积变换 $\mathcal{C}_f$ 的所有特征值也恰为 $\hat{f}(\chi)$, 其中 $\chi\in\widehat{G}$.

考虑子集 A 的特征函数 f_A 定义的卷积变换 $\mathcal{C}_{f_A}$, 容易计算得到 $\mathcal{C}_{f_A}(\delta_a)=\sum_{b\in A}\delta_{ab}$, 即 $\mathcal{C}_{f_A}$ 在 $L^2(G)$ 的基 $\{\delta_a\mid a\in G\}$ 下的矩阵就是 Cayley 图 $\mathrm{Cay}(G,A)$ 的邻接矩阵, 从而 Cayley 图 $\mathrm{Cay}(G,A)$ 的特征值就是卷积变换 $\mathcal{C}_{f_A}$ 的特征值. 由前面的讨论我们得到 Cayley 图 $\mathrm{Cay}(G,A)$ 的所有特征值恰为 $\widehat{f_A}(\chi)$, 其中 $\chi\in\widehat{G}$, 由例 8.4 我们知道 $\widehat{f_A}(\chi)=\chi(A)=\sum_{a\in A}\chi(a)$, 从而 Cayley 图 $\mathrm{Cay}(G,A)$ 的所有特征值恰为 $\chi(A)$, 其中 χ 跑遍 $\widehat{G}$ 中的所有元素. 由 G 的主特征可以得到 $\mathrm{Cay}(G,A)$ 的一个特征值 $\chi_0(A)=|A|$.

超立方体图是加法群 $\mathbb{F}_2^n$ 上的 Cayley 图 $\mathrm{Cay}(\mathbb{F}_2^n,A)$, 其中 A 为 $\mathbb{F}_2^n$ 中所有 Hamming 重量为 1 的向量构成的集合, 即 $A=\{v\in\mathbb{F}_2^n\mid w_H(v)=1\}$, 则显然有 $(0,0,\ldots,0)=1_{\mathbb{F}_2^n}\notin A$ 且 $-A=A$. 对每个 $a\in\mathbb{F}_2^n$, 记 $a=(a_1,a_2,\cdots,a_n)$, 其中 $a_1,a_2,\ldots,a_n\in\mathbb{F}_2$, 我们可以得到超立方体图的一个特征值为

$$\chi_a(A)=\sum_{i=1}^{n}(-1)^{a_i}=n-2w_H(a),$$

当 a 跑遍 $\mathbb{F}_2^n$ 中的所有元素我们就得到超立方体图的所有特征值. 显然对任意 $a\in\mathbb{F}_2^n$, $0\leq w_H(a)\leq n$, 所以超立方体图的互不相同的特征值有 $n+1$ 个, 分别为 n, $n-2$, $n-4$, $\ldots$, $-n+2$, $-n$. □

8.3 Gauss 和

设 λ 和 χ 分别是有限域 $\mathbb{F}_q$ 的一个加法特征和乘法特征, 定义 Gauss 和 $G(\chi,\lambda)$ 为

$$G(\chi,\lambda)=\sum_{c\in\mathbb{F}_q^*}\chi(c)\lambda(c).$$

由于 $\lambda\in\widehat{\mathbb{F}_q}$, 所以 λ 是 $\mathbb{F}_q$ 上的复值函数且 $\lambda(0)=1$, $\lambda|_{\mathbb{F}_q^*}$ 是 $\mathbb{F}_q^*$ 上的复值函数, 由 Gauss 和的定义可知 $G(\chi,\lambda)$ 就是 $\lambda|_{\mathbb{F}_q^*}$ 的 Fourier 变换在 χ 处的取值, 即 $G(\chi,\lambda)=\widehat{\lambda|_{\mathbb{F}_q^*}}(\chi)$. 由定理 8.10 得到对任意 $c\in\mathbb{F}_q^*$ 有

$$\lambda(c)=\frac{1}{q-1}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}G(\chi,\lambda)\overline{\chi}(c).$$

另一方面, χ 是 $\mathbb{F}_q^*$ 上的复值函数, 我们可以通过定义 $\chi(0)=0$ 把 χ 扩展为 $\mathbb{F}_q$ 上的复值函数, 则这时有 $G(\chi,\lambda)=\sum_{c\in\mathbb{F}_q}\chi(c)\lambda(c)$, 故它也可以看成是 χ 的 Fourier 变换在 λ 处的取值, 即

$G(\chi,\lambda)=\widehat{\chi}(\lambda)$. 这时继续利用 Fourier 反变换我们得到对任意 $x\in\mathbb{F}_q$ 有

$$\chi(x)=\frac{1}{q}\sum_{\lambda\in\widehat{\mathbb{F}_q}}G(\chi,\lambda)\overline{\lambda}(x).$$

我们定义了对任意 $\chi\in\widehat{\mathbb{F}_q^*}$, $\chi(0)=0$, 所以在上式中令 $x=0$, 则对任意给定的 $\chi\in\widehat{\mathbb{F}_q^*}$ 有

$$\sum_{\lambda\in\widehat{\mathbb{F}_q}}G(\chi,\lambda)=0.$$

进一步地, 由例 8.2 我们知道, 对于任意 $c\in\mathbb{F}_q^*$, $\chi(c)$ 为 ζ_{q-1} 的方幂, 而 $\lambda(c)$ 是 ζ_p 的方幂, 其中 $p=\mathrm{char}\mathbb{F}_q$, 由此 $G(\chi,\lambda)$ 形为 $G(\chi,\lambda)=\sum_{i,j}a_{ij}\zeta_{q-1}^i\zeta_p^j$, 其中 $a_{ij}\in\mathbb{Z}$. 由于 ζ_{q-1} 和 ζ_p 都是单位根, 从而都是代数整数, 故 $G(\chi,\lambda)$ 也是代数整数. 再利用例 8.2, $\mathbb{F}_q$ 的每个加法特征形如 λ_a, 对某个 $a\in\mathbb{F}_q$, 其中 λ_a 的定义为 $\lambda_a(c)=\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ac)}$. 若我们取 $\lambda=\lambda_a$, 其中 $a\in\mathbb{F}_q$, 则 Gauss 和 $G(\chi,\lambda)$ 也记作 $G_a(\chi)$, 即

$$G_a(\chi)=\sum_{c\in\mathbb{F}_q^*}\chi(c)\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ac)}.$$

特别地, 若 $a=1$, 即 λ 为 $\mathbb{F}_q$ 的典范加法特征, 则 Gauss 和 $G_1(\chi)$ 记作 $G(\chi)$. 下面我们依然用 λ_0 和 χ_0 分别表示 $\mathbb{F}_q$ 的主加法特征和主乘法特征.

定理 8.16: 设 $\lambda\in\widehat{\mathbb{F}_q}$, $\chi\in\widehat{\mathbb{F}_q^*}$, 则有

$$G(\chi,\lambda)=\begin{cases}q-1, & \text{若 }\chi=\chi_0,\ \lambda=\lambda_0,\\ -1, & \text{若 }\chi=\chi_0,\ \lambda\neq\lambda_0,\\ 0, & \text{若 }\chi\neq\chi_0,\ \lambda=\lambda_0,\end{cases}$$

而若 $\chi\neq\chi_0$ 且 $\lambda\neq\lambda_0$, 则有 $|G(\chi,\lambda)|=\sqrt{q}$.

证明: $G(\chi_0,\lambda_0)=q-1$ 是显然的. 利用定理 8.6, 对于 $\lambda\neq\lambda_0$ 以及 $\chi\neq\chi_0$, 我们有

$$G(\chi_0,\lambda)=\sum_{c\in\mathbb{F}_q^*}\chi_0(c)\lambda(c)=\sum_{c\in\mathbb{F}_q^*}\lambda(c)=\sum_{c\in\mathbb{F}_q}\lambda(c)-\lambda(0)=0-1=-1$$

和

$$G(\chi,\lambda_0)=\sum_{c\in\mathbb{F}_q^*}\chi(c)\lambda_0(c)=\sum_{c\in\mathbb{F}_q^*}\chi(c)=0.$$

对于 $\chi\neq\chi_0$ 且 $\lambda\neq\lambda_0$, 我们有

$$|G(\chi,\lambda)|^2=\overline{G(\chi,\lambda)}G(\chi,\lambda)=\sum_{c\in\mathbb{F}_q^*}\overline{\chi(c)\lambda(c)}\sum_{d\in\mathbb{F}_q^*}\chi(d)\lambda(d)=\sum_{c,d\in\mathbb{F}_q^*}\chi(c^{-1}d)\lambda(-c+d),$$

令 $a=c^{-1}d$, 即 $d=ca$, 则有

$$|G(\chi,\lambda)|^2=\sum_{c,a\in\mathbb{F}_q^*}\chi(a)\lambda(c(a-1))=\sum_{a\in\mathbb{F}_q^*}\chi(a)\left(\sum_{c\in\mathbb{F}_q}\lambda(c(a-1))-1\right)=\sum_{a\in\mathbb{F}_q^*}\chi(a)\sum_{c\in\mathbb{F}_q}\lambda(c(a-1)).$$

由于

$$\sum_{c\in\mathbb{F}_q}\lambda(c(a-1))=\begin{cases}q, & \text{若 }a=1,\\ 0, & \text{若 }a\neq1,\end{cases}$$

所以 $|G(\chi,\lambda)|^2=\chi(1)q=q$, 从而 $|G(\chi,\lambda)|=\sqrt{q}$. □

定理 8.17: Gauss 和有如下性质:

(i) 对任意 $a\in\mathbb{F}_q^*$, $b\in\mathbb{F}_q$, 有 $G_{ab}(\chi)=\overline{\chi(a)}G_b(\chi)$. 特别地, $G_a(\chi)=\overline{\chi(a)}G(\chi)$.

(ii) $G(\chi,\overline{\lambda})=\chi(-1)G(\chi,\lambda)$, $G(\overline{\chi},\lambda)=\chi(-1)\overline{G(\chi,\lambda)}$.

(iii) 设 $\chi\neq\chi_0$ 且 $\lambda\neq\lambda_0$, 则 $G(\chi,\lambda)G(\overline{\chi},\lambda)=\chi(-1)q$.

(iv) 设 $p=\mathrm{char}\mathbb{F}_q$, 则对任意 $b\in\mathbb{F}_q$ 有 $G_b(\chi^p)=G_{b^p}(\chi)$.

证明: (i) 对任意 $c\in\mathbb{F}_q$, $\lambda_{ab}(c)=\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(abc)}=\lambda_b(ac)$, 从而

$$G_{ab}(\chi)=\sum_{c\in\mathbb{F}_q^*}\chi(c)\lambda_{ab}(c)=\chi(a^{-1})\sum_{c\in\mathbb{F}_q^*}\chi(ac)\lambda_b(ac)=\overline{\chi(a)}G(\chi,\lambda_b)=\overline{\chi(a)}G_b(\chi).$$

(ii) 对任意 $c\in\mathbb{F}_q^*$, $\overline{\lambda}(c)=\lambda^{-1}(c)=\lambda(-c)$, 所以

$$G(\chi,\overline{\lambda})=\sum_{c\in\mathbb{F}_q^*}\chi(c)\overline{\lambda}(c)=\chi(-1)\sum_{c\in\mathbb{F}_q^*}\chi(-c)\lambda(-c)=\chi(-1)G(\chi,\lambda).$$

进一步地, 由于 $\chi(-1)=\pm1$, 所以 $\overline{\chi}(-1)=\overline{\chi(-1)}=\chi(-1)$, 从而

$$G(\overline{\chi},\lambda)=\overline{\chi}(-1)G(\overline{\chi},\overline{\lambda})=\chi(-1)\overline{G(\chi,\lambda)}.$$

(iii) 由 (ii) 和定理 8.16 得到对于 $\chi\neq\chi_0$ 且 $\lambda\neq\lambda_0$,

$$G(\chi,\lambda)G(\overline{\chi},\lambda)=\chi(-1)G(\chi,\lambda)\overline{G(\chi,\lambda)}=\chi(-1)|G(\chi,\lambda)|^2=\chi(-1)q.$$

(iv) 由于对任意 $c\in\mathbb{F}_q^*$, $\chi^p(c)=\chi(c^p)$, $\lambda_b(c)=\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(bc)}=\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b^pc^p)}=\lambda_{b^p}(c^p)$, 所以

$$G_b(\chi^p)=\sum_{c\in\mathbb{F}_q^*}\chi^p(c)\lambda_b(c)=\sum_{c\in\mathbb{F}_q^*}\chi(c^p)\lambda_{b^p}(c^p)=\sum_{c^p\in\mathbb{F}_q^*}\chi(c^p)\lambda_{b^p}(c^p)=G_{b^p}(\chi),$$

上面最后这个求和我们用到当 c 跑遍 $\mathbb{F}_q$ 时, c^p 也跑遍 $\mathbb{F}_q$ (这是因为 $c\mapsto c^p$ 是域 $\mathbb{F}_q$ 的一个自同构). □

若域 $\mathbb{F}_q$ 的特征为 2, 则对任意 $\chi\in\widehat{\mathbb{F}_q^*}$ 有 $\chi(-1)=\chi(1)=1$. 而在特征为奇素数的域 $\mathbb{F}_q$ 中, 设 α 为 $\mathbb{F}_q$ 的一个本原元素, 则 $-1=\alpha^{\frac{q-1}{2}}$, 所以对任意 $\chi\in\widehat{\mathbb{F}_q^*}$, 我们有 $\chi(-1)^2=\chi(1)=1$, 故 $\chi(-1)=\pm1$. 进一步地, 设 χ 为 $\mathbb{F}_q$ 的 d 阶乘法特征, 其中 $d\mid(q-1)$. 若 $\chi(-1)=-1$, 由于 $\chi(-1)^d=\chi^d(-1)=\chi_0(-1)=1$, 所以 d 一定为偶数. 另外若 d 为偶数, 由于 χ 为 $\mathbb{F}_q$ 的 d 阶乘法特征, 所以 $\chi(\alpha)$ 为 d 次本原单位根, 即 $\chi(\alpha)^{\frac{d}{2}}=-1$. 从而

$$\chi(-1)=\chi(\alpha^{\frac{q-1}{2}})=\chi(\alpha)^{\frac{q-1}{2}}=(\chi(\alpha)^{\frac{d}{2}})^{\frac{q-1}{d}}=(-1)^{\frac{q-1}{d}},$$

故 $\chi(-1)=-1$ 当且仅当 $\frac{q-1}{d}$ 为奇数. 由于 q 为奇数, 所以若 $\frac{q-1}{d}$ 为奇数则必有 d 为偶数. 这样我们便证明了对于任意 $\chi\in\widehat{\mathbb{F}_q^*}$, $\chi(-1)=-1$ 当且仅当 $\frac{q-1}{d}$ 为奇数, 其中 d 为 χ 在群 $\widehat{\mathbb{F}_q^*}$ 中的阶. 特别地, 对于 2 阶乘法特征 η, $\eta(-1)=-1$ 当且仅当 $\frac{q-1}{2}$ 为奇数, 即当且仅当 $q\equiv3\,(\mathrm{mod}\ 4)$.

由定理 8.16 我们得到 $G_0(\chi)=q-1$ 或者 0, 而对于 $a\neq0$, 由定理 8.17 (i) 知 $G_a(\chi)=\overline{\chi(a)}G(\chi)$, 所以在 Gauss 和的计算中, 我们只需计算 Gauss 和 $G(\chi)$ 即可. 我们知道 $G(\chi_0)=$

-1, 而对 $\chi \neq \chi_0$, $|G(\chi)| = \sqrt{q}$, 所以 $G(\chi) = e^{i\theta}\sqrt{q}$, 其中 $0 \leq \theta < 2\pi$, 故计算 $G(\chi)$ 也就是求出辐角 θ. 计算 Gauss 和的确切值是代数数论的一个重要问题, 目前也只计算了部分 $G(\chi)$ 的值, 历史上 Gauss 首先研究了素域 $\mathbb{F}_p$ 上的 Gauss 和并用于解决一些数论问题.

设 q 为奇素数幂, χ_0 是 $\mathbb{F}_q$ 唯一的 1 阶乘法特征, η 是 $\mathbb{F}_q$ 唯一的 2 阶乘法特征, 下面我们来求 Gauss 和 $G(\eta)$. 由于 $\overline{\eta} = \eta$, 所以由定理 8.17 (iii) 得到 $G(\eta)^2 = \eta(-1)q$. 因为

$$\eta(-1) = \begin{cases} 1, & \text{若 } q \equiv 1 \,(\mathrm{mod}\ 4), \\ -1, & \text{若 } q \equiv 3 \,(\mathrm{mod}\ 4), \end{cases}$$

所以

$$G(\eta) = \begin{cases} \pm\sqrt{q}, & \text{若 } q \equiv 1 \,(\mathrm{mod}\ 4), \\ \pm i\sqrt{q}, & \text{若 } q \equiv 3 \,(\mathrm{mod}\ 4), \end{cases}$$

而困难之处是确定其中的正负号.

首先假设 $q = p$ 为一个奇素数, 这时 $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$, $\widehat{\mathbb{F}_p} = \{\lambda_0, \lambda_1, \ldots, \lambda_{p-1}\}$, 其中 $\lambda_j(c) = \zeta_p^{jc}$, $0 \leq j, c \leq p-1$. 设群 $\mathbb{F}_p^*$ 的一个生成元为 g, 即 $\mathbb{F}_p^* = \{g^k \mid 0 \leq k \leq p-2\}$, 则 $\widehat{\mathbb{F}_p^*} = \{\chi_0, \chi_1, \ldots, \chi_{p-2}\}$, 其中 $\chi_i(g^k) = \zeta_{p-1}^{ik}$, $0 \leq i, k \leq p-2$. 由第 8.2 节我们知道 $\{\delta_a \mid a \in \mathbb{F}_p^*\}$ 和 $\widehat{\mathbb{F}_p^*}$ 都是复线性空间 $L^2(\mathbb{F}_p^*)$ 的基. 在 $L^2(\mathbb{F}_p^*)$ 上定义变换 T 如下: 对任意 $h \in L^2(\mathbb{F}_p^*)$, $c \in \mathbb{F}_p^*$, 定义

$$T(h)(c) = \sum_{k=1}^{p-1} \zeta_p^{ck} h(k) = \sum_{k=1}^{p-1} \lambda_c(k) h(k),$$

则容易验证 T 为 $L^2(\mathbb{F}_p^*)$ 上的线性变换. 特别地, 对任意 $\chi \in \widehat{\mathbb{F}_p^*}$, $c \in \mathbb{F}_p^*$, 由定理 8.17 (i) 有

$$T(\chi)(c) = \sum_{k=1}^{p-1} \chi(k)\lambda_c(k) = G_c(\chi) = \overline{\chi}(c)G(\chi) = (G(\chi)\overline{\chi})(c),$$

所以 $T(\chi) = G(\chi)\overline{\chi}$. 由于 $\overline{\chi_0} = \chi_0$, $\overline{\eta} = \eta$ ($\eta = \chi_{\frac{p-1}{2}}$), 而对其它 χ_j, $j \neq 0, \frac{p-1}{2}$, $\overline{\chi_j} = \chi_j^{-1} = \chi_{p-1-j}$. 所以线性变换 T 在基 $\chi_0, \eta, \chi_1, \overline{\chi_1}, \ldots, \chi_{\frac{p-3}{2}}, \overline{\chi_{\frac{p-3}{2}}}$ 下的矩阵为

$$\begin{pmatrix} G(\chi_0) & & & & & & & \\ & G(\eta) & & & & & & \\ & & 0 & G(\overline{\chi_1}) & & & & \\ & & G(\chi_1) & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & & 0 & G(\overline{\chi_{\frac{p-3}{2}}}) \\ & & & & & & G(\chi_{\frac{p-3}{2}}) & 0 \end{pmatrix}. \tag{8.5}$$

注意到对于 $1 \leq j \leq \frac{p-3}{2}$, $\chi_j(-1) = \chi_j(g^{\frac{p-1}{2}}) = \zeta_{p-1}^{j\frac{p-1}{2}} = (\zeta_{p-1}^{\frac{p-1}{2}})^j = (-1)^j$. 故对于矩阵 (8.5) 中

的每一个子矩阵

$$\begin{pmatrix} 0 & G(\overline{\chi_j}) \\ G(\chi_j) & 0 \end{pmatrix},$$

其中 $1 \le j \le \frac{p-3}{2}$, 由定理 8.17 (iii) 得到其行列式为

$$-G(\chi_j)G(\overline{\chi_j}) = -\chi_j(-1)p = (-1)^{j+1}p.$$

由于 $G(\chi_0) = -1$, 所以线性变换 T 的行列式为

$$\det(T) = -G(\eta)\prod_{j=1}^{\frac{p-3}{2}}((-1)^{j+1}p) = (-1)^{\frac{p-1}{2}}G(\eta)(-1)^{\frac{(p-1)(p-3)}{8}}p^{\frac{p-3}{2}} = (-1)^{\frac{p-1}{2}}G(\eta)i^{\frac{(p-1)(p-3)}{4}}p^{\frac{p-3}{2}}.$$

容易计算得到

$$i^{\frac{(p-1)^2}{4}} = \begin{cases} 1, & \text{若 } p \equiv 1 \pmod 4, \\ i, & \text{若 } p \equiv 3 \pmod 4, \end{cases}$$

所以 $G(\eta) = \pm i^{\frac{(p-1)^2}{4}}p^{\frac{1}{2}}$, 从而

$$\det(T) = \pm(-1)^{\frac{p-1}{2}}i^{\frac{(p-1)^2}{4}+\frac{(p-1)(p-3)}{4}}p^{\frac{p-2}{2}} = \pm(-1)^{\frac{p-1}{2}}i^{\frac{(p-1)(p-2)}{2}}p^{\frac{p-2}{2}}. \tag{8.6}$$

另一方面, 对任意 $1 \le j \le p-1$ 和 $c \in \mathbb{F}_p^*$, 我们有

$$T(\delta_j)(c) = \sum_{k=1}^{p-1}\zeta_p^{ck}\delta_j(k) = \zeta_p^{cj},$$

从而 $T(\delta_j) = \sum_{k=1}^{p-1}\zeta_p^{kj}\delta_k$, 故线性变换 T 在基 $\{\delta_1, \delta_2, \ldots, \delta_{p-1}\}$ 下的矩阵为 $(t_{kj})_{1\le k,j\le p-1}$, 其中 $t_{kj} = \zeta_p^{kj}$. 这时我们可以得到线性变换 T 的行列式为

$$\begin{aligned} \det(T) &= \begin{vmatrix} \zeta_p & \zeta_p^2 & \cdots & \zeta_p^{p-1} \\ \zeta_p^2 & \zeta_p^4 & \cdots & \zeta_p^{2(p-1)} \\ \vdots & \vdots & & \vdots \\ \zeta_p^{p-1} & \zeta_p^{2(p-1)} & \cdots & \zeta_p^{(p-1)^2} \end{vmatrix} = (\zeta_p\zeta_p^2\cdots\zeta_p^{p-1}) \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \zeta_p & \zeta_p^2 & \cdots & \zeta_p^{p-1} \\ \vdots & \vdots & & \vdots \\ \zeta_p^{p-2} & \zeta_p^{2(p-2)} & \cdots & \zeta_p^{(p-1)(p-2)} \end{vmatrix} \\ &= \prod_{1\le m<n\le p-1}(\zeta_p^n - \zeta_p^m). \end{aligned}$$

令 $\xi = e^{\frac{\pi i}{p}}$, 即 $\zeta_p = \xi^2$, 则有

$$\begin{aligned} \det(T) &= \prod_{1\le m<n\le p-1}(\xi^{2n} - \xi^{2m}) = \prod_{1\le m<n\le p-1}\xi^{n+m}(\xi^{n-m} - \xi^{-(n-m)}) \\ &= \prod_{1\le m<n\le p-1}\xi^{n+m}\prod_{1\le m<n\le p-1}(\xi^{n-m} - \xi^{-(n-m)}). \end{aligned}$$

简单计算可得

$$\sum_{1\le m<n\le p-1}(n+m) = \frac{p(p-1)(p-2)}{2},$$

从而

$$\prod_{1\le m<n\le p-1}\xi^{n+m} = \xi^{\frac{p(p-1)(p-2)}{2}} = (-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{p-1}{2}}.$$

由于

$$\xi^{n-m}-\xi^{-(n-m)}=2i\sin\frac{(n-m)\pi}{p},$$

所以

$$\prod_{1\le m<n\le p-1}(\xi^{n-m}-\xi^{-(n-m)})=\prod_{1\le m<n\le p-1}2i\sin\frac{(n-m)\pi}{p}=i^{\frac{(p-1)(p-2)}{2}}\prod_{1\le m<n\le p-1}2\sin\frac{(n-m)\pi}{p}.$$

再由对任意满足条件 $1\le m<n\le p-1$ 的对 (m,n) 来说, 有 $1\le n-m\le p-2$, 故 $\sin\frac{(n-m)\pi}{p}>0$. 令 $A=\prod_{1\le m<n\le p-1}2\sin\frac{(n-m)\pi}{p}$, 则有 $A>0$ 且

$$\det(T)=(-1)^{\frac{p-1}{2}}i^{\frac{(p-1)(p-2)}{2}}A,$$

对比式 (8.6) 我们得到式 (8.6) 中的符号一定为正号且 $A=p^{\frac{p-2}{2}}$. 所以

$$G(\eta)=i^{\frac{(p-1)^2}{4}}p^{\frac{1}{2}}=\begin{cases}\sqrt{p}, & \text{若 } p\equiv 1\,(\mathrm{mod}\ 4),\\ i\sqrt{p}, & \text{若 } p\equiv 3\,(\mathrm{mod}\ 4).\end{cases}\tag{8.7}$$

我们知道, 当 p 为奇素数时, 对任意 $c\in\mathbb{F}_p^*$, $\eta(c)$ 就是 Legendre 符号 $(\frac{c}{p})$, 从而 $G(\eta)=\sum_{c=1}^{p-1}(\frac{c}{p})\zeta_p^c$. 历史上 Gauss 用了 4 年的时间首先计算出了 $G(\eta)$. 对于一般的奇素数幂 q, 为计算有限域 $\mathbb{F}_q$ 上的 Gauss 和 $G(\eta)$, 我们需要下面将证明的 Davenport-Hasse 定理.

设 s 为一个正整数, 对任意 $\lambda\in\widehat{\mathbb{F}_q}$ 和 $\chi\in\widehat{\mathbb{F}_q^*}$, 定义 $\lambda^{(s)}=\lambda\circ\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$ 和 $\chi^{(s)}=\chi\circ\mathrm{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$, 则由于 $\mathrm{Tr}_{\mathbb{F}_q^s/\mathbb{F}_q}$ 保持加法以及 $\mathrm{N}_{\mathbb{F}_q^s/\mathbb{F}_q}$ 保持乘法, 有 $\lambda^{(s)}\in\widehat{\mathbb{F}_{q^s}}$ 和 $\chi^{(s)}\in\widehat{\mathbb{F}_{q^s}^*}$, 分别称 $\lambda^{(s)}$ 和 $\chi^{(s)}$ 为 $\mathbb{F}_q$ 的加法特征 λ 和乘法特征 χ 在扩域 $\mathbb{F}_{q^s}$ 上的提升. 显然主特征的提升依然为主特征. 进一步地, 容易验证, 若 $\lambda=\lambda_1$ 为 $\mathbb{F}_q$ 的典范加法特征, 则 $\lambda^{(s)}$ 也是 $\mathbb{F}_{q^s}$ 上的典范加法特征. 又 $\beta\in\mathbb{F}_{q^s}^*$ 为 $\mathbb{F}_{q^s}$ 中的平方元当且仅当 $\mathrm{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\beta)$ 为 $\mathbb{F}_q$ 中的平方元, 所以若 $\chi=\eta$ 为 $\mathbb{F}_q$ 的 2 阶乘法特征, 则 $\eta^{(s)}$ 也是 $\mathbb{F}_{q^s}$ 上的 2 阶乘法特征. 下面定理给出了 χ 和 λ 得到的 $\mathbb{F}_q$ 上的 Gauss 和 $G(\chi,\lambda)$ 与它们的提升得到的 $\mathbb{F}_{q^s}$ 上的 Gauss 和 $G(\chi^{(s)},\lambda^{(s)})$ 的关系.

定理 8.18: (Davenport-Hasse 定理) 设 λ 和 χ 分别为 $\mathbb{F}_q$ 的一个加法特征和一个乘法特征, 它们不全为主特征, 设 $\lambda^{(s)}$ 和 $\chi^{(s)}$ 分别为 λ 和 χ 在扩域 $\mathbb{F}_{q^s}$ 上的提升, 则有

$$-G(\chi^{(s)},\lambda^{(s)})=(-G(\chi,\lambda))^s.$$

证明: 下面我们用 $\mathcal{M}$ 表示 $\mathbb{F}_q$ 上所有首一多项式构成的集合, $\mathcal{M}_k$ 表示 $\mathbb{F}_q$ 上所有 k 次首一多项式构成的集合, $\mathcal{I}$ 表示 $\mathbb{F}_q$ 上所有首一不可约多项式构成的集合. 对任意 $f(x)\in\mathcal{M}$, 记 $f(x)=x^n-c_{n-1}x^{n-1}+\cdots+(-1)^nc_0$, 定义 $\rho(f)=\chi(c_0)\lambda(c_{n-1})$, 这里我们依然定义对任意 $\chi\in\widehat{\mathbb{F}_q^*}$ 有 $\chi(0)=0$. 特别地, 定义 $\rho(1)=1$. 则 ρ 是集合 $\mathcal{M}$ 上的复值函数且容易验证 ρ 保持乘法, 即对任意 $f(x),g(x)\in\mathcal{M}$ 有 $\rho(fg)=\rho(f)\rho(g)$.

对 $\alpha\in\mathbb{F}_{q^s}^*$, 设 α 在 $\mathbb{F}_q$ 上的极小多项式为 $f(x)$, 则有

$$\rho(f)=\chi(\mathrm{N}_{\mathbb{F}_q(\alpha)/\mathbb{F}_q}(\alpha))\lambda(\mathrm{Tr}_{\mathbb{F}_q(\alpha)/\mathbb{F}_q}(\alpha)).$$

由于 $[\mathbb{F}_{q^s}:\mathbb{F}_q(\alpha)]=\frac{s}{\deg(f)}$, 所以

$$\begin{aligned}\rho(f)^{\frac{s}{\deg(f)}} &= \chi\left(\mathrm{N}_{\mathbb{F}_q(\alpha)/\mathbb{F}_q}(\alpha)^{\frac{s}{\deg(f)}}\right)\lambda\left(\tfrac{s}{\deg(f)}\mathrm{Tr}_{\mathbb{F}_q(\alpha)/\mathbb{F}_q}(\alpha)\right)\\ &= \chi(\mathrm{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha))\lambda(\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha))=\chi^{(s)}(\alpha)\lambda^{(s)}(\alpha).\end{aligned}$$

而对 $\alpha=0$, 由 $\chi(0)=0$ 也得到 $\chi^{(s)}(0)=0$, 从而

$$\begin{aligned}G(\chi^{(s)},\lambda^{(s)}) &= \sum_{\alpha\in\mathbb{F}_{q^s}^*}\chi^{(s)}(\alpha)\lambda^{(s)}(\alpha)=\sum_{\alpha\in\mathbb{F}_{q^s}}\chi^{(s)}(\alpha)\lambda^{(s)}(\alpha)\\ &= \sum_{f(x)\in\mathcal{I},\ \deg(f)|s}\ \sum_{f(\alpha)=0}\chi^{(s)}(\alpha)\lambda^{(s)}(\alpha)=\sum_{f(x)\in\mathcal{I},\ \deg(f)|s}\deg(f)\rho(f)^{\frac{s}{\deg(f)}}.\end{aligned}\tag{8.8}$$

设 z 为未定元, 考虑幂级数

$$L(z)=\sum_{k=0}^{\infty}\left(\sum_{g(x)\in\mathcal{M}_k}\rho(g)\right)z^k,\tag{8.9}$$

由于 $|\mathcal{M}_k|=q^k$ 且对任意 $g(x)\in\mathcal{M}_k$ 有 $|\rho(g)|=1$ 或 0, 故 $|\sum_{g(x)\in\mathcal{M}_k}\rho(g)|\le q^k$, 所以当 $|z|<q^{-1}$ 时幂级数 $L(z)$ 绝对收敛. 由多项式的唯一因式分解以及 ρ 保持乘法, 我们有

$$\begin{aligned}L(z) &= \sum_{g(x)\in\mathcal{M}}\rho(g)z^{\deg(g)}\\ &= \sum_{f(x)\in\mathcal{I}}\left(1+\rho(f)z^{\deg(f)}+\rho(f^2)z^{\deg(f^2)}+\cdots\right)\\ &= \sum_{f(x)\in\mathcal{I}}\left(1+\rho(f)z^{\deg(f)}+\rho(f)^2z^{2\deg(f)}+\cdots\right)\\ &= \prod_{f(x)\in\mathcal{I}}\frac{1}{1-\rho(f)z^{\deg(f)}}.\end{aligned}$$

对 $L(z)$ 取对数并求导 (这里取对数和求导都是对形式幂级数的运算, 因此不涉及复变函数理论) 后再乘以 z 得到

$$z\frac{d\ln L(z)}{dz}=\sum_{f(x)\in\mathcal{I}}\frac{\rho(f)\deg(f)z^{\deg(f)}}{1-\rho(f)z^{\deg(f)}},$$

把上式右端的 $(1-\rho(f)z^{\deg(f)})^{-1}$ 展成幂级数得到

$$\begin{aligned}z\frac{d\ln L(z)}{dz} &= \sum_{f(x)\in\mathcal{I}}\rho(f)\deg(f)z^{\deg(f)}\sum_{j=0}^{\infty}\left(\rho(f)z^{\deg(f)}\right)^j\\ &= \sum_{f(x)\in\mathcal{I}}\deg(f)\sum_{j=1}^{\infty}\left(\rho(f)z^{\deg(f)}\right)^j\\ &= \sum_{j=1}^{\infty}\sum_{f(x)\in\mathcal{I}}\deg(f)\rho(f)^jz^{j\deg(f)}\\ &= \sum_{j=1}^{\infty}L_jz^j,\end{aligned}\tag{8.10}$$

其中对任意 $j \geq 1$ 有

$$L_j = \sum_{f(x)\in\mathcal{I},\ \deg(f)|j} \deg(f)\rho(f)^{\frac{j}{\deg(f)}},$$

对照式 (8.8), 我们有 $L_s = G(\chi^{(s)}, \lambda^{(s)})$.

进一步地, 由于 $\mathcal{M}_0 = \{1\}$ 又 $\rho(1) = 1$, 所以

$$\sum_{g(x)\in\mathcal{M}_0} \rho(g) = 1.$$

显然 $\mathcal{M}_1 = \{x - a \mid a \in \mathbb{F}_q\}$, 又 $\rho(x - a) = \chi(a)\lambda(a)$, 故

$$\sum_{g(x)\in\mathcal{M}_1} \rho(g) = \sum_{a\in\mathbb{F}_q} \chi(a)\lambda(a) = G(\chi, \lambda).$$

对于 $k \geq 2$, 我们有

$$\begin{aligned}\sum_{g(x)\in\mathcal{M}_k} \rho(g) &= \sum_{c_0,\ldots,c_{k-1}\in\mathbb{F}_q} \rho(x^k - c_{k-1}x^{k-1} + \cdots + (-1)^k c_0) = \sum_{c_0,\ldots,c_{k-1}\in\mathbb{F}_q} \chi(c_0)\lambda(c_{k-1}) \\ &= q^{k-2}\left(\sum_{c_0\in\mathbb{F}_q} \chi(c_0)\right)\left(\sum_{c_{k-1}\in\mathbb{F}_q} \lambda(c_{k-1})\right) = 0.\end{aligned}$$

所以式 (8.9) 定义的幂级数 $L(z) = 1 + G(\chi, \lambda)z$, 故

$$z\frac{d\ln L(z)}{dz} = \frac{G(\chi,\lambda)z}{1 + G(\chi,\lambda)z} = G(\chi,\lambda)z\sum_{j=0}^{\infty}(-G(\chi,\lambda)z)^j = \sum_{j=1}^{\infty}(-1)^{j+1}G(\chi,\lambda)^j z^j,$$

比较式 (8.10), 我们得到 $G(\chi^{(s)}, \lambda^{(s)}) = L_s = (-1)^{s+1}G(\chi,\lambda)^s = -(-G(\chi,\lambda))^s$. □

下面考察一般有限域 $\mathbb{F}_q$ 上的 Gauss 和 $G(\eta)$, 其中 η 为 $\mathbb{F}_q$ 的 2 阶乘法特征. 设 $q = p^s$, 则 $\mathbb{F}_q$ 为 $\mathbb{F}_p$ 的 s 次扩张, 由于 $\mathbb{F}_p$ 的典范加法特征和 2 阶乘法特征在 $\mathbb{F}_q$ 上的提升分别为 $\mathbb{F}_q$ 的典范加法特征和 2 阶乘法特征, 由定理 8.18 得到 $G(\eta) = (-1)^{s-1}G(\eta')^s$, 其中 η' 是 $\mathbb{F}_p$ 的 2 阶乘法特征, 由式 (8.7) 我们便证明了如下定理.

定理 8.19: 设 p 为奇素数, s 为正整数, $q = p^s$, 设 χ 为有限域 $\mathbb{F}_q$ 的 2 阶乘法特征, 则有

$$G(\eta) = \begin{cases} (-1)^{s-1}\sqrt{q}, & \text{若 } p \equiv 1 \,(\mathrm{mod}\ 4), \\ (-1)^{s-1}i^s\sqrt{q}, & \text{若 } p \equiv 3 \,(\mathrm{mod}\ 4). \end{cases}$$

□

对于 $\mathbb{F}_q$ 的阶数较小的乘法特征 χ, Gauss 和 $G(\chi)$ 也已经被算出, 但在计算过程中用到了代数数论中比较高深的知识, 这已经超出本书的范围. 本节的最后我们再给出一个用较初等的方法得到的 Gauss 和的计算结果.

定理 8.20: (Stickelberger 定理) 设 q 为素数幂, χ 为 $\mathbb{F}_{q^2}$ 的乘法特征, χ 不为主特征且在 $\widehat{\mathbb{F}^*_{q^2}}$

中的阶 m 满足 $m \mid (q+1)$, 则由 χ 得到 $\mathbb{F}_{q^2}$ 上的 Gauss 和 $G(\chi)$ 为

$$\begin{aligned} G(\chi) &= \begin{cases} q, & \text{若 } q \text{ 为偶数或 } q \text{ 为奇数且 } \frac{q+1}{m} \text{ 为偶数}, \\ -q, & \text{若 } q \text{ 和 } \frac{q+1}{m} \text{ 均为奇数}, \end{cases} \\ &= \begin{cases} q, & \text{若 } m \text{ 为奇数或 } \frac{q+1}{m} \text{ 为偶数}, \\ -q, & \text{若 } m \text{ 为偶数且 } \frac{q+1}{m} \text{ 为奇数}. \end{cases} \end{aligned}$$

证明: 设 γ 为 $\mathbb{F}_{q^2}$ 的一个本原元素, 令 $g = \gamma^{q+1} = \mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\gamma)$, 则 g 为 $\mathbb{F}_q$ 的一个本原元素. 群 $\mathbb{F}_{q^2}^*$ 关于它的子群 $\mathbb{F}_q^*$ 有 $q+1$ 个陪集, $\{\gamma^k \mid 0 \le k \le q\}$ 为陪集代表元集, 所以 $\mathbb{F}_{q^2}^*$ 中每个元素都可以唯一地表示成 $g^j\gamma^k$ 的形式, 其中 $0 \le j \le q-2$, $0 \le k \le q$. 注意到由于 χ 的阶整除 $q+1$, 我们有 $\chi(g) = \chi(\gamma^{q+1}) = \chi^{q+1}(\gamma) = 1$, 再令 λ_1 为 $\mathbb{F}_{q^2}$ 的典范加法特征, 故

$$\begin{aligned} G(\chi) &= \sum_{j=0}^{q-2}\sum_{k=0}^{q}\chi(g^j\gamma^k)\lambda_1(g^j\gamma^k) = \sum_{k=0}^{q}\chi(\gamma^k)\sum_{j=0}^{q-2}\lambda_1(g^j\gamma^k) \\ &= \sum_{k=0}^{q}\chi(\gamma)^k\sum_{b\in\mathbb{F}_q^*}\lambda_1(b\gamma^k). \end{aligned} \tag{8.11}$$

令 τ_1 为 $\mathbb{F}_q$ 的典范加法特征, 则有 $\lambda_1(b\gamma^k) = \tau_1(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(b\gamma^k)) = \tau_1(b\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\gamma^k))$, 从而

$$\sum_{b\in\mathbb{F}_q^*}\lambda_1(b\gamma^k) = \sum_{b\in\mathbb{F}_q^*}\tau_1(b\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\gamma^k)) = \begin{cases} -1, & \text{若 } \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\gamma^k) \ne 0, \\ q-1, & \text{若 } \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\gamma^k) = 0. \end{cases} \tag{8.12}$$

进一步地, $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\gamma^k) = \gamma^k + \gamma^{kq}$, 所以 $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\gamma^k) = 0$ 当且仅当 $\gamma^{k(q-1)} = -1$.

当 q 为奇数时, 若 $\gamma^{k(q-1)} = -1$, 则 $\gamma^{2k(q-1)} = 1$, 从而 $(q^2-1) \mid 2k(q-1)$, 即 $(q+1) \mid 2k$, 又 $0 \le k \le q$, 故 $k = \frac{q+1}{2}$. 所以式 (8.12) 可以改写为

$$\sum_{b\in\mathbb{F}_q^*}\lambda_1(b\gamma^k) = \begin{cases} -1, & \text{若 } 0 \le k \le q \text{ 但是 } k \ne \frac{q+1}{2}, \\ q-1, & \text{若 } k = \frac{q+1}{2}, \end{cases}$$

代入式 (8.11) 得到

$$G(\chi) = -\sum_{0\le k\le q,\ k\ne\frac{q+1}{2}}\chi(\gamma)^k + (q-1)\chi(\gamma)^{\frac{q+1}{2}} = -\sum_{0\le k\le q}\chi(\gamma)^k + q\chi(\gamma)^{\frac{q+1}{2}}. \tag{8.13}$$

由于

$$\sum_{0\le k\le q}\chi(\gamma)^k = \frac{1-\chi(\gamma)^{q+1}}{1-\chi(\gamma)} = \frac{1-\chi^{q+1}(\gamma)}{1-\chi(\gamma)} = 0,$$

而 $\chi(\gamma)^{\frac{q+1}{2}} = \chi^{\frac{q+1}{2}}(\gamma)$. 若 $\frac{q+1}{m}$ 为偶数, 则

$$\chi^{\frac{q+1}{2}}(\gamma) = (\chi^m)^{\frac{q+1}{2m}}(\gamma) = \chi_0(\gamma) = 1,$$

其中 χ_0 为 $\mathbb{F}_{q^2}$ 的主乘法特征. 若 $\frac{q+1}{m}$ 为奇数, 则 m 必为偶数, 故

$$\chi^{\frac{q+1}{2}}(\gamma) = (\chi^{\frac{m}{2}})^{\frac{q+1}{m}}(\gamma) = (\chi^{\frac{m}{2}}(\gamma))^{\frac{q+1}{m}} = (-1)^{\frac{q+1}{m}} = -1.$$

由式 (8.13), 我们有当 q 为奇数时,

$$G(\chi)=\begin{cases} q, & \text{若 } \frac{q+1}{m} \text{ 为偶数},\\ -q, & \text{若 } \frac{q+1}{m} \text{ 为奇数}. \end{cases}$$

当 q 为偶数时, 若 $\gamma^{k(q-1)}=-1=1$, 则 $(q^2-1)\mid k(q-1)$, $(q+1)\mid k$, 又 $0\leq k\leq q$, 故 $k=0$. 这时式 (8.12) 可以改写为

$$\sum_{b\in\mathbb{F}_q^*}\lambda_1(b\gamma^k)=\begin{cases} -1, & \text{若 } 1\leq k\leq q,\\ q-1, & \text{若 } k=0, \end{cases}$$

代入式 (8.11) 得到

$$G(\chi)=-\sum_{k=1}^{q}\chi(\gamma)^k+(q-1)=-\sum_{k=0}^{q}\chi(\gamma)^k+q=q.$$

把 q 为奇数和偶数这两种情形综合起来就得到定理结论的第一个表达式. 注意到由于 $m\mid(q+1)$, 所以当 q 为偶数时, m 一定为奇数. 反之若 m 为奇数, 则一定有 q 为偶数或者 q 为奇数且 $\frac{q+1}{m}$ 为偶数, 这样我们便得到定理结论的第二个表达式. □

8.4 Jacobi 和

本节中我们记 χ_0 为域 $\mathbb{F}_q$ 的主乘法特征, 即对任意 $c\in\mathbb{F}_q^*$ 均有 $\chi_0(c)=1$. 设 $\chi_1,\chi_2,\ldots,\chi_k$ 为 $\mathbb{F}_q$ 的 k 个乘法特征 (允许有相同的, 也允许等于 χ_0), $a\in\mathbb{F}_q$, 定义

$$J_a(\chi_1,\chi_2,\ldots,\chi_k)=\sum_{c_1+c_2+\cdots+c_k=a}\chi_1(c_1)\chi_2(c_2)\cdots\chi_k(c_k),$$

其中的求和取遍所有满足 $c_1+c_2+\cdots+c_k=a$ 的 $c_1,c_2,\ldots,c_k\in\mathbb{F}_q$ (后面的求和都作这样的假设). 注意到我们依然假设对任意 $\chi\in\widehat{\mathbb{F}_q^*}$, 令 $\chi(0)=0$, 所以如上的求和事实上取遍所有满足 $c_1+c_2+\cdots+c_k=a$ 的 k-元组 $(c_1,c_2,\ldots,c_k)\in\mathbb{F}_q^{*k}$, 但有时在整个域 $\mathbb{F}_q$ 上考虑可能更方便些, 这样我们就认为上面的求和有 q^{k-1} 项 (虽然有些项为 0).

若 $a\neq 0$, 令 $c_1=ab_1,c_2=ab_2,\ldots,c_k=ab_k$, 则 $c_1+c_2+\cdots+c_k=a$ 等价于 $b_1+b_2+\cdots+b_k=1$, 从而

$$\begin{aligned} J_a(\chi_1,\chi_2,\ldots,\chi_k) &= \sum_{b_1+b_2+\cdots+b_k=1}\chi_1(ab_1)\chi_2(ab_2)\cdots\chi_k(ab_k)\\ &= (\chi_1(a)\chi_2(a)\cdots\chi_k(a))\sum_{b_1+b_2+\cdots+b_k=1}\chi_1(b_1)\chi_2(b_2)\cdots\chi_k(b_k)\\ &= (\chi_1\chi_2\cdots\chi_k)(a)J_1(\chi_1,\chi_2,\ldots,\chi_k), \end{aligned}$$

所以为讨论一般的指数和 $J_a(\chi_1,\chi_2,\ldots,\chi_k)$, 其中 $a\neq 0$, 我们只需研究 $J_1(\chi_1,\chi_2,\ldots,\chi_k)$ 即可. 定义 Jacobi 和即 $J_1(\chi_1,\chi_2,\ldots,\chi_k)$, 并简记为 $J(\chi_1,\chi_2,\ldots,\chi_k)$.

若 $k=1$, 则对任意 $\chi\in\widehat{\mathbb{F}_q^*}$, 有 $J(\chi)=\chi(1)=1$, 所以 Jacobi 和只在 $k\geq 2$ 时才有意义. 当 $k\geq 2$ 时, 显然 Jacobi 和 $J(\chi_1,\chi_2,\ldots,\chi_k)$ 与其中的乘法特征 χ_i 的次序无关,

$1 \le i \le k$, 这对 $J_0(\chi_1, \chi_2, \ldots, \chi_k)$ 也是如此. 显然若 $\chi_1, \chi_2, \ldots, \chi_k$ 均为 $\mathbb{F}_q$ 的主乘法特征 χ_0, 则 $J(\chi_1, \chi_2, \ldots, \chi_k)$ 等于满足 $c_1 + c_2 + \cdots + c_k = 1$ 的 k-元组 $(c_1, c_2, \cdots, c_k) \in \mathbb{F}_q^{*k}$ 的个数, 即从满足 $c_1 + c_2 + \cdots + c_k = 1$ 的 k-元组 $(c_1, c_2, \cdots, c_k) \in \mathbb{F}_q^k$ (共 q^{k-1} 个) 中去掉使得某些 c_i 为 0 的那部分, 由容斥原理可求出

$$J(\chi_0, \chi_0, \ldots, \chi_0) = q^{k-1} - \binom{k}{1} q^{k-2} + \binom{k}{2} q^{k-3} + \cdots + (-1)^{k-1} \binom{k}{k-1} = \frac{(q-1)^k - (-1)^k}{q}.$$

而当 $c_1 + c_2 + \cdots + c_k = 0$ 时, 又多出现 $c_1 = c_2 = \cdots = c_k = 0$ 这一项, 所以当 $\chi_1, \chi_2, \ldots, \chi_k$ 均为 $\mathbb{F}_q$ 的主乘法特征 χ_0 时, 我们有

$$\begin{aligned} J_0(\chi_0, \chi_0, \ldots, \chi_0) &= q^{k-1} - \binom{k}{1} q^{k-2} + \binom{k}{2} q^{k-3} + \cdots + (-1)^{k-1} \binom{k}{k-1} + (-1)^k \\ &= J(\chi_0, \chi_0, \ldots, \chi_0) + (-1)^k = \frac{(q-1)^k + (-1)^k (q-1)}{q}. \end{aligned}$$

由此我们得到如下定理.

定理 8.21: 设 $\chi_1, \chi_2, \ldots, \chi_k$ 均为 $\mathbb{F}_q$ 的主乘法特征 χ_0, 则有

$$J(\chi_1, \chi_2, \ldots, \chi_k) = \frac{(q-1)^k - (-1)^k}{q}$$

和

$$J_0(\chi_1, \chi_2, \ldots, \chi_k) = J(\chi_1, \chi_2, \ldots, \chi_k) + (-1)^k = \frac{(q-1)^k + (-1)^k (q-1)}{q}.$$

□

下面假设 $\chi_1, \chi_2, \ldots, \chi_k$ 不全为 $\mathbb{F}_q$ 的主乘法特征, 由于 Jacobi 和的值与乘法特征的次序无关, 我们不妨假设 χ_k 不是主特征. 由于

$$\begin{aligned} J_0(\chi_1, \chi_2, \ldots, \chi_k) &= \sum_{c_1 + c_2 + \cdots + c_k = 0} \chi_1(c_1) \chi_2(c_2) \cdots \chi_k(c_k) \\ &= \sum_{c_k \in \mathbb{F}_q^*} \chi_k(c_k) \sum_{c_1 + \cdots + c_{k-1} = -c_k} \chi_1(c_1) \cdots \chi_{k-1}(c_{k-1}) \\ &= \sum_{c_k \in \mathbb{F}_q^*} \chi_k(c_k) J_{-c_k}(\chi_1, \ldots, \chi_{k-1}) \\ &= J(\chi_1, \ldots, \chi_{k-1}) \sum_{c_k \in \mathbb{F}_q^*} \chi_k(c_k) (\chi_1 \cdots \chi_{k-1})(-c_k) \\ &= (\chi_1 \cdots \chi_{k-1})(-1) J(\chi_1, \ldots, \chi_{k-1}) \sum_{c_k \in \mathbb{F}_q^*} (\chi_1 \cdots \chi_{k-1} \chi_k)(c_k) \end{aligned} \tag{8.14}$$

又因为

$$\sum_{c_k \in \mathbb{F}_q^*} (\chi_1 \cdots \chi_{k-1} \chi_k)(c_k) = \begin{cases} 0, & \text{若 } \chi_1 \cdots \chi_{k-1} \chi_k \ne \chi_0, \\ q-1, & \text{若 } \chi_1 \cdots \chi_{k-1} \chi_k = \chi_0, \end{cases}$$

从而当 $\chi_1 \cdots \chi_{k-1} \chi_k \ne \chi_0$ 时由 (8.14) 我们有 $J_0(\chi_1, \chi_2, \ldots, \chi_k) = 0$. 而当 $\chi_1 \cdots \chi_{k-1} \chi_k = \chi_0$ 时, $\chi_1 \cdots \chi_{k-1} = \chi_k^{-1} = \overline{\chi_k}$, 故 $(\chi_1 \cdots \chi_{k-1})(-1) = \overline{\chi_k}(-1) = \chi_k(-1)$, 从而由 (8.14) 得到

$$J_0(\chi_1, \chi_2, \ldots, \chi_k) = \chi_k(-1)(q-1) J(\chi_1, \ldots, \chi_{k-1}). \tag{8.15}$$

进一步地, 当 $\chi_1\cdots\chi_{k-1}\chi_k=\chi_0$ 时, $\chi_k=\chi_1^{-1}\cdots\chi_{k-1}^{-1}$, 我们有

$$\begin{aligned}
J(\chi_1,\chi_2,\ldots,\chi_k) &= \sum_{c_1+c_2+\cdots+c_k=1}\chi_1(c_1)\chi_2(c_2)\cdots\chi_k(c_k)\\
&= \sum_{c_k\in\mathbb{F}_q^*}\sum_{c_1+\cdots+c_{k-1}=1-c_k}\chi_1(c_1)\cdots\chi_{k-1}(c_{k-1})(\chi_1^{-1}\cdots\chi_{k-1}^{-1})(c_k)\\
&= \sum_{c_k\in\mathbb{F}_q^*}\sum_{c_1+\cdots+c_{k-1}=1-c_k}\chi_1(c_1)\cdots\chi_{k-1}(c_{k-1})\chi_1(c_k^{-1})\cdots\chi_{k-1}(c_k^{-1})\\
&= \sum_{c_k\in\mathbb{F}_q^*}\sum_{\frac{c_1}{c_k}+\cdots+\frac{c_{k-1}}{c_k}=\frac{1-c_k}{c_k}}\chi_1\left(\frac{c_1}{c_k}\right)\cdots\chi_{k-1}\left(\frac{c_{k-1}}{c_k}\right)\\
&= J_0(\chi_1,\ldots,\chi_{k-1})+\sum_{c_k\in\mathbb{F}_q^*,\,c_k\neq 1}J_{\frac{1-c_k}{c_k}}(\chi_1,\ldots,\chi_{k-1})\\
&= J_0(\chi_1,\ldots,\chi_{k-1})+J(\chi_1,\ldots,\chi_{k-1})\sum_{c_k\in\mathbb{F}_q^*,\,c_k\neq 1}(\chi_1\cdots\chi_{k-1})\left(\frac{1-c_k}{c_k}\right).
\end{aligned}\tag{8.16}$$

由于 $\chi_1\cdots\chi_{k-1}\chi_k=\chi_0$ 而 $\chi_k\neq\chi_0$, 从而 $\chi_1\cdots\chi_{k-1}\neq\chi_0$, 故由刚才的证明有 $J_0(\chi_1,\ldots,\chi_{k-1})=0$. 由于 c_k 遍历 $\mathbb{F}_q^*\backslash\{1\}$, 从而 $\frac{1-c_k}{c_k}=c_k^{-1}-1$ 遍历 $\mathbb{F}_q^*\backslash\{-1\}$, 故

$$\sum_{c_k\in\mathbb{F}_q^*,\,c_k\neq 1}(\chi_1\cdots\chi_{k-1})\left(\frac{1-c_k}{c_k}\right)=-(\chi_1\cdots\chi_{k-1})(-1)=-\chi_k(-1).$$

这样由 (8.16) 得到

$$J(\chi_1,\chi_2,\ldots,\chi_k)=-\chi_k(-1)J(\chi_1,\ldots,\chi_{k-1})\tag{8.17},$$

再由 (8.15) 得到

$$J_0(\chi_1,\chi_2,\ldots,\chi_k)=-(q-1)J(\chi_1,\chi_2,\ldots,\chi_k),$$

这便证明了如下定理.

定理 8.22: 设 $\chi_1,\chi_2,\ldots,\chi_k$ 为 $\mathbb{F}_q$ 的乘法特征且它们不全是主特征, 则有

$$J_0(\chi_1,\chi_2,\ldots,\chi_k)=\begin{cases}0, & \text{若 } \chi_1\chi_2\cdots\chi_k\neq\chi_0,\\ -(q-1)J(\chi_1,\chi_2,\ldots,\chi_k), & \text{若 } \chi_1\chi_2\cdots\chi_k=\chi_0.\end{cases}$$

□

定理 8.23: (约化公式) 设 $\chi_1,\chi_2,\ldots,\chi_k$ 为 $\mathbb{F}_q$ 的乘法特征且 $\chi_k\neq\chi_0$, 则有

$$J(\chi_1,\chi_2,\ldots,\chi_k)=\begin{cases}(-1)^{k-1}, & \text{若 } \chi_1=\cdots=\chi_{k-1}=\chi_0,\\ J(\chi_k,\chi_1\cdots\chi_{k-1})J(\chi_1,\ldots,\chi_{k-1}), & \text{若 } \chi_1\cdots\chi_{k-1}\neq\chi_0,\\ -qJ(\chi_1,\ldots,\chi_{k-1}), & \text{其它.}\end{cases}$$

证明: 首先简单计算可得

$$\begin{aligned} J(\chi_1,\chi_2,\ldots,\chi_k) &= \sum_{c_1+c_2+\cdots+c_k=1} \chi_1(c_1)\chi_2(c_2)\cdots\chi_k(c_k) \\ &= \sum_{c_k\in\mathbb{F}_q^*} \chi_k(c_k) \sum_{c_1+\cdots+c_{k-1}=1-c_k} \chi_1(c_1)\cdots\chi_{k-1}(c_{k-1}) \\ &= \sum_{c_k\in\mathbb{F}_q^*} \chi_k(c_k) J_{1-c_k}(\chi_1,\ldots,\chi_{k-1}) \\ &= J_0(\chi_1,\ldots,\chi_{k-1}) + J(\chi_1,\ldots,\chi_{k-1}) \sum_{c_k\in\mathbb{F}_q^*,\, c_k\neq 1} \chi_k(c_k)(\chi_1\cdots\chi_{k-1})(1-c_k) \\ &= J_0(\chi_1,\ldots,\chi_{k-1}) + J(\chi_1,\ldots,\chi_{k-1}) J(\chi_k,\chi_1\cdots\chi_{k-1}). \end{aligned} \tag{8.18}$$

因为 $\chi_k \neq \chi_0$, 故

$$J(\chi_k,\chi_0) = \sum_{c\in\mathbb{F}_q} \chi_k(c)\chi_0(1-c) = \sum_{c\in\mathbb{F}_q^*,\, c\neq 1} \chi_k(c) = -\chi_k(1) = -1.$$

所以若 $\chi_1 = \cdots = \chi_{k-1} = \chi_0$, 则 $\chi_1\cdots\chi_{k-1} = \chi_0$, 从而由 (8.18) 和定理 8.21 得到

$$J(\chi_1,\chi_2,\ldots,\chi_k) = J_0(\chi_1,\ldots,\chi_{k-1}) - J(\chi_1,\ldots,\chi_{k-1}) = (-1)^{k-1}.$$

下面设 $\chi_1,\cdots,\chi_{k-1}$ 不全是主乘法特征, 则当 $\chi_1\cdots\chi_{k-1}\neq\chi_0$ 时, 由定理 8.22 得到 $J_0(\chi_1,\ldots,\chi_{k-1}) = 0$, 从而由 (8.18) 有

$$J(\chi_1,\chi_2,\ldots,\chi_k) = J(\chi_k,\chi_1\cdots\chi_{k-1}) J(\chi_1,\ldots,\chi_{k-1}).$$

而当 $\chi_1\cdots\chi_{k-1} = \chi_0$ 时, 由 $J(\chi_k,\chi_1\cdots\chi_{k-1}) = -1$, 式 (8.18) 和定理 8.22 得到

$$\begin{aligned} J(\chi_1,\chi_2,\ldots,\chi_k) &= J_0(\chi_1,\ldots,\chi_{k-1}) - J(\chi_1,\ldots,\chi_{k-1}) \\ &= -(q-1)J(\chi_1,\ldots,\chi_{k-1}) - J(\chi_1,\ldots,\chi_{k-1}) = -qJ(\chi_1,\ldots,\chi_{k-1}). \end{aligned}$$

□

定理 8.24: 设 $\chi_1,\chi_2,\ldots,\chi_k$ 为 $\mathbb{F}_q$ 的乘法特征且不全为主特征, 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, 则有

$$J(\chi_1,\chi_2,\ldots,\chi_k) = \begin{cases} \dfrac{G(\chi_1,\lambda)G(\chi_2,\lambda)\cdots G(\chi_k,\lambda)}{G(\chi_1\chi_2\cdots\chi_k,\lambda)}, & \text{若 } \chi_1\chi_2\cdots\chi_k \neq \chi_0, \\ -\dfrac{G(\chi_1,\lambda)G(\chi_2,\lambda)\cdots G(\chi_k,\lambda)}{q}, & \text{若 } \chi_1\chi_2\cdots\chi_k = \chi_0. \end{cases}$$

证明: 由定义可知

$$\begin{aligned} G(\chi_1,\lambda)G(\chi_2,\lambda)\cdots G(\chi_k,\lambda) &= \left(\sum_{c_1\in\mathbb{F}_q}\chi_1(c_1)\lambda(c_1)\right)\left(\sum_{c_2\in\mathbb{F}_q}\chi_2(c_2)\lambda(c_2)\right)\cdots\left(\sum_{c_k\in\mathbb{F}_q}\chi_k(c_k)\lambda(c_k)\right)\\ &= \sum_{c_1,c_2,\ldots,c_k\in\mathbb{F}_q}\chi_1(c_1)\chi_2(c_2)\cdots\chi_k(c_k)\lambda(c_1+c_2+\cdots+c_k)\\ &= \sum_{a\in\mathbb{F}_q}\lambda(a)\sum_{c_1+c_2+\cdots+c_k=a}\chi_1(c_1)\chi_2(c_2)\cdots\chi_k(c_k)\\ &= \sum_{a\in\mathbb{F}_q}\lambda(a)J_a(\chi_1,\chi_2,\ldots,\chi_k). \end{aligned} \tag{8.19}$$

若 $\chi_1\chi_2\cdots\chi_k\neq\chi_0$, 则由定理 8.22 有 $J_0(\chi_1,\chi_2,\ldots,\chi_k)=0$, 从而

$$\begin{aligned} \sum_{a\in\mathbb{F}_q}\lambda(a)J_a(\chi_1,\chi_2,\ldots,\chi_k) &= \sum_{a\in\mathbb{F}_q^*}\lambda(a)J_a(\chi_1,\chi_2,\ldots,\chi_k)\\ &= \sum_{a\in\mathbb{F}_q^*}\lambda(a)(\chi_1\chi_2\cdots\chi_k)(a)J(\chi_1,\chi_2,\ldots,\chi_k)\\ &= J(\chi_1,\chi_2,\ldots,\chi_k)\sum_{a\in\mathbb{F}_q^*}\lambda(a)(\chi_1\chi_2\cdots\chi_k)(a)\\ &= J(\chi_1,\chi_2,\ldots,\chi_k)G(\chi_1\chi_2\cdots\chi_k,\lambda). \end{aligned}$$

由于 λ 不是主加法特征, 所以 $G(\chi_1\chi_2\cdots\chi_k,\lambda)\neq 0$, 故由上式和 (8.19) 得到

$$J(\chi_1,\chi_2,\ldots,\chi_k)=\frac{G(\chi_1,\lambda)G(\chi_2,\lambda)\cdots G(\chi_k,\lambda)}{G(\chi_1\chi_2\cdots\chi_k,\lambda)}.$$

若 $\chi_1\chi_2\cdots\chi_k=\chi_0$, 由假设不妨设 $\chi_k\neq\chi_0$, 则 $\chi_1\cdots\chi_{k-1}=\overline{\chi_k}\neq\chi_0$, 由式 (8.17), 定理 8.17 (iii) 和前面的证明有

$$\begin{aligned} J(\chi_1,\chi_2,\ldots,\chi_k) &= -\chi_k(-1)J(\chi_1,\ldots,\chi_{k-1})\\ &= -\chi_k(-1)\frac{G(\chi_1,\lambda)\cdots G(\chi_{k-1},\lambda)}{G(\chi_1\cdots\chi_{k-1},\lambda)}\\ &= -\chi_k(-1)\frac{G(\chi_1,\lambda)\cdots G(\chi_{k-1},\lambda)G(\chi_k,\lambda)}{G(\overline{\chi_k},\lambda)G(\chi_k,\lambda)}\\ &= -\chi_k(-1)\frac{G(\chi_1,\lambda)\cdots G(\chi_{k-1},\lambda)G(\chi_k,\lambda)}{\chi_k(-1)q}\\ &= -\frac{G(\chi_1,\lambda)G(\chi_2,\lambda)\cdots G(\chi_k,\lambda)}{q}. \end{aligned}$$

□

特别地, 取 λ 为 $\mathbb{F}_q$ 的典范加法特征, 则由定理 8.24 立得如下推论.

推论 8.25: 设 $\chi_1,\chi_2,\ldots,\chi_k$ 为 $\mathbb{F}_q$ 的乘法特征且不全为主特征, 则有

$$J(\chi_1,\chi_2,\ldots,\chi_k)=\begin{cases}\dfrac{G(\chi_1)G(\chi_2)\cdots G(\chi_k)}{G(\chi_1\chi_2\cdots\chi_k)}, & \text{若 } \chi_1\chi_2\cdots\chi_k\neq\chi_0,\\ -\dfrac{G(\chi_1)G(\chi_2)\cdots G(\chi_k)}{q}, & \text{若 } \chi_1\chi_2\cdots\chi_k=\chi_0.\end{cases}$$

□

由定理 8.16 知, 若 $\chi \in \widehat{\mathbb{F}^*}$ 和 $\lambda \in \widehat{\mathbb{F}_q}$ 均非主特征, 则 $|G(\chi,\lambda)| = q^{\frac{1}{2}}$, 再由定理 8.24 有如下定理.

定理 8.26: 设 $\chi_1, \chi_2, \ldots, \chi_k$ 均为 $\mathbb{F}_q$ 的非主乘法特征, 则有

$$|J(\chi_1,\chi_2,\ldots,\chi_k)| = \begin{cases} q^{\frac{k-1}{2}}, & \text{若 } \chi_1\chi_2\cdots\chi_k \neq \chi_0, \\ q^{\frac{k-2}{2}}, & \text{若 } \chi_1\chi_2\cdots\chi_k = \chi_0. \end{cases}$$

□

例 8.8: 设 q 为奇素数幂, $\chi_1, \chi_2, \ldots, \chi_k$ 均为 $\mathbb{F}_q$ 的 2 阶乘法特征 η, 我们来求 Jacobi 和 $J(\underbrace{\eta,\eta,\ldots,\eta}_{k\text{ 个}})$, 简记此 Jacobi 和为 $J^{(k)}(\eta)$. 若 k 为偶数, 则 $\eta^k = \chi_0$, 由推论 8.25 和定理 8.17 (iii) 有

$$J^{(k)}(\eta) = -\frac{1}{q}G(\eta)^k = -\frac{1}{q}(G(\eta)^2)^{\frac{k}{2}} = -\frac{1}{q}(\eta(-1)q)^{\frac{k}{2}} = -q^{\frac{k}{2}-1}\eta((-1)^{\frac{k}{2}}).$$

若 k 为奇数, 则 $\eta^k = \eta$, 仍由推论 8.25 和定理 8.17 (iii) 有

$$J^{(k)}(\eta) = G(\eta)^{k-1} = (G(\eta)^2)^{\frac{k-1}{2}} = (\eta(-1)q)^{\frac{k-1}{2}} = q^{\frac{k-1}{2}}\eta((-1)^{\frac{k-1}{2}}).$$

综合起来我们有

$$J^{(k)}(\eta) = \begin{cases} -q^{\frac{k}{2}-1}\eta((-1)^{\frac{k}{2}}), & \text{若 } k \text{ 为偶数}, \\ q^{\frac{k-1}{2}}\eta((-1)^{\frac{k-1}{2}}), & \text{若 } k \text{ 为奇数}. \end{cases}$$

进一步地, 记 $J_0^{(k)}(\eta)$ 为 $J_0(\underbrace{\eta,\eta,\ldots,\eta}_{k\text{ 个}})$, 则由定理 8.22 我们得到

$$J_0^{(k)}(\eta) = \begin{cases} (q-1)q^{\frac{k}{2}-1}\eta((-1)^{\frac{k}{2}}), & \text{若 } k \text{ 为偶数}, \\ 0, & \text{若 } k \text{ 为奇数}. \end{cases}$$

设 q 为奇素数幂, $a_1, a_2, \ldots, a_n \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, 我们来求方程 $a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = b$ 在 $\mathbb{F}_q^n$ 中的解的个数 $N_q(a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = b)$. 显然

$$\begin{aligned} & N_q(a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = b) \\ = & \sum_{c_1+c_2+\cdots+c_n=b} N_q(a_1x_1^2 = c_1)N_q(a_2x_2^2 = c_2)\cdots N_q(a_nx_n^2 = c_n) \\ = & \sum_{c_1+c_2+\cdots+c_n=b} [1+\eta(a_1c_1)][1+\eta(a_2c_2)]\cdots[1+\eta(a_nc_n)] \\ = & q^{n-1} + \sum_{c_1+c_2+\cdots+c_n=b} \eta(a_1c_1)\eta(a_2c_2)\cdots\eta(a_nc_n) \\ = & q^{n-1} + \eta(a_1a_2\cdots a_n)J_b^{(n)}(\eta), \end{aligned}$$

其中 $J_b^{(n)}(\eta)$ 为 $J_b(\underbrace{\eta,\eta,\ldots,\eta}_{n\text{ 个}})$. 利用上面计算出的 Jacobi 和, 若 $b \neq 0$, 则

$$J_b^{(n)}(\eta) = \eta^n(b)J^{(n)}(\eta) = \begin{cases} J^{(n)}(\eta), & \text{若 } n \text{ 为偶数}, \\ \eta(b)J^{(n)}(\eta), & \text{若 } n \text{ 为奇数}, \end{cases}$$

从而

$$N_q(a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2=b)=\begin{cases} q^{n-1}-q^{\frac{n}{2}-1}\eta((-1)^{\frac{n}{2}}a_1a_2\cdots a_n), & \text{若 } n \text{ 为偶数},\\ q^{n-1}+q^{\frac{n-1}{2}}\eta((-1)^{\frac{n-1}{2}}ba_1a_2\cdots a_n), & \text{若 } n \text{ 为奇数}. \end{cases}$$

而若 $b=0$, 则有

$$N_q(a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2=0)=\begin{cases} q^{n-1}+(q-1)q^{\frac{n}{2}-1}\eta((-1)^{\frac{n}{2}}a_1a_2\cdots a_n), & \text{若 } n \text{ 为偶数},\\ q^{n-1}, & \text{若 } n \text{ 为奇数}. \end{cases}$$

这样我们又证明了定理 7.21.

本例的最后我们来证明 Gauss 的二次互反律. 设 p 和 r 是两个互异的奇素数, 在域 $\mathbb{F}_p$ 上考虑 Jacobi 和 $J^{(r)}(\eta)$, 其中 η 是 $\mathbb{F}_p$ 的 2 阶乘法特征, 由上面的计算结果我们有

$$J^{(r)}(\eta)=p^{\frac{r-1}{2}}\eta((-1)^{\frac{r-1}{2}})=p^{\frac{r-1}{2}}\left((-1)^{\frac{r-1}{2}}\right)^{\frac{p-1}{2}}=\left(\frac{p}{r}\right)(-1)^{\frac{(p-1)(r-1)}{4}}. \tag{8.20}$$

进一步地, 由于 η 在 $\mathbb{F}_p$ 上的取值为 0 或者 ±1, 所以 Jacobi 和

$$J^{(r)}(\eta)=\sum_{c_1+c_2+\cdots+c_r=1}\eta(c_1c_2\cdots c_r)$$

的每一项都是整数. 对每个 r-元组 $(c_1,c_2,\ldots,c_r)\in\mathbb{F}_p^r$, 若这些分量 c_i 不全相同, 则 $(c_1,c_2,\ldots,c_r)$ 的循环移位可得到 r 个不同的 r-元组 $(c_1,c_2,\ldots,c_r)$, $(c_2,c_3,\ldots,c_1)$, $\ldots$, $(c_r,c_1,\ldots,c_{r-1})$ (注意这里依赖于 r 为素数), 这些 r-元组在 $J^{(r)}(\eta)$ 中的项是相同的, 所以这 r 项的和 $\equiv 0\,(\mathrm{mod}\ r)$. 而若 $c_1=c_2=\cdots=c_r$, 由于 $c_1+c_2+\cdots+c_r=1$, 所以 $c_1=c_2=\cdots=c_r=r^{-1}$, 这时 $J^{(r)}(\eta)$ 中对应的项为 $\eta^r(r^{-1})=\eta(r^{-1})=\eta(r)$ (注意这里 η^r 中的 r 为整数, 由于 r 为奇数, 所以 $\eta^r=\eta$. 而 r^{-1} 中的 r 是 $\mathbb{F}_p^*$ 中的元素, r^{-1} 为 r 在 $\mathbb{F}_p^*$ 中的逆元, 由于 $\eta(r^2)=1$, 所以 $\eta(r^{-1})=\eta(r)$). 把 $J^{(r)}(\eta)$ 中的项按对应的 r-元组的循环移位分组, 即把同一个 r-元组循环移位得到的 r 个 r-元组合成一组, 则有 $J^{(r)}(\eta)\equiv\eta(r)\,(\mathrm{mod}\ r)$, 同余式两边同时乘以 $\eta(r)$ 得到 $\eta(r)J^{(r)}(\eta)\equiv1\,(\mathrm{mod}\ r)$. 由于 $\eta(r)=\left(\frac{r}{p}\right)$, 由式 (8.20) 得到

$$\left(\frac{r}{p}\right)\left(\frac{p}{r}\right)(-1)^{\frac{(p-1)(r-1)}{4}}\equiv1\,(\mathrm{mod}\ r),$$

上面同余式两边同时乘以 $(-1)^{\frac{(p-1)(r-1)}{4}}$ 得到

$$\left(\frac{r}{p}\right)\left(\frac{p}{r}\right)\equiv(-1)^{\frac{(p-1)(r-1)}{4}}\,(\mathrm{mod}\ r), \tag{8.21}$$

由于同余式 (8.21) 的两边的整数只能为 ±1, 又 $r\geq3$, 所以 (8.21) 的同余恰为相等, 即

$$\left(\frac{r}{p}\right)\left(\frac{p}{r}\right)=(-1)^{\frac{(p-1)(r-1)}{4}}.$$

□

例 8.9: 设 $p\equiv1\,(\mathrm{mod}\ 4)$ 为奇素数, 由于 $4\mid(p-1)$, 所以域 $\mathbb{F}_p$ 有 4 阶乘法特征 χ. 对任意 $a\in\mathbb{F}_p^*$, 有 $\chi(a)^4=\chi^4(a)=\chi_0(a)=1$, 从而 $\chi(a)=\pm1$ 或 $\pm i$. 令 $\eta=\chi^2$, 即 $\mathbb{F}_p$ 的 2 阶乘法特征, 则 Jacobi 和

$$J(\chi,\eta)=\sum_{c_1+c_2=1}\chi(c_1)\eta(c_2)=\sum_{c\in\mathbb{F}_q^*,\,c\neq1}\chi(c)\eta(1-c)=A+Bi,$$

其中 $A, B \in \mathbb{Z}$. 由于 χ, η 和 $\chi\eta = \chi^3$ 都不是主特征, 所以由定理 8.26 可得

$$p = |J(\chi, \eta)|^2 = A^2 + B^2,$$

这便证出每个模 4 余 1 的素数一定是两个整数的平方和. □

定理 8.24 给出用 Gauss 和表示 Jacobi 和的表达式, 反之如何? 下面我们给出一个部分结果.

定理 8.27: 设 χ 为 $\mathbb{F}_q$ 的阶为 $m \geq 2$ 的乘法特征, λ 是 $\mathbb{F}_q$ 的一个非主加法特征, 则有

$$G(\chi, \lambda)^m = \chi(-1)q \prod_{j=1}^{m-2} J(\chi, \chi^j).$$

证明: 若 $m = 2$, 则 $\chi = \overline{\chi}$, 由定理 8.17 (iii) 得到 $G(\chi, \lambda)^2 = G(\chi, \lambda)G(\overline{\chi}, \lambda) = \chi(-1)q$, 结论成立. 下面设 $m \geq 3$, 则对任意 $1 \leq j \leq m-2$, χ, χ^j 和 $\chi\chi^j = \chi^{j+1}$ 都不是主特征, 由定理 8.24 有

$$J(\chi, \chi^j) = \frac{G(\chi, \lambda)G(\chi^j, \lambda)}{G(\chi^{j+1}, \lambda)},$$

从而

$$\prod_{j=1}^{m-2} J(\chi, \chi^j) = \prod_{j=1}^{m-2} \frac{G(\chi, \lambda)G(\chi^j, \lambda)}{G(\chi^{j+1}, \lambda)} = \frac{G(\chi, \lambda)^{m-1}}{G(\chi^{m-1}, \lambda)}.$$

由于 $\chi^m = \chi_0$, 所以 $\chi^{m-1} = \overline{\chi}$, 故由定理 8.17 (iii) 可得

$$G(\chi, \lambda)^m = G(\chi, \lambda)G(\overline{\chi}, \lambda)\frac{G(\chi, \lambda)^{m-1}}{G(\overline{\chi}, \lambda)} = \chi(-1)q \prod_{j=1}^{m-2} J(\chi, \chi^j).$$

□

本节的最后, 我们来讨论域 $\mathbb{F}_q$ 的乘法特征 $\chi_1, \chi_2, \ldots, \chi_k$ 在扩域 $\mathbb{F}_{q^s}$ 上的提升 $\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_k^{(s)}$ 构成 $\mathbb{F}_{q^s}$ 上的 Jacobi 和 $J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_k^{(s)})$ 与 $\mathbb{F}_q$ 上的 Jacobi 和 $J(\chi_1, \chi_2, \ldots, \chi_k)$ 的关系. 显然主特征 χ_0 的提升 $\chi_0^{(s)}$ 为 $\mathbb{F}_{q^s}$ 的主乘法特征, 而 $\chi_1\chi_2\cdots\chi_k$ 的提升也恰为 $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_k^{(s)}$. 取 $\mathbb{F}_q$ 的一个非主加法特征 λ, 设它在 $\mathbb{F}_{q^s}$ 上的提升为 $\lambda^{(s)}$, 则由定理 8.18, 对每个 $1 \leq i \leq k$, 有 $G(\chi_i^{(s)}, \lambda^{(s)}) = (-1)^{s-1}G(\chi_i, \lambda)^s$ 和 $G(\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_k^{(s)}, \lambda^{(s)}) = (-1)^{s-1}G(\chi_1\chi_2\cdots\chi_k, \lambda)^s$. 由定理 8.24, 设 $\chi_1, \chi_2, \ldots, \chi_k$ 不全为主特征, 若 $\chi_1\chi_2\cdots\chi_k \neq \chi_0$, 则 $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_k^{(s)}$ 也不是主特征, 从而

$$\begin{aligned} J(\chi_1^{(s)}, \chi_2^{(s)}, \ldots, \chi_k^{(s)}) &= \frac{G(\chi_1^{(s)}, \lambda^{(s)})G(\chi_2^{(s)}, \lambda^{(s)})\cdots G(\chi_k^{(s)}, \lambda^{(s)})}{G(\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_k^{(s)}, \lambda^{(s)})} \\ &= \frac{(-1)^{s-1}G(\chi_1, \lambda)^s(-1)^{s-1}G(\chi_2, \lambda)^s\cdots(-1)^{s-1}G(\chi_k, \lambda)^s}{(-1)^{s-1}G(\chi_1\chi_2\cdots\chi_k, \lambda)^s} \\ &= (-1)^{(s-1)(k-1)}J(\chi_1, \chi_2, \ldots, \chi_k)^s. \end{aligned}$$

而若 $\chi_1\chi_2\cdots\chi_k=\chi_0$, 则 $\chi_1^{(s)}\chi_2^{(s)}\cdots\chi_k^{(s)}$ 也是主特征, 从而

$$\begin{aligned}J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_k^{(s)}) &= -\frac{1}{q^s}G(\chi_1^{(s)},\lambda^{(s)})G(\chi_2^{(s)},\lambda^{(s)})\cdots G(\chi_k^{(s)},\lambda^{(s)})\\ &= -\frac{1}{q^s}(-1)^{(s-1)k}G(\chi_1,\lambda)^sG(\chi_2,\lambda)^s\cdots G(\chi_k,\lambda)^s\\ &= (-1)^{(s-1)(k-1)}\left(-\frac{1}{q}G(\chi_1,\lambda)G(\chi_2,\lambda)\cdots G(\chi_k,\lambda)\right)^s\\ &= (-1)^{(s-1)(k-1)}J(\chi_1,\chi_2,\ldots,\chi_k)^s.\end{aligned}$$

这样我们便证明了如下定理.

定理 8.28: 设 $\chi_1,\chi_2,\ldots,\chi_k$ 为 $\mathbb{F}_q$ 的乘法特征且不全为主特征, 它们在扩域 $\mathbb{F}_{q^s}$ 上的提升分别为 $\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_k^{(s)}$, 则有

$$J(\chi_1^{(s)},\chi_2^{(s)},\ldots,\chi_k^{(s)})=(-1)^{(s-1)(k-1)}J(\chi_1,\chi_2,\ldots,\chi_k)^s.$$

□

8.5 特征和

本节我们来讨论由 $\mathbb{F}_q$ 的一个非主特征 (加法特征或乘法特征) χ 构造的特征和 $\sum_c\chi(c)$, 其中 c 取自域 $\mathbb{F}_q$ 的某些子集. 通常我们不能给出这样的特征和 (甚至于特征和的模) 的精确值, 实际上在很多应用中, 我们只需知道特征和模的上界即可.

设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, $a,b\in\mathbb{F}_q$, 和式

$$K(\lambda;a,b)=\sum_{c\in\mathbb{F}_q^*}\lambda(ac+bc^{-1})$$

称为一个 Kloosterman 和. 由定义显然有 $K(\lambda;a,b)=K(\lambda;b,a)$. 若 $a=b=0$, 则 $K(\lambda;0,0)=q-1$, 而若 a,b 中一个为 0, 另一个非零, 则 $K(\lambda;a,b)=-1$, 所以我们只需讨论 a,b 均非零的情形. 进一步地, 由于

$$\overline{K(\lambda;a,b)}=\sum_{c\in\mathbb{F}_q^*}\overline{\lambda}(ac+bc^{-1})=\sum_{c\in\mathbb{F}_q^*}\lambda(-ac-bc^{-1})=\sum_{-c\in\mathbb{F}_q^*}\lambda(a(-c)+b(-c)^{-1})=K(\lambda;a,b)$$

得到 $K(\lambda;a,b)$ 一定为实数 (上面用到了若 c 取遍 $\mathbb{F}_q^*$, 则 $-c$ 也取遍 $\mathbb{F}_q^*$).

$\mathbb{F}_q$ 的每一个加法特征 λ 可以提升为扩域 $\mathbb{F}_{q^s}$ 的加法特征 $\lambda^{(s)}=\lambda\circ\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$, 下面我们讨论由 $\lambda^{(s)}$ 构造的 Kloosterman 和与由 λ 构造的 Kloosterman 和的关系, 类似于定理 8.18 的证明这需要引入幂级数, 下面把其证明方法一般化.

用 $\mathcal{M}$ 表示 $\mathbb{F}_q$ 上所有首一多项式构成的集合, $\mathcal{M}_k$ 表示 $\mathbb{F}_q$ 上所有 k 次首一多项式构成的集合, $\mathcal{I}$ 表示 $\mathbb{F}_q$ 上所有首一不可约多项式构成的集合. 设 ρ 是集合 $\mathcal{M}$ 上的一个复值函数满足 $\rho(1)=1$, 对任意 $g(x)\in\mathcal{M}$ 有 $|\rho(g)|\le 1$, 且对任意 $g(x),h(x)\in\mathcal{M}$ 有 $\rho(gh)=\rho(g)\rho(h)$.

设 z 为未定元, 定义幂级数

$$L(z)=\sum_{k=0}^{\infty}\left(\sum_{g(x)\in\mathcal{M}_k}\rho(g)\right)z^k,$$

由于 $|\mathcal{M}_k|=q^k$ 且对任意 $g(x)\in\mathcal{M}_k$ 有 $|\rho(g)|\le 1$, 故 $|\sum_{g(x)\in\mathcal{M}_k}\rho(g)|\le q^k$, 所以当 $|z|<q^{-1}$ 时幂级数 $L(z)$ 绝对收敛. 在定理 8.18 的证明中我们已经得到

$$z\frac{d\ln L(z)}{dz}=\sum_{s=1}^{\infty}L_s z^s, \tag{8.22}$$

其中对任意 $s\ge 1$ 有

$$L_s=\sum_{f(x)\in\mathcal{I},\,\deg(f)|s}\deg(f)\rho(f)^{\frac{s}{\deg(f)}}. \tag{8.23}$$

进一步地, 假设存在一个正整数 t 使得对所有 $k>t$ 都有 $\sum_{g(x)\in\mathcal{M}_k}\rho(g)=0$, 则 $L(z)$ 是一个次数 $\le t$ 的复系数多项式且其常数项为 1, 故存在复数 $\omega_1,\omega_2,\dots,\omega_t\in\mathbb{C}$ 使得

$$L(z)=(1-\omega_1 z)(1-\omega_2 z)\cdots(1-\omega_t z).$$

从而

$$z\frac{d\ln L(z)}{dz}=-\sum_{m=1}^{t}\frac{\omega_m z}{1-\omega_m z}=-\sum_{m=1}^{t}\omega_m z\sum_{j=0}^{\infty}\omega_m^j z^j=-\sum_{s=1}^{\infty}\left(\sum_{m=1}^{t}\omega_m^s\right)z^s$$

对照式 (8.22), 对任意 $s\ge 1$, 我们有

$$L_s=-\sum_{m=1}^{t}\omega_m^s.$$

定理 8.29: 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, $\lambda^{(s)}$ 是 λ 在 $\mathbb{F}_{q^s}$ 上的提升, $a,b\in\mathbb{F}_q^*$, 则存在或为复共轭或者都是实数的复数 $\omega_1,\omega_2\in\mathbb{C}$ (仅依赖于 λ, a 和 b) 使得对任意正整数 s 有

$$K(\lambda^{(s)};a,b)=\sum_{\gamma\in\mathbb{F}_{q^s}^*}\lambda^{(s)}(a\gamma+b\gamma^{-1})=-\omega_1^s-\omega_2^s.$$

证明: 对任意 $f(x)\in\mathcal{M}$, 记 $f(x)=x^n-c_{n-1}x^{n-1}+\cdots+(-1)^{n-1}c_1x+(-1)^n c_0$, 定义

$$\rho(f)=\begin{cases}1, & \text{若 } f(x)=1,\\ 0, & \text{若 } n\ge 1 \text{ 且 } c_0=0,\\ \lambda(ac_{n-1}+bc_1c_0^{-1}), & \text{若 } n\ge 1 \text{ 且 } c_0\ne 0.\end{cases}$$

容易验证 ρ 满足上面所要求的性质, 即 $\rho(1)=1$, 对每个 $f(x)\in\mathcal{M}$ 有 $|\rho(f)|\le 1$ 且对于任意 $g(x),h(x)\in\mathcal{M}$ 有 $\rho(gh)=\rho(g)\rho(h)$. 由于 $\mathcal{M}_1=\{x-c\mid c\in\mathbb{F}_q\}$, 当 $c=0$ 时, $\rho(x)=0$, 而当 $c\ne 0$ 时, $\rho(x-c)=\lambda(ac+bc^{-1})$, 所以

$$\sum_{g(x)\in\mathcal{M}_1}\rho(g)=\sum_{c\in\mathbb{F}_q^*}\lambda(ac+bc^{-1})=K(\lambda;a,b).$$

又对 $c_0\ne 0$, 有 $\rho(x^2-c_1x+c_0)=\lambda(ac_1+bc_1c_0^{-1})=\lambda(c_1(a+bc_0^{-1}))$, 所以

$$\sum_{g(x)\in\mathcal{M}_2}\rho(g)=\sum_{c_0\in\mathbb{F}_q^*}\sum_{c_1\in\mathbb{F}_q}\lambda(c_1(a+bc_0^{-1})),$$

由于

$$\sum_{c_1\in\mathbb{F}_q}\lambda(c_1(a+bc_0^{-1}))=\begin{cases} q, & \text{若 } c_0=-a^{-1}b,\\ 0, & \text{若 } c_0\neq -a^{-1}b,\end{cases}$$

故 $\sum_{g(x)\in\mathcal{M}_2}\rho(g)=q$. 进一步地, 对于 $k\geq 3$,

$$\begin{aligned}\sum_{g(x)\in\mathcal{M}_k}\rho(g) &= \sum_{c_1,\ldots,c_{k-1}\in\mathbb{F}_q}\sum_{c_0\in\mathbb{F}_q^*}\lambda(ac_{k-1}+bc_1c_0^{-1})\\ &= q^{k-3}\left(\sum_{c_{k-1}\in\mathbb{F}_q}\lambda(ac_{k-1})\right)\left(\sum_{c_1\in\mathbb{F}_q}\sum_{c_0\in\mathbb{F}_q^*}\lambda(bc_1c_0^{-1})\right)\\ &= 0,\end{aligned}$$

所以

$$L(z)=\sum_{k=0}^{\infty}\left(\sum_{g(x)\in\mathcal{M}_k}\rho(g)\right)z^k=1+K(\lambda;a,b)z+qz^2.$$

设 $L(z)=(1-\omega_1 z)(1-\omega_2 z)$, 则显然 ω_1,ω_2 仅依赖于 λ, a 和 b, 又 $L(z)$ 的系数都是实数, 所以 ω_1 与 ω_2 或者为互为共轭的复数或者都是实数, 同时我们得到对任意正整数 s 有 $L_s=-\omega_1^s-\omega_2^s$.

下面我们来看由 (8.23) 定义的 L_s, 由于常数项为 0 的首一不可约多项式只有 $f(x)=x$, 又 $\rho(x)=0$, 所以

$$L_s=\sum_{f(x)\in\mathcal{I},\,\deg(f)|s}\deg(f)\rho(f)^{\frac{s}{\deg(f)}}=\sum_{f(x)\in\mathcal{I}\backslash\{x\},\,\deg(f)|s}\deg(f)\rho(f)^{\frac{s}{\deg(f)}}.$$

对每个 $f(x)\in\mathcal{I}\backslash\{x\}$ 且 $\deg(f)\mid s$, $f(x)$ 在 $\mathbb{F}_{q^s}$ 中有 $\deg(f)$ 个互不相同的非零根, 对 $f(x)$ 的每个非零根 γ, 容易看出 $\gamma,\gamma^q,\ldots,\gamma^{q^{s-1}}$ 就是 $f(x)$ 的所有根重复出现了 $\frac{s}{\deg(f)}$ 次, 故

$$f(x)^{\frac{s}{\deg(f)}}=(x-\gamma)(x-\gamma^q)\cdots(x-\gamma^{q^{s-1}}),$$

记 $f(x)^{\frac{s}{\deg(f)}}=x^s-c_{s-1}x^{s-1}+\cdots+(-1)^{s-1}c_1x+(-1)^sc_0$, 由迹的定义, 比较系数可得到 $c_{s-1}=\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\gamma)$ 和 $c_1c_0^{-1}=\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\gamma^{-1})$. 从而

$$\rho(f)^{\frac{s}{\deg(f)}}=\rho(f^{\frac{s}{\deg(f)}})=\lambda(a\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\gamma)+b\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\gamma^{-1}))=\lambda^{(s)}(a\gamma+b\gamma^{-1}).$$

由于 $f(x)$ 的 $\deg(f)$ 个互不相同的根在 $\mathbb{F}_q$ 上互相共轭, 它们在 $\mathbb{F}_q$ 上的极小多项式都是 $f(x)$, 所以

$$\deg(f)\rho(f)^{\frac{s}{\deg(f)}}=\sum_{\gamma\in\mathbb{F}_{q^s}^*,\,f(\gamma)=0}\lambda^{(s)}(a\gamma+b\gamma^{-1}).$$

从而

$$L_s=\sum_{f(x)\in\mathcal{I}\backslash\{x\},\,\deg(f)|s}\ \sum_{\gamma\in\mathbb{F}_{q^s}^*,\,f(\gamma)=0}\lambda^{(s)}(a\gamma+b\gamma^{-1})=\sum_{\gamma\in\mathbb{F}_{q^s}^*}\lambda^{(s)}(a\gamma+b\gamma^{-1})=K(\lambda^{(s)};a,b),$$

这样我们便证出 $K(\lambda^{(s)};a,b)=-\omega_1^s-\omega_2^s$. □

注意到定理 8.29 中出现的 ω_1 和 ω_2 满足 $\omega_1\omega_2 = q$, 所以若 ω_1 和 ω_2 是共轭的复数, 则容易导出 $|\omega_1| = |\omega_2| = \sqrt{q}$. 事实上, 若 ω_1 和 ω_2 都是实数, 我们依然有 $|\omega_1| = |\omega_2| = \sqrt{q}$ (证明略). 又 Kloosterman 和 $K(\lambda; a, b) = -\omega_1 - \omega_2$, 故

$$|K(\lambda; a, b)| \leq |\omega_1| + |\omega_2| = 2\sqrt{q},$$

这证明了如下定理.

定理 8.30: 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, $a, b \in \mathbb{F}_q^*$, 则 $|K(\lambda; a, b)| \leq 2\sqrt{q}$. □

对任意正整数 s, $x_1^s + x_2^s$ 为二元对称多项式, 可以由二元初等对称多项式表示出来, 由 §6.2 知这个表达式为

$$x_1^s + x_2^s = \sum_{j=0}^{\lfloor \frac{s}{2} \rfloor} (-1)^j \frac{s}{s-j} \binom{s-j}{j} (x_1 + x_2)^{s-2j} (x_1 x_2)^j.$$

把 x_1, x_2 用 ω_1, ω_2 代入, 则可以得到

$$K(\lambda^{(s)}; a, b) = -(\omega_1^s + \omega_2^s) = \sum_{j=0}^{\lfloor \frac{s}{2} \rfloor} (-1)^{s-j-1} \frac{s}{s-j} \binom{s-j}{j} q^j K(\lambda; a, b)^{s-2j},$$

从而我们可以直接由 $K(\lambda; a, b)$ 得到 $K(\lambda^{(s)}; a, b)$. 另外, 由于

$$\omega_1^s + \omega_2^s = (\omega_1^{s-1} + \omega_2^{s-1})(\omega_1 + \omega_2) - (\omega_1^{s-2} + \omega_2^{s-2})\omega_1\omega_2,$$

所以当 $s \geq 2$ 时, 有

$$K(\lambda^{(s)}; a, b) = -K(\lambda^{(s-1)}; a, b) K(\lambda; a, b) - qK(\lambda^{(s-2)}; a, b),$$

其中 $K(\lambda^{(0)}; a, b) = -2$, $K(\lambda^{(1)}; a, b) = K(\lambda; a, b)$. 这是计算 $K(\lambda^{(s)}; a, b)$ 的递推公式, 例如 $K(\lambda^{(2)}; a, b) = -K(\lambda; a, b)^2 + 2q$, 但是最重要的还是需要算出 $K(\lambda; a, b)$.

定理 8.31: 设 q 为奇素数幂, λ 为 $\mathbb{F}_q$ 的一个非主加法特征, η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, $a, b \in \mathbb{F}_q^*$, 则有

$$K(\lambda; a, b) = \sum_{c \in \mathbb{F}_q} \eta(c^2 - 4ab)\lambda(c).$$

证明: 对于给定的 $d \in \mathbb{F}_q$, 用 $N_q(d)$ 表示满足 $ac + bc^{-1} = d$ 的 $c \in \mathbb{F}_q^*$ 的个数. 由于 $ac + bc^{-1} = d$ 等价于 $(2ac - d)^2 = d^2 - 4ab$, 所以以 c 为未知量的方程 $ac + bc^{-1} = d$ 的解数为 $N_q(d) = 1 + \eta(d^2 - 4ab)$. 从而

$$\begin{aligned} K(\lambda; a, b) &= \sum_{c \in \mathbb{F}_q^*} \lambda(ac + bc^{-1}) = \sum_{d \in \mathbb{F}_q} N_q(d)\lambda(d) \\ &= \sum_{d \in \mathbb{F}_q} (1 + \eta(d^2 - 4ab))\lambda(d) = \sum_{d \in \mathbb{F}_q} \lambda(d) + \sum_{d \in \mathbb{F}_q} \eta(d^2 - 4ab)\lambda(d) \\ &= \sum_{d \in \mathbb{F}_q} \eta(d^2 - 4ab)\lambda(d). \end{aligned}$$

□

下面我们来讨论另一种特征和, 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, $f(x)\in\mathbb{F}_q[x]$, 其次数 $\deg(f)=n\geq 1$, 形如

$$\sum_{c\in\mathbb{F}_q}\lambda(f(c))$$

的特征和常称为 Weil 和. 显然若 $\deg(f)=1$, 不妨设 $f(x)=ax+b$, 其中 $a,b\in\mathbb{F}_q$ 且 $a\neq 0$, 则

$$\sum_{c\in\mathbb{F}_q}\lambda(f(c))=\sum_{c\in\mathbb{F}_q}\lambda(ac+b)=\lambda(b)\sum_{c\in\mathbb{F}_q}\lambda(ac)=0,$$

所以我们只需讨论次数 ≥ 2 的多项式.

首先我们考察 $f(x)$ 为二项式, 即 $f(x)=ax^n+b$ 的情形, 其中 $a\in\mathbb{F}_q^*$, $b\in\mathbb{F}_q$, 下面的定理给出了这类 Weil 和与 Gauss 和的联系.

定理 8.32: 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, n 为正整数, $d=\gcd(n,q-1)$, χ 为 $\mathbb{F}_q$ 的一个 d 阶乘法特征, $a\in\mathbb{F}_q^*$, $b\in\mathbb{F}_q$, 则有

$$\sum_{c\in\mathbb{F}_q}\lambda(ac^n+b)=\lambda(b)\sum_{j=1}^{d-1}\overline{\chi}^j(a)G(\chi^j,\lambda).$$

证明: 对于 $\psi\in\widehat{\mathbb{F}_q^*}$, 由 Gauss 和的定义知 $G(\psi,\lambda)$ 就是 $\lambda|_{\mathbb{F}_q^*}$ 的 Fourier 变换在 ψ 处的取值, 故由 Fourier 逆变换得到对任意 $c\in\mathbb{F}_q^*$ 有

$$\lambda(ac^n)=\frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}_q^*}}G(\psi,\lambda)\overline{\psi}(ac^n)=\frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}_q^*}}G(\psi,\lambda)\overline{\psi}(a)\overline{\psi}^n(c).$$

所以

$$\sum_{c\in\mathbb{F}_q}\lambda(ac^n+b)=\lambda(b)\sum_{c\in\mathbb{F}_q}\lambda(ac^n)=\lambda(b)\left(1+\frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}_q^*}}\overline{\psi}(a)G(\psi,\lambda)\sum_{c\in\mathbb{F}_q^*}\overline{\psi}^n(c)\right).\tag{8.24}$$

注意到

$$\sum_{c\in\mathbb{F}_q^*}\overline{\psi}^n(c)=\begin{cases}q-1, & \text{若 }\overline{\psi}^n=\chi_0,\\ 0, & \text{若 }\overline{\psi}^n\neq\chi_0,\end{cases}$$

其中 χ_0 为 $\mathbb{F}_q$ 的主乘法特征. 显然 $\overline{\psi}^n=\chi_0$ 当且仅当 $\psi^n=\chi_0$. 由于 $d=\gcd(n,q-1)$, 所以 $\psi^n=\chi_0$ 当且仅当 ψ 在群 $\widehat{\mathbb{F}_q^*}$ 中的阶为 d 的因子, 又由于 $\widehat{\mathbb{F}_q^*}$ 为循环群, χ 在 $\widehat{\mathbb{F}_q^*}$ 中的阶为 d, 从而 ψ 的阶整除 d 当且仅当存在 $0\leq j\leq d-1$ 使得 $\psi=\chi^j$. 这样我们便证出 $\overline{\psi}^n=\chi_0$ 当且仅当 $\psi=\chi^j$, $0\leq j\leq d-1$, 所以

$$1+\frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}_q^*}}\overline{\psi}(a)G(\psi,\lambda)\sum_{c\in\mathbb{F}_q^*}\overline{\psi}^n(c)=1+\sum_{j=0}^{d-1}\overline{\chi}^j(a)G(\chi^j,\lambda)=\sum_{j=1}^{d-1}\overline{\chi}^j(a)G(\chi^j,\lambda),$$

代入式 (8.24) 就完成了证明. □

特别地, 在定理 8.32 中若 $d=1$, 则 $\chi=\chi_0$, 我们有如下推论.

推论 8.33: 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, n 为正整数且 $\gcd(n,q-1)=1$, 则对任意 $a\in\mathbb{F}_q^*$ 和 $b\in\mathbb{F}_q$, 有

$$\sum_{c\in\mathbb{F}_q}\lambda(ac^n+b)=0.$$

□

由定理 8.9 知, 若正整数 n 满足 $\gcd(n,q-1)=1$, 则对任意 $a,b\in\mathbb{F}_q$ 且 $a\neq 0$, 多项式 ax^n+b 为 $\mathbb{F}_q$ 上的置换多项式. 而实际上由例 6.1 我们知道多项式 ax^n+b 为 $\mathbb{F}_q$ 上的置换多项式当且仅当 $\gcd(n,q-1)=1$. 进一步地, 由定理 8.16, 对任意 $1\leq j\leq d-1$, $|G(\chi^j,\lambda)|=\sqrt{q}$, 再由定理 8.32, 我们有如下结论.

定理 8.34: 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, n 为正整数且 $d=\gcd(n,q-1)$, 则对任意 $a\in\mathbb{F}_q^*$ 和 $b\in\mathbb{F}_q$, 有

$$\left|\sum_{c\in\mathbb{F}_q}\lambda(ac^n+b)\right|\leq(d-1)\sqrt{q}.$$

□

若 q 为奇素数幂, $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$, 其中 $a_2\neq 0$, 则有 $n=\deg(f)=2$, 故 $d=\gcd(n,q-1)=2$. 又

$$f(x)=a_2(x+a_1(2a_2)^{-1})^2+a_0-a_1^2(4a_2)^{-1},$$

而定理 8.32 中的乘法特征 χ 就是 2 阶乘法特征 η, 所以对 $\mathbb{F}_q$ 的任意非主加法特征 λ, 由定理 8.32 得到

$$\sum_{c\in\mathbb{F}_q}\lambda(a_2c^2+a_1c+a_0)=\lambda(a_0-a_1^2(4a_2)^{-1})\eta(a_2)G(\eta,\lambda).$$

由例 8.2 知 $\mathbb{F}_q$ 的每个非主加法特征一定形如 λ_a, 其中 $a\in\mathbb{F}_q^*$, 而由定理 8.17 (i) 知 $G(\eta,\lambda_a)=\eta(a)G(\eta)$, 上式表明我们可以求出由二次多项式得到的 Weil 和. 下面考察另一类多项式, 即 $\mathbb{F}_q$ 上的仿射多项式, 我们也可以算出这类多项式定义的 Weil 和. 下面依然使用符号 λ_b 来表示 $\mathbb{F}_q$ 的加法特征, 其中 $b\in\mathbb{F}_q$, 这里的 λ_b 定义为对 $x\in\mathbb{F}_q$, $\lambda_b(x)=\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(bx)}$, 其中 $p=\mathrm{char}\mathbb{F}_q$, 而 $\zeta_p=e^{\frac{2\pi i}{p}}$. 所以 λ_0 为主加法特征, 而 λ_b 为非主加法特征当且仅当 $b\neq 0$, 又显然有 $\lambda_b(x)=\lambda_1(bx)$.

定理 8.35: 设 $p=\mathrm{char}\mathbb{F}_q$, $f(x)=a_rx^{p^r}+a_{r-1}x^{p^{r-1}}+\cdots+a_1x^p+a_0x+a$ 为 $\mathbb{F}_q$ 上的仿射 p-多项式, λ_b 是 $\mathbb{F}_q$ 的非主加法特征 (等价于 $b\in\mathbb{F}_q^*$), 则有

$$\sum_{c\in\mathbb{F}_q}\lambda_b(f(c))=\begin{cases}\lambda_b(a)q, & \text{若 } ba_r+b^pa_{r-1}^p+\cdots+b^{p^{r-1}}a_1^{p^{r-1}}+b^{p^r}a_0^{p^r}=0,\\ 0, & \text{其它.}\end{cases}$$

证明: 设

$$L(x)=ba_rx^{p^r}+ba_{r-1}x^{p^{r-1}}+\cdots+ba_1x^p+ba_0x=b(f(x)-a),$$

则 $L(x)$ 是 $\mathbb{F}_q$ 上的线性化多项式. 对任意 $c\in\mathbb{F}_q$, 定义 $\tau(c)=\lambda_1(L(c))$, 则由于 L 保持加法, 又 λ_1 为 $\mathbb{F}_q$ 的加法特征, 所以 τ 也是 $\mathbb{F}_q$ 的加法特征, 从而

$$\sum_{c\in\mathbb{F}_q}\lambda_b(f(c))=\sum_{c\in\mathbb{F}_q}\lambda_1(bf(c))=\lambda_b(a)\sum_{c\in\mathbb{F}_q}\lambda_1(L(c))=\lambda_b(a)\sum_{c\in\mathbb{F}_q}\tau(c)=\begin{cases}\lambda_b(a)q, & \text{若 } \tau=\lambda_0,\\ 0, & \text{其它.}\end{cases}$$

故接下来我们需要确定何时有 $\tau=\lambda_0$. 由于

$$\tau(c)=\lambda_1(L(c))=\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(L(c))},$$

所以 $\tau=\lambda_0$ 当且仅当对任意 $c\in\mathbb{F}_q$ 有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(L(c))=0$. 设 $q=p^s$, 则由于

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(L(c))=\sum_{j=0}^{s-1}L(c)^{p^j},$$

所以对任意 $c\in\mathbb{F}_q$ 有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(L(c))=0$ 当且仅当

$$\sum_{j=0}^{s-1}L(x)^{p^j}\equiv 0\,(\mathrm{mod}\ (x^q-x)). \tag{8.24}$$

由于

$$\begin{aligned}\sum_{j=0}^{s-1}L(x)^{p^j} &= \sum_{j=0}^{s-1}\left(\sum_{i=0}^{r}ba_ix^{p^i}\right)^{p^j}=\sum_{j=0}^{s-1}\sum_{i=0}^{r}b^{p^j}a_i^{p^j}x^{p^{i+j}}\\ &\equiv \sum_{k=0}^{s-1}\left(\sum_{i=0}^{r}b^{p^{k-i}}a_i^{p^{k-i}}\right)x^{p^k}\ (\mathrm{mod}\ (x^q-x)),\end{aligned}$$

其中用到了若 $m\equiv n\,(\mathrm{mod}\ s)$ 则有 $x^{p^m}\equiv x^{p^n}\ (\mathrm{mod}\ (x^q-x))$, 注意到上式中当 $k<i$ 时, $\mathbb{F}_q$ 中的元素 $b^{p^{k-i}}$, $a_i^{p^{k-i}}$ 的含义是明确的, 负指数 $k-i$ 在 mod s 意义下理解为相应的非负数. 所以 (8.24) 成立当且仅当对所有的 $k=0,1,\ldots,s-1$, 有

$$\sum_{i=0}^{r}b^{p^{k-i}}a_i^{p^{k-i}}=0,$$

而这又等价于

$$\sum_{i=0}^{r}b^{p^{r-i}}a_i^{p^{r-i}}=\left(\sum_{i=0}^{r}b^{p^{k-i}}a_i^{p^{k-i}}\right)^{p^{r-k}}=0,$$

这便证明了定理. □

若 q 为偶数, 则 $\mathbb{F}_q$ 的特征为 $p=2$. 设 $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$, $a_2\neq 0$, $b\in\mathbb{F}_q^*$, 则 $ba_2+b^2a_1^2=0$ 当且仅当 $a_2=ba_1^2$, 由定理 8.35 我们有如下推论.

推论 8.36: 设 q 为偶数, $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$, $a_2\neq 0$, $b\in\mathbb{F}_q^*$, 则有

$$\sum_{c\in\mathbb{F}_q}\lambda_b(f(c))=\begin{cases}\lambda_b(a_0)q, & \text{若 } a_2=ba_1^2,\\ 0, & \text{其它,}\end{cases}$$

或者改写为

$$\sum_{c\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(b(a_2c^2+a_1c))}=\begin{cases}q, & \text{若 } a_2=ba_1^2,\\ 0, & \text{其它,}\end{cases}$$

□

接下来我们讨论 $\mathbb{F}_q$ 的非主加法特征 λ 在扩域 $\mathbb{F}_{q^s}$ 上的提升 $\lambda^{(s)}$ 对多项式 $f(x)\in\mathbb{F}_q[x]$ 构造的 Weil 和.

定理 8.37: 设多项式 $f(x)\in\mathbb{F}_q[x]$, $\deg(f)=n\geq 2$ 且 $\gcd(n,q)=1$, 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, 则存在仅依赖于 $f(x)$ 和 λ 的复数 $\omega_1,\omega_2,\ldots,\omega_{n-1}$ 使得对任意正整数 s 有

$$\sum_{\gamma\in\mathbb{F}_{q^s}}\lambda^{(s)}(f(\gamma))=-\omega_1^s-\omega_2^s-\cdots-\omega_{n-1}^s.$$

证明: 对正整数 j 和 k, 令 $s_j(x_1,x_2,\ldots,x_k)=x_1^j+x_2^j+\cdots+x_k^j$, 这是以 $x_1,x_2,\ldots,x_k$ 为未定元的对称多项式, 可由初等对称多项式 $\sigma_r:=\sigma_r(x_1,x_2,\ldots,x_k)$ 表出, 其中 $1\leq r\leq k$ 且 $\sigma_r(x_1,x_2,\ldots,x_k)$ 定义为

$$\sigma_r(x_1,x_2,\ldots,x_k)=\sum_{1\leq j_1<j_2<\cdots<j_r\leq k}x_{j_1}x_{j_2}\cdots x_{j_r}.$$

由 Waring 公式, 我们有

$$s_j(x_1,x_2,\ldots,x_k)=\sum_{i_1+2i_2+\cdots+ki_k=j}(-1)^{i_2+i_4+\cdots+i_{2\lfloor\frac{k}{2}\rfloor}}\frac{(i_1+i_2+\cdots+i_k-1)!j}{i_1!i_2!\cdots i_k!}\sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_k^{i_k},$$

其中求和取遍所有满足 $i_1+2i_2+\cdots+ki_k=j$ 的非负整数组成的 k 元组 $(i_1,i_2,\ldots,i_k)$. 显然 $s_1(x_1,x_2,\ldots,x_k)=\sigma_1$, 当 $2\leq j\leq k$ 时, $i_1+2i_2+\cdots+ki_k=j$ 有一组解为 $i_j=1$ 且对所有 $\ell\neq j$, $i_\ell=0$, $s_j(x_1,x_2,\ldots,x_k)$ 的表达式中对应着这组解的项是 $(-1)^{j-1}j\sigma_j$, 而 $i_1+2i_2+\cdots+ki_k=j$ 的其它解必满足 $i_j=i_{j+1}=\cdots=i_k=0$, 故 $s_j(x_1,x_2,\ldots,x_k)$ 的表达式中对应着这些其它解的项只包含 $\sigma_1,\ldots,\sigma_{j-1}$, 由此我们得到

$$s_j(x_1,x_2,\ldots,x_k)=\begin{cases}\sigma_1, & \text{若 } j=1,\\ (-1)^{j-1}j\sigma_j+G_j(\sigma_1,\ldots,\sigma_{j-1}), & \text{若 } 2\leq j\leq k,\\ H_j(\sigma_1,\sigma_2,\ldots,\sigma_k), & \text{若 } j>k,\end{cases}$$

其中 G_j 和 H_j 分别是 $\mathbb{F}_q$ 上的 $j-1$ 元和 k 元多项式. 设 $f(x)=b_nx^n+\cdots+b_1x+b_0$, 其中 $b_n\neq 0$. 则

$$\begin{aligned}\sum_{i=1}^k f(x_i) &= b_ns_n(x_1,x_2,\ldots,x_k)+\cdots+b_1s_1(x_1,x_2,\ldots,x_k)+kb_0\\ &= \begin{cases}(-1)^{n-1}nb_n\sigma_n+G(\sigma_1,\ldots,\sigma_{n-1}), & \text{若 } k\geq n,\\ H(\sigma_1,\sigma_2,\ldots,\sigma_k), & \text{若 } 1\leq k<n,\end{cases}\end{aligned}\tag{8.25}$$

其中 G 和 H 分别是 $\mathbb{F}_q$ 上的 $n-1$ 元和 k 元多项式.

下面在 $\mathbb{F}_q$ 上的所有首一多项式集合 $\mathcal{M}$ 上定义复值函数 $\rho:\mathcal{M}\to\mathbb{C}$ 如下: 令 $\rho(1)=1$, 而对于 $k\geq 1$, 设 $g(x)=x^k-a_{k-1}x^{k-1}+\cdots+(-1)^{k-1}a_1x+(-1)^ka_0\in\mathcal{M}_k$, 若 $g(x)$ 在 $\mathbb{F}_q$ 的扩域中的根为 $\alpha_1,\alpha_2,\ldots,\alpha_k$, 则有 $\sigma_r(\alpha_1,\alpha_2,\ldots,\alpha_k)=a_{k-r}$, $1\leq r\leq k$, 从而由 (8.25) 知道 $\sum_{i=1}^k f(\alpha_i)\in\mathbb{F}_q$. 我们定义 $\rho(g)=\lambda(\sum_{i=1}^k f(\alpha_i))$, 则显然对任意 $g(x)\in\mathcal{M}$ 有 $|\rho(g)|=1$ 且容

易验证 ρ 保持乘法. 若 $k \geq n$, 由 (8.25) 得到

$$\sum_{i=1}^{k} f(\alpha_i) = (-1)^{n-1} n b_n \sigma_n + G(\sigma_1, \ldots, \sigma_{n-1}) = (-1)^{n-1} n b_n a_0 + G(a_{k-1}, \ldots, a_{k-n+1}).$$

由于 $\gcd(n, q) = 1$, 我们有 $b = (-1)^{n-1} n b_n \neq 0$, 从而

$$\begin{aligned}
\sum_{g(x)\in\mathcal{M}_k} \rho(g) &= \sum_{a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_q} \lambda(ba_0 + G(a_{k-1}, \ldots, a_{k-n+1})) \\
&= q^{k-n} \sum_{a_0, a_{k-n+1}, \ldots, a_{k-1} \in \mathbb{F}_q} \lambda(ba_0)\lambda(G(a_{k-1}, \ldots, a_{k-n+1})) \\
&= q^{k-n} \left(\sum_{a_0 \in \mathbb{F}_q} \lambda(ba_0) \right) \left(\sum_{a_{k-n+1}, \ldots, a_{k-1} \in \mathbb{F}_q} \lambda(G(a_{k-1}, \ldots, a_{k-n+1})) \right) \\
&= 0.
\end{aligned}$$

这表明前面定义的 $L(z)$ 是一个次数不超过 $n-1$ 的复系数多项式, 与前面的讨论相同, 存在复数 $\omega_1, \omega_2, \ldots, \omega_{n-1}$ (显然仅依赖于 $f(x)$ 和 λ) 使得对任意正整数 s 有

$$L_s = -\sum_{j=1}^{n-1} \omega_j^s. \tag{8.26}$$

再来看由 (8.23) 定义的 L_s, 这时

$$L_s = \sum_{g(x)\in\mathcal{I},\, \deg(g)|s} \deg(g) \rho(g)^{\frac{s}{\deg(g)}}.$$

对每一个次数整除 s 的首一不可约多项式 $g(x)$, 设 γ 是 $g(x)$ 在 $\mathbb{F}_{q^s}$ 中的一个根, 则有

$$g(x) = (x-\gamma)(x-\gamma^q)\cdots(x-\gamma^{q^{\deg(g)-1}}),$$

故

$$\rho(g) = \lambda\left(\sum_{i=0}^{\deg(g)-1} f(\gamma^{q^i}) \right) = \lambda\left(\sum_{i=0}^{\deg(g)-1} f(\gamma)^{q^i} \right) = \lambda\left(\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}(f(\gamma)) \right),$$

所以

$$\rho(g)^{\frac{s}{\deg(g)}} = \lambda\left(\frac{s}{\deg(g)} \mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}(f(\gamma)) \right) = \lambda\left(\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(f(\gamma)) \right) = \lambda^{(s)}(f(\gamma)).$$

又 γ 换成 $g(x)$ 的其它的根得到同样的结果, 从而我们有

$$\deg(g)\rho(g)^{\frac{s}{\deg(g)}} = \sum_{\gamma\in\mathbb{F}_{q^s},\, g(\gamma)=0} \lambda^{(s)}(f(\gamma)),$$

和

$$L_s = \sum_{g(x)\in\mathcal{I},\, \deg(g)|s} \deg(g)\rho(g)^{\frac{s}{\deg(g)}} = \sum_{g(x)\in\mathcal{I},\, \deg(g)|s} \sum_{\gamma\in\mathbb{F}_{q^s},\, g(\gamma)=0} \lambda^{(s)}(f(\gamma)) = \sum_{\gamma\in\mathbb{F}_{q^s}} \lambda^{(s)}(f(\gamma)).$$

对比 (8.26) 就得到定理的证明. □

类似于定理 8.29 中的复数 ω_1 和 ω_2, 也可以证明定理 8.37 中的复数 $\omega_1, \omega_2, \ldots, \omega_{n-1}$ 的模都是 $\sqrt{q}$ (但其证明已经超出本书的范围), 由此我们可以得到如下定理.

定理 8.38: (Weil 定理) 设 $f(x)\in\mathbb{F}_q[x]$, $\deg(f)=n\geq 1$ 且 $\gcd(n,q)=1$, 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, 则有

$$\left|\sum_{c\in\mathbb{F}_q}\lambda(f(c))\right|\leq (n-1)\sqrt{q}.$$

□

设 $f(x)\in\mathbb{F}_q[x]$, 下面我们考虑特征和

$$\sum_{c\in\mathbb{F}_q}\chi(f(c)),$$

其中 χ 是 $\mathbb{F}_q$ 的一个非主乘法特征, 这里我们依然定义 $\chi(0)=0$. 若 $f(x)$ 的次数为 1, 不妨设 $f(x)=ax+b$, 其中 $a\neq 0$, 则有

$$\sum_{c\in\mathbb{F}_q}\chi(f(c))=\sum_{c\in\mathbb{F}_q}\chi(ac+b)=\chi(a)\sum_{c\in\mathbb{F}_q}\chi(c+a^{-1}b)=0,$$

所以我们只需讨论次数 ≥ 2 的多项式. 又若 $f(x)=ax^n$, 其中 $a\in\mathbb{F}_q^*$, 设 χ 在 $\widehat{\mathbb{F}_q^*}$ 中的阶为 $m\geq 2$, 则有

$$\sum_{c\in\mathbb{F}_q}\chi(f(c))=\sum_{c\in\mathbb{F}_q}\chi(ac^n)=\chi(a)\sum_{c\in\mathbb{F}_q}\chi^n(c)=\begin{cases}\chi(a)(q-1), & \text{若 } \chi^n=\chi_0,\\ 0, & \text{若 } \chi^n\neq\chi_0,\end{cases}$$

其中 χ_0 为 $\mathbb{F}_q$ 的主乘法特征. 由于 $\chi^n=\chi_0$ 当且仅当 $m\mid n$, 从而我们有

$$\sum_{c\in\mathbb{F}_q}\chi(ac^n)=\begin{cases}\chi(a)(q-1), & \text{若 } m\mid n,\\ 0, & \text{若 } m\nmid n.\end{cases}$$

例 8.10: 设 q 为奇素数幂, η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$, 其中 $a_2\neq 0$, 我们来求特征和 $\sum_{c\in\mathbb{F}_q}\eta(f(c))$. 由于 $\eta(4a_2^2)=1$, 所以

$$\begin{aligned}\sum_{c\in\mathbb{F}_q}\eta(f(c)) &= \eta(4a_2^2)\sum_{c\in\mathbb{F}_q}\eta(a_2c^2+a_1c+a_0)=\eta(a_2)\sum_{c\in\mathbb{F}_q}\eta(4a_2^2c^2+4a_1a_2c+4a_0a_2)\\ &= \eta(a_2)\sum_{c\in\mathbb{F}_q}\eta((2a_2c+a_1)^2-(a_1^2-4a_0a_2))=\eta(a_2)\sum_{b\in\mathbb{F}_q}\eta(b^2-d)\end{aligned}$$

其中 $b=2a_2c+a_1$, $d=a_1^2-4a_0a_2$. 若 $d=0$, 则显然 $\sum_{b\in\mathbb{F}_q}\eta(b^2-d)=q-1$. 若 $d\neq 0$, 用 $S_q(d)$ 表示满足 $c^2=b^2-d$ 的对 $(b,c)\in\mathbb{F}_q^2$ 的个数, 由引理 7.20 得到 $S_q(d)=q-1$. 又对于给定的 $b\in\mathbb{F}_q$, 满足 $c^2=b^2-d$ 的 $c\in\mathbb{F}_q$ 的个数为 $1+\eta(b^2-d)$, 从而

$$q-1=S_q(d)=\sum_{b\in\mathbb{F}_q}(1+\eta(b^2-d))=q+\sum_{b\in\mathbb{F}_q}\eta(b^2-d),$$

故 $\sum_{b\in\mathbb{F}_q}\eta(b^2-d)=-1$. 我们继续利用整数值函数符号 υ, 其中 $\upsilon(0)=q-1$, 而对 $d\in\mathbb{F}_q^*$ 有 $\upsilon(d)=-1$. 综合我们上面的讨论我们得到

$$\sum_{c\in\mathbb{F}_q}\eta(a_2c^2+a_1c+a_0)=\eta(a_2)\upsilon(a_1^2-4a_0a_2).$$

□

任一 $\mathbb{F}_q$ 的乘法特征 χ 都可以提升为扩域 $\mathbb{F}_{q^s}$ 的乘法特征 $\chi^{(s)} = \chi \circ \mathrm{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$, 我们有类似于定理 8.37 的结论, 其证明也与定理 8.37 的证明类似. 这里我们只列出下面这个关于指数和模的上界的定理.

定理 8.39: 设 χ 为 $\mathbb{F}_q$ 的一个 $m \geq 2$ 阶乘法特征, 设首一多项式 $f(x) \in \mathbb{F}_q[x]$ 且 $f(x)$ 不是一个多项式的 m 次方, d 为 $f(x)$ 在它的分裂域中的互异根的个数, 则对任意 $a \in \mathbb{F}_q$ 有

$$\left| \sum_{c \in \mathbb{F}_q} \chi(af(c)) \right| \leq (d-1)\sqrt{q}.$$

□

8.6 两个应用

本节我们给出 Gauss 和以及 Jacobi 和的两个应用, 第一个是关于迹给定的本原元素存在性的应用.

设 $\mathbb{F}_{q^n}$ 是 $\mathbb{F}_q$ 的 n 次扩张, 我们知道 $\mathbb{F}_{q^n}$ 的本原元素存在 (实际上有 $\phi(q^n-1)$ 个). 对于给定的 $a \in \mathbb{F}_q$, 是否存在 $\mathbb{F}_{q^n}$ 的本原元素 α 使得 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = a$? 这等价于是否存在 $\mathbb{F}_q$ 上的 n 次本原多项式使其 x^{n-1} 的系数为 $-a$. 容易知道, 若 $n = 2$, 则不存在 $\mathbb{F}_{q^2}$ 的本原元素 α 使得 $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 0$. 事实上, 若对于 $\beta \in \mathbb{F}_{q^2}^*$ 有 $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) = \beta + \beta^q = 0$, 则有 $\beta^{q-1} = -1$, 从而 $\beta^{2(q-1)} = 1$. 由于对容易素数幂 q 有 $2(q-1) < q^2 - 1$, 故 β 不是 $\mathbb{F}_{q^2}$ 的本原元素. 下面我们证明对于给定的 $a \in \mathbb{F}_q$, 除了有限对 (q, n) 外, 域 $\mathbb{F}_{q^n}$ 一定有本原元素使得其迹为 a. 我们先给出有限域 $\mathbb{F}_q$ 中的元素为本原元素的一个刻画.

引理 8.40: 对于正整数 $d \mid (q-1)$, 令 M_d 表示 $\mathbb{F}_q$ 的所有 d 阶乘法特征构成的集合, 则对任意 $c \in \mathbb{F}_q^*$, 有

$$\sum_{d|(q-1)} \frac{\mu(d)}{\phi(d)} \sum_{\chi \in M_d} \chi(c) = \begin{cases} \dfrac{q-1}{\phi(q-1)}, & \text{若 } c \text{ 为 } \mathbb{F}_q \text{ 的本原元素,} \\ 0, & \text{其它,} \end{cases}$$

其中 μ 为 Möbius 函数而 ϕ 为 Euler ϕ-函数.

证明: 由于 Möbius 函数 μ 和 Euler ϕ-函数 ϕ 都是乘积函数 (正整数集合上的函数 f 称为乘积函数若对任意互素正整数 m 和 n 有 $f(mn) = f(m)f(n)$), 我们有

$$\sum_{d|(q-1)} \frac{\mu(d)}{\phi(d)} \sum_{\chi \in M_d} \chi(c) = \prod_{p|(q-1)} \left(1 + \frac{\mu(p)}{\phi(p)} \sum_{\chi \in M_p} \chi(c) \right) = \prod_{p|(q-1)} \left(1 - \frac{1}{p-1} \sum_{\chi \in M_p} \chi(c) \right), \tag{8.27}$$

其中后面的求和指标 p 取遍 $q-1$ 的所有互异素因子. 这是因为根据 Möbius 函数 $\mu(d)$ 的定义, 只需考虑对不能被任何素数的平方整除的正整数 d 求和即可, 另由循环群 $\widehat{\mathbb{F}_q^*}$ 的结构, 对互异素数 $p_1, \ldots, p_k$, 每个 $d = p_1 \cdots p_k$ 阶乘法特征 χ 都可以唯一地表示为 $\chi_1, \ldots, \chi_k$ 的乘积, 其

中 χ_i 是 p_i 阶乘法特征, 且所有这样的乘法特征的乘积 $\chi_1\cdots\chi_k$ 都是 d 阶乘法特征. 选取 $\mathbb{F}_q$ 的一个本原元素 ω, 设 $c=\omega^k$, $0\leq k\leq q-2$. 若存在 $q-1$ 的某个素因子 p 使得 $p\mid k$, 由于 $|M_p|=\phi(p)=p-1$, 故

$$\sum_{\chi\in M_p}\chi(c)=\sum_{\chi\in M_p}\chi(\omega^k)=\sum_{\chi\in M_p}\chi^k(\omega)=\sum_{\chi\in M_p}\chi_0(\omega)=p-1.$$

若对 $q-1$ 的每个素因子 p 都有 $p\nmid k$, 设 τ 是 $\mathbb{F}_q$ 的一个给定的 p 阶乘法特征, 则 $M_p=\{\tau^j\mid 1\leq j\leq p-1\}$. 又 $\tau(\omega)$ 为 p 次本原单位根, 故 $\tau(c)=\tau(\omega)^k\neq 1$, 从而

$$\sum_{\chi\in M_p}\chi(c)=\sum_{j=1}^{p-1}\tau^j(c)=\frac{1-\tau(c)^p}{1-\tau(c)}-1=-1.$$

注意到对 $q-1$ 的每个素因子 p 都有 $p\nmid k$ 等价于 $\gcd(k,q-1)=1$, 后者也等价于 $c=\omega^k$ 为 $\mathbb{F}_q$ 的本原元素. 由上面的讨论, (8.27) 可以写成

$$\sum_{d\mid(q-1)}\frac{\mu(d)}{\phi(d)}\sum_{\chi\in M_d}\chi(c)=\begin{cases}\displaystyle\prod_{p\mid(q-1)}\left(1+\frac{1}{p-1}\right), & \text{若 } c \text{ 为 } \mathbb{F}_q \text{ 的本原元素},\\ 0, & \text{其它},\end{cases}$$

又由

$$\prod_{p\mid(q-1)}\left(1+\frac{1}{p-1}\right)=\prod_{p\mid(q-1)}\frac{p}{p-1}=\frac{q-1}{\phi(q-1)},$$

便给出引理的证明. □

对于给定的 $a\in\mathbb{F}_q$, 令 $U_a=\mathrm{Tr}^{-1}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a)=\{\gamma\in\mathbb{F}_{q^n}\mid \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma)=a\}$, 则由迹的线性性显然得到对任意 $a\in\mathbb{F}_q^*$, 有 $U_a=aU_1$. 给定 $\mathbb{F}_{q^n}$ 的任一乘法特征 ψ, 令

$$S_a(\psi)=\sum_{\gamma\in U_a}\psi(\gamma).$$

用 ψ_0 表示 $\mathbb{F}_{q^n}$ 的主乘法特征, 由于对任意 $a\in\mathbb{F}_q$, 有 $|U_a|=q^{n-1}$, 又 $0\in U_0$ 且 $\psi_0(0)=0$, 我们容易得到 $S_0(\psi_0)=q^{n-1}-1$ 且对 $a\in\mathbb{F}_q^*$ 有 $S_a(\psi_0)=q^{n-1}$. 下面设 $\psi\neq\psi_0$, 对任意 $a\in\mathbb{F}_q^*$, 由于 $U_a=aU_1$, 故 $S_a(\psi)=\psi(a)S_1(\psi)$. 由于 $\mathbb{F}_{q^n}$ 为这些 U_a 的不交并, 其中 a 取遍 $\mathbb{F}_q$ 中所有元素, 从而

$$0=\sum_{\gamma\in\mathbb{F}_{q^n}}\psi(\gamma)=S_0(\psi)+\sum_{a\in\mathbb{F}_q^*}S_a(\psi)=S_0(\psi)+S_1(\psi)\sum_{a\in\mathbb{F}_q^*}\psi(a).$$

注意到

$$\sum_{a\in\mathbb{F}_q^*}\psi(a)=\begin{cases}0, & \text{若 } \psi\notin(\mathbb{F}_q^*)^\sharp,\\ q-1, & \text{若 } \psi\in(\mathbb{F}_q^*)^\sharp\backslash\{\psi_0\},\end{cases}$$

所以

$$S_0(\psi)=-S_1(\psi)\sum_{a\in\mathbb{F}_q^*}\psi(a)=\begin{cases}0, & \text{若 } \psi\notin(\mathbb{F}_q^*)^\sharp,\\ -(q-1)S_1(\psi), & \text{若 } \psi\in(\mathbb{F}_q^*)^\sharp\backslash\{\psi_0\}.\end{cases}\tag{8.28}$$

任取 $\mathbb{F}_q$ 的一个非主加法特征 λ, 设 $\lambda^{(n)}$ 为 λ 在 $\mathbb{F}_{q^n}$ 上的提升, 则有

$$\begin{aligned} G(\psi,\lambda^{(n)}) &= \sum_{\gamma\in\mathbb{F}_{q^n}}\psi(\gamma)\lambda^{(n)}(\gamma)=\sum_{\gamma\in U_0}\psi(\gamma)\lambda^{(n)}(\gamma)+\sum_{a\in\mathbb{F}_q^*}\sum_{\gamma\in U_a}\psi(\gamma)\lambda^{(n)}(\gamma)\\ &= \sum_{\gamma\in U_0}\psi(\gamma)\lambda(0)+\sum_{a\in\mathbb{F}_q^*}\sum_{\gamma\in U_a}\psi(\gamma)\lambda(a)=S_0(\psi)+\sum_{a\in\mathbb{F}_q^*}S_a(\psi)\lambda(a)\\ &= S_0(\psi)+S_1(\psi)\sum_{a\in\mathbb{F}_q^*}\psi(a)\lambda(a)=S_0(\psi)+S_1(\psi)G(\psi',\lambda), \end{aligned}$$

其中 $\psi'=\psi|_{\mathbb{F}_q^*}$ 为 ψ 在 $\mathbb{F}_q^*$ 上的限制. 注意到若 $\psi\in(\mathbb{F}_q^*)^\sharp\backslash\{\psi_0\}$, 则 ψ' 为 $\mathbb{F}_q$ 的主乘法特征, 由定理 8.16 得到 $G(\psi',\lambda)=-1$. 故由 (8.28) 可以得到

$$G(\psi,\lambda^{(n)})=\begin{cases} S_1(\psi)G(\psi',\lambda), & \text{若 } \psi\notin(\mathbb{F}_q^*)^\sharp,\\ -qS_1(\psi), & \text{若 } \psi\in(\mathbb{F}_q^*)^\sharp\backslash\{\psi_0\}. \end{cases}$$

由于 λ 为 $\mathbb{F}_q$ 的非主加法特征, 故 $\lambda^{(n)}$ 也是 $\mathbb{F}_{q^n}$ 的非主加法特征, 所以 $|G(\psi,\lambda^{(n)})|=q^{\frac{n}{2}}$. 上式两端取模可得

$$|S_1(\psi)|=\begin{cases} q^{\frac{n-1}{2}}, & \text{若 } \psi\notin(\mathbb{F}_q^*)^\sharp,\\ q^{\frac{n-2}{2}}, & \text{若 } \psi\in(\mathbb{F}_q^*)^\sharp\backslash\{\psi_0\}. \end{cases}$$

注意到对于任意 $a\in\mathbb{F}_q^*$, $|S_a(\psi)|=|\psi(a)||S_1(\psi)|=|S_1(\psi)|$, 再由式 (8.28) 可以得到

$$|S_0(\psi)|=\begin{cases} 0, & \text{若 } \psi\notin(\mathbb{F}_q^*)^\sharp,\\ (q-1)q^{\frac{n-2}{2}}, & \text{若 } \psi\in(\mathbb{F}_q^*)^\sharp\backslash\{\psi_0\}. \end{cases}$$

用 g_a 表示包含在 U_a 中 $\mathbb{F}_{q^n}$ 的本原元素的个数, 对有限域 $\mathbb{F}_{q^n}$ 利用引理 8.40, 等式两边对 $c\in U_a$ 求和得到

$$\sum_{d|(q^n-1)}\frac{\mu(d)}{\phi(d)}\sum_{\psi\in M_d}S_a(\psi)=\frac{q^n-1}{\phi(q^n-1)}\cdot g_a,$$

注意这时 M_d 表示 $\mathbb{F}_{q^n}$ 的所有 d 阶乘法特征构成的集合. 若对某个 $a\in\mathbb{F}_q$, U_a 中没有 $\mathbb{F}_{q^n}$ 的本原元素, 则 $g_a=0$, 从而

$$\sum_{d|(q^n-1)}\frac{\mu(d)}{\phi(d)}\sum_{\psi\in M_d}S_a(\psi)=0. \tag{8.29}$$

记 $N=\frac{q^n-1}{q-1}$, 则由于 $(\mathbb{F}_q^*)^\sharp\cong\widehat{\mathbb{F}_{q^n}^*/\mathbb{F}_q^*}\cong\mathbb{Z}_N$, 且循环群 $\widehat{\mathbb{F}_{q^n}^*}$ 的同构于 $\mathbb{Z}_N$ 的子群唯一, 即 $(\mathbb{F}_q^*)^\sharp$, 我们得到对任意 $\psi\in\widehat{\mathbb{F}_{q^n}^*}$, $\psi\in(\mathbb{F}_q^*)^\sharp\backslash\{\psi_0\}$ 当且仅当 ψ 在 $\widehat{\mathbb{F}_{q^n}^*}$ 中的阶 d 满足 $d\mid N$ 且 $d\neq1$. 式 (8.29) 可以改写为

$$\sum_{d|(q^n-1),\,d\nmid N}\frac{\mu(d)}{\phi(d)}\sum_{\psi\in M_d}S_a(\psi)+\sum_{d|N,\,d\neq1}\frac{\mu(d)}{\phi(d)}\sum_{\psi\in M_d}S_a(\psi)=-S_a(\psi_0),$$

两边取模得到

$$\sum_{d|(q^n-1),\,d\nmid N}\frac{|\mu(d)|}{\phi(d)}\sum_{\psi\in M_d}|S_a(\psi)|+\sum_{d|N,\,d\neq1}\frac{|\mu(d)|}{\phi(d)}\sum_{\psi\in M_d}|S_a(\psi)|\geq|S_a(\psi_0)|. \tag{8.30}$$

我们知道对任意正整数 m, $\sum_{d|m}|\mu(d)|=2^\ell$, 其中 ℓ 为 m 的互异素因子的个数 (参见习题 1.8). 记 s 和 t 分别为 q^n-1 和 N 的互异素因子的个数, 由于 $|M_d|=\phi(d)$, 在 (8.30) 中代入 $|S_a(\psi)|$ 的值得到若 $a\in\mathbb{F}_q^*$, 则有

$$q^{\frac{n-1}{2}}\sum_{d|(q^n-1),\,d\nmid N}|\mu(d)|+q^{\frac{n-2}{2}}\sum_{d|N,\,d\neq1}|\mu(d)|\geq q^{n-1},$$

即 $q^{\frac{n-1}{2}}(2^s-2^t)+q^{\frac{n-2}{2}}(2^t-1)\geq q^{n-1}$, 或写成 $q^{\frac12}(2^s-2^t)+(2^t-1)\geq q^{\frac n2}$. 而若 $a=0$ 则有

$$(q-1)q^{\frac{n-2}{2}}\sum_{d|N,\,d\neq1}|\mu(d)|\geq q^{n-1}-1,$$

或改写为 $q^{\frac{n-2}{2}}(2^t-1)\geq\frac{q^{n-1}-1}{q-1}$, 由此我们证明了如下定理.

定理 8.41: 记 s 和 t 分别为 q^n-1 和 $q^{n-1}+q^{n-2}+\cdots+q+1$ 的互异素因子的个数, $a\in\mathbb{F}_q$, 若 $\mathbb{F}_{q^n}$ 的子集 U_a 中不存在 $\mathbb{F}_{q^n}$ 的本原元素, 则有

$$\begin{aligned}(2^s-2^t)q^{\frac12}+(2^t-1)&\geq q^{\frac n2}, &&\text{若 } a\neq0,\\ (2^t-1)q^{\frac{n-2}{2}}&\geq q^{n-2}+\cdots+q+1, &&\text{若 } a=0.\end{aligned}$$

□

为了应用如上定理, 我们还需估计一个正整数的互异素因子的个数. 设 m 为一个正整数且其互异素因子个数为 ℓ, 任意选定一个正整数 b, 用 S 表示 $\leq b$ 的一些素数构成的集合并设 m 的每个 $<b$ 的素因子都在 S 中, 令 $|S|=c$, 记 P 为 S 中元素的乘积, 则有 $\ell\leq\frac{\log m-\log P}{\log b}+c$ (其中对数的底是无关紧要的). 事实上, 设 M 为 m 的互异素因子构成的集合, 则有 $|M|=\ell$ 且对任意 $p\in M\backslash S$ 有 $p\geq b$. 由于 $M\cup S=M\cup(S\setminus M)=S\cup(M\setminus S)$, 所以

$$\prod_{p\in M}p\cdot\prod_{p\in S\backslash M}p=\prod_{p\in S}p\cdot\prod_{p\in M\backslash S}p,$$

故

$$m\geq\prod_{p\in M}p=\frac{\displaystyle\prod_{p\in S}p\cdot\prod_{p\in M\backslash S}p}{\displaystyle\prod_{p\in S\backslash M}p}\geq\frac{P\cdot b^{|M\backslash S|}}{b^{|S\backslash M|}}=b^{|M|-|S|}\cdot P=b^{\ell-c}\cdot P,$$

两边取对数就得到 $(\ell-c)\log b\leq\log m-\log P$, 即 $\ell\leq\frac{\log m-\log P}{\log b}+c$.

由定理 8.41, 对于 $a\neq0$, 若 $\mathbb{F}_{q^n}$ 的子集 U_a 中不存在 $\mathbb{F}_{q^n}$ 的本原元素, 则有

$$(2^s-2^t)q^{\frac12}+(2^t-1)\geq q^{\frac n2},$$

由此可推出 $2^s>q^{\frac{n-1}{2}}$. 取以 2 为底的对数, 我们有 $s>\frac{n-1}{2}\log_2 q$. 另一方面, s 是 q^n-1 的互异素因子的个数, 我们取 $b=32$, $S=\{2,3,5,7,11,13,17,19,23,29,31\}$, 则 $c=11$, $P=200560490130>2\cdot10^{11}$, 所以 $\log_2 P>37.5$, 又 $\log_2(q^n-1)<n\log_2 q$. 由前面的说明我们有

$$\frac{n-1}{2}\log_2 q<s<\frac{n\log_2 q-37.5}{5}+11,$$

由此得到 $(3n-5)\log_2 q < 35$, 即 $q^{3n-5} < 2^{35}$. 类似地, 对于 $a=0$, 若 $\mathbb{F}_{q^n}$ 的子集 U_0 中不存在 $\mathbb{F}_{q^n}$ 的本原元素, 则有 $q^{3n-8} < 2^{37}$. 由于只有有限多组 (q,n) 满足 $q^{3n-5} < 2^{35}$ 或 $q^{3n-8} < 2^{37}$, 所以最多有有限多组 (q,n,a) 使得不存在 $\mathbb{F}_{q^n}$ 的迹为 a 的本原元素, 其中 q 为素数幂, n 为正整数, $a \in \mathbb{F}_q$.

如上我们给出了迹给定的本原元素存在性的渐进结果 (比如我们得到了若 $q^{3n-5} \geq 2^{35}$, 则对于任意 $a \in \mathbb{F}_q$, 一定存在 $\mathbb{F}_{q^n}$ 的迹为 a 的本原元素), 但实际上的结论要好的多, 现已证明了对 $n \geq 2$, 当 $n=2$ 或者 $(n,q)=(3,4)$ 时假设 $a \neq 0$, 则一定存在 $\mathbb{F}_{q^n}$ 的本原元素 α 使得 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = a$.

本节的第二个应用是估计对角形方程解的个数, 所谓 $\mathbb{F}_q$ 上的对角形方程即形如

$$a_1 x_1^{k_1} + a_2 x_2^{k_2} + \cdots + a_n x_n^{k_n} = b \tag{8.31}$$

的方程, 其中 $k_1, k_2, \cdots, k_n$ 为正整数, $a_1, a_2, \ldots, a_n \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$. 我们在 7.5 节讨论过 2 次对角形方程的解数, 本节来讨论一般的对角形方程 (8.31) 的解数估计, 下面用 $N_q(a_1 x_1^{k_1} + \cdots + a_n x_n^{k_n} = b)$ 表示方程 (8.31) 在 $\mathbb{F}_q^n$ 中解的个数. 先看 $n=1$ 的情形, 此时方程为 $ax^k = b$, 其中 $a \neq 0$. 该方程可改写为 $x^k = c$, 其中 $c = a^{-1}b$. 若 $c=0$, 显然它有唯一解 $x=0$. 若 $c \neq 0$, 由定理 8.9 有 (群 G 取为 $\mathbb{F}_q^*$)

$$N_q(x^k = c) = \frac{1}{q-1} \sum_{u \in \mathbb{F}_q^*} \sum_{\psi \in \widehat{\mathbb{F}_q^*}} \psi(u^k)\overline{\psi}(c) = \frac{1}{q-1} \sum_{\psi \in \widehat{\mathbb{F}_q^*}} \overline{\psi}(c) \sum_{u \in \mathbb{F}_q^*} \psi(u^k).$$

注意到

$$\sum_{u \in \mathbb{F}_q^*} \psi(u^k) = \sum_{u \in \mathbb{F}_q^*} \psi^k(u) = \begin{cases} q-1, & \text{若 } \psi^k = \chi_0, \\ 0, & \text{若 } \psi^k \neq \chi_0, \end{cases}$$

其中 χ_0 为 $\mathbb{F}_q$ 的主乘法特征. 令 $d = \gcd(k, q-1)$, 则 $\psi^k = \chi_0$ 当且仅当 $\psi^d = \chi_0$, 即 ψ 的阶整除 d. 取 χ 为 $\mathbb{F}_q$ 的一个 d 阶乘法特征, 则 ψ 的阶整除 d 当且仅当 $\psi = \chi^j$, $0 \leq j \leq d-1$. 故我们有

$$N_q(x^k = c) = \sum_{j=0}^{d-1} \overline{\chi}^j(c) = \sum_{j=0}^{d-1} \chi^j(c),$$

其中我们用到了对于 $0 \leq j \leq d-1$, $\overline{\chi}^j = \chi^{d-j}$. 把 $c=0$ 和 $c \neq 0$ 两种情形综合到一起, 我们可以得到

$$N_q(x^k = c) = 1 + \sum_{j=1}^{d-1} \chi^j(c), \tag{8.32}$$

其中若 $d=1$, 则令 $\sum_{j=1}^{d-1} \chi^j(c) = 0$. 特别地, 当 q 为奇数且 $k=2$ 时, $N_q(x^2 = c) = 1 + \eta(c)$, 这是我们之前得到的结论.

一般地, 我们有

$$N_q(a_1 x_1^{k_1} + \cdots + a_n x_n^{k_n} = b) = \sum_{c_1 + \cdots + c_n = b} N_q(a_1 x_1^{k_1} = c_1) \cdots N_q(a_n x_n^{k_n} = c_n),$$

对于 $1 \le i \le n$, 令 $d_i = \gcd(k_i, q-1)$, 并设 χ_i 为 $\mathbb{F}_q$ 的一个 d_i 阶乘法特征, 则由 (8.32) 得到

$$N_q(a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = b) = \sum_{c_1+\cdots+c_n=b} \left(1 + \sum_{j_1=1}^{d_1-1} \chi_1^{j_1}(a_1^{-1}c_1)\right) \cdots \left(1 + \sum_{j_n=1}^{d_n-1} \chi_n^{j_n}(a_n^{-1}c_n)\right),$$

注意到上式右端乘积中除首尾外的其它项在满足条件 $c_1, \ldots, c_n \in \mathbb{F}_q$ 且 $c_1 + \cdots + c_n = b$ 的求和下为 0, 所以我们得到

$$\begin{aligned}
& N_q(a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = b) \\
= & \sum_{c_1+\cdots+c_n=b} \left(1 + \sum_{j_1=1}^{d_1-1} \chi_1^{j_1}(a_1^{-1}c_1) \cdots \sum_{j_n=1}^{d_n-1} \chi_n^{j_n}(a_n^{-1}c_n)\right) \\
= & q^{n-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \sum_{c_1+\cdots+c_n=b} \chi_1^{j_1}(a_1^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) \chi_1^{j_1}(c_1) \cdots \chi_n^{j_n}(c_n) \\
= & q^{n-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \chi_1^{j_1}(a_1^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J_b(\chi_1^{j_1}, \ldots, \chi_n^{j_n}).
\end{aligned}$$

若 $b = 0$, 用 T 表示对每个 $1 \le i \le n$ 有 $1 \le j_i \le d_i - 1$ 且 $\chi_1^{j_1} \cdots \chi_n^{j_n} = \chi_0$ 的 n-元整数组 $(j_1, \cdots, j_n) \in \mathbb{Z}^n$ 构成的集合, 则由定理 8.22 可得

$$N_q(a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = 0) = q^{n-1} - (q-1) \sum_{(j_1,\cdots,j_n)\in T} \chi_1^{j_1}(a_1^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}).$$

若 $b \ne 0$, 则 $J_b(\chi_1^{j_1}, \ldots, \chi_n^{j_n}) = (\chi_1^{j_1} \cdots \chi_n^{j_n})(b) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n})$, 从而

$$N_q(a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = b) = q^{n-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \chi_1^{j_1}(a_1^{-1}b) \cdots \chi_n^{j_n}(a_n^{-1}b) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}).$$

由此我们证明了如下定理.

定理 8.42: 对任意 $1 \le i \le n$, 设 $d_i = \gcd(k_i, q-1)$ 且 χ_i 为 $\mathbb{F}_q$ 的一个 d_i 阶乘法特征, 则对角形方程 $a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = 0$ 在 $\mathbb{F}_q^n$ 中解的个数为

$$N_q(a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = 0) = q^{n-1} - (q-1) \sum_{(j_1,\cdots,j_n)\in T} \chi_1^{j_1}(a_1^{-1}) \cdots \chi_n^{j_n}(a_n^{-1}) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}),$$

其中 T 为满足对每个 $1 \le i \le n$ 有 $1 \le j_i \le d_i - 1$ 且 $\chi_1^{j_1} \cdots \chi_n^{j_n} = \chi_0$ 的 n-元整数组 $(j_1, \cdots, j_n) \in \mathbb{Z}^n$ 构成的集合. 而对任意 $b \in \mathbb{F}_q^*$, 对角形方程 $a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = b$ 在 $\mathbb{F}_q^n$ 中解的个数为

$$N_q(a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = b) = q^{n-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \chi_1^{j_1}(a_1^{-1}b) \cdots \chi_n^{j_n}(a_n^{-1}b) J(\chi_1^{j_1}, \ldots, \chi_n^{j_n}).$$

□

对于一般的对角形方程, 由于没有 Jacobi 和的精确计算公式, 所以不能如同 2 次对角形方程那样给出解数的确切值, 下面给出对角形方程解数的一个估计. 我们知道 $\widehat{\mathbb{F}_q^*}$ 是一个 $q-1$ 阶循环群, 设 χ 是群 $\widehat{\mathbb{F}_q^*}$ 的一个生成元, 对于 $1 \le i \le n$, 由于 χ_i 为 $\mathbb{F}_q$ 的一个 d_i 阶乘法特征, 不妨可以取 $\chi_i = \chi^{\frac{q-1}{d_i}}$. 从而对于 $1 \le j_i \le d_i - 1$, $\chi_1^{j_1} \cdots \chi_n^{j_n} = \chi^{(\frac{j_1}{d_1}+\cdots+\frac{j_n}{d_n})(q-1)}$, 故 $\chi_1^{j_1} \cdots \chi_n^{j_n} = \chi_0$

当且仅当 $\frac{j_1}{d_1}+\cdots+\frac{j_n}{d_n}$ 为整数. 用 $M(d_1,\ldots,d_n)$ 表示对每个 $1\le i\le n$ 有 $1\le j_i\le d_i-1$ 且 $\frac{j_1}{d_1}+\cdots+\frac{j_n}{d_n}$ 为整数的 n-元整数组 $(j_1,\cdots,j_n)\in\mathbb{Z}^n$ 的个数, 则有 $|T|=M(d_1,\ldots,d_n)$. 由定理 8.26 和 8.42 得到

$$|N_q(a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=0)-q^{n-1}|\le M(d_1,\ldots,d_n)(q-1)q^{\frac{n-2}{2}},$$

而对 $b\in\mathbb{F}_q^*$,

$$\begin{aligned}|N_q(a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=b)-q^{n-1}| &\le \left(\prod_{i=1}^n(d_i-1)-|T|\right)q^{\frac{n-1}{2}}+|T|q^{\frac{n-2}{2}}\\ &= \left(\prod_{i=1}^n(d_i-1)-(1-q^{-\frac12})M(d_1,\ldots,d_n)\right)q^{\frac{n-1}{2}}.\end{aligned}$$

显然 $M(d_1,\ldots,d_n)\le\prod_{i=1}^n(d_i-1)$, 当然也可能有 $M(d_1,\ldots,d_n)=0$, 比如在某个 $d_i=1$ 的平凡情形, 或者存在某个 d_j 与其它的所有 d_k 都互素的情形. 下面用反证法证明后面这种情形, 事实上, 不失一般性设 $\gcd(d_1,d_i)=1$, $2\le i\le n$. 若 $M(d_1,\ldots,d_n)\ne0$, 则存在 $(j_1,j_2,\cdots,j_n)\in\mathbb{Z}^n$ 使得对每个 $1\le i\le n$ 有 $1\le j_i\le d_i-1$, 且 $\frac{j_1}{d_1}+\frac{j_2}{d_2}+\cdots+\frac{j_n}{d_n}=m\in\mathbb{Z}$, 所以存在某个 $j\in\mathbb{Z}$ 使得

$$j_1d_2\cdots d_n+jd_1=md_1d_2\cdots d_n,$$

从而 $d_1\mid j_1d_2\cdots d_n$, 再由 $\gcd(d_1,d_2\cdots d_n)=1$ 得到 $d_1\mid j_1$, 与 $1\le j_1\le d_1-1$ 矛盾. 显然若 $M(d_1,\ldots,d_n)=0$, 则有 $N_q(a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=0)=q^{n-1}$. 另外如果存在某个 $d_i=1$, 即有某个 k_i 与 $q-1$ 互素, 则对任意 $b\in\mathbb{F}_q$, 均有 $N_q(a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=b)=q^{n-1}$.

由定理 8.42 可以看出, 对角形方程 $a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=b$ 在 $\mathbb{F}_q^n$ 中的解数并不与 k_i 直接相关, 但是却基于最大公因数 d_i, 所以不失一般性, 我们在讨论方程 $a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=b$ 在 $\mathbb{F}_q^n$ 中的解数时, 可以假设对每个 k_i, $1\le i\le n$, 都有 $k_i\mid(q-1)$.

例 8.11: 由方程 $x^d+y^d=1$ 确定的曲线称为 Fermat 曲线, 下面估计 Fermat 曲线在有限域 $\mathbb{F}_q$ 上的射影平面中的点的个数. 我们先看 Fermat 曲线上的有理点, 即包含在 $\mathbb{F}_q^2$ 中的点. Fermat 曲线上的有理点的个数即方程 $x^d+y^d=1$ 在 $\mathbb{F}_q^2$ 中的解数, 由前面的说明, 我们可以假设 $d\mid(q-1)$. 由定理 8.42, 我们得到

$$N_q(x^d+y^d=1)=q+\sum_{1\le i,j\le d-1}J(\chi^i,\chi^j),$$

其中 χ 为 $\mathbb{F}_q$ 的一个 d 阶乘法特征. 对于 Jacobi 和 $J(\chi^i,\chi^j)$, 若 $\chi^i\chi^j=\chi^{i+j}=\chi_0$, 由 (8.17) 得到 $J(\chi^i,\chi^j)=-\chi^i(-1)$, 而 $\chi^i\chi^j=\chi_0$ 当且仅当 $i+j=d$, 从而

$$N_q(x^d+y^d=1)=q+\sum_{1\le i,j\le d-1}J(\chi^i,\chi^j)=q-\sum_{i=1}^{d-1}\chi^i(-1)+\sum_{1\le i,j\le d-1,\,i+j\ne d}J(\chi^i,\chi^j).$$

把方程 $x^d+y^d=1$ 射影化得到射影曲线 $x^d+y^d=z^d$, 它在 $\mathbb{F}_q$ 上的射影平面中的无穷远点 $[x:y:0]$ 满足 $x^d+y^d=0$, 其中 $x,y\in\mathbb{F}_q^*$, 从而无穷远点为 $[1:\frac{y}{x}:0]$ 且满足 $(\frac{y}{x})^d=-1$. 由

(8.32) 得知这样的 $\frac{y}{x}$ 的个数为 $\sum_{i=0}^{d-1}\chi^i(-1)$. 把有理点和无穷远点放在一起就得到 Fermat 射影曲线 $x^d+y^d=z^d$ 在 $\mathbb{F}_q$ 上的射影平面中的点的个数为

$$N=N_q(x^d+y^d=1)+\sum_{i=0}^{d-1}\chi^i(-1)=q+1+\sum_{1\le i,j\le d-1,\, i+j\ne d}J(\chi^i,\chi^j).$$

由于当 $i+j\ne d$ 时有 $|J(\chi^i,\chi^j)|=\sqrt{q}$, 从而

$$|N-(q+1)|\le (d-1)(d-2)\sqrt{q},$$

这表明, 当 q 充分大时, 对于给定的 d, Fermat 射影曲线 $x^d+y^d=z^d$ 的射影点数 N 与射影直线上的点数 $q+1$ 相差一个阶比 q 小的数. □

本节的最后, 我们用另一种方式来讨论对角形方程 (8.31) 在 $\mathbb{F}_q^n$ 中的解数. 由本章第 1 节最后的说明, 我们有

$$\begin{aligned}
&N_q(a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=b)\\
=\ &\frac{1}{q}\sum_{c_1,\dots,c_n\in\mathbb{F}_q}\sum_{\lambda\in\widehat{\mathbb{F}_q^*}}\lambda(a_1c_1^{k_1}+\cdots+a_nc_n^{k_n})\overline{\lambda}(b)\\
=\ &\frac{1}{q}\sum_{\lambda\in\widehat{\mathbb{F}_q^*}}\overline{\lambda}(b)\sum_{c_1,\dots,c_n\in\mathbb{F}_q}\lambda(a_1c_1^{k_1}+\cdots+a_nc_n^{k_n})\\
=\ &\frac{1}{q}\left(q^n+\sum_{\lambda\in\widehat{\mathbb{F}_q^*},\,\lambda\ne\lambda_0}\overline{\lambda}(b)\left(\sum_{c_1\in\mathbb{F}_q}\lambda(a_1c_1^{k_1})\right)\cdots\left(\sum_{c_n\in\mathbb{F}_q}\lambda(a_nc_n^{k_n})\right)\right),
\end{aligned}$$

其中 λ_0 是 $\mathbb{F}_q$ 的主加法特征. 对于每个 $1\le i\le n$, 设 $d_i=\gcd(k_i,q-1)$ 且 χ_i 是 $\mathbb{F}_q$ 的一个 d_i 阶乘法特征, 则由定理 8.32, 我们有

$$\begin{aligned}
&N_q(a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=b)\\
=\ &q^{n-1}+\frac{1}{q}\sum_{\lambda\in\widehat{\mathbb{F}_q^*},\,\lambda\ne\lambda_0}\overline{\lambda}(b)\left(\sum_{j_1=1}^{d_1-1}\overline{\chi_1}^{j_1}(a_1)G(\chi_1^{j_1},\lambda)\right)\cdots\left(\sum_{j_n=1}^{d_n-1}\overline{\chi_n}^{j_n}(a_n)G(\chi_n^{j_n},\lambda)\right)\\
=\ &q^{n-1}+\frac{1}{q}\sum_{j_1=1}^{d_1-1}\overline{\chi_1}^{j_1}(a_1)\cdots\sum_{j_n=1}^{d_n-1}\overline{\chi_n}^{j_n}(a_n)\sum_{\lambda\in\widehat{\mathbb{F}_q^*},\,\lambda\ne\lambda_0}\overline{\lambda}(b)G(\chi_1^{j_1},\lambda)\cdots G(\chi_n^{j_n},\lambda).
\end{aligned}\tag{8.33}$$

由例 8.2 我们知道 $\widehat{\mathbb{F}_q^*}=\{\lambda_a\mid a\in\mathbb{F}_q\}$, 这里 λ_a 定义为对 $c\in\mathbb{F}_q$, $\lambda_a(c)=\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ac)}$, 其中 $p=\mathrm{char}\mathbb{F}_q$, $\zeta_p=e^{\frac{2\pi i}{p}}$. 显然 λ_0 为主加法特征且对任意 $a,b\in\mathbb{F}_q$ 有 $\lambda_a(b)=\lambda_b(a)$. 利用定理 8.17 (i), 我们有

$$\begin{aligned}
\sum_{\lambda\in\widehat{\mathbb{F}_q^*},\,\lambda\ne\lambda_0}\overline{\lambda}(b)G(\chi_1^{j_1},\lambda)\cdots G(\chi_n^{j_n},\lambda) &= \sum_{a\in\mathbb{F}_q^*}\overline{\lambda_a}(b)G_a(\chi_1^{j_1})\cdots G_a(\chi_n^{j_n})\\
&= G(\chi_1^{j_1})\cdots G(\chi_n^{j_n})\sum_{a\in\mathbb{F}_q^*}\overline{\lambda_b}(a)\overline{\chi_1}^{j_1}(a)\cdots\overline{\chi_n}^{j_n}(a)\\
&= G(\chi_1^{j_1})\cdots G(\chi_n^{j_n})G(\overline{\chi_1}^{j_1}\cdots\overline{\chi_n}^{j_n},\overline{\lambda_b}).
\end{aligned}$$

将上式代入 (8.33) 得到

$$\begin{aligned} & N_q(a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=b) \\ = \ & q^{n-1}+\frac{1}{q}\sum_{j_1=1}^{d_1-1}\overline{\chi_1}^{j_1}(a_1)\cdots\sum_{j_n=1}^{d_n-1}\overline{\chi_n}^{j_n}(a_n)G(\chi_1^{j_1})\cdots G(\chi_n^{j_n})G(\overline{\chi_1}^{j_1}\cdots\overline{\chi_n}^{j_n},\overline{\lambda_b}) \\ = \ & q^{n-1}+\frac{1}{q}\sum_{j_1=1}^{d_1-1}\cdots\sum_{j_n=1}^{d_n-1}G_{a_1}(\chi_1^{j_1})\cdots G_{a_n}(\chi_n^{j_n})G(\overline{\chi_1}^{j_1}\cdots\overline{\chi_n}^{j_n},\overline{\lambda_b}). \end{aligned} \tag{8.34}$$

对于 $b=0$, $\overline{\lambda_b}=\lambda_0$, 由定理 8.16 我们有

$$G(\overline{\chi_1}^{j_1}\cdots\overline{\chi_n}^{j_n},\overline{\lambda_b})=\begin{cases} q-1, & \text{若 } \chi_1^{j_1}\cdots\chi_n^{j_n}=\chi_0, \\ 0, & \text{若 } \chi_1^{j_1}\cdots\chi_n^{j_n}\neq\chi_0, \end{cases}$$

从而

$$N_q(a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=0)=q^{n-1}+\left(1-\frac{1}{q}\right)\sum_{(j_1,\cdots,j_n)\in T}G_{a_1}(\chi_1^{j_1})\cdots G_{a_n}(\chi_n^{j_n}), \tag{8.35}$$

其中 T 的定义如定理 8.42, 即 T 为对每个 $1\leq i\leq n$ 有 $1\leq j_i\leq d_i-1$ 且 $\chi_1^{j_1}\cdots\chi_n^{j_n}=\chi_0$ 的 n-元整数组 $(j_1,\cdots,j_n)\in\mathbb{Z}^n$ 构成的集合.

最后要强调的是这里我们利用 Gauss 和来表示对角形方程在 $\mathbb{F}_q^n$ 中的解数, 实际上 (8.34) 和 (8.35) 与定理 8.42 的结论是一致的, 利用 Gauss 和与 Jacobi 和之间的关系可以互相导出.

8.7 习题

8.1 设 G 为有限交换群, H 是 G 的一个真子群, $g\in G$ 但是 $g\notin H$, 证明存在 $\chi\in H^\sharp$ 使得 $\chi(g)\neq 1$.

8.2 设 G 为有限交换群, m 为正整数, $g\in G$, 证明存在 $h\in G$ 使得 $g=h^m$ 当且仅当对任意满足 χ^m 为主特征的 $\chi\in\widehat{G}$ 均有 $\chi(g)=1$.

8.3 设 p 为素数, 矩阵 C 为群 $\mathbb{Z}_p$ 的特征表, 证明对任意 $1\leq k\leq p$, C 的任意 k 阶子矩阵一定可逆.

8.4 设 G 为有限交换群, T 为 $\widehat{G}$ 的一个非空子集, 定义

$$T^\perp=\{a\in G\mid \text{对所有 } \chi\in T \text{ 有 } \chi(a)=1\},$$

(a) 证明 $T^\perp\leq G$.

(b) 设 $H\leq G$, $T\leq\widehat{G}$, $\chi\in\widehat{G}$, $b\in G$, 证明

$$\sum_{a\in H}\chi(a)=\begin{cases} |H|, & \text{若 } \chi\in H^\sharp, \\ 0, & \text{若 } \chi\notin H^\sharp, \end{cases} \qquad \text{和} \qquad \sum_{\psi\in T}\psi(b)=\begin{cases} |T|, & \text{若 } b\in T^\perp, \\ 0, & \text{若 } b\notin T^\perp, \end{cases}$$

8.5 设 χ 为 $\mathbb{F}_q$ 的一个非主乘法特征, 再令 $\chi 0=0$, 设 $a,b\in\mathbb{F}_q$ 且 $a\neq b$, 证明

$$\sum_{c\in\mathbb{F}_q}\chi(c+a)\overline{\chi(c+b)}=-1.$$

8.6 设 χ 为域 $\mathbb{F}_{q^s}$ 的一个 m 阶乘法特征, 证明 χ 在 $\mathbb{F}_q$ 上的限制 $\chi^* = \chi|_{\mathbb{F}_q}$ 是 $\mathbb{F}_q$ 的乘法特征且其阶为 $m/\gcd(m, \frac{q^s-1}{q-1})$, 并由此证明 χ^* 为 $\mathbb{F}_q$ 的主乘法特征当且仅当 $m \mid \frac{q^s-1}{q-1}$.

8.7 设 χ 为域 $\mathbb{F}_q$ 的一个乘法特征, $\chi^{(s)}$ 为 χ 在域 $\mathbb{F}_{q^s}$ 上的提升, 证明 $\chi^{(s)}$ 在 $\mathbb{F}_q$ 上的限制 $(\chi^{(s)})^*$ 恰为 χ^s.

8.8 设 τ 为 $\mathbb{F}_{q^s}$ 的一个乘法特征, 证明存在 $\chi \in \widehat{\mathbb{F}_q^*}$ 使得 $\tau = \chi^{(s)}$ 当且仅当 τ^{q-1} 为 $\mathbb{F}_{q^s}$ 的主乘法特征.

8.9 设 $p = \mathrm{char}\mathbb{F}_q$, 对于 $a \in \mathbb{F}_q$, 求多项式 $x^p - x - a$ 在 $\mathbb{F}_q$ 中的根的个数.

8.10 设 q 为奇数, η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, 证明 $\eta(2) = (-1)^{\frac{q^2-1}{8}}$.

8.11 设 G 为有限交换群, $H \leq G$, $f, g \in L^2(G)$, 证明

$$\begin{aligned}
\frac{1}{|G|}\sum_{\chi\in H^\sharp}\hat{f}(\chi)\hat{g}(\chi) &= \frac{1}{|H|}\sum_{a\in H}(f*g)(a),\\
\frac{1}{|H|}\sum_{a\in H}f(a)g(a) &= \frac{1}{|G|^2}\sum_{\chi\in H^\sharp}(\hat{f}*\hat{g})(\chi),\\
\sum_{\chi\in\widehat{G}}|\hat{f}(\chi)|^4 &= |G|\sum_{a\in G}|(f*f)(a)|^2,
\end{aligned}$$

其中 $*$ 是卷积.

8.12 设 $\mathbb{F}_q^n$ 是 $\mathbb{F}_q$ 上的 n-维向量空间, $\mathbb{F}_q^n$ 中每个元素都可以唯一表示成 $\mathbf{a} = (a_1, a_2, \cdots, a_n)$ 的形式, 其中 $a_i \in \mathbb{F}_q$, $1 \leq i \leq n$. 对于 $\mathbf{a} = (a_1, a_2, \cdots, a_n), \mathbf{b} = (b_1, b_2, \cdots, b_n) \in \mathbb{F}_q^n$, 定义 $\mathbf{a} \cdot \mathbf{b} = a_1b_1 + a_2b_2 + \cdots + a_nb_n$, 并称其为 $\mathbf{a}$ 和 $\mathbf{b}$ 在 $\mathbb{F}_q^n$ 中的内积. 考虑 $\mathbb{F}_q^n$ 的加法群, 设 $\mathrm{char}\mathbb{F}_q = p$, 对于给定的 $\mathbf{a} \in \mathbb{F}_q^n$ 和任意 $\mathbf{u} \in \mathbb{F}_q^n$, 定义 $\lambda_{\mathbf{a}}(\mathbf{u}) = \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathbf{a}\cdot\mathbf{u})}$, 证明 $\lambda_{\mathbf{a}}$ 为加法群 $\mathbb{F}_q^n$ 的特征且 $\widehat{\mathbb{F}_q^n} = \{\lambda_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{F}_q^n\}$.

8.13 设 $\mathbb{F}_q^n$ 是 $\mathbb{F}_q$ 上的 n-维向量空间, 对于向量 $\mathbf{v} \in \mathbb{F}_q^n$, 定义 $\mathbf{v}$ 的 (Hamming) 重量 $w_H(\mathbf{v})$ 为 $\mathbf{v}$ 中非零分量的个数. 设 C 为 $\mathbb{F}_q^n$ 的子空间, 令 A_i 为 C 中重量为 i 的向量个数, 其中 $0 \leq i \leq n$, 定义 C 的重量计数多项式为 (参看例 8.6)

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i.$$

进一步地, 定义子空间 C 的对偶 $C^\perp$ 为

$$C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n \mid \text{对任意 } \mathbf{c} \in C \text{ 均有 } \mathbf{v} \cdot \mathbf{c} = 0\}.$$

证明

(a) $C^\perp$ 为 $\mathbb{F}_q^n$ 的子空间, $\dim C^\perp = n - \dim C$, 且 $(C^\perp)^\perp = C$.

(b) (MacWilliams 恒等式, 例 8.6 即 $q = 2$ 时的情形.)

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y).$$

8.14 设 Γ 为一个图, Γ 的顶点集合为 $\{v_1, v_2, \ldots, v_n\}$, 定义图 Γ 的邻接矩阵为一个 $n \times n$ 矩阵 $A_\Gamma = (a_{ij})_{1 \le i,j \le n}$, 其中

$$a_{ij} = \begin{cases} 1, & \text{若 } v_i \text{ 与 } v_j \text{ 相邻}, \\ 0, & \text{其它}, \end{cases}$$

证明 Cayley 图 $\mathrm{Cay}(G, A)$ 的邻接矩阵恰为由子集 A 的特征函数 f_A 定义的卷积变换 $\mathcal{C}_{f_A}$ 在 $L^2(G)$ 的基 $\{\delta_a \mid a \in G\}$ 下的矩阵 (参见例 8.7).

8.15 定义 Krawtchouk 多项式 $K_r(x; n)$ 为

$$K_r(x; n) = \sum_{j=0}^{r} (-1)^j \binom{x}{j} \binom{n-x}{r-j},$$

其中对任意正整数 j 有 $\binom{x}{j} = \frac{x(x-1)\cdots(x-j+1)}{j!}$, $\binom{x}{0} = 1$, 而对负整数 j 则有 $\binom{x}{j} = 0$. 证明:

(a) $K_0(x; n) = 1$, $K_1(x; n) = n - 2x$, $K_2(x; n) = \binom{n}{2} - 2nx + 2x^2$.

(b) 三项递推关系式 $(k+1)K_{k+1}(x; n) = (n - 2x)K_k(x; n) - (n - k + 1)K_{k-1}(x; n)$.

(c) 正交关系式

$$\sum_{i=0}^{n} \binom{n}{i} K_a(i; n) K_b(i; n) = 2^n \binom{n}{a} \delta_{a,b}.$$

(d) 对任意整数 i, $0 \le i \le n$ 有

$$\sum_{k=0}^{n} K_k(i; n) z^k = (1 + z)^{n-i} (1 - z)^i.$$

(e) 对任意 i 和 k, $0 \le i, k \le n$ 有

$$\binom{n}{i} K_k(i; n) = \binom{n}{k} K_i(k; n).$$

(f) 设 r 为正整数, 加法群 $G = \mathbb{F}_2^n$, $A = \{\mathbf{v} \in \mathbb{F}_2^n \mid w_H(\mathbf{v}) = r\}$, 则 Cayley 图 $\mathrm{Cay}(G, A)$ 的全部特征值为 $K_r(w_H(\mathbf{a}); n)$, 其中 $\mathbf{a}$ 跑遍 $\mathbb{F}_2^n$ 的所有元素.

8.16 设 p 为素数, G 为域 $\mathbb{F}_{p^2}$ 的加法群, $A = \mathrm{Ker}(\mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}) = \{\alpha \in \mathbb{F}_{p^2} \mid \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}$, 证明对 Cayley 图 $\mathrm{Cay}(G, A)$ 的任意不等于 $p + 1$ 的特征值 λ 均有 $|\lambda| \le 2\sqrt{p}$.

8.17 对任意给定的 $\mathbb{F}_q$ 的加法特征 λ, 证明

$$\sum_{\chi \in \widehat{\mathbb{F}_q^*}} G(\chi, \lambda) = (q - 1)\lambda(1).$$

8.18 设 $k \mid (q-1)$, A_k 是 $\widehat{\mathbb{F}_q^*}$ 的一个 k 阶子群, $a \in \mathbb{F}_q^*$, λ_a 是例 8.2 中定义的 $\mathbb{F}_q$ 的加法特征, 证明

$$\sum_{x \in \mathbb{F}_q} \lambda_a(x^k) = \sum_{\chi \in A_k} \overline{\chi(a)} G(\chi).$$

8.19 确定所有的奇素数 p 使得 $(\frac{-3}{p})=1$, 并确定所有的奇素数幂 q 使得 $\eta(3)=1$, 其中 η 为 $\mathbb{F}_q$ 的 2 阶乘法特征.

8.20 对 $q=23, 25, 27, 29$, 具体求出 $\mathbb{F}_q$ 上的 Gauss 和 $G(\eta)$, 其中 η 为 $\mathbb{F}_q$ 的 2 阶乘法特征.

8.21 设 p 为奇素数, $q=p^s$ 使得 $(\frac{-3}{p})=1$, η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, 证明 $G(\eta)=(-1)^{\frac{q+1}{2}}i^{\frac{s(p^2+2p+5)}{4}}q^{\frac{1}{2}}$.

8.22 设 p 和 r 是不同的奇素数, 利用 $\mathbb{F}_p$ 上的 Gauss 和 $G(\eta)$ 证明二次互反律, 即证明

$$\left(\frac{r}{p}\right)\left(\frac{p}{r}\right)=(-1)^{\frac{(p-1)(r-1)}{4}}.$$

8.23 设 k 为正整数, 用 $N_k(0)$ 和 $N_k(1)$ 分别表示满足 $c_1+c_2+\cdots+c_k=0$ 和 $c_1+c_2+\cdots+c_k=0$ 的 k-元组 $(c_1,c_2,\cdots,c_k)\in\mathbb{F}_q^{*k}$ 的个数, 证明 $N_1(0)=0$, $N_1(1)=1$, 且当 $k\geq 2$ 时有 $N_k(0)=(q-1)N_{k-1}(1)$ 和 $N_k(1)=N_{k-1}(0)+(q-2)N_{k-1}(1)$, 并由此给出定理 8.21 的证明.

8.24 设 $\chi_1,\chi_2,\ldots,\chi_k$ 为 $\mathbb{F}_q$ 的乘法特征且不全为主特征, 证明

$$\sum_{a\in\mathbb{F}_q}J_a(\chi_1,\chi_2,\ldots,\chi_k)=0,$$

并由此证明定理 8.22.

8.25 证明

$$\sum_{\chi\in\widehat{\mathbb{F}_q^*}}J(\chi,\chi_1,\chi_2,\ldots,\chi_k)=(q-1)J_0(\chi_1,\chi_2,\ldots,\chi_k)+J(\chi_1,\chi_2,\ldots,\chi_k).$$

8.26 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, $a,b_1,b_2,\ldots,b_k\in\mathbb{F}_q$, 证明

$$\sum_{c_1+c_2+\cdots+c_k=a}\lambda(b_1c_1+b_2c_2+\cdots+b_kc_k)=\begin{cases}q^{k-1}\lambda(ab_1), & \text{若 } b_1=b_2=\cdots=b_k,\\ 0, & \text{其它},\end{cases}$$

并用此证明定理 8.24.

8.27 设 $\chi_1,\chi_2,\ldots,\chi_k$ 为 $\mathbb{F}_q$ 的乘法特征且不全为主特征, λ 为 $\mathbb{F}_q$ 的一个非主加法特征, 证明

$$J(\chi_1,\chi_2,\ldots,\chi_k)=\frac{1}{q}G(\chi_1,\lambda)G(\chi_2,\lambda)\cdots G(\chi_k,\lambda)G(\overline{\chi_1\chi_2\cdots\chi_k},\overline{\lambda}).$$

8.28 设 χ 为 $\mathbb{F}_q$ 的阶为 $m\geq 2$ 的乘法特征, λ 是 $\mathbb{F}_q$ 的一个非主加法特征, 证明

$$G(\chi,\lambda)^m=\begin{cases}-qJ^{(k)}(\chi), & \text{若 } m\mid k,\\ G(\chi^k,\lambda)J^{(k)}(\chi), & \text{其它}.\end{cases}$$

8.29 设 q 为奇素数幂, k 为正整数, η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, 证明

$$J^{(k)}(\eta)=\begin{cases}(-1)^{\frac{k(q-1)+4}{4}}q^{\frac{k}{2}-1}, & \text{若 } k \text{ 为偶数},\\ (-1)^{\frac{(k-1)(q-1)}{4}}q^{\frac{k-1}{2}}, & \text{若 } k \text{ 为奇数}.\end{cases}$$

8.30 设奇数 $m \geq 3$, χ 为 $\mathbb{F}_q$ 的阶为 m 的乘法特征, 证明 $J(\chi, \chi^2, \ldots, \chi^{m-1}) = -q^{\frac{m-3}{2}}$.

8.31 设 q 为奇素数幂, χ 为 $\mathbb{F}_q$ 的乘法特征且 $\chi \neq \chi_0$, η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, 证明 $J(\chi, \eta) = \chi(4)J(\chi, \chi)$.

8.32 设 q 为奇素数幂, $f(x), g(x) \in \mathbb{F}_q[x]$ 且 $\deg(f) = \deg(g) = 2$, 设 λ 为 $\mathbb{F}_q$ 的一个非主加法特征, 用 Kloosterman 和来表示

$$\sum_{c \in \mathbb{F}_q,\, g(c) \neq 0} \lambda(f(c)g(c)^{-1}).$$

8.33 设 χ 和 λ 分别是 $\mathbb{F}_q$ 的乘法特征和加法特征, $a, b \in \mathbb{F}_q$, 定义广义 Kloosterman 和为

$$K(\chi, \lambda; a, b) = \sum_{c \in \mathbb{F}_q^*} \chi(c)\lambda(ac + bc^{-1}).$$

证明:

(a) 在 $ab = 0$ 时, 广义 Kloosterman 和可以简化为 Gauss 和如下:

$$K(\chi, \lambda; a, b) = \begin{cases} \chi(b)G(\overline{\chi}, \lambda), & \text{若 } a = 0,\ b \neq 0, \\ \overline{\chi}(a)G(\chi, \lambda), & \text{若 } a \neq 0,\ b = 0, \\ G(\chi, \lambda_0), & \text{若 } a = b = 0, \end{cases}$$

其中 λ_0 为 $\mathbb{F}_q$ 的主加法特征.

(b) 设 q 为奇素数幂, η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, $a, b \in \mathbb{F}_q$ 且 $\eta(ab) = -1$, 则对 $\mathbb{F}_q$ 的任意加法特征 λ 有 $K(\eta, \lambda; a, b) = 0$.

(c) 设 q 为奇素数幂, η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, $a, b \in \mathbb{F}_q$ 且 $ab = d^2$, 其中 $d \in \mathbb{F}_q^*$, 则对 $\mathbb{F}_q$ 的任意加法特征 λ 有

$$K(\eta, \lambda; a, b) = \eta(b)G(\eta, \lambda)(\lambda(2d) + \lambda(-2d)).$$

8.34 设 q 为奇素数幂, η 为 $\mathbb{F}_q$ 的 2 阶乘法特征, n 为正整数, 对于 $a \in \mathbb{F}_q^*$, 定义

$$H_n(a) = \sum_{c \in \mathbb{F}_q} \eta(c)\eta(c^n + a), \qquad \text{和} \qquad I_n(a) = \sum_{c \in \mathbb{F}_q} \eta(c^n + a),$$

称 $H_n(a)$ 为 Jacobsthal 和. 证明:

(a) 对任意 $a \in \mathbb{F}_q^*$ 有 $H_1(a) = -1$, $I_1(a) = 0$ 且对所有正整数 n 有

$$I_{2n}(a) = I_n(a) + H_n(a).$$

进一步地, 若 n 为奇数, 则对任意 $a \in \mathbb{F}_q^*$ 有

$$H_n(a) = \eta(a)I_n(a^{-1}) - 1$$

和

$$I_{2n}(a) = \eta(a)H_n(a^{-1}) + H_n(a) + \eta(a).$$

(b) 设 n 为正整数, $d=\gcd(n,q-1)$, χ 为 $\mathbb{F}_q$ 的一个 d 阶乘法特征, 则对任意 $a\in\mathbb{F}_q^*$ 有

$$I_n(a)=\eta(a)\sum_{j=1}^{d-1}\chi^j(-a)J(\chi^j,\eta).$$

(c) 设 n 为正整数, $v_2(q-1)$ 表示能整除 $q-1$ 的 2 的最高次幂的指数, 则对任意 $a\in\mathbb{F}_q^*$ 有

$$H_n(a)=\begin{cases}0, & \text{若 } 2^{v_2(q-1)}\mid n,\\ \eta(a)\psi(-1)\sum_{j=1}^{d-1}\psi^{j+1}(a)J(\psi^{2j+1},\eta), & \text{若 } 2^{v_2(q-1)}\nmid n,\end{cases}$$

其中 $d=\gcd(n,q-1)$, ψ 为 $\mathbb{F}_q$ 的一个 $2d$ 阶乘法特征.

(d) 若 $q\equiv 3\pmod 4$, 则对任意 $a\in\mathbb{F}_q^*$ 有 $I_4(a)=-1$.

8.35 用 $M(d_1,\dots,d_n)$ 表示对每个 $1\le i\le n$ 有 $1\le j_i\le d_i-1$ 且 $\frac{j_1}{d_1}+\cdots+\frac{j_n}{d_n}$ 为整数的 n-元整数组 $(j_1,\cdots,j_n)\in\mathbb{Z}^n$ 的个数, 证明

$$M(d_1,\dots,d_n)=(-1)^n+\sum_{r=1}^{n}(-1)^{n-r}\sum_{1\le i_1<\cdots<i_r\le n}\frac{d_{i_1}\cdots d_{i_r}}{\operatorname{lcm}(d_{i_1},\dots,d_{i_r})}.$$

8.36 设 $f(x_1,x_2,\dots,x_n)$ 是 $\mathbb{F}_q$ 上的一个非退化二次型, λ 是 $\mathbb{F}_q$ 的一个非主加法特征, 计算和式

$$\sum_{c_1,c_2,\dots,c_n\in\mathbb{F}_q}\lambda(f(c_1,c_2,\dots,c_n)).$$

8.37 设 α 为域 $\mathbb{F}_q$ 的一个本原元素, N 为正整数且 $N\mid(q-1)$. 令 $C_0=\langle\alpha^N\rangle$, 则 C_0 为 $\mathbb{F}_q^*$ 的 $\frac{q-1}{N}$ 阶子群, $\mathbb{F}_q^*$ 关于子群 C_0 的所有陪集

$$C_0,\ C_1=\alpha C_0,\ C_2=\alpha^2C_0,\ \dots,\ C_{N-1}=\alpha^{N-1}C_0$$

称为 $\mathbb{F}_q$ 的 N 阶分圆类. 设 λ 为 $\mathbb{F}_q$ 的典范加法特征, 定义 Gauss 周期为

$$g_a=\sum_{\beta\in C_a}\lambda(\beta),$$

其中 $0\le a\le N_1$. 证明对任意 a 均有 $|g_a|\le\sqrt{q}$.

8.38 设 G 为一个有限交换群, X 是一个集合, 映射 $f:X\to G$, 证明对每个 $a\in G$, a 的原像 $f^{-1}(a)$ 中的元素个数都相同 (即 f 取 G 中每个值同样的次数) 当且仅当对 G 的任意非主特征 χ 均有

$$\sum_{x\in X}\chi(f(x))=0.$$

8.39 设 A 和 B 是两个有限交换群, 函数 $f:A\to B$ 称为 bent 函数若对 A 的任意特征 χ 和 B 的任意非主特征 ψ, 有

$$\left|\sum_{a\in A}\chi(a)\psi(f(a))\right|=\sqrt{|A|}.$$

(a) 把群 A, B 中的运算都写成加法, 对任意 $a \in A \setminus \{0\}$, 定义函数 $f_a : A \to B$ 为 $f_a(x) = f(x+a) - f(x)$, 其中 $x \in A$. 证明 f 为 bent 函数当且仅当对任意 $a \in A \setminus \{0\}$, 函数 f_a 取 B 中每个值同样次数.

(b) 设 p 为素数, 证明 $f : \mathbb{F}_p^n \to \mathbb{F}_p$ 为 bent 函数当且仅当对任意 $\mathbf{y} \in \mathbb{F}_p^n$ 有

$$\left| \sum_{\mathbf{x} \in \mathbb{F}_p^n} \zeta_p^{f(\mathbf{x}) + \mathbf{x} \cdot \mathbf{y}} \right| = p^{\frac{n}{2}},$$

其中 $\zeta_p = e^{\frac{2\pi i}{p}}$, $\mathbf{x} \cdot \mathbf{y}$ 为 $\mathbf{x}$ 和 $\mathbf{y}$ 在 $\mathbb{F}_p^n$ 中的内积 (参考例 8.5).

参考文献

[1] B.C. Berndt, R.J. Evans and K.S. Williams, *Guass and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998.

[2] X. Hou, *Lectures on Finite Fields*, Graduate Studies in Mathematics 190, American Mathematical Society, Providence, Rhode Island, 2018.

[3] D. Jungnickel, *Finite Fields: Structure and Arithmetics*, Bibiographisches Institut, Mannheim, 1993.

[4] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, 2nd Edition, Cambridge University Press, Cambridge, 1997.

[5] R.J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, Bosten, 1987.

[6] G.L. Mullen and D. Panario, *Handbook of Finite Fields*, CRC Press, Taylor & Francis Group, Boca Raton, 2013.

[7] A. Terras, *Fourier Analysis on Finite Groups and Applications*, London Mathematical Society Student Texts 43, Cambridge University Press, Cambridge, 1999.

[8] Z. Wan, *Finite Fields and Galois Rings*, World Scientific, Singapore, 2012.

[9] 冯克勤, 廖群英: *有限域及其应用*, 大连理工大学出版社, 大连, 2011 年.

[10] 林东岱: *代数学基础与有限域*, 高等教育出版社, 北京, 2006 年.