arXiv:2601.09201v1 [math.RA] 14 Jan 2026

有限域上多项式的 $\mathbb{F}_q$阶以及 r本原元和 k正规元的性质

Maithri K.、Vadiraja Bhatta G. R.*、Indira K. P.、Prasanna Poojary

印度卡纳塔克邦Manipal的MAHE Manipal理工学院

摘要

有限域上的多项式与元素具有密切相关的代数结构，许多针对元素定义的性质也自然适用于多项式。元素的阶和 $\mathbb{F}_q$阶的概念已得到广泛研究。本文探讨了 r本原元和 k正规元的若干性质。此外，我们利用多项式的 $\mathbb{F}_q$阶这一概念，研究 k正规多项式的性质。

1 引言

设 q 为素数幂， n为正整数。则 $\mathbb{F}_{q^n}$ 表示含有 q^n 个元素的有限域，它是 $\mathbb{F}_q$ 的 n次扩张。该域具有两种基本的代数结构：它是 $\mathbb{F}_q$上的 n维向量空间，且其乘法群 $\mathbb{F}_{q^n}^*$ 是一个阶为 q^n-1的循环群。这些结构产生了两类特殊元素：正规元和本原元。

若元素 $\alpha \in \mathbb{F}_{q^n}$ 的共轭元集合 $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ 构成 $\mathbb{F}_q$上向量空间 $\mathbb{F}_{q^n}$ 的一组基，则称其为 $\mathbb{F}_q$ 上的正规元 。若一个元素的乘法阶为 q^n-1，即它生成整个乘法群 $\mathbb{F}_{q^n}^*$，则称其为本原元 。

对本原元和正规元的研究始于 Ore [1] 和 Carlitz [2, 3, 4], 的早期工作，他们探讨了这两类元素的主要性质，并为后续有限域研究奠定了基础。由于本原正规元素将这两种性质集于一身，且在密码学和编码理论中有应用，因此尤其受到关注。因此，许多研究聚焦于本原正规元素的存在性与构造 [5, 6, 7, 8]。

本原元和正规元的概念已扩展至 r-本原 元和 k- 正规 元。由于它们在密码学和编码理论中具有重要意义，近年来受到广泛关注。大量研究聚焦于此类元素的存在性及其代数性质 [9, 10]。更为专门的研究包括关于本原1-正规元存在性的结果 [11]。后续研究考察了有限域扩张 [12], 中 r-本原元与 k-正规元对 的存在性，以及通过逆型关系 [13]对它们进行刻画。若干研究还探讨了由本原元、 r-本原元和 k-正规元构成的等差数列 [14, 15]。此外，许多作者还研究了附加约束下的此类元素，例如具有指定范数的等差数列,

r-本原 k-正规元，且具有指定的范数和迹，以及具有固定范数的r-本原元等差数列 [16, 17, 18]。

本原元和正规元在密码学中发挥着核心作用，而本原多项式则广泛用于通过反馈移位寄存器（FSRs）生成伪随机数。这体现了研究元素及其多项式性质的重要性，尤其是本原多项式和正规多项式。本原多项式根据其根的阶来定义，此类多项式的阶为 q^n-1，如 [19] 中所述。M. Alizadeh 等人 [20]，引入的 k-正规多项式是通过其根来描述的。自然会让人好奇，能否将 $\mathbb{F}_q$- 阶的概念引入多项式，并定义 k- 正规多项式。Ore 在其著作 [1] 中曾简要提及这一概念。本文仿照元素的情形，给出多项式 $\mathbb{F}_q$-阶的精确定义，并据此研究其结构性质，得出有关 k-正规多项式的新结果。

本文结构如下。第 2 节汇总全文所需的预备知识和基础结果。第 3 节定义多项式的 $\mathbb{F}_q$-阶概念，并考察其主要性质和结构特征。第 4 节研究有限域上的 r-本原元和 k-正规元，并分析它们的代数性质。

2 预备知识

本节概述研究所需的有限域理论基本概念。这些内容构成了贯穿全文的基础框架和术语。

2.1 乘法阶与 r-本原元

对于 $\alpha \in \mathbb{F}_{q^n}^*$，满足 $\alpha^d = 1$ 的最小正整数 d 称为 α 的乘法阶，记为 $ord(\alpha)$。阶为 q^n-1 的元素称为本原元。更一般地，如果 $ord(\alpha) = \frac{q^n-1}{r}$，且 r 整除 q^n-1 [21]，则称元素为 r-本原元。 $r=1$的情形给出本原元。——

2.2 $\mathbb{F}_q$-阶与 k-正规元

令 $\sigma_q(\beta) = \beta^q$ 表示 $\mathbb{F}_{q^n}/\mathbb{F}_q$上的 Frobenius 自同构。对于 $\alpha \in \mathbb{F}_{q^n}$， α的 $\mathbb{F}_q$-阶记为 $Ord(\alpha)$，它是满足$g(\sigma_q)(\alpha) = 0$的次数最小的唯一首一多项式 $g(x) \in \mathbb{F}_q[x]$ 。等价地，它是在 Frobenius 作用下消去 α 的 $\mathbb{F}_q$ 上的最小多项式。它总是整除 x^n-1。

若元素 $\alpha \in \mathbb{F}_{q^n}$ 满足集合 $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ 构成 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$上的一组基，则称其为关于 $\mathbb{F}_q$的正规元 。Mullen 等人 [9] 引入了 k-正规元 的概念，其定义条件为 $\deg(Ord(\alpha)) = n-k$，这等价于

$$\dim_{\mathbb{F}_q}\langle \alpha, \alpha^q, \ldots, \alpha^{q^{n-1}} \rangle = n-k.$$

情形 $k=0$ 对应正规元素。

2.3 m-自由元和 g-自由元

此外，我们还利用有限域元素的一种额外刻画——自由性，研究 r-本原和 k-正规元素。

定义 1. *1.* 对于 $m \mid q^n - 1$，若对于 m 的任意因子 d， $\alpha = \beta^d$ 蕴含 $d = 1$，则称 $\alpha \in \mathbb{F}_{a^n}^*$ 是 m- 自由的。

2. 对于 $M \mid x^n - 1$，若 $\alpha = H(\beta)$，则称 $\alpha \in \mathbb{F}_{q^n}$ 是 M-自由的，其中 H 是 M 的因子 h 的 q-伴随元，并且 $h = 1$*[9]*。

3 $\mathbb{F}_q$-阶多项式

对于有限域中的元素，乘法阶与 $\mathbb{F}_q$-阶表现出密切相关的行为；特别是，这两个概念都受类似结构原理的支配。对于有限域上的多项式，也存在类似现象。关于 $\mathbb{F}_{q^n}$ 上多项式的阶这一概念已经十分成熟：多项式 $f(x)$ 的阶定义为满足以下条件的最小正整数 e：

$$f(x) \mid (x^e - 1).$$

受这一类比启发，我们引入多项式的 $\mathbb{F}_q$-阶这一概念，并研究其基本性质。我们证明，对于有限域上的多项式，阶与 $\mathbb{F}_q$-阶这两个概念表现出平行的结构行为，与域元素情形中观察到的关系十分相似。

这一思想可追溯到 Ore 的工作：他引入了属于 p-多项式类的多项式。然而，对这一概念的系统而详细的研究仍然有限。在本文中，我们在现代有限域框架下对其进行更正式的处理，将这一概念解释为多项式的 $\mathbb{F}_q$阶，并对经典定义作适当的细化。

定义 2. 设 $f \in \mathbb{F}_q[x]$ 为次数为 $m \geq 1$的多项式。若 g 是满足 $f|g \circ x$的首一最低次数多项式，则称 g 为 f 的 $\mathbb{F}_q$阶。记作 $Ord(f)$。

例 3. 考虑域 $\mathbb{F}_{5^2}$。设 $f = x + 1$。由于 f 是满足整除 $x^5 - x$的最低次数多项式，因此 f 的 $\mathbb{F}_q$阶为 $x - 1$。

对于不可约多项式，下面的结果揭示了多项式的 $\mathbb{F}_q$阶与其根之间的关系。事实上，两者的 $\mathbb{F}_q$ 阶相等。

命题 4. 若 $f \in \mathbb{F}_q[x]$ 是 $\mathbb{F}_q$ 上次数为 m 的不可约多项式，则 $Ord(f) = Ord(\alpha)$，其中 α 是 f 的根。

证明。设 $Ord(f) = g$，则由定义可得 $f|g \circ x$，这意味着 $g \circ x = f(x).h(x)$，其中 $h(x)$ 是某个多项式。由于 α 是 f 的根，$g \circ \alpha = 0$。
设 k 是 $\mathbb{F}_q[x]$ 中的一个多项式，其次数小于 g 和 $h \circ \alpha = 0$ 的次数。这意味着 $h \circ \alpha^{q^i} = 0$，$\forall\, i = 1, 2, \ldots\ldots, m$，由此得到 $f|h \circ x$，矛盾。因此 $\alpha = g$ 的 $\mathbb{F}_q$-阶。

□

推论 5. 若 $f \in \mathbb{F}_q[x]$ 是 $\mathbb{F}_q$上的次数为 m的不可约多项式，则 $Ord(f)|x^m - 1$。

命题 6. 设 $f \in \mathbb{F}_q[x]$ 是一个多项式，使得对于某个 $g \in \mathbb{F}_q[x]$， $f|g \circ x$ 当且仅当 $Ord(f)|g$。

证明。令 $h = Ord(f)|g$，则 $f|h \circ x$。由于 $h \circ x|g \circ x$，我们得到 $f|g \circ x$。
反过来，令 $f|g \circ x$，则 $deg(g) \geq deg(h)$。因此，对于某个 k， $r \in \mathbb{F}_q[x]$ 有$0 \leq deg(r) < deg(h)$，使得 $g = hk + r$。现在， $g \circ x = (hk) \circ x + r \circ x$。此外， $f|g \circ x$ 且 $f|(hk) \circ x$。因此 $f|r \circ x$，这意味着 $r \circ x = 0$, 进而意味着 $r = 0$。因此 $h|g$。 □

推论 7。 若 h, g 是两个非常数多项式，则 $gcd(h \circ x, g \circ x) = k \circ x$，其中$k = gcd(h, g)$。

现在我们考察各种类型的不可约多项式，看看它们的 $\mathbb{F}_q$-阶会如何变化。

命题 8. 设 $g \in \mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上不可约，且对于某个正整数 b， $f = g^b$ 。设 t 是满足 $p^t \geq b$ 的最小正整数，其中 p 是 $\mathbb{F}_q$的特征。则$Ord(f) = Ord(g)x^t$。

证明。设 $Ord(g) = h$，且 $Ord(f) = k$。于是， $g|h \circ x$，这意味着 $g^b|(h \circ x)^b$, $g^b|(h \circ x)^{q^t}$，进而得到 $g^b|h \circ x^{q^t}$。利用 $g^b = f$，可得 $f|h \circ x^{q^t}$。因此， $Ord(f)|hx^t$。
设 $deg(h) = s$。我们有 $g|h \circ x$，这意味着 $g^b|(h \circ x)^b$，其中 $deg((h \circ x)^b) = q^s b$。设 $\alpha_1, \cdots, \alpha_m$是 g的互异根。我们知道， h的根构成一个子空间 U。由于 h是 g的 $\mathbb{F}_q$-阶，U 是包含 $\alpha_1, \cdots, \alpha_m$的最小子空间。设 L是满足 $g^b|L$ 的次数最低的线性化多项式（这样的多项式存在，因为 $g^b|(h \circ x)^{q^t}$）。那么 L 应包含因子 $(x - \alpha_i)^{q^t}$。由于 L 的根构成子空间 V，且L 是满足 $g^b|L$的次数最低的线性化多项式，因此 $V = U$，由此得到 $q^s b \leq deg(L)$。根据 t的选取, $q^s q^t \leq deg(L)$。此外，由命题 6 可得 $L|(hx^t) \circ x$。因此，$q^s q^t \geq deg(L) \implies L = (hx^t) \circ x$。于是 $Ord(f) = Ord(g)x^t$。 □

命题9. 设 $g_1, g_2, \ldots, g_k$ 是 $\mathbb{F}_q[x]$上的两两互素多项式，且$f = g_1 g_2 \ldots g_k$。则 $Ord(f) = lcm\{Ord(g_1)$ $Ord(g_2) \ldots, Ord(g_k)\}$。

证明. 设 $Ord(g_i) = h_i \ \forall \ i, 1 \leq i \leq k$且 $l = lcm\{h_1, h_2, \ldots h_k\}$，则 $h_i|l \ \forall \ i$，进一步有 $H_i|l \circ x \ \forall \ i$，其中 $H_i = h_i \circ x$。我们有 $g_i|H_i \ \forall \ i$，这意味着 $g_1 g_2 \ldots g_k|lcm\{H_1, H_2, \ldots, H_k\}|l \circ x$。因此， $f|l \circ x$，这意味着 $Ord(f)|l$。设 $Ord(f) = j$, 则 $f|j \circ x$，这意味着 $g_i|j \circ x \ \forall \ i$。由于 $Ord(g_i) = h_i, h_i|j \ \forall \ i$，这意味着 $lcm\{h_1, h_2, \ldots, h_k\}|j = Ord(f)$。 □

如果元素在 $\mathbb{F}_{q^n}$ 中的 $\mathbb{F}_q$阶为 $x^n - 1$，那么该元素是正规元。正规多项式也是如此，其定义为有限域 [19]中正规元的最小多项式。

命题10。 次数为 m 的多项式 $f \in \mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上是正规多项式，当且仅当 f 是首一的，且 $Ord(f) = x^m - 1$。

证明。令 f 为 $\mathbb{F}_q[x]$中的一个正规多项式，且 $g = Ord(f)$。这意味着 $f|g \circ x$。令 α 为 f 的根，则 $Ord(\alpha) = x^m - 1$。由于 $f|g \circ x$， $g \circ \alpha = 0 \implies g = Ord(f) = x^m - 1$。反之，令 $Ord(f) = x^m - 1$。假设 f 可约，则要么 $f = g^b$，其中某个不可约多项式 g；要么 $f = gh$，且 g， h 不可约；要么 $f = g^a h^b$，其中某些互素

多项式 g, h，且 a, $b \geq 1$
假设 $f = g^b$，那么根据命题 8, $x|Ord(f) \implies x|x^m - 1$，这就产生了矛盾。
假设 $f = g^a h^b$，其中 g^a 和 h^b 互素，且 a 或 $b \geq 1$，那么 $Ord(f) = lcm(Ord(g^a)\ Ord(h^b))$，这是命题9中的 x 的倍式，由此可得 $x|x^m - 1$，矛盾。

假设 $f = gh$，其中 f, g不可约, $deg(g) = e_1$且 $deg(h) = e_2$，那么 $m = e_1 + e_2$。我们知道 $x^m - 1 = Ord(f) = lcm(Ord(g)\ Ord(h))$。现在根据推论 5 $Ord(g)|x^{e_1} - 1$, $Ord(h)|x^{e_2} - 1$。所以 $lcm(Ord(g)\ Ord(h))|lcm(x_1^e - 1,\ x_2^e - 1)$，这意味着 $x^m - 1|lcm(x_1^e - 1,\ x_2^e - 1)$，由此得到, $m < e_1 + e_2$ 矛盾。

因此, f 是一个在 F_q上的不可约多项式。由命题 4 可知，其所有根的 F_q-阶均为 $x^m - 1$。因此这些根都是正规元，故 f是正规多项式。 □

我们知道具有特定 $\mathbb{F}_q$-阶的元素个数。现在推导一个公式，用于计算次数固定且 $\mathbb{F}_q$-阶相同的不可约多项式的个数。

引理 11。若 α 是一个 $\mathbb{F}_q$-阶为 f的元素，则 α,$deg(m_\alpha(x)) = min\{r \geq 1 :\ f(x)|x^r - 1\} = ord(f)$ 的最小多项式的次数。

证明。考虑 Frobenius 自同构 σ，它对每个 α都将 α 映射为 α^q。由于 $f(x)$是 α的 $\mathbb{F}_q$-阶，$(f(x)) = \{g(x) :\ g(\sigma)(\alpha) = 0\}$。条件$\alpha^{q^r} = \alpha$ 等价于$(x^r - 1)(\sigma)(\alpha) = 0$，这当且仅当 $x^r - 1 \in (f(x))$成立，或者等价地，$f|x^r - 1$成立。
现在，利用第 19 章中关于 [22], 的最小多项式次数的结果: $m_\alpha(x) = min\{r > 0 :\ \alpha^{q^r} = \alpha\}$; 根据先前的讨论，这与 $min\{r \geq 1 :\ f(x)|x^r - 1\} = ord(f)$ 相同。
□

命题 12. $\mathbb{F}_q$-阶为 f 的 n 次不可约多项式的数量为 $\phi(f)\ n$，仅当 $ord(f)$ 为 n 时成立，否则为 0。

证明。**情况 1:** $ord(f) = n$
设 $g_1, g_2, \ldots, g_k$ 为次数为 n 且 $\mathbb{F}_q$-阶为 f 的不可约多项式, S 为它们所有根的集合。于是 $|S| = nk$。另外, B 为 $\mathbb{F}_{q^n}$ 中所有 $\mathbb{F}_q$-阶为 f 的元素组成的集合。由命题 4 可得, $S \subseteq T$。

由引理 11, T 中所有元素的最小多项式次数相同。由于 $S \subseteq T, S \neq \phi$，任意一个 $\alpha \in S$ 的最小多项式次数均为 n，也就是说，根据定义，它是某个 g_i。因此, T 中所有元素的最小多项式次数均为 n。所以它必定是某个 g_i。于是 $S = T$。因此，次数为 n 且 $\mathbb{F}_q$-阶为 f 的不可约多项式的数量由 $\phi(f)\ n$ 给出，只要 $n|\phi(f)$ 成立即可。

情形 2: $ord(f) \neq n$
若 f 的阶不是 n，则根据引理 11，具有$\mathbb{F}_q$-阶 f 的元素的最小多项式次数不等于 n。因此，它们不属于 g_i。所以数量为零。
□

k-正规多项式由 Mahmood Alizadeh 等人定义 [20]。有限域 $\mathbb{F}_q$ 上次数为 n 的首一不可约多项式，若其根是域 $\mathbb{F}_{q^n}$上的 k-正规元素，则称其为 k-正规多项式。利用上述结果，次数为 n 将等于

$$\sum_{\substack{h|x^n-1 \\ deg(h)=n-k \\ n|\phi(h)}} \frac{\phi(h)}{n}.$$

定理 13. 设 $f \in \mathbb{F}_q[x]$ 满足 $deg(g) \geq 1$. 设 $a \in \mathbb{F}_q$ 满足条件 h 是满足 $f(x)|(h \circ x - a)$的最低次数多项式。那么 $Ord(f) = Ord(a).h$

证明。令 $k = Ord(f)$，则 $f(x)|k \circ x$这意味着 $deg(k) \geq deg(h)$。因此

根据带余除法 $k = hm + n$，有 $0 \leq deg(n) < deg(h)$ 或 $n = 0$，这意味着 es

$$(hm + n) \circ x \equiv 0 \ modf(x)$$

从而得到

$$n \circ x \equiv -m \circ a \ modf(x)$$

如 $(hm) \circ x = m \circ h \circ x \equiv m \circ a \ modf(x)$.
因此 $n = 0$，从而 $Ord(a)|m$，其中 $m \circ a = 0$。因此 $(Ord(a)h)|hm = k$。反之,

$$(Ord(a)h) \circ x \equiv Ord(a) \circ a \equiv 0 \ modf(x)$$

因此 $k|Ord(a)h$。 □

4 r-本原元与 k-正规元的代数与组合性质

以下引理有助于在高次扩域中构造 r-本原元和 k-正规元。

引理 14. 设 $m|n$ 和 $\alpha \in \mathbb{F}_{q^m}$，则 α 在 $\mathbb{F}_{q^m}$ 中是 r-本原的，当且仅当 α 在 $\mathbb{F}_{q^n}$中是 kr-本原的，其中 $k = \frac{q^n - 1}{q^m - 1}$.

引理 15. 设 $m|n$ 和 $\alpha \in \mathbb{F}_{q^m}$，则 α 在 $\mathbb{F}_{q^m}$ 中是 k-正规的，当且仅当 α 在 $\mathbb{F}_{q^n}$中是 $n - m + k$-正规的。

在循环域中，$ord(ab) = lcm(ord(a)\ ord(b))$，其中 a 和 b 的阶互素。利用这一概念，我们得到以下结果。

命题16. 设 $\mathbb{F}_{q^n}$ 为一个域，且 a为 r_1-本原元，b 在 $\mathbb{F}_{q^n}$中为 r_2-本原元。若$gcd(\frac{q^n - 1}{r_1}, \frac{q^n - 1}{r_2}) = 1$，则 ab 在 $\mathbb{F}_{q^n}$中为 $gcd(r_1, r_2)$-本原元。

证明。 a在 $\mathbb{F}_{q^n}$中是 r_1-本原的，b在 $\mathbb{F}_{q^n}$中是 r_2-本原的
于是，$ord(a) = \frac{q^n - 1}{r_1}$ 且 $ord(b) = \frac{q^n - 1}{r_2}$.
由于 $gcd(ord(a)\ ord(b)) = 1$，$ord(ab) = lcm(ord(a)\ ord(b)) = lcm(\frac{q^n - 1}{r_1}, \frac{q^n - 1}{r_2})$
$= \frac{q^n - 1}{gcd\ r_1}(, r_2)$，这意味着元素 ab 在 $\mathbb{F}_{q^n}$中是 $gcd(r_1, r_2)$-本原的。 □

可以将所有 k-正规元 [13]的集合划分。相比之下，在 r-本原元的情形下，t 是 r 的倍式的 t-本原元可用于划分由 r 次幂构成的元素集合。利用以下结果，可以给出 $\sum_{d|n} \phi(d) = n$ 的另一种证明。

定理 17. 对于 q^n-1 的任意因子 r，令$\mathrm{B}=\{\beta^r \mid \beta \in \mathbb{F}_{q^n}\}$ 和 $\mathrm{A_t}=\{\alpha \in \mathbb{F}_{q^n} \mid ord(\alpha) = \frac{q^n-1}{t}\}$, 其中 t 是 r 的倍式。那么

$$\mathrm{B}=\bigcup_{r|t} \mathrm{A_t}.$$

证明。令 $a \in \bigcup \mathrm{A_t}$，则 $a \in \mathrm{A_t}$，其中 t 是 $r.$ 的某个倍式。根据 $\mathrm{A_t}$的定义，$_{r|t}ord(a) = \frac{q^n-1}{t}$，其中 $t|q^n-1$，且 $t=kr$ 对某个 $k \in \mathbb{N}$成立。由于 a 是 t-本原的，$a=\gamma^t$, 其中 γ 是一个本原元。即 $a=\gamma^{kr}=(\gamma^k)^r=\beta^r$，其中 $\beta=\gamma^k \in \mathbb{F}_{q^n}.$。因此，$a \in B.$。令 $a \in \mathrm{B}$，则 $a=\beta^r$ 对某个 r成立。

令 a 对某个 $t|q^n-1$是 t-本原的。
考虑，$a^{\frac{q^n-1}{r}}=(\beta^r)^{\frac{q^n-1}{r}}=1.$。由于 $ord(a)$ 是 $\frac{q^n-1}{t}$，我们得到，$\frac{q^n-1}{t} \mid \frac{q^n-1}{r}$，这表明 t 是 r的一个倍式。因此 $a \in A_t$，这意味着 $a \in \bigcup_{r|t} \mathrm{A_t}.$

Thus, $\mathrm{B}=\bigcup_{r|t} \mathrm{A_t}.$ □

定理 17 中定义的不同集合的元素个数由以下观察和命题给出。

观察 18。 *1.* $\bigcup_{r|t} \mathrm{A_t}$ 构成 $B.$ 的一个划分

2. $|A_t|=\phi(\frac{q^n-1}{t})$, *for any* t.

3. $|B|=\sum_{r|t}\phi(\frac{q^n-1}{t})$

命题 19。 设 $r|q^n-1$ 且 $\mathrm{B}=\{\beta^r \mid \beta \in \mathbb{F}^*_{q^n}\}$，则 $|\mathrm{B}|=\frac{q^n-1}{r}$.

证明。设 $\sigma: \mathbb{F}^*_{q^n} \longrightarrow \mathbb{F}^*_{q^n}$ 由 $\sigma(x)=x^r.$ 定义
Then, σ 是一个 homomorphism.
事实上，对于任意 $x, y \in \mathbb{F}^*_{q^n}$, $\sigma(xy)=(xy)^r=x^ry^r=\sigma(x)\sigma(y)$。
现在，$Ker\ \sigma=\{x \in \mathbb{F}^*_{q^n} \mid x^r=1\}$ 和 $Im\ \sigma=\{x^r \mid x \in \mathbb{F}^*_{q^n}\}=\mathrm{B}$。
由于 $r|q^n-1$, x^r-1 在 $\mathbb{F}^*_{q^n}$ 中完全分裂，且 x^r-1 在 $\mathbb{F}^*_{q^n}$中有 r 个不同的根，这是因为 x^r-1与其导数没有公共根。Thus, $|Ker\ \sigma|=r.$
根据第一同构定理，$\mathbb{F}^*_{q^n}/Ker\ \sigma \cong B$，因此，$|B|=\frac{q^n-1}{r}$. □

对于 q^n-1的任意因子 r，令 $\frac{q^n-1}{r}=k$, $r|t$ 等价于 $l=\frac{q^n-1}{t} \mid \frac{q^n-1}{r}$。则前一个命题中定义的集合 B 的基数为 $k.$。根据观察 3，我们得到$|\mathrm{B}|=\sum_{r|t}\phi(\frac{q^n-1}{t})=\frac{q^n-1}{r}$，这就证明了 $\sum \phi(l)=k$。

$\mathbb{F}_q$-阶也呈现出与经典阶类似的性质。具体而言，所有 $\mathbb{F}_q$-阶为 f 倍式的元素构成的集合会形成类似的划分结构。

命题20. 对于 x^n-1 的任意因子 f，令

$$B=\{\,a\in\mathbb{F}_{q^n}^*:f\mid \mathrm{Ord}(a)\,\},$$

对于 f 的每个倍式 g，定义

$$A_g=\left\{\,\alpha\in\mathbb{F}_{q^n}^*\;\middle|\;\mathrm{Ord}(\alpha)=\frac{x^n-1}{g}\right\}.$$

Then

$$B=\bigcup_{f\mid g}A_g.$$

证明。假设 $a\in\bigcup A_g$。那么，对于 f 的某个倍式 g，有 $a\in A_g$，因此 $\mathrm{Ord}(a)=\frac{x^n-1}{g}$.

存在一个正规元 $b\in\mathbb{F}_{q^n}^*$，使得 $a=g(b)$。由于 g 是 f 的倍式，写作 $g=hf$，其中 h 是某个多项式。因此

$$a=hf(b)=f(h(b))=f(c),$$

其中 $c=h(b)\in\mathbb{F}_{q^n}^*$。因此 $a\in B$，得到

$$\bigcup_{f\mid g}A_g\subseteq B.$$

反过来，假设 $a\in B$。那么，对某个 $b\in\mathbb{F}_{q^n}^*$，有 $a=f(b)$，并且

$$\mathrm{Ord}(a)=\frac{x^n-1}{g}.$$

现在考虑

$$\frac{x^n-1}{f}\circ a=\frac{x^n-1}{f}\circ(f(b))=(x^n-1)\circ(b)=0,$$

由于阶$(a)=\dfrac{x^n-1}{g}$，

$$\frac{x^n-1}{g}\mid\frac{x^n-1}{f}\quad\Longrightarrow\quad f\mid g.$$

因此 $a\in A_g$，这意味着

$$B\subseteq\bigcup_{f\mid g}A_g.$$

因此，$B=\bigcup_{f\mid g}A_g$。 □

命题21. 设 $f|x^n-1$和 $B=\{\,a\in\mathbb{F}_{q^n}^*:\ \ f\mid$阶$(a)\,\}$，则 $|B|=q^{n-degf}$。

证明。 设 $\sigma_f\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ 由 $\sigma_f(x) = f(x)$定义。则 σ_f是一个同态。事实上，对于任意 a，$b \in \mathbb{F}_{q^n}$，

$$\sigma_f(a+b) = f(a+b) = f(a) + f(b) = \sigma_f(a) + \sigma_f(b).$$

考虑 $Ker\sigma_f = \{\alpha \in \mathbb{F}_{q^n}\colon\ f(\alpha) = 0\}$，即所有 $\mathbb{F}_q$-阶整除 f 的元素组成的集合。因此，

$$|Ker\sigma_f| = \sum_{h|f} \phi(h)\, q^{\deg(f)-\deg(h)}.$$

σ_f 的像为 $\mathrm{Im}(\sigma_f) = \{f(\alpha)\colon\ \alpha \in \mathbb{F}_{q^n}\} = B$。
根据第一同构定理，

$$\frac{\mathbb{F}_{q^n}}{\ker \sigma_f} \cong \mathrm{Im}(\sigma_f) = B.$$

因此，

$$|B| = \frac{q^n}{|\ker \sigma_f|} = q^{\,n-\deg(f)}.$$

□

利用上述结果，可以对恒等式给出另一种证明

$$\sum_{g|f} \phi(g) = q^{\deg(f)}.$$

r-本原元和 k-正规元的研究在很大程度上分别依赖于 m-自由元和 g-自由元。 m-自由元的数量可见以下评注。这也促使我们计算 g-自由元的数量。

注22。 $\mathbb{F}_{q^n}$ 上的 m-自由元素数量为 $\phi(m)(q^n-1)\,m$ 。

命题23。 有限域 $\mathbb{F}_{q^n}$ 上的 g-自由元素数量为 $\begin{matrix}\phi & g & q^n \\ q^{deg(g)} & & \end{matrix}$ ()。

r k证明。 设 $x^n - 1 = (\prod_{i=1} f_i(x))^a$ 和 $g = \prod_{i=1}(f_i(x))^{b_i}$，其中每个 f_i 都是次数为 n_i 和 $k \le r$的不可约多项式。已知，当且仅当最大公因式 $\begin{pmatrix} x^n-1 & g \\ Ord\ \alpha & \end{pmatrix} = 1$时， $\alpha \in \mathbb{F}_{q^n}$ 是 g-自由的。因此， $Ord(\alpha)$的形式为 $f_1^a f_2^a \dots f_k^a h$，其中 h是 $f_{k+1}^a \dots f_r^a$的一个因子。因此， g-自由元素的数量等于，

$$\begin{aligned}
&= \sum_{h|f_{k+1}^a \cdots f_r^a} \phi(f_1^a f_2^a \dots f_k^a h) \\
&= \phi(f_1^a f_2^a \dots f_k^a) \sum_{h|f_{k+1}^a \cdots f_r^a} \phi(h) \\
&= \phi(f_1^a f_2^a \dots f_k^a) \sum_{i_{k+1}=0}^{a} \sum_{i_{k+2}=0}^{a} \cdots \sum_{i_r=0}^{a} \phi(f_{k+1}^{i_{k+1}} f_{k+2}^{i_{k+2}} \dots f_r^{i_r})
\end{aligned}$$

进一步计算可得， g-自由元素的数量为 $\phi(g)q^n$

$\overline{q_{deg(g)}}$。

□

如果 α 是 r-本原的，那么在任意域$\mathbb{F}_{q^n}$中，其逆元也将是 r-本原的。然而，涉及 k-正规时，情况并非总是如此。只有在二次扩张域中或对于 $k=n-1$，这种情况才会发生。

命题24。 在任意域 $\mathbb{F}_{q^n}$中，如果 α 是$(n-1)$-正规元，那么 α^{-1} 是$(n-1)$-正规元。

证明。 设 α是$(n-1)$-正规元，则 α的 $\mathbb{F}_q$阶为某个 $a\in\mathbb{F}_q$的 $f=x+a$。这意味着$(x+a)\circ\alpha=0 \implies \alpha^q+a\alpha=0$。因此，$\alpha^q=-a\alpha$。现在，考虑 $f^*\ x\ =xa^{-1}f\ \frac{1}{x}\ =x+a^{-1}$ $f^*\circ\alpha^{-1}=\ \alpha^{-1}\ {}^q+a^{-1}\alpha^{-1}=-a^{-1}\alpha^{-1}=(\,)(\,)$。
0 α^{-1} $n-1$
于是，( )。因此，的 $\mathbb{F}_q$阶为 f^*，故它是(-)-正规元。

□

推论25。 设 $\alpha\in\mathbb{F}_{q^2}$。如果 α 是 *0*-正规元，那么 α^{-1} 也是 *0*-正规元；如果 α 是 *1*-正规元，那么 α^{-1} 也是 *1*-正规元。

定理16给出了关于 r-本原元乘积的一条性质。在 $\mathbb{F}_q$-阶的背景下，我们考虑 $\mathbb{F}_q$-阶互素的元素之和。

命题26。 设 $\alpha,\beta\in\mathbb{F}_{q^n}$满足 $Ord(\alpha)=f$、$Ord(\beta)=g$且最大公因式$(f,g)=1$。则 $Ord(\alpha+\beta)=fg$。

证明。 设 $k=$Ord$(\alpha+\beta)$ 且 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_mx^m, g(x)=b_0+b_1x+\cdots+b_lx^l$。考虑:

$$\begin{aligned}
fg\circ(\alpha+\beta) &= f\circ(b_0(\alpha+\beta)+b_1(\alpha+\beta)^q+b_2(\alpha+\beta)^{q^2}+\cdots+b_l(\alpha+\beta)^{q^l})\\
&= f\circ((b_0\alpha+b_1\alpha^q+\cdots+b_l\alpha^{q^l})+(b_0\beta+b_1\beta^q+\cdots+b_l\beta^{q^l}))\\
&= f\circ((b_0\alpha+b_1\alpha^q+\cdots+b_l\alpha^{q^l})+g\circ\beta)\\
&= a_0(b_0\alpha+b_1\alpha^q+\cdots+b_l\alpha^{q^l})+a_1(b_0\alpha+b_1\alpha^q+\cdots+b_l\alpha^{q^l})^q+\ldots\\
&\quad +a_m(b_0\alpha+b_1\alpha^q+\cdots+b_l\alpha^{q^l})^{q^m}\\
&= b_0(a_0\alpha+a_1\alpha^q+\ldots a_m\alpha^{q^m})+b_1(a_0\alpha^q+a_1\alpha^{q^2}+\ldots a_m\alpha^{q^{m+1}})+\ldots\\
&\quad +b_n(a_0\alpha^{q^m}+a_1\alpha^{q^{m+1}}+\ldots a_m\alpha^{q^{m+l}})\\
&= b_0(f\circ\alpha)+b_1(f\circ\alpha^q)+\cdots+b_n(f\circ\alpha^{q^l})\\
&= 0.
\end{aligned}$$

因此 $k\mid fg$。现在， $k\circ(\alpha+\beta)=k\circ\alpha+k\circ\beta=0$，这意味着 $k\circ\alpha=-k\circ\beta=k\circ(-\beta)$。接着， $f\circ(k\circ\alpha)=f\circ(k\circ(-\beta))$，这意味着 $fk\circ\beta=0$。因此 $g\mid fk$，这意味着 $g\mid k$。类似地， $f\mid k$。因此 $fg\mid k$。所以 $k=fg$

□

推论27. 设 $\alpha,\beta\in\mathbb{F}_{q^n}$满足 阶$(\alpha)=f$、阶$(\beta)=g$，且 最大公因式$(f,g)=1$。设 α是k_1-正规元， β是 k_2-正规元。那么 $\alpha+\beta$是 k_1+k_2-n-正规元。

推论 28. 设 $\alpha_1,\alpha_2,\ldots,\alpha_k\in\mathbb{F}_{q^n}$，其中 $Ord(\alpha_i)=g_i,\ \forall\, i, 1\le i\le k$ 和 $g_1,g_2,\ldots,g_k$ 是 $\mathbb{F}_q[x]$上的两两互素多项式。则 $Ord(\alpha_1+\alpha_2+\cdots+\alpha_k)=lcm\{g_1,g_2,\ldots,g_k\}$。

我们注意到，在域 $\mathbb{F}_{q^n}$ 中，有 $\frac{q^n-1}{q-1}$ 个元素具有相同的范数，且有 p^{n-1} 个元素具有相同的迹。我们利用这一事实推导出以下结果。

引理 29. 设 $\alpha \in \mathbb{F}_{q^n}$ 的 $\mathbb{F}_q$-阶为 F，其中 $(x-1) \nmid F$。则 $trace(\alpha) = 0$。

证明. $x^n-1=(x-1)(1+x+x^2+\cdots+x^{n-1})$。由于，$(x-1) \nmid F$, $F \mid (1+x+x^2+\cdots+x^{n-1}) = f$。因此，根据 $\mathbb{F}_q$-阶和迹的定义，$trace(\alpha) = 0$。 □

Proposition 30. $\sum_{\substack{F \mid x^n-1 \\ (x-1) \nmid F}} \phi(F) = p^{n-1}$ *with* $gcd(n,p) = 1$.

证明. 设 α 为阶为 F的元素。
断言：若 $(x-1) \mid F$，则 $trace(\alpha) \neq 0$。
假设 $trace(\alpha) = 0$，则 $F \mid 1+x+\cdots+x^{n-1}$。由于 $(x-1) \mid F$，我们得到 $(x-1) \mid 1+x+\cdots+x^{n-1}$，这就产生矛盾。($\because gcd(n,p) = 1$)。
根据前述命题可知，若 $(x-1) \nmid F$，则 $trace(\alpha) = 0$。此外，域中有 p^{n-1} 个迹相同的元素 $\mathbb{F}_{p^n}$。因此，$\sum_{F \mid x^n-1 (x-1) \nmid F} \phi(F) = p^{n-1}$。

□

5 结论

本文探讨了有限域上 r-本原元和 k-正规元的理论，并通过 $\mathbb{F}_q$-阶的概念将这些思想拓展到多项式情形。通过建立不可约多项式的 $\mathbb{F}_q$-阶与其根的阶之间的联系，我们进一步揭示了基于元素的方法与基于多项式的方法之间的紧密联系。这一视角为研究具有指定 $\mathbb{F}_q$-阶的不可约多项式提供了统一且系统的框架，并得出了明确的计数结果。本文还给出了次数固定的 k-正规多项式的精确计数公式。此外，我们分析了基于阶和基于 $\mathbb{F}_q$-阶的划分，从而为欧拉 φ 函数及其多项式对应物相关的经典恒等式提供了另一种推导方法。我们还讨论了 r-本原元和 k-正规元的一些代数与组合性质。

参考文献

[1] O. Ore, 《有限域理论的贡献》, 美国数学会汇刊, 第36卷, 第2期, 第243–274页, 1934年。[2] L. Carlitz, 《有限域中的本原根》, 美国数学会汇刊, 第73卷, 第3期, 第373–382页, 1952年。[3] L. Carlitz, 《有限域中第一类和第二类本原根之和》, 数学新闻, 第12卷, 第3-4期, 第155–172页, 1954年。[4] L. Carlitz, 《有限域中涉及本原根的一些问题》, 美国国家科学院院刊, 第38卷, 第4期, 第314–318页, 1952年。

[5] H. W. Lenstra 和 R. J. Schoof，《有限域的本原正规基》，计算数学，第48卷，第177期，第217–231页，1987年。[6] S. Cohen 和 D. Hachenberger，《具有指定迹的本原正规基》，工程、通信与计算中的应用代数，第9卷，第383–403页，1999年5月。[7] S. D. Cohen 和 S. Huczynska，《无需计算机的本原正规基定理》，伦敦数学会会刊，第67卷，第1期，第41–56页，2003年。[8] A. K. Sharma、M. Rani 和 S. K. Tiwari，《具有指定范数和迹的本原正规对》，有限域及其应用，第78卷，第101976页，2022年。[9] S. Huczynska、G. L. Mullen、D. Panario 和 D. Thomson，《有限域上k-正规元的存在性及其性质》，有限域及其应用，第24卷，第170–183页，2013年。[10] J. Aguirre、C. Carvalho 和 V. Neumann，《关于有限域中的r-本原元和k-正规元》，设计、编码与密码学，第91卷，第1–12页，2022年8月。[11] L. Reis 和 D. Thomson，《有限域中本原1-正规元的存在性》，有限域及其应用，第51卷，第238–269页，2018年。[12] J. Aguirre 和 V. Neumann，《有限域中的r-本原元素与k-正规元素对》，巴西数学会通报，新系列，第54卷，2023年4月。[13] M. Rani、A. K. Sharma、S. K. Tiwari 和 A. Panigrahi，《有限域上r-本原k-正规元的逆元》，拉马努金杂志，第63卷，2023年10月。[14] V. G. L. N. Josimar J. R. Aguirre、Ab´íl io Lemos 和 S. Ribas，《有限域上等差数列中的r-本原k-正规元》，代数通讯，第52卷，第1期，第427–442页，2024年。[15] J. Sharma、R. Sarma 和 S. Laishram，《域中r-本原元的等差数列》，巴西数学会通报 ´巴西数学，第55卷，2024年8月。[16] K. Chatterjee、H. S harma、A. Shukla 和 S. Tiwari，《具有指定范数的有限域中的等差数列》，数学论坛，2024年3月。[17] M. Rani、A. K. Sharma、S. K. Tiwari 和 A. Panigrahi，《有限域上具有指定范数和迹的r-本原k-正规元》，有限域及其应用，第91卷，第102253页，2023年。[18] A. Choudhary 和 J. Sharma，《有限域中某些特殊元素的等差数列》，代数通讯，第0卷，第0期，第1–17页，2025年。[19] R. Lidl 和 H. Niederreiter，有限域及其应用，第20卷，数学及其应用百科全书。剑桥大学出版社，1996年。[20] M. Alizadeh、M. Darafsheh 和 S. Mehrabi，《有限域上的k-正规元与多项式》，意大利纯粹与应用数学杂志，第451–464页，2018年2月。[21] G. Kapetanakis 和 L. Reis，《本原正规基定理的变体》，设计、编码与密码学，第87卷，2019年7月。

[22] V.Shoup, 数论与代数的计算导论。剑桥大学出版社，第2版，2009年。