On the center of a finite Dickson nearfield

PRUDENCE DJAGBA

African Institute for Mathematical Sciences
South Africa
e-mail: prudence@aims.ac.za

Abstract: We study the center of a finite Dickson nearfield that arises from Dickson pair \((q, n)\).

Keywords: Center, Dickson nearfield

2010 MSC: 16Y30;12K05

1 Introduction

Nearfields were first studied by Dickson in 1905 and were applied immediately by mathematicians to geometry. Lacking one side distributive law makes the study of nearfields difficult despite they look a lot like fields. Zassenhaus [10], Dancs [3, 4], Karzel and Ellers [2] have solved some important problems in this area. Recently the author in [5] has investigated on the generalized distributive set of a finite nearfield.

In the paper [2], Eller and Karzel showed that the center of a finite Dickson that arises from Dickson pair \((q, n)\) is equal to a finite field of order \(q^n\). In the present work, we provide a simple and shortest proof of a result due to Eller and Karzel on the presentation of the center of a finite Dickson nearfield that arises from a Dickson pair \((q, n)\).

Let \(S\) be any group with identity 0. We will use \(S^*\) to denote \(S \setminus \{0\}\).

Definition 1.1. ([7]) Let \((R, +, \cdot)\) be a triple such that \((R, +)\) is a group, \((R, \cdot)\) is a semigroup, and \(a \cdot (b + c) = a \cdot b + a \cdot c\) for all \(a, b, c \in R\). Then \((R, +, \cdot)\) is a (left) nearring. If in addition \((R^*, \cdot)\) is a group then \((R, +, \cdot)\) is called a nearfield.

So a nearfield is an algebraic structure similar to a skewfield (sometimes called a division ring) except that it has only one of the two distributive laws. It is well known that the additive group of a (left) nearfield is abelian, see for instance [10 11]. Throughout this paper we will make use of (left) nearfields.

Furthermore, as we know from the definition of a (left) nearfield, we do not necessarily have the right distributivity law and commutativity of multiplication. For this reason, the following concepts have been defined and they will be used in the next chapters.

Definition 1.2. ([8]) Let \(R\) be a nearfield.

- The multiplicative center of \((R, \cdot)\) denoted by \(C(R)\), is defined as follows:

\[
C(R) = \{x \in R : x \cdot y = y \cdot x \text{ for all } y \in R\}.
\]

i.e., it is the set of elements of \(R\) that commute with every element of \(R\).
• We use $D(R)$ to denote the set of all distributive elements of $R$, also called the kernel of $(R, +, \cdot)$. It is defined as follows:

$$D(R) = \{ \lambda \in R : (\alpha + \beta) \cdot \lambda = \alpha \cdot \lambda + \beta \cdot \lambda \text{ for all } \alpha, \beta \in R \}.$$ 

To construct finite Dickson nearfields, we need two concepts: Dickson pair and coupling map.

**Definition 1.3.** (8) A pair of positive integers $(q, n)$ is called a Dickson pair if the following conditions are satisfied:

(i) $q$ is some power $p^l$ of some prime $p$,

(ii) each prime divisor of $n$ divides $q - 1$,

(iii) $q \equiv 3 \mod 4$ implies 4 does not divide $n$.

Let $(q, n)$ be a Dickson pair with $n \in \{1, \ldots, n\}$. We will denote the positive integer $\frac{q^k - 1}{q - 1}$ by $[k]_q$.

**Definition 1.4.** (8) Let $R$ be a nearfield and $\text{Aut}(R, +, \cdot)$ the set of all automorphisms of $R$. A map $\phi : R^* \rightarrow \text{Aut}(R, +, \cdot)$ defined by $a \mapsto \phi_a$ is called a coupling map if for all $a, b \in R^*$, $\phi_a \circ \phi_b = \phi_{\phi_a(b) \cdot a}$.

Every Dickson pair $(q, n)$ gives rise to a finite Dickson nearfield. This is obtained by replacing the usual multiplication “$\cdot$” in the finite field $F_{q^n}$ of order $q^n$ with a new multiplication “$\circ$”. We shall denote the set of Dickson nearfields arising from the Dickson pair $(q, n)$ by $DN(q, n)$ and the Dickson nearfield arising from the Dickson pair $(q, n)$ with generator $g$ by $DN_g(q, n)$. Furthermore in (8) the new multiplication is constructed as follows:

Let $g$ be such that $F_{q^n} = \langle g \rangle$ and $H = \langle g^n \rangle$. The quotient group is given by

$$F_{q^n}/H = \{ g^{[1]}H, g^{[2]}H, \ldots, g^{[n]}H \}$$

$$= \{ H, gh, \ldots, g^{n-1}H \}.$$ 

The coupling map $\phi$ is defined as

$$\begin{align*}
F_{q^n}^* &\rightarrow \text{Aut}(F_{q^n}, +, \cdot) \\
\alpha &\mapsto \phi_\alpha = \varphi^k(\alpha)
\end{align*}$$

where $\varphi$ is the Frobenius automorphism of $F_{q^n}$ and $k$ is a positive integer ($k \in \{1, \ldots, n\}$) such that $\alpha \in g_{[k]_q}H$. Let $\alpha, \beta \in F_{q^n}$, the we have

$$\alpha \circ \beta = \begin{cases}
\alpha \cdot \phi_\beta(\beta) & \text{if } \alpha \neq 0 \\
0 & \text{if } \alpha = 0
\end{cases}$$

$$= \begin{cases}
\alpha \cdot \varphi^k(\beta) & \text{if } \alpha \in g_{[k]_q}H \\
0 & \text{if } \alpha = 0
\end{cases}$$

$$= \begin{cases}
\alpha \cdot \beta^k & \text{if } \alpha \in g_{[k]_q}H \\
0 & \text{if } \alpha = 0
\end{cases}$$

for $k \in \{1, \ldots, n\}$. Thus $DN_g(q, n) := (F_{q^n}, +, \circ)$ is the finite Dickson nearfield constructed by taking $H = \langle g^n \rangle$. By taking all Dickson pairs, all finite Dickson nearfields arise in this way [1]. Furthermore we deduce the following.

**Lemma 1.5.** (8) Let $(q, n)$ be a Dickson pair with $q = p^l$ for some prime $p$ and positive integers $l, n$. Let $g$ be a generator of $F_{q^n}$ and $R$ the nearfield constructed with $H = \langle g^n \rangle$. Then $n$ divides $[n]_q$ and $g_{[n]_q}H = H$. 

2
2 Alternative proofs

In 1964 Ellers and Karzel showed that \( C(R) = D(R) \cong F_q \) where \( R \) is a finite Dickson nearfield that arises from the Dickson pair \((q,n)\). Note that \( C(R) \) denote the center and \( D(R) \) the set of all distributive elements of \( R \). In this section we give an alternative proof of the fact that \( C(R) = F_q \).

The following is well known.

**Theorem 2.1.** (\([6]\)) If \( K \subseteq F \) is a field extension (i.e., \( K \) is subfield of \( F \)), then \( F \) is a vector space over \( K \).

**Corollary 2.2.** (\([6]\)) If \( K \subseteq F \) is a field extension and \( F \) is finite, then \( |F| = |K|^n \) for some \( n \in \mathbb{R} \).

**Lemma 2.3.** (\([6]\)) A polynomial equation of degree \( n \) has at most \( n \) roots over any field.

Furthermore,

**Lemma 2.4.** (\([6]\)) The set of elements fixed by a field automorphism is a field.

**Lemma 2.5.** (\([6]\)) The subfields of \( F_{p^m} \) are precisely those \( F_{p^t} \) where \( t \mid m \) and they are unique. Furthermore, they are the fields fixed by the automorphism \( \psi^t : x \mapsto x^{p^t} \).

We now deduce the following:

**Theorem 2.6.** Let \((q,n)\) be a Dickson pair with \( q = p^l \) for some prime \( p \) and positive integers \( l, n \). Let \( g \) be a generator of \( F_{q^n}^* \) and \( R \) the finite nearfield constructed with \( H = \langle g^n \rangle \). Let \( F_q \) be the unique subfield of order \( q \) of \( F_{q^n} \). Then

\[
F_q \subseteq C(R).
\]

**Proof.** By Lemma 2.5, \( F_q \) is the solution set to the equation \( x^q - x = 0 \) in \( F_{q^n} \). Let \( g \) be a generator of \( F_{q^n}^* \) and take \( x \in F_q^* \) and write \( x = g^t \). Since \( x \in F_q \), \( x^q = x \), i.e., \( x^{q-1} = 1 \). Then \( (g^t)^{q-1} = 1 \), i.e., \( g^{l(q-1)} = 1 \). Thus \( |g| = q^n - 1 \) divides \( l(q-1) \), i.e., \( [n]_q \mid l \). Thus \( F_q^* = \langle g^{[n]_q} \rangle \). Since \( n \mid [n]_q \) then \( \langle g^{[n]_q} \rangle \) is a subset of \( \langle g^n \rangle \). Thus we have \( F_q^* \subseteq H \). Furthermore for \( x \in F_q^* \), \( x \in H = g^{[n]_q}H \). By the Dickson construction, \( \phi_x(y) = \varphi^n(y) = y^{q^n} = y \), hence \( \phi_x = id \). Take any \( t \in R \). We have

\[
x \circ t = x \cdot \phi_x(t) = x \cdot t.
\]

Moreover, since \( x \in F_q \) then \( \varphi(x) = x^q = x \). Thus \( \varphi^t(x) = x \) and

\[
t \circ x = t \cdot \phi_t(x) = t \cdot \varphi^t(x) = t \cdot x = x \cdot t.
\]

Therefore \( t \circ x = x \circ t \) for all \( t \in R \). So \( x \in C(R) \).

In fact, it is well known in field theory that:

**Theorem 2.7.** (\([6]\)) Let \( F \) be a finite field of order \( p^n \) with characteristic \( p \) where \( p \) is prime. We have \( (a+b)^{p^n} = a^{p^n} + b^{p^n} \) for all \( a, b \in F \) and \( m \in \mathbb{N} \).
We have the following.

**Lemma 2.8.** Let \((q,n)\) be a Dickson pair with \(q = p^l\) for some prime \(p\) and positive integers \(l,n\). Let \(g\) be a generator of \(\mathbb{F}_{q^n}^{\ast}\). Then \(\mathbb{F}_p\langle g^n \rangle = \mathbb{F}_{q^n}\) where \(\mathbb{F}_p\) is the unique subfield of \(\mathbb{F}_{q^n}\) of order \(p\).

**Proof.** Let \(f\) be the smallest positive integer such that \((g^n)^{p^f} = g^n\). Then \(g^n\) is a solution to the equation \(x^{p^f} - x = 0\). In fact every \(x\) in \(\mathbb{F}_p\langle g^n \rangle\) satisfies \(x^{p^f} - x = 0\).

We have \(x = \sum_{i \in I} a_i g^{nb_i}\), where \(a_i \in \mathbb{F}_p\) and \(b_i \in \mathbb{Z}\). Then

\[
x^{p^f} = \left( \sum_{i \in I} a_i g^{nb_i} \right)^{p^f} = \sum_{i \in I} (a_i g^{nb_i})^{p^f} \quad \text{by Theorem 2.7}
\]

\[
= \sum_{i \in I} a_i^{p^f} \left( (g^n)^{p^f} \right)^{b_i} = \sum_{i \in I} a_i g^{nb_i}
\]

\[
= x.
\]

Thus \(\mathbb{F}_p\langle g^n \rangle \subseteq \mathbb{F}_{p^f}\). But note that since \(f\) is minimal, \(\mathbb{F}_p\langle g^n \rangle = \mathbb{F}_{p^f}\).

Furthermore, since \((g^n)^{p^f} = g^n\), we have,

\[
(g^n)^{p^f - 1} = 1 \iff g^{n(p^f - 1)} = 1,
\]

hence

\[
|g| = q^n - 1 = p^{ln} - 1 \mid n(p^f - 1).
\]

Since \(\mathbb{F}_p\langle g^n \rangle = \mathbb{F}_{p^f} \subseteq \mathbb{F}_{p^n}\), \(f \mid ln\). Suppose that \(f \neq ln\), then \(f \leq \frac{ln}{2}\) and

\[
p^{ln} - 1 \mid n(p^f - 1) \Rightarrow p^{ln} - 1 \leq n(p^f - 1) \leq n(p^{ln} - 1).
\]

Dividing by \(p^{ln} - 1\), we get

\[
p^{ln} + 1 \leq n,
\]

but

\[
p^{ln} + 1 \geq 2^{\frac{ln}{2}} + 1 \geq 2^{\frac{n}{2}} + 1 > n.
\]

This leads to a contradiction. Thus \(f = ln\), so \(\mathbb{F}_p\langle g^n \rangle = \mathbb{F}_{q^n}\). \(\square\)

**Theorem 2.9.** Let \((q,n)\) be a Dickson pair with \(q = p^l\) for some prime \(p\) and positive integers \(l,n\). Let \(g\) be a generator of \(\mathbb{F}_{q^n}^{\ast}\) and \(R\) the finite nearfield constructed with \(H = \langle g^n \rangle\). Let \(\mathbb{F}_q\) be the unique subfield of order \(q\) of \(\mathbb{F}_{q^n}\). Then

\[
C(R) \subseteq \mathbb{F}_q.
\]
Proof. Take $x \in C(R)$. Then $x \circ t = t \circ x$ for all $t \in R$. Let $t = g^n \in H$. Then

$$t \circ x = t \cdot \phi_t(x) = g^n \cdot \phi_{g^n}(x) = g^n \cdot x \text{ since } \phi_{g^n} = id.$$ 

Also

$$x \circ t = x \cdot \phi_x(t) = x \cdot \phi_x(g^n).$$

Since $x \circ t = t \circ x$, $g^n \cdot x = x \cdot \phi_x(g^n)$. Hence $\phi_x(g^n) = g^n$. Furthermore, since $\mathbb{F}_p$ is fixed by $\psi$, the Frobenius map, $\phi_x$ fixes $\mathbb{F}_p$. Therefore $\phi_x$ fixes $\mathbb{F}_p(g^n)$, the smallest subfield of $\mathbb{F}_{q^n}$ that contains $\mathbb{F}_p$ and $g^n$. By Lemma 2.8, $\phi_x = id$. Now take $t = g \in g^{[1]} \cap H$, So $\phi_t = \phi_g = \varphi = \psi^l$. Then

$$t \circ x = g \circ x = g \cdot \phi_g(x) = g \cdot \varphi(x).$$

Also,

$$x \circ t = x \cdot \phi_x(t) = x \cdot t = x \cdot g.$$ 

Thus $t \circ x = x \circ t \iff g \cdot \varphi(x) = x \cdot g \iff \varphi(x) = x \iff x^q = x$. So $x \in \mathbb{F}_q$. \qed

3 Concluding comments

By Theorem 2.6 and Theorem 2.9, we have shown that $C(R) = \mathbb{F}_q$ where $R \in DN(q,n)$. An interesting research line is to characterize all the automorphism of a finite Dickson nearfield.

References

[1] Dickson Leonard Eugene, On finite algebras Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, 358-393, 1905.

[2] Erich Ellers und Helmut Karzel, Endliche Inzidenzgruppen, Abhandl.Math.Seminar Hamburg 27 (1964): 250-264.

[3] Susan Dancs, The sub-near-field structure of finite near-fields, Bulletin of the Australian Mathematical Society 5.2 (1971): 275-280.

[4] Susan Dancs, On finite Dickson near-field, Abhandl.Math.Seminar Hamburg 37 (1972): 254-257.

[5] Prudence Djagba, On the generalized distributive set of a finite nearfield, Journal of Algebra, accepted to appear 2019.

[6] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge university press, 1994.

[7] Meldrum, John DP, Near rings and their links with groups, Number 134, Pitman Advanced Publishing Program, 1985.
[8] Pilz Gunter, Near-rings: the theory and its applications, volumes 23. Elsevier, 2011.

[9] Wähling, Heinz, Theorie der Fastkörper, Thales Verlag, volume 1, 1987.

[10] H. Zassenhaus, über endliche fastkörper. In Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, volume 11, pages 187–220. Springer, 1935.