Int. J. Nonlinear Anal. Appl. 14 (2023) 10, 155–161
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2023.30795.4495

Construction of a finite Dickson nearfield

Prudence Djagba

Department of Mathematics, Nelson Mandela University, South Africa

(Communicated by Abasalt Bodaghi)

Abstract

For a Dickson pair (q, n) we show that $\left\{\frac{q^k-1}{q-1}, 1 \leq k \leq n\right\}$ forms a finite complete set of different residues modulo n. We also study the construction of a finite Dickson nearfield that arises from the Dickson pair (q, n).

Keywords: Dickson pair, Dickson nearfield
2020 MSC: 16Y30, 12K05

1 Introduction

The interest of nearrings and nearfields started in 1905 when Leonard Eugene Dickson ([2]) wanted to know what structure arises if one axiom in the list of axioms for skew-fields (division rings) was removed. He found that there do exist "nearfields", which fulfill all axioms for skew-fields except one distributive law. Dickson achieved this by starting with a field and changing the multiplication into a new operation. In his honor, these types of nearfields are called "Dickson nearfields". In 1966 the first type of near-vector spaces was introduced by Beidleman [1] which generalises the concept of a vector space to a non-linear structure and used nearring modules over a nearfield. Following that, in his thesis, the authors in [3] has extended the theory of Beidleman near-vector spaces. In [6, 4] the authors described the R-subgroups of finite dimensional Beidleman near-vector spaces. Zassenhauss [11], Karzel and Ellers [7] have solved some important problems in this area. Recently the author in [4] has investigated on the generalized distributive set of a finite nearfield. In his thesis, the authors in [3] has extended the theory of Beidleman near-vector spaces. In [6, 4] the authors described the R-subgroups of finite dimensional Beidleman near-vector spaces and introduced the notion of R-dimension, R-basis, seed set and seed number of an R-subgroup. In [5] the authors gave an alternative proof of the center of a finite Dickson nearfield.

2 Preliminary materials

A nearfield is an algebraic structure similar to a skew-field sometimes called division ring, except that it has only one of the two distributive laws.

Definition 2.1. ([9]) A nearfield is a set N together with two binary operations $+$ (addition) and $\cdot$ (multiplication) satisfying the following axioms:

- $(N, +)$ is an abelian group with the identity 0,

Email address: pudence@aims.ac.za (Prudence Djagba)

Received: May 2023 *Accepted:* August 2023

- $(N, \cdot)$ is a semi-group i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all elements $a, b, c \in N$ (the associative law for multiplication),
- $(a + b) \cdot c = a \cdot c + b \cdot c$ for all elements $a, b, c \in N$ (the right distributive law),
- N contains an element 1 such that $1 \cdot a = a \cdot 1 = a$ for all element $a \in N$ (multiplicative identity),
- For every non-zero element a of N, there exists an element a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$ (multiplicative inverse).

We will use $N^{\times}$ to denote $N \backslash \{0\}$.

Definition 2.2. A proper nearfield is a nearfield that is not a field.

Throughout this note we will consider right nearfields and use N to denote a nearfield.

Example 2.3. [9] Consider the finite field $\big(GF(3^2), +, \cdot\big)$, it is explicitly constructed in the following way

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

It follows that $GF(3^2) := \{0, 1, 2, \beta, 1 + \beta, 2 + \beta, 2\beta, 1 + 2\beta, 2 + 2\beta\}$ where β is a zero of $X^2 + 1 \in \mathbb{Z}_3[X]$. The addition table on $GF(3^2)$ is defined by

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

It is observed in [9] that $N_9 := (GF(3^2), +, \circ)$ with a new multiplication defined by

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

is a finite proper nearfield.

We will see in the next section that this example of a finite nearfield is a finite Dickson nearfield. As we will prove later, it is the smallest finite proper nearfield.

Definition 2.4. Let F be a field. The map

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

is called the Frobenius automorphism of F.

Now, we introduce maps that are useful to define a new multiplication.

Definition 2.5. ([9]) Let N be a nearfield and $Aut(N, +, \cdot)$ the set of all automorphisms of N. A map

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

is called a coupling map if for all $n, m \in N^{\times}, \phi_n \circ \phi_m = \phi_{\phi_n(m) \cdot n}$.

Definition 2.6. ([9]) Let N be a nearfield and ϕ a coupling map on N. Then one defines a new binary operation on N by

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

To see this, let $m, n \in N$, then if $m = 0$, $n \circ_\phi m = 0$. If $m \neq 0, \phi_m(n) \in N$ and $m \in N^\times$ so $\phi_m(n) \cdot m \in N^\times$. It follows that $n \circ_\phi m \in N$. Thus N is closed under the new operation.

Lemma 2.7. ([9]) Let N be a nearfield and ϕ be a coupling map. Then the set

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

is a group under composition of maps.

Remark 2.8.

- $(G, \circ)$ is a subgroup of $(Aut(N), \circ)$.
- $(G, \circ)$ is called a Dickson-group.

Theorem 2.9. ([9]) Let N be a nearfield and ϕ be a coupling map on N. Then $(N, +, \circ_\phi)$ is again a nearfield where $\circ_\phi$ is defined as in Definition 2.

3 Dickson construction

The first finite proper nearfield was discovered by L.E Dickson [2]. He constructed the first example of a finite Dickson nearfield. His technique was to "distort" the multiplication of a finite field.

Definition 3.1. ([9]) Let $(N, +, \cdot)$ be a nearfield and ϕ a coupling map on $N^\times$. Then $(N, +, \circ_\phi)$ is called $\phi-$derivation of $(N, +, \cdot)$ and is denoted by N^ϕ. The group $(G, \circ)$ is called the Dickson group of ϕ with G defined as in Lemma 2.7. N is said to be a Dickson nearfield if N is the $\phi-$derivation of some field F, i.e., $N = F^\phi$.

Remark 3.2. Let us consider the coupling map $\phi : n \mapsto id_N$. In this case

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

It is the trivial coupling map because the new operation is the same as the usual multiplication. For this coupling map we have that:

- Let $(N, +, \cdot)$ be a proper nearfield. The $\phi-$derivation of $(N, +, \cdot)$ is $(N, +, \circ_\phi)$ i.e., $N^\phi = N$ is also a nearfield but not a Dickson nearfield.
- Let $(F, +, \cdot)$ be a field. The $\phi-$derivation of $(F, +, \cdot)$ is $(F, +, \circ_\phi)$ i.e., $F^\phi = F$. It follows that every field is a Dickson nearfield.

We would like to construct finite Dickson nearfields.

Definition 3.3. ([9]) A pairs of numbers $(q, n) \in \mathbb{N}^2$ is called a Dickson pair if

- q is some power p^l of a prime p,
- Each prime divisor of n divides $q - 1$,
- If $q \equiv 3 \bmod 4$ implies 4 does not divide n.

Example 3.4. The following pairs are Dickson numbers: $(13, 6)$, $(7, 3)$, $(5, 2)$, $(9, 2)$, $(3, 2)$, $(4, 3)$, $(5, 2)$, $(5, 4)$, $(7, 2)$, $(11, 2)$, $(23, 2)$, $(59, 2)$, $(p, 1)$ for p prime.

Lemma 3.5. The set $\left\{\frac{q^k-1}{q-1}, 1 \leq k \leq n\right\}$ residues modulo n is the set $\left\{i, 0 \leq i \leq n-1\right\}$ where (q, n) are Dickson pairs.

Proof . Let $i(k) = \frac{q^k-1}{q-1}$ for $k = 1, \ldots, n$. We would like to show that the set $\{i(1), i(2), \ldots, i(n)\}$ residues modulo n is the set $\{0, 1, \ldots, n-1\}$. It suffice to show that the set $\left\{\frac{q^k-1}{q-1}, 1 \leq k < n\right\}$ are distinct residues modulo n. Suppose that

$$\frac{q^k-1}{q-1} \equiv \frac{q^l-1}{q-1} \mod n, \quad 1 \leq k < l < n. \tag{3.1}$$

This implies that

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

By the definition of Dickson pair every prime divisor p of n divide $q-1$, so p does not divide q. It follows that gcd $(q, n) = 1$. Therefore

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

Assume that $\frac{q^t-1}{q-1} \equiv 0 \mod n$ for some $1 \leq t < n$. It follows that for all i,

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

where $n = \prod p_i^{\alpha_i}$ is the unique prime factorisation. We assume without loss of generality that $n = p^m$. We know that $q \equiv 1 \mod p$. So we can write $q = 1 + p\epsilon$ for some $\epsilon \in \mathbb{N}$. Assuming that p^m divides $\frac{q^t-1}{q-1}$, we want to show that $n = p^m$ divides t leads to contradiction. In fact

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

Hence

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

For instance

- if $m = 1$, then the assumption is

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

  leads to contradiction since $p = n > t$.

- if $m = 2$,

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

  But then $\binom{t}{2} = \frac{t(t-1)}{2}$, so $p/\binom{t}{2}$. Hence $p^2/\binom{t}{2} p\epsilon$. Thus p^2/t leads to contradiction.

- By the same approach for some m, $p^m / \frac{q^t-1}{q-1} \Rightarrow n = p^m/t$ leads to contradiction.

  Therefore the assumption 3.1 can not hold. Thus the set $\left\{\frac{q^k-1}{q-1}, 1 \le k \le n\right\}$ are distinct residues modulo n.

□

We will see in the next theorem that for each pair of Dickson numbers, we will be able to construct a finite Dickson nearfield containing q^n elements. For any Dickson pair (q, n), we will denote the associated Dickson nearfield by $DN(q, n)$.

Theorem 3.6. ([9])

For all pairs of Dickson numbers (q, n), there exists some associated finite Dickson nearfields, of order q^n which arise by taking the Galois Field $GF(q^n)$ and changing the multiplication such that $DN(q, n) = GF(q^n)^\phi = \big(GF(q^n), +, \circ\big)$.

Proof .

- Let (q, n) be a Dickson pair where $q = p^l$.
- Let $(F, +, \cdot)$ be a finite field with characteristic p where p is prime. There exists an integer $ln \ge 1$ such that $|F| = p^{ln}$. This field is called the Galois Field $F := GF(q^n) = GF(p^{ln})$ containing q^n elements. The multiplicative group $(F^\times, \cdot)$ is cyclic. So $F^\times$ is generated by an element denoted g, i.e. $F^\times = \langle g\rangle$. Let us consider H, the subgroup of $(F^\times, \cdot)$ generated by g^n, i.e., $H = \langle g^n\rangle$. So $F^\times/H$ is the group of all right cosets of H. Each coset is of the form $Hg^j = \{hg^j, \forall g^j \in F^\times\}$ where $j = 0, \dots, n-1$. Since H is a subgroup of $F^\times$, the number of right cosets of H in $F^\times$ is the index $(F^\times : H)$ of H in $F^\times$. Since $F^\times$ is finite $(F^\times : H)$ is finite and by Lagrange's Theorem $(F^\times : H) = |F^\times/H| = n = \frac{|F^\times|}{|H|}$. Thus

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

  Let $i(k) = \frac{q^k-1}{q-1}$ for $k = 1, \dots, n$. It can be shown that the set $\big\{i(1), i(2), \dots, i(n)\big\}$ forms a complete set of the powers of the coset representatives because the set $\big\{i(1), i(2), \dots, i(n)\big\}$ of residues modulo n give the set $\big\{0, 1, \dots, n-1\big\}$. Therefore $F^\times/H$ can also be represented as follows

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

- Now let us consider

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

  which is a power of the Frobenius automorphism, i.e., $\alpha = \psi^l$ (by Definition 2.4).

- The map

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

  is well-defined: suppose $Hg^{\frac{q^{k_1}-1}{q-1}}, Hg^{\frac{q^{k_2}-1}{q-1}} \in F^\times/H$ such that $Hg^{\frac{q^{k_1}-1}{q-1}} = Hg^{\frac{q^{k_2}-1}{q-1}}$. Then

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

- The map

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

  is a canonical bijection which satisfies the homomorphism property. So π is a canonical bijection.

- The composition map is defined as

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

which is a coupling map on $F^{\times}$. We need to show that $DN(q,n) = F^{\phi}$ i.e., $\phi_a \circ \phi_b = \phi_{\phi_a(b)a}$ for all $a, b \in F^{\times}$. Since $F^{\times}/H$ can be presented as $F^{\times}/H = \{Hg^{i(1)}, Hg^{i(2)}, \dots, Hg^{i(n)}\}$ then

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

Therefore the elements of $F^{\times}$ can be written as $g^{\frac{q^k-1}{q-1}+n\delta}$ for $\delta \in \mathbb{N}$ and $1 \le k \le n$. It follows that if $a = g^{i(k_1)+n\delta_1}$ and $b = g^{i(k_2)+n\delta_2}$, then $\pi(a) = Hg^{\frac{q^{k_1}-1}{q-1}}$, $\pi(b) = Hg^{\frac{q^{k_2}-1}{q-1}}$. So $\phi_a = (\lambda \circ \phi)(a) = \alpha^{k_1}$ and $\phi_b = (\lambda \circ \phi)(b) = \alpha^{k_2}$. It follows that $\phi_a \circ \phi_b = \alpha^{k_1} \circ \alpha^{k_2} = \alpha^{k_1+k_2}$.

Also $\phi_a(b)a = \alpha^{k_1}(b) \cdot a = b^{q^{k_1}} a = g^{\left(\frac{q^{k_2}-1}{q-1}+n\delta_2\right)q^{k_1}} g^{\frac{q^{k_1}-1}{q-1}+n\delta_1} =$ $g^{\frac{q^{k_1+k_2}-q_1^k+q^{k_1}-1}{q-1}+n\delta_2 q^{k_1}+n\delta_1} = g^{\frac{q^{k_1+k_2}-1}{q-1}+n(\delta_1+q^{k_1}\delta_2)}$. It follows that $\phi_{\phi_a(b)a} = \alpha^{k_1+k_2}$. Thus $\phi_a \circ \phi_b = \phi_{\phi_a(b)a}$.

Thus if we consider the field $F := (GF(q^n), +, \cdot)$ and the coupling map ϕ such that $DN(q,n) = F^{\phi} = (GF(q^n), +, \circ_{\phi})$ (as a $\phi-$derivation of the finite field F). Then by Definition 3.1 $DN(q,n)$ is a Dickson nearfield containing q^n elements.

□

Lemma 3.7. For all Dickson pair (q,n) where $n \neq 1$, any Dickson nearfields constructed by the Galois Field $GF(q^n)$ are proper finite nearfields.

Proof . From finite Dickson construction

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

We would like to show that $\big(GF(q^n), +, \circ\big)$ is not fields i.e., there exist $a, b \in (GF(q^n)$ such that $a \circ b \neq b \circ a$. The coupling map is

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

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

For $a, b \in (GF(q^n)$

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

Let $a = g^n \in Hg^{\frac{q^n-1}{q-1}}$ and $b = gHg^{\frac{q^1-1}{q-1}}$. We have

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

Also

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

Assume that $g^{nq+1} = g^{n+1}$, then $g^{n(q-1)} = 1$. But since $F^{\times} = \langle g \rangle$, then $\texttt{ord}\ (g) = q^n - 1$. It follows that if $g^t = 1 \Rightarrow q^n - 1/t$. Moreover, since $g^{n(q-1)} = 1$, we have $q^n - 1/n(q-1)$. Thus,

$$1 + q + \cdots + q^{n-1}/n.$$

But $q = p^l > 1$ so $1 + q + \cdots + q^{n-1} > n$. It follows that $1 + q + \cdots + q^{n-1}$ does not divides n. Thus $g^{n(q-1)} \neq 1$. This means that $g^n \circ g \neq g \circ g^n$. There exists $a = g^n \in Hg^{\frac{q^n-1}{q-1}}$ and $b = gHg^{\frac{q^1-1}{q-1}}$ such that $n \circ b \neq a \circ b$. Thus the finite Dickson nearfields associated to the pair (q, n) where $q \neq 1$ are proper finite nearfields (not fields). □

Theorem 3.8. [2] By taking all pairs of Dickson numbers, all finite Dickson nearfields arise in the way described in Theorem 3.6.

Proof . See [2] for more details. □

4 Concluding comments

As differences, for a finite field up to isomorphism, there exists a unique finite field of order p^n , but for a finite Dickson nearfield that arises from the pair (q, n), there does not exist a unique finite Dickson nearfield. The multiplicative group of a finite field is cyclic but the multiplicative group of a Dickson nearfield is metacyclic.

References

[1] J.C. Beidleman, *On near-rings and near-ring modules.* PhD thesis, Pennsylvanian State University, 1966.

[2] L.E. Dickson, *On finite algebras*, Nachr. Gesellsch. Wissensch. Gött. Math.-Phys. Klasse **1905** (1905), 358–393.

[3] P. Djagba, *Contributions to the theory of Beidleman near-vector spaces*, PhD thesis, Stellenbosch University, 2019.

[4] P. Djagba, *On the generalized distributive set of a finite nearfield*, J. Algebra **542** (2020), 130–161.

[5] P. Djagba, *On the center of a finite Dickson nearfield*, arXiv preprint arXiv:2003.08306, 2020.

[6] P. Djagba and K.-T. Howell *The subspace structure of finite dimensional near-vector spaces*, Linear Multilinear Algebra **68** (2020), no. 11, 2316–2336.

[7] E. Ellers and H. Karzel, *Endliche Inzidenzgruppen*, Abhandl. Math. Seminar Hamburg **27** (1964), no. 3-4, 250–264.

[8] J.D.P. Meldrum, *Near Rings and Their Links with Groups*, volume 134 of Research Notes in Mathematics. Pitman (Advanced Publishing Program), Boston, MA, 1985.

[9] G. Pilz, *Near-Rings: The Theory and its Applications*, Elsevier, 2011.

[10] H. Wähling, Heinz, *Theorie der Fastkörper*, Thales Verlag, W. Germany, 1987.

[11] H. Zassenhaus, *Über endliche fastkörper*, Abhandl. Math. Seminar Univ. Hamburg **11** (1935), 187–220.