arXiv:2305.06653v1 [math.NT] 11 May 2023

有限 Dickson 近体的构造

Prudence Djagba

纳尔逊·曼德拉大学，南非数学系 电子邮箱：
prudence@aims.ac.za

摘要：对于 Dickson 对 (q,n)，我们证明 $\left\{\frac{q^k-1}{q-1}, 1 \leq k < n\right\}$ 构成模 n 的一个有限完备不同剩余系。我们还研究了由 Dickson 对 (q,n) 导出的有限 Dickson 近体的构造。

关键词：Dickson 对，Dickson 近域

2010年数学学科分类：16Y30;
12K05

1 引言

对近环和近体的研究始于1905年，当时 Leonard Eugene Dickson ([5]) 希望了解，如果从斜域（除环）的公理列表中删除一条公理，会产生何种代数结构。他发现，确实存在满足斜域所有公理（除一条分配律外）的“近体”。Dickson 通过以一个域为基础，并将乘法改为一种新的运算，实现了这一构造。为纪念他，这类近体被称为“Dickson 近体”。1966年，Beidleman [1] 首次引入了第一类近向量空间，将向量空间的概念推广到非线性结构，并使用近体上的近环模。此后，在其学位论文中，[4] 中的作者扩展了 Beidleman 近向量空间理论。在 [2, 3] 中，作者描述了有限维 Beidleman 近向量空间的 R-子群。Zassenhauss [10], 、Karzel 和 Ellers [6] 解决了该领域的一些重要问题。最近，[3] 中的作者研究了有限近体的广义分配集。在其学位论文中，[4] 中的作者扩展了 Beidleman 近向量空间理论。在 [2, 3] 中，作者描述了有限维 Beidleman 近向量空间的 R- 子群，并引入了 R- 维数、R- 基、种子集以及 R-子群的种子数等概念。在 [11] 中，作者给出了有限 Dickson 近体的中心的一种替代证明。

近场是一种类似于斜体（有时称为除环）的代数结构，不同之处在于它只满足两条分配律中的一条。

定义 1.1. (*[8]*) 近场是一个集合 N，配备两个二元运算 $+$（加法）和 $\cdot$（乘法），并满足以下公理：

- $(N,+)$ 是一个单位元为 0 的阿贝尔群，
- $(N,\cdot)$ 是一个半群，即对于所有元素 $a,b,c \in N$，均有 $(a\cdot b)\cdot c = a\cdot(b\cdot c)$（乘法结合律），
- $(a+b)\cdot c = a\cdot c + b\cdot c$ 对于所有元素 $a,b,c \in N$ 均成立（右分配律），
- N 包含一个元素 1，使得对于所有元素 $a \in N$，$1\cdot a = a\cdot 1 = a$（乘法单位元），

- 对于 N中的每个非零元素 a，都存在一个元素 a^{-1}，使得 $a \cdot a^{-1} = a^{-1} \cdot a = 1$（乘法逆元）。

我们将用 $N^{\times}$ 表示 $N\backslash\{0\}$。

定义 1.2. 真近体是指不是域的近体。

在本文中，我们将始终考虑右拟域，并用 N 表示一个拟域。

例 1.3. 域和斜域都是近域。

例 1.4. *[8]*考虑有限域 $(GF(3^2), +, \cdot)$，它的具体构造方式如下

$$GF(3^2) \cong \mathbb{Z}_3[X]/(X^2+1).$$

由此可得 $GF(3^2) := \{0, 1, 2, \beta, 1+\beta, 2+\beta, 2\beta, 1+2\beta, 2+2\beta\}$ 其中 β 是 $X^2+1 \in \mathbb{Z}_3[X]$ 的一个零点。$GF(3^2)$ 上的加法表定义为

$$(a+b\beta)+(c+d\beta) = (a+c) mod\ 3 + ((b+d) mod\ 3)\beta$$

可以发现，在 *[8]* 中，$N_9 := (GF(3^2), +, \circ)$，其乘法定义如下。

$$x \circ y = \begin{cases} x \cdot y \ if\ y\ is\ a\ square\ in\ (GF(3^2), +, \cdot) \\ x^3 \cdot y \ otherwise \end{cases}$$

是一个有限真近域。

我们将在下一节看到，这个有限近体的例子是一个有限 Dickson 近体。正如我们稍后将要证明的，它是最小的有限真近体。

定义 1.5. 映射

$$\begin{aligned} \psi \ : F &\to F \\ a &\mapsto a^p \end{aligned}$$

称为 F 的弗罗贝尼乌斯自同构。

现在，我们引入一些映射，这些映射有助于定义一种新的乘法运算。

定义 1.6.（*[8]*）设 N 为一个近域，$Aut(N, +, \cdot)$ 表示 N 的所有自同构构成的集合。一个映射

$$\begin{aligned} \phi : \quad N^{\times} &\to Aut(N, +, \cdot) \\ n &\mapsto \phi_n \end{aligned}$$

称为耦合映射，当且仅当对所有 $n, m \in N^{\times}, \phi_n \circ \phi_m = \phi_{\phi_n(m) \cdot n}$.

定义 1.7. (*[8]*) 设 N 为一个近域，ϕ 为 N上的一个耦合映射。则在 N 上定义一个新的二元运算如下:

$$n \circ_\phi m = \begin{cases} \phi_m(n) \cdot m \ if\ m \neq 0 \\ 0 \ if\ m = 0. \end{cases}$$

为说明这一点，令 $m, n \in N$，则若 $m = 0$, $n \circ_\phi m = 0$。若 $m \neq 0, \phi_m(n) \in N$且 $m \in N^{\times}$，则 $\phi_m(n) \cdot m \in N^{\times}$。由此可得 $n \circ_\phi m \in N$。因此，N在新的运算下封闭。

引理 1.8. (*[8]*) 设 N 是一个近体，ϕ 是一个耦合映射。则集合

$$G = \{\phi_n : n \in N^\times\}$$

在映射的复合运算下构成一个群。

注 1.9。

- $(G, \circ)$ 是 (Aut(N) $\circ$) 的一个子群。
- $(G, \circ)$ 称为一个狄克逊群。

定理 1.10. (*[8]*) 设 N 是一个近域，ϕ 是 N 上的耦合映射。那么 $(N, +, \circ_\phi)$ 仍然是一个近域，其中 $\circ_\phi$ 的定义如定义 1.7 所示。

2 迪克森构造

第一个有限真近体由 L.E. Dickson [5] 发现。他构造了第一个有限 Dickson 近体。他的方法是对有限域的乘法进行“扭曲”。

定义 2.1.（*[8]*）设（N，$+$，$\cdot$）为一个近域，且 ϕ 是 $N^\times$ 上的一个耦合映射。则（N，$+$，$\circ_\phi$）称为（N，$+$，$\cdot$）的 $\phi-$ 导出，并记为 N^ϕ。群（G，$\circ$）称为 ϕ 的 Dickson 群，其中 G 的定义如引理 1.8 所示。若 N 是某个域 F 的 $\phi-$ 导出，即 $N = F^\phi$.，则称 N 为 Dickson 近域。

注记 2.2。考虑耦合映射 ϕ：$n \mapsto id_N$。在此情形下

$$n \circ_\phi m = \begin{cases} \phi_m(n) \cdot m = id_N(n) \cdot m = n \cdot m & if\ m \neq 0 \\ 0 \quad if\ m = 0 \end{cases}$$

这是平凡耦合映射，因为新运算与通常的乘法相同。对于此耦合映射，我们有：

- 设 $(N, +, \cdot)$ 是一个真近体。$(N, +, \cdot)$ 的 $\phi-$导出为 $(N, +, \circ_\phi)$，即 $N^\phi = N$ 也是一个近体，但不是狄克逊近体。
- 设 $(F, +, \cdot)$ 为一个域。$(F, +, \cdot)$ 的 $\phi-$导出为 $(F, +, \circ_\phi)$，即 $F^\phi = F$。由此可知，每个域都是一个狄克逊近域。

我们希望构造有限 Dickson 近体。

定义 2.3. (*[8]*) 数对 $(q, n) \in \mathbb{N}^2$ 称为 Dickson 对，如果

- q 是素数 p 的某个幂 p^l，
- n 的每个素因子都整除 $q - 1$,
- 如果 $q \equiv 3$ 模 4，则 4 不整除 n。

例 2.4. 以下各对都是 Dickson 数：(13, 6)、(7, 3)、(5, 2)、(9, 2)、(3, 2)、(4, 3)、(5, 2)、(5, 4)、(7, 2)、(11, 2)、(23, 2)、(59, 2)、$(p, 1)$，其中 p 为素数。

引理 2.5. $\left\{\frac{q^k-1}{q-1}, 1 \leq k < n\right\}$ 模 n 的剩余类集合为集合 $\{i, 0 \leq i < n\}$，其中(q, n)是 Dickson 对。

证明。设 $i(k) = \frac{q^k-1}{q-1}$，其中 $k = 1$、$\cdots$、n。

我们希望证明，$\{i(1)\ i(2)\ \cdots, i(n)\}$ 模 n 的剩余类集合为 $\{0, 1, \cdots, n-1\}$。只需证明集合 $\left\{\frac{q^k-1}{q-1}, 1 \le k < n\right\}$ 中的元素模 n两两不同。

假设

$$\frac{q^k-1}{q-1} \equiv \frac{q^l-1}{q-1} \mod n \quad 1 \le k < l < n. \tag{1}$$

这意味着

$$\begin{aligned} &1 + q + \cdots + q^{k-1} \equiv 1 + q + \cdots + q^{l-1} \mod n \\ &\Rightarrow q^k + \cdots + q^{l-1} \equiv 0 \mod n \\ &\Rightarrow q^k(1 + \cdots + q^{l-k-1}) \equiv 0 \mod n \end{aligned}$$

根据 Dickson 对的定义，n 的每个素因子 p 都整除 $q-1$，因此 p 不整除 q。由此可得 $\gcd(q, n) = 1$。因此

$$\begin{aligned} q^k(1 + \cdots + q^{l-k-1}) \equiv 0 \mod n &\Rightarrow 1 + \cdots + q^{l-k-1} \equiv 0 \mod n \\ &\Rightarrow \frac{q^{l-k}-1}{q-1} \equiv 0 \mod n. \end{aligned}$$

假设对于某个 $1 \le t < n.$，$\frac{q^t-1}{q-1} \equiv 0$ 模 n。由此可得，对所有 i,

$$\frac{q^t-1}{q-1} \equiv 0 \mod p_i^{\alpha_i}$$

其中$n = \prod p_i^{\alpha_i}$是唯一的素因数分解。

不失一般性，假设 $n = p^m$.

我们知道 $q \equiv 1$ 模 p。因此，对于某个 $\epsilon \in \mathbb{N}.$，我们可以写成 $q = 1 + p\epsilon$

假设 $\frac{q^t-1}{q-1}$ 被 p^m 整除，我们证明 $n = p^m$ 整除 t 会导致矛盾。

事实上

$$q^t = (1 + p\epsilon)^t = \sum_{k=0}^{t} \binom{t}{k} (p\epsilon)^k.$$

因此

$$\frac{q^t-1}{q-1} = \sum_{k=1}^{t} \binom{t}{k} (p\epsilon)^{k-1} = \cdots + \binom{t}{2} p\epsilon + t.$$

例如

- 如果 $m = 1$，那么假设是

$$p / \frac{q^t-1}{q-1} \Leftrightarrow p / \sum_{k=1}^{t} \binom{t}{k} (p\epsilon)^{k-1} \Leftrightarrow p/t$$

这会导致矛盾，因为 $p = n > t$。

• 如果 $m = 2$,

$$p^2 / \frac{q^t - 1}{q - 1} \Leftrightarrow p^2 / \sum_{k=1}^{t} \binom{t}{k} (p\epsilon)^{k-1} \Leftrightarrow p / \binom{t}{2} p\epsilon + t \Rightarrow p/t$$

但随后 $\binom{t}{2} = {}^{t}\!\underline{(t-1)\,2}$，因此 $p / \binom{t}{2}$。由此可得 $p^2 / \binom{t}{2} p\epsilon.$，因此 p^2/t，这就导致了矛盾。

• 用同样的方法可得，对于某些 $m, p^m / \frac{q^t - 1}{q-1} \Rightarrow n = p^m/t$，会导致矛盾。

因此，假设 1 不可能成立。于是集合 $\{^{q}{}_{k} \ \frac{-1}{q-1}、\ 1 \le k < n\}$ 是模 n的不同剩余类。

□

我们将在下一个定理中看到，对于每一对 Dickson 数，我们都能构造一个包含 q^n 个元素的有限 Dickson 近体。对于任意 Dickson 对 (q, n)，我们将用 $DN(q, n)$ 表示与之关联的 Dickson 近体。

定理 2.6. (*[8]*)

对于所有 Dickson 数对 (q, n)，都存在相应的有限 Dickson 近体，其阶为 q^n。这些近体可通过对伽罗瓦域 $GF(q^n)$ 改变乘法运算而得到，使得 $DN(q, n) = GF(q^n)^{\phi} = \big(GF(q^n)$ $+, \circ\big)$。

证明。

• 设 (q, n) 是一个 Dickson 对，其中 $q = p^l$。

• 设 $(F, +, \cdot)$ 是一个特征为 p 的有限域，其中 p 是素数。存在一个整数 $ln \ge 1$，使得 $|F| = p^{ln}.$。此域称为伽罗瓦域 $F := GF(q^n) = GF(p^{ln})$，含有 q^n 个元素。乘法群 $(F^{\times}, \cdot)$ 是循环的（证明可见 [?]）。因此，$F^{\times}$ 由一个记作 g 的元素生成，即 $F^{\times} = \langle g \rangle$。考虑由 g^n 生成的 $(F^{\times}, \cdot)$ 的子群 H，即 $H = \langle g^n \rangle$。因此，$F^{\times}/H$ 是 H 的所有右陪集构成的群。每个陪集的形式为 $Hg^j = \{hg^j, \forall g^j \in F^{\times}\}$，其中 $j = 0$，....., $n - 1$。由于 H 是 $F^{\times}$ 的子群，H 在 $F^{\times}$ 中的右陪集数就是 H 在 $F^{\times}$ 中的指数 $(F^{\times} : H)$。由于 $F^{\times}$ 是有限的，$(F^{\times} : H)$ 也是有限的；根据拉格朗日定理，$(F^{\times} : H) = |F^{\times}/H| = n = \frac{|F^{\times}|}{|H|}$。因此

$$F^{\times}/H = \big\{Hg^j : 0 \le j \le n - 1\big\} = \big\{Hg^0, Hg^1, \ldots, Hg^{n-1}\big\}.$$

令 $i(k) = \frac{q^k - 1}{q-1}$ for $k = 1, \ldots, n$。可以证明，集合 $\big\{i(1)\ i(2) \ldots, i(n)\big\}$构成陪集代表元的幂的完全集，因为模 n 的剩余类集合$\big\{i(1)\ i(2) \ldots, i(n)\big\}$ 给出了集合 $\big\{0, 1, \ldots, n - 1\big\}$。因此，$F^{\times}/H$ 也可以表示如下

$$F^{\times}/H = \big\{Hg^{i(1)}, Hg^{i(2)}, \ldots, Hg^{i(n)}\big\} = \big\{Hg^{\frac{q^1 - 1}{q-1}}, Hg^{\frac{q^2 - 1}{q-1}}, \ldots, Hg^{\frac{q^n - 1}{q-1}}\big\}.$$

• 现在来考虑

$$\begin{aligned} \alpha : \quad & F \to F \\ & f \mapsto f^q \end{aligned}$$

它是 Frobenius 自同构的幂，即 $\alpha = \psi^l$（根据定义 1.5）。

- 映射

$$\lambda: \quad F^{\times}/H \to Aut(F,+,\cdot)$$
$$Hg^{\frac{q^k-1}{q-1}} \mapsto \alpha^k$$

定义良好：假设 $Hg^{\frac{q^{k_1}-1}{q-1}}$、$Hg^{\frac{q^{k_2}-1}{q-1}} \in F^{\times}/H$ 满足 $Hg^{\frac{q^{k_1}-1}{q-1}} = Hg^{\frac{q^{k_2}-1}{q-1}}$。那么

$$Hg^{\frac{q^{k_1}-1}{q-1}} = Hg^{\frac{q^{k_2}-1}{q-1}} \Rightarrow g^{\frac{q^{k_1}-1}{q-1}} = g^{\frac{q^{k_2}-1}{q-1}} \Rightarrow \frac{q^{k_1}-1}{q-1} = \frac{q^{k_2}-1}{q-1} \Rightarrow k_1 = k_2$$
$$\Rightarrow \alpha^{k_1} = \alpha^{k_2} \Rightarrow \lambda\big(Hg^{\frac{q^{k_1}-1}{q-1}}\big) = \lambda\big(Hg^{\frac{q^{k_2}-1}{q-1}}\big).$$

- 映射

$$\pi : F^{\times} \to F^{\times}/H$$
$$f \mapsto Hg^{\frac{q^k-1}{q-1}}$$

是一个满足同态性质的典范双射。因此 π 是一个典范双射。

- 复合映射定义为

$$\phi = \lambda \circ \pi : F^{\times} \to Aut(F,+,\cdot)$$
$$f \mapsto \alpha^k \text{ for } f \in Hg^{\frac{q^k-1}{q-1}}$$

这是 $F^{\times}$. 上的一个耦合映射。我们需要证明 $DN(q,n) = F^{\phi}$ 即$\phi_a \circ \phi_b = \phi_{\phi_a(b)a}$ 对所有 $a,b \in F^{\times}$. 都成立。
由于 $F^{\times}/H$ 可以表示为 $F^{\times}/H = \{Hg^{i(1)}, Hg^{i(2)}, \ldots, Hg^{i(n)}\}$，因此

$$F^{\times} = Hg^{i(1)} \cup Hg^{i(2)} \cup \cdots \cup Hg^{i(n)}.$$

因此，$F^{\times}$中的元素可以写成 $g^{\frac{q^k-1}{q-1}+n\delta}$，其中 $\delta \in \mathbb{N}$且$1 \le k \le n$。由此可知，若 $a = g^{i(k_1)+n\delta_1}$ 且 $b = g^{i(k_2)+n\delta_2}$，则 $\pi(a) = Hg^{\frac{q^{k_1}-1}{q-1}}$，$\pi(b) = Hg^{\frac{q^{k_2}-1}{q-1}}$.因此，$\phi_a = (\lambda \circ \phi)(a) = \alpha^{k_1}$且 $\phi_b = (\lambda \circ \phi)(b) = \alpha^{k_2}$。由此可知 $\phi_a \circ \phi_b = \alpha^{k_1} \circ \alpha^{k_2} = \alpha^{k_1+k_2}$.

此外，$\phi_a(b)a = \alpha^{k_1}(b) \cdot a = b^{q^{k_1}}a = g^{\left(\frac{q^{k_2}-1}{q-1}+n\delta_2\right)q^{k_1}} g^{\frac{q^{k_1}-1}{q-1}+n\delta_1} =$

$g^{\frac{q^{k_1+k_2}-q^k_1+q^{k_1}-1}{q-1}+n\delta_2 q^{k_1}+n\delta_1} = g^{\frac{q^{k_1+k_2}-1}{q-1}+n(\delta_1+q^{k_1}\delta_2)}$。由此可得 $\phi_{\phi_a(b)a} = \alpha^{k_1+k_2}$。
因此 $\phi_a \circ \phi_b = \phi_{\phi_a(b)a}$。
因此，如果我们考虑域 $F := (GF(q^n), +, \cdot)$ 以及耦合映射 ϕ，使得 $DN(q,n) = F^{\phi} = (GF(q^n), +, \circ_{\phi})$（作为有限域 F 的 $\phi-$ 导子），那么根据定义 2.1 DN，(q,n) 是一个含有 q^n 个元素的狄克逊近域。

□

引理 2.7. 对于所有满足 $n \neq 1$ 的 Dickson 对 (q,n)，由伽罗瓦域 $GF(q^n)$ 构造的任何 Dickson 近体都是真正的有限近体。

证明. 根据有限迪克森构造

$$DN(q,n) := GF(q^n)^{\phi} = \big(GF(q^n), +, \circ\big).$$

我们希望证明 $\big(GF(q^n)\ +, \circ\big)$ 不是域，也就是说，存在 $a, b \in GF(q^n)$ 使得 $a \circ b \neq b \circ a$. 耦合映射是

$$\begin{aligned} \phi = \lambda \circ \pi : \quad & F^{\times} \to Aut(F, +, \cdot) \\ & f \mapsto \alpha^k \quad \text{for} \quad k = 1, \cdots, n. \end{aligned}$$

$$\Leftrightarrow \phi : f \mapsto \begin{cases} \alpha & \text{if } f \in Hg^{\frac{q-1}{q-1}} \\ \alpha^2 & \text{if } f \in Hg^{\frac{q^2-1}{q-1}} \\ \vdots \quad & \vdots \\ \alpha^n & \text{if } f \in Hg^{\frac{q^n-1}{q-1}}. \end{cases}$$

对于 $a, b \in GF(q^n)$

$$a \circ_{\phi} b = \begin{cases} \phi_a(n) \cdot b & \text{if } b \neq 0 \\ 0 & \text{if } b = 0 \end{cases} = \begin{cases} \alpha(a) \cdot b & \text{if } b \in Hg^{\frac{q-1}{q-1}} \\ \alpha^2(a) \cdot b & \text{if } b \in Hg^{\frac{q^2-1}{q-1}} \\ \vdots \quad \vdots & \\ \alpha^n(a) \cdot b & \text{if } b \in Hg^{\frac{q^n-1}{q-1}} \end{cases} = \begin{cases} a^q \cdot b & \text{if } b \in Hg^{\frac{q-1}{q-1}} \\ a^{q^2} \cdot b & \text{if } b \in Hg^{\frac{q^2-1}{q-1}} \\ \vdots \quad \vdots & \\ a^{q^n} \cdot b & \text{if } b \in Hg^{\frac{q^n-1}{q-1}} \end{cases}$$

q^n-1 q^1-1设 $a = g^n \in Hg^{\overline{q-1}}$和 $b = gHg^{\overline{q-1}}$

我们有

$$\begin{aligned} g^n \circ g &= \alpha^1(g^n)g \\ &= (g^n)^q g \\ &= g^{nq+1}. \end{aligned}$$

Also

$$\begin{aligned} g \circ g^n &= \alpha^n(g)g^n \\ &= g^{n+1} \quad \text{because} \quad \alpha^n = id. \end{aligned}$$

假设 $g^{nq+1} = g^{n+1}$，则 $g^{n(q-1)} = 1$.

但由于 $F^{\times} = \langle g \rangle$，因此 ord $(g) = q^n - 1$.

由此可知，如果 $g^t = 1 \Rightarrow q^n - 1/t$。

此外，由于

$$\begin{aligned} g^{n(q-1)} = 1 &\Rightarrow q^n - 1/n(q-1) \\ &\Rightarrow 1 + q + \cdots + q^{n-1}/n \end{aligned}$$

但是 $q = p^l > 1$所以 $1 + q + \cdots + q^{n-1} > n$。由此可知，$1 + q + \cdots + q^{n-1}$不整除 n.

因此 $g^{n(q-1)} \neq 1$. 这意味着 $g^n \circ g \neq g \circ g^n$。 ^{1}

^{q}存在 $a = g^n \in Hg^{\overline{n}}$ $_{q^{q-1}}$且 $b = gHg_{-1^{\overline{q-1}}}$使得 $n \circ b \neq a \circ b$. 因此，与满足 $q \neq 1$ $_{-1}$

的数对（q, n）相关联的有限 Dickson 近体都是真有限近体（而非域）。 □

定理 2.8。 *[5]* 取遍所有 Dickson 数对，便可得到所有按定理 2.6 所述方式构造的有限 Dickson 近体。

证明。更多细节请参见 [5] 。 □

注 2.9。

- 对于 $n = 1$，我们有 $F^{\times} = \langle g \rangle$ 和 $H = \langle g \rangle$。由此可得 $F^{\times}/H = \{H\}$，进而耦合映射是恒等映射，因为 $\phi\colon\ f \mapsto \alpha = f^q = f$。因此，所有有限域都由 Dickson 对 $(q,1)$ 得到。
- 注意，对于所有满足 $n = 1$ 的数对 (q,n)，都存在唯一一个阶为 $q = p^l$ 的有限 Dickson 近体，它同时也是有限域。
- 对于 $n \neq 1$ ，存在阶为 $q^n.$ 的有限真近体。在这种情况下，阶为 $q^n.$ 的有限 Dickson 近体不一定唯一。通过此构造得到的非同构 Dickson 近体的数量（对应于 g 的不同取值）为 $\varphi_{(n)}\, i$ ，其中 φ 是欧拉函数， i 是 p 模 n 的阶。
- 一般来说，Dickson 近体既可以是有限的，也可以是无限的。

3 结论

区别在于，对于有限域，在同构意义下，存在唯一一个阶为 p^n 的有限域；而对于由数对 (q,n) 构造的有限 Dickson 近体，则不存在唯一的有限 Dickson 近体。有限域的乘法群是循环的，而 Dickson 近体的乘法群是亚循环的。

参考文献

[1] James C. Beidleman，关于近环及近环模。博士论文，宾夕法尼亚州立大学，1966 年。[2] P.Djagba and K.-T. Howell 有限维近向量空间的子空间结构。《线性与多重线性代数》，第 1–21 页，2019 年。doi: 10.1.80/03081087.2019.1582610。[3] P. Djagba，关于有限近域的广义分配集，《代数学杂志》，2020 年。[4] P. Djagba，Beidleman 近向量空间理论的研究贡献，博士论文，斯泰伦博斯大学，2019 年。[5] Dickson Leonard Eugene，关于有限代数，《哥廷根科学院院刊》数学物理类，第 358–393 页，1905 年。[6] Erich Ellers und Helmut Karzel，有限关联群，《汉堡数学研讨会论文集》27（1964）：250–264。[7] Meldrum John DP，近环及其与群的联系，第 134 卷，皮特曼高级出版计划，1985 年。[8] Pilz Gunter，近环：理论及其应用，第 23 卷。爱思唯尔，2011 年。[9] Wähling Heinz，近体理论，Thales 出版社，第 1 卷，1987 年。

[10] H. Zassenhaus, ¨超有限快速域。在汉堡大学数学研讨会论文集中，第 11 卷，第 187–220 页。Springer，1935 年。[11] P. Djagba，关于有限 Dickson 近体的中心，arXiv 预印本 arXiv:2003.08306，2020 年。