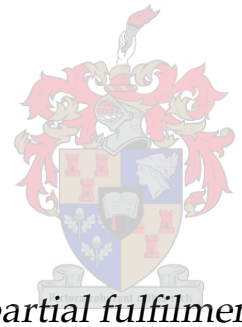
Contributions to the Theory of Beidleman Near-Vector Spaces

by

Prudence Djagba



Thesis presented in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Mathematics in the Faculty of Science at Stellenbosch University

Supervisors: Dr Karin-Therese Howell and Dr Gareth Boxall

December 2019

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: December 2019 .....

Abstract

Contributions to the Theory of Beidleman Near-Vector Spaces

Prudence Djagba

Department of Mathematical Sciences,
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.

Thesis: PhD

December 2019

==========

The study of nearfields was started in 1905 by L.E. Dickson. This thesis is a first step toward a detailed study of J.C. Beidleman near-vector spaces, as first introduced by Beidleman in 1966. Recalling well-known results, we conduct a detailed study of finite nearfields by showing how to construct a finite Dickson nearfield and presenting the center of a finite Dickson nearfield that arises from the Dickson pair (q, n). Furthermore, as main results of this thesis, we present the following. We characterise the finite dimensional Beidleman near-vector spaces. We develop an algorithm called *EGE (Expanded Gaussian Elimination)* which determines the smallest R-subgroup containing a given finite set of vectors $v_1, \ldots, v_k \in R^m$ where R is a proper nearfield and k, m are positive integers, defined as $gen(v_1, \ldots, v_k)$. We also classify all the subspaces of R^m by designing an algorithm called the *Adjustment of the EGE algorithm*. We study the concept of *seed number* of an R-subgroup T (i.e., the minimal cardinality of all the possible finite sets of vectors that generate T) and *R-dimension* of $gen(v_1, \ldots, v_k)$ (i.e., the number of vectors obtained after the implementation of *the EGE algorithm* on the finite set of vectors $v_1, \ldots, v_k$). We evaluate the seed number

of R^m for some positive integer m satisfying $m \leq |R| + 1$. Furthermore from the *EGE algorithm* we also study, for a given pair (α, β) in R^2, the *generalized distributive set* defined as $D(\alpha, \beta) = \{\lambda \in R : (\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda\}$, where " $\circ$ " is the multiplication of the nearfield. We find that in contrast to the situation of $D(R) = \{\lambda \in R : (\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda \text{ for all } \alpha, \beta \in R\}$ from the work of Zemmer in 1964, *the generalized distributive set* $D(\alpha, \beta)$ is not always a subnearfield of R where R is a finite Dickson nearfield arising from the Dickson pair (q, n). We find a sufficient condition on α and β such that $D(\alpha, \beta)$ is a subfield of the finite field of order q^n and develop an algorithm that tests whether $D(\alpha, \beta)$ is a subfield of $\mathbb{F}_{q^n}$ or not. We then investigate $D(\alpha, \beta)$ where α, β and $\alpha + \beta$ are all in distinct $g^{\frac{q^i-1}{q-1}}H$ (where g is a generator of $\mathbb{F}_{q^n}^*$ and H is the subgroup generated by g^n) and we obtain a construction of a subfield of $\mathbb{F}_{q^n}$ by making use of $D(\alpha, \beta)$.

Acknowledgements

Firstly, I would like to convey my deepest gratitude to my supervisors, Dr Gareth Boxall and Dr Karin-Therese Howell, for not only playing a decisive role in getting me accepted at the institution but also for the immeasurable support they have extended to me. Their deep and penetrating knowledge of mathematics as well as their patience and understanding throughout these professionally and personally turbulent years in reading and correcting my writing.

Secondly I thank Prof Amador Martin-Pizarro for accepting me at Freiburg University for a few months of research visit in Germany.

Thirdly I would like to express my sincere gratitude to Georg Anegg (who was initially my tutor during my AIMS program) for his technical support and toward the work within this project. I am glad to have been communicating mathematics with him.

The financial assistance of the DAAD (Deutscher Akademischer Austausch Dienst) scholarship and AIMS-SA (African Institute for Mathematical Sciences South Africa) toward this research are hereby acknowledged. This work is based on the research supported in part by the National Research Foundation of South Africa (grant numbers: 93050, 96234).

I thank CIMPA for giving me the opportunities for attending some research schools in number theory at Wits University and topics in ring theory at AIMS-South Africa.

I thank Dr Dirk Basson (Mathematics Division at Stellenbosch University) for some fruitful conversations. I thank Dr Tim Boykett, Prof Gunter Pilz

and Prof Erhard Aichinger for having me at Kepler University (Institute for Algebra, at Linz (Austria)) for some research interactions and during AAA 98 conference. I am also grateful to Prof Johannes Meyer (Free State University, South Africa) for his fruitful discussions whenever I needed him, and to have met him during AAA 98 conference at Dresden (Germany).

I thank Dr Audace Dossou-Olory for his friendship and words of encouragement that enabled me to see this journey through. I thank my spiritual father Dr David Oyedepo for his guidance throughout his ministration of the Word of Faith. I am blessed to be a member of Winner chapel. Most importantly, the divine support from my Lord and Savior Jesus-Christ is hereby acknowledged.

Dedications

To my lovely parents «Djagba Firmin» and «Kinhou Marcelline».

Contents

List of Tables

Nomenclature

Symbols and Definitions

$\mathbb{N}$ the set of positive integers.

$\mathbb{Z}$ the set of integers.

$\mathbb{R}$ the set of real numbers.

$(\mathbb{H}, +, \cdot)$ the skewfield of real quaternions.

$(R, +, \circ)$ a (left) nearfield, also called nearfield with the addition $+$ and the multiplication $\circ$.

M_R a (right) nearring module where $(M, +)$ is a group and R a nearfield.

$M_R \cong N_R$ the nearring modules M_R and N_R are R-isomorphic.

$R^{k\times m}$ the set of all $k \times m$ matrices with entries in R.

R^m the set of all vectors of size m with entries in R.

S^* the set $S \setminus \{0\}$ where S is any set containing "zero element" 0.

$|S|$ the number of elements that the set S contains.

G/H the set of left cosets of H in G where G is a group with subgroup H.

$|x|$ the order of x in the group G.

$DN(q, n)$ the set of Dickson nearfields arising from the Dickson pair (q, n).

$DN_g(q, n)$ the Dickson nearfield arising from the Dickson pair (q, n) with generator g.

$D(\alpha, \beta)$ the generalized distributive set of R for a given pair $(\alpha, \beta) \in R^2$.

$D(R)$ the set of distributive elements in R.

$C(R)$ the center of the multiplicative group $(R, \circ)$ where $(R, +, \circ)$ is a nearfield.

$\mathbb{F}_{q^n}$ the finite field with order q^n.

$gen(v_1, \ldots, v_k)$ the smallest R-subgroup containing $v_1, \cdots, v_k$.

EGE the Expanded Gaussian Elimination algorithm.

$AEGE$ Adjustment of the Expanded Gaussian Elimination algorithm.

DSS the Distributive Set Subfields algorithm.

$s(R^m)$ the seed number of R^m where m is a positive integer.

$R\text{-}dim(T)$ the R-dimension of an R-subgroup T.

$RREF(M)$ the Reduced Row Echelon Form of the matrix M.

$G_{q,n}$ the multiplicative group of a finite Dickson nearfield that arises from a Dickson pair (q, n).

$I(v_1, \ldots, v_k)$ the index of R-linearity of $v_1, \ldots, v_k$.

$S(G)$ the set of all mappings from $(G, +)$ to $(G, +)$, also called nearring mappings.

id the identity map.

$\mathbb{F}_{q^n}\langle x \rangle$ the field generated by x over the finite field $\mathbb{F}_{q^n}$.

$a \equiv b \mod m$ the integer a is congruent to b modulo m, i.e. $a - b$ is a multiple of m.

$\text{GCD}(a, b)$ the Greatest Common Divisor of the two integers a and b.

$\text{LCM}(a, b)$ the Least Common Multiple of the two integers a and b.

Chapter 1

Introduction

Given a near-vector space of the form R^m where R is a nearfield and m a positive integer, what can be said about its subspaces? The question becomes substantially more interesting when one considers different notions of near-vector spaces. In providing an answer to this question, the set of distributive elements of R comes to play an useful role. What can be said about them?

1.1 Objectives

The first notion of near-vector spaces was introduced by J.C. Beidleman. Later J. André introduced a similar notion in a different way. André's version has been studied in many recent papers while Beidleman near-vector spaces have not been investigated by other researchers since Beidleman's thesis. The present thesis will fill this gap, developing the theory of Beidleman near-vector spaces. There are also interesting questions related to finite Dickson nearfields involved. We shall conduct a detailed study of Beidleman near-vector spaces and finite Dickson nearfields. Specifically, we will focus on finite dimensional Beidleman near-vector spaces by classifying their R-subgroups (i.e., their subgroups which are closed under scalar multiplication), their subspaces and also determining their seed number (i.e., the minimal cardinality of all the possible finite sets of vectors that generate the whole space). We will also solve various problems arising from the distributive elements of finite Dickson nearfields.

1.2 An overview of prior work

Some years ago, interest emerged in algebraic structures with binary operations "addition" and "multiplication" satisfying all the ring axioms except one of the distributive laws and the commutativity of addition. Such structures are called "nearrings". Nearrings provide non-linear generalisation of rings. In 1905 J.E. Dickson [10] wanted to know what structure arose if one axiom in the list of axioms for skewfields was weakened. He defined such structures to be "nearfields". J.E. Dickson achieved this by starting with a field and distorting the multiplication [10]. Some years later, these nearfields showed up again and proved to be useful in coordinatising certain important classes of geometric planes. Thirty years after Dickson's discovery, H. Zassenhauss classified all the finite nearfields in [30] and showing that finite nearfields are either finite Dickson nearfields or one of the seven exceptional ones. Nearfields are useful in geometry. If one wants to represent points in an incidence geometry as pairs of "numbers in a structure S" and the (non-vertical) lines by the usual equation $y = ax + b$, one clearly needs an addition and a multiplication in S. O. Veblen and J. Maclagan-Wedderburn found out that for this "coordinisation" of important geometric planes S has to be exactly a nearfield, see [28] for more details. A more recent application of nearfields is in the construction of ciphers for data-encryption such as Hill ciphers, see [14] for more details. Also S. Dancs [8, 9], H. Karzel and E. Ellers [13] have solved some important problems in the structure of nearfields. S. Dancs found that the subnearfield structure of finite nearfields is analogous to the subfield structure of finite fields. There are many known results for finite Dickson nearfields, such as that they always have their centers equal to the set of distributive elements, which is always a subfield, proved by H. Karzel and E. Ellers [13].

For nearrings, commutativity of addition is not required but in nearfields, it is a consequence of the remaining axioms, as proved in different ways by J.E. Dickson [10], H. Zassenhaus[30], B.H. Neuman [25] and J. Zemmer [32]. The main examples of nearrings are the ones of the type $S(G) := \{f : G \to G\}$ consisting of all functions from an additive group G to itself with point-wise addition "$+$" and composition "$\circ$". It has been shown by J. Malone and H. Heatherly in 1969 that every nearring can be embedded in some

$S(G)$ i.e., every nearring can be considered as a subnearring of a nearring of the form $S(G)$ [23]. In 1999 J.A. Beachy [4] showed that every ring can be embedded in the endomorphism ring of an abelian group, with the same operations as in $S(G)$. We can describe rings as systems of "linear" functions on groups, while nearrings as "non-linear" systems. For computations in the area of nearrings, an excellent software "Sonata" was developed by E. Aichinger based on GAP [1]. In 2004 Aichinger, jointly with M. Farag in [2], showed that the multiplicative center of a nearring is not always a subnearring. Later the authors in [7] introduced the concept of generalized center and have shown that for certain classes of nearrings, the center $C(R)$ is a subnearring of R if and only if the generalized center of R is the center of R.

The literature contains diverse concepts of near-vertor spaces. The first notion of near-vector spaces was defined by J. Beidleman in 1966 [5] where he contributed to the theory of nearring modules and especially to near-vector spaces. Subsequently, several researchers like H. W*ä*hling [29], J. André [3] and H. Karzel introduced a similar notion in different ways. André near-vector spaces have been studied by many researchers including J. Meyer, A. van der Walt, K-T Howell, T. Boykett, S. Sanon. In 1992 van der Walt [27] characterised the finite dimensional André near-vector spaces. According to his theorem we can specify a finite dimensional André near-vector space by taking m copies of a (right) nearfield R for which there are semigroup isomorphisms $\phi_i : (R, \cdot) \to (R, \cdot)$, where $i \in \{1, \ldots, m\}$. Then we take R^m, with m a positive integer, as the additive group of the André near-vector space and define

$$(x_1, \ldots, x_m)\alpha := (x_1\phi_1(\alpha), \ldots, x_m\phi_m(\alpha)),$$

for all $\alpha \in R$. In 2008 K-T Howell [16] gave an exposition and expanded the theory of André near-vector spaces in her PhD thesis. Appealing to the result of van der Walt [27], K-T Howell and J. Meyer [18] determined the finite dimensional André near-vector spaces over finite fields $\mathbb{F}_{p^n}$. From [18], given a sequence of integers $q_1, q_2, \ldots, q_m$ satisfying $1 \leq q_j \leq p^n - 1$ and $\text{GCD}(q_j, p^n - 1) = 1$ for $j \in \{1, \ldots, m\}$, R^m is an André near-vector space with the scalar multiplication

$$(x_1, x_2, \ldots, x_m)\alpha = (x_1\alpha^{q_1}, x_2\alpha^{q_2}, \ldots, x_m\alpha^{q_m})$$

for $\alpha \in \mathbb{F}_{p^n}$ and $(x_1, x_2, \ldots, x_m) \in \mathbb{F}_{p^n}^m$. In 2015 K-T Howell investigated the subspaces of André near-vector spaces of the form R^m [17]. She found the following. If we consider the sequence of integers $(q_1, q_2, \ldots, q_m) = (1, \ldots, 1)$ then $\phi_i(\alpha) = \alpha$ for all $i \in \{1, \ldots, m\}$. Furthermore, for some fixed distributive elements d_{ji} of R where $1 \leq i, j \leq k$, all the subspaces of R^m of dimension k, are of the form

$$\{(x_1, \ldots, x_k, \sum_{i=1}^{k} d_{1i}x_i, \sum_{i=1}^{k} d_{2i}x_i, \ldots, \sum_{i=1}^{k} d_{(m-k)i}x_i) : x_i \in R\}.$$

1.3 Layout of the thesis

The outline of the dissertation may be sketched as follows. In Chapter 2 we give preliminary material. It is a collection of basic definitions, notations and results that will be useful in the remaining chapters. We also characterize finite dimensional Beidleman near-vector spaces. In Chapter 3 we study finite Dickson nearfields.

In Chapter 4 we add to the theory of near-vector spaces originally defined by Beidleman. As in [17] for André near-vector spaces, we investigate some properties of the substructures of Beidleman near-vector spaces. We also highlight differences and similarities between these two types of near-vector spaces. Let R be a (left) nearfield. We characterize and classify the smallest R-subgroup (see Definition 2.2.8) containing a given set of vectors $v_1, \ldots, v_k$ of the near-vector space R^m where m is a positive integer, defined as $gen(v_1, \ldots, v_k)$. We provide an algorithm in Sage for computations which is called *EGE* (Expanded Gaussian Elimination). We also classify all the subspaces of R^m. The main contribution of this Chapter can be summarized as follows.

Theorem A. *Let $v_1, v_2, \ldots, v_k \in R^m$.*

(i) Suppose R is a proper nearfield. Then $gen(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} u_i R$, where the u_i (obtained from the v_j's by an explicit procedure) for $i \in \{1, \ldots, k'\}$ are the rows of a matrix $U = (u_i^j) \in R^{k' \times m}$ each of whose columns has at most one non-zero entry.

(ii) Suppose R is a proper nearfield. The subspaces of R^m are all of the form $S_1 \times S_2 \times \ldots \times S_m$ where $S_i = \{0\}$ or $S_i = R$ for $i = 1, \ldots, m$.

(iii) Suppose R is a proper finite nearfield. If $m \leq |R| + 1$ then there exist v and w in R^m such that $gen(v, w) = R^m$.

Within the application of *EGE* some non-distributive elements must be chosen for the determination of R-subgroups of R^m.

In Chapter 5, we introduce the generalized distributive set $D(\alpha, \beta)$ i.e., the set of elements in R that distribute over a given pair (α, β) in R^2. We study its properties for the case where R is a finite Dickson nearfield that arises from a Dickson pair (see Definition 3.2.11). The main contribution of this Chapter can be summarized as follows.

Theorem B. *Given (q, n) a Dickson pair with $q = p^l$ for some prime p and positive integers l, n, let us consider g to be a generator of $\mathbb{F}_{q^n}^*$ and R to be the finite nearfield constructed with $H = \langle g^n \rangle$ and $\alpha, \beta \in R^*$. Then $D(\alpha, \beta)$ is an $\mathbb{F}$-vector space for some finite field $\mathbb{F}$. Furthermore, $D(\alpha, \beta)$ is not always a subfield of $\mathbb{F}_{q^n}$.*

In contrast to the existing work by Zemmer, we find that the generalized distributive set is not always a subnearfield of a finite Dickson nearfield. Furthermore we find a sufficient condition on α, β for $D(\alpha, \beta)$ to be a subfield of $\mathbb{F}_{q^n}$. We also look at $D(\alpha, \beta)$ where α, β and $\alpha + \beta$ are all in distinct H-cosets (see Definition 5.2.5) and we obtain a construction of a subfield of $\mathbb{F}_{q^n}$ by making use of $D(\alpha, \beta)$.

The main contributions of this thesis are presented in Chapters 4 and 5. However some detailed proofs for some existing results are given in Chapter 3. This dissertation includes some materials of two original papers: see [12] (*accepted for publication in Linear and Multilinear Algebra*) and [11] (*submitted for publication in Journal of Algebra*). The work also emphasizes future directions of research on the present topic. These suggestions are incorporated throughout, in chapters.

Chapter 2

Terminology and preliminary material

2.1 Introduction

The purpose of this chapter is to fix the main vocabulary and introduce the preliminary material needed for this thesis. Furthermore, we give the formal definitions of nearrings, nearfields and nearring modules. We also define and provide some basic results on Beidleman near vector spaces. It is well known (see [16] and [5]) that every field or nearfield over itself are the simplest examples of near-vector spaces (both André and Beidleman version). In the last section we will construct some further examples of Beidleman near-vector spaces (see Theorem 2.5.2). New terms will be defined in later chapters when they are needed. Later we will use Theorem 2.5.2 to classify R-subgroups and subspaces of finite dimensional Beidleman near-vector spaces.

2.2 Basic definitions and results

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

Definition 2.2.1. *([24]) A (left) nearring is a set R together with two binary operations $+$ (addition) and $\cdot$ (multiplication) satisfying the following axioms :*

(i) $(R, +)$ *is a group with the identity* 0,

(ii) $(R, \cdot)$ *is a semi-group i.e.,* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all elements* $a, b, c \in R$ *(the associative law for multiplication),*

(iii) $a(b + c) = ab + ac$ *for all elements* $a, b, c \in R$ *(the left distributive law).*

Let R be a nearring. So for all $r \in R$ we have $r0 = 0$. Furthermore, it is not true in general that $0r = 0$ for all $r \in R$. Define $R_0 = \{r \in R : 0r = 0\}$ to be the zero-symmetric part of R. A nearring is called zero-symmetric if $R = R_0$ i.e., $0r = r0 = 0$ for all $r \in R$. A nearfield is an algebraic structure similar to a skew-field (division ring) except that it has only one of the two distributive laws.

Definition 2.2.2. *([26]) Let R be a (left) nearring. If $(R^*, \cdot)$ is a group then $(R, +, \cdot)$ is called a (left) nearfield.*

Definition 2.2.3. *A proper nearfield is a nearfield that is not a field.*

We will make use of left nearfields and right nearring modules throughout the thesis. J.E. Dickson [10], H. Zassenhauss [30], B.H. Neumann [25], H. Karzel [13] and J. Zemmer [32] have shown by different methods that the additive group of a nearfield is abelian. We will look at Dickson's proof in the next chapter for this.

Theorem 2.2.4. *([10, 26]) The additive group of a nearfield is abelian.*

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

Definition 2.2.5. *([26]) 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:*

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

Remark 2.2.6. *Clearly $C(R) \subseteq D(R)$. To see this, let $x \in C(R)$ and $y, z \in R$. Then*

$$\begin{aligned} x \cdot (y+z) &= x \cdot y + x \cdot z \\ &= y \cdot x + z \cdot x. \end{aligned}$$

But $x \cdot (y+z) = (y+z) \cdot x$. So $(y+z) \cdot x = y \cdot x + z \cdot x$. Thus $x \in D(R)$.

The concept of a ring module can be extended to a more general concept called a nearring module where the set of scalars is taken to be a nearring. From now on we will always choose a nearring R to be zero-symmetric.

Definition 2.2.7. *([24]) An additive group $(M, +)$ is called a (right) nearring module over a (left) nearring R if there exists a mapping,*

$$\begin{aligned} \eta : M \times R &\to M \\ (m, r) &\to mr \end{aligned}$$

such that $m(r_1 + r_2) = mr_1 + mr_2$ and $m(r_1 r_2) = (mr_1)r_2$ for all $r_1, r_2 \in R$ and $m \in M$.

We write M_R to denote that M is a (right) nearring module over a (left) nearring R. Note that the additive group $(M, +)$ need not be abelian.

Definition 2.2.8. *([5]) A subset H of a nearring module M_R is called an R-subgroup if:*

(i) H is a subgroup of $(M, +)$,

(ii) $HR = \{hr : h \in H, r \in R\} \subseteq H$.

Definition 2.2.9. *([5]) A nearring module M_R is said to be irreducible if M_R contains no proper R-subgroups. In other words, the only R-subgroups of M_R are M_R and $\{0\}$.*

Definition 2.2.10. *([5]) A nearring module M_R is said to be unitary if R contains an identity "1" and $m \cdot 1 = m$ for all $m \in M$.*

Corollary 2.2.11. *([5]) Let M_R be a unitary nearring module. Then M_R is irreducible if and only if $mR = M_R$ for every non-zero element $m \in M$.*

Definition 2.2.12. *([5]) Let M_R be a nearring module. A subset H of M_R is called a submodule of M_R if:*

(i) $(H,+)$ *is a normal subgroup of* $(M,+)$,

(ii) $(m+h)r - mr \in H$ *for all* $m \in M, h \in H$ *and* $r \in R$.

Proposition 2.2.13. *([5]) Let R be a zero-symmetric nearring and H be a submodule of M_R. Then H is an R-subgroup of M_R.*

Note that the converse of this proposition is not true in general. In his thesis ([5], page 14) Beidleman gives a counter example. However,

Lemma 2.2.14. *If M_R is a ring module, then the notions of R-subgroup and submodule of M_R coincide.*

Proof. By Proposition 2.2.13, every submodule is an R-subgroup. Let H be an R-subgroup of M_R. Then $hr \in H$ for all $h \in H$ and $r \in R$. But $hr = (m+h)r - mr$ for all $m \in M$. Noting that H is normal because $(M,+)$ is abelian. Hence H is a submodule of M_R. □

Theorem 2.2.15. *([5]) Let R be a nearring that contains the identity element $1 \neq 0$. We have, R is a nearfield if and only if R (considered as a nearring module over itself) contains no proper R-subgroups.*

2.3 Internal direct sum of submodules

In the following, let $\{M_i\}_{i\in I}$ be a collection of submodules of the nearring module M_R.

Definition 2.3.1. *Let $m \in M_R$. We will say that m is called a sum of elements of the submodules M_i if there exists $m_i \in M_i$ such that $m = \sum_{i\in I} m_i$, where $m_i \neq 0$ for at most finitely many i. In this case we write $M_R = \sum_{i\in I} M_i$.*

Definition 2.3.2. *([5]) The nearring module M_R is said to be a direct sum of the submodules M_i, for $i \in I$, if the additive group $(M,+)$ is a direct sum of the normal subgroups $(M_i,+)$, i.e., if every $m \in M$ is a sum of the elements of the submodules M_i, for $i \in I$. In this case we write $M_R = \bigoplus_{i\in I} M_i$.*

We have that

Proposition 2.3.3. *([5]) Suppose that $M_R = \bigoplus_{i\in I} M_i$. Then $M_R = \sum_{i\in I} M_i$ and $m_i + m_j = m_j + m_i$ for all $m_i \in M_i$ and $m_j \in M_j$ such that $i \neq j$.*

Proof. Assume that $M_R = \bigoplus_{i\in I} M_i$ where $\{M_i : i \in I\}$ are normal subgroups of M_R. Let $m_i \in M_i$ and $m_j \in M_j$ such that $i \neq j$. Indeed $m_i + m_j - m_i - m_j \in M_i$ since $m_j - m_i - m_j \in M_i$ since $(M_i, +)$ is a normal subgroup of $(M, +)$. Also $m_i + m_j - m_i - m_j \in M_j$ since $m_i + m_j - m_i \in M_j$. It follows that $m_i + m_j - m_i - m_j \in M_i \cap M_j \subseteq M_j \cap \sum_{i\in I, i\neq j} M_i = \{0\}$. But $M_i \cap M_j \neq \emptyset$ since $0 \in M_i \cap M_j$, so $M_i \cap M_j = \{0\}$. It follows that $m_i + m_j - m_i - m_j \in M_i \cap M_j = \{0\}$. Hence $m_i + m_j = m_j + m_i$. □

According to the definition of a nearring module, we do not have distributivity of elements in R over the elements of M. If we consider M_R as direct sum of the collection of submodules $\{M_i\}_{i\in I}$ of the nearring module M_R, then the following result will allow us to distribute the elements of R over elements which are contained in distinct submodules in the direct sum. The result is useful in the concept of Beidleman near-vector spaces.

Lemma 2.3.4. *([5]) Let $M_R = \bigoplus_{i\in I} M_i$ where each M_i is a submodule of M_R. If $m = \sum_{i\in I} m_i$ where $m_i \in M_i$ and $r \in R$ then*

$$mr = (\sum_{i\in I} m_i)r = \sum_{i\in I}(m_i r).$$

Proof. Suppose $I = \{1, \ldots, n\}$ where $n \in \mathbb{N}$. We proceed by induction on n. For $n = 2$, let $M_R = M_1 \oplus M_2$. So $M_R = M_1 + M_2$ and $M_1 \cap M_2 = \{0\}$ where M_1 and M_2 are submodules of M. Let $m \in M_R$. Then $m = m_1 + m_2$ for $m_1 \in M_1$ and $m_2 \in M_2$. We need to show that $mr = (m_1 + m_2)r = m_1 r + m_2 r$. It suffices to show that

$$(m_1 + m_2)r - m_1 r - m_2 r \in M_1 \cap M_2.$$

Since M_2 is submodule of M, $(m_1 + m_2)r - m_1 r \in M_2$. Then $(m_1 + m_2)r - m_1 r - m_2 r \in M_2$. Also we have $(m_2 + m_1)r - m_2 r \in M_1$. So $(m_2 + m_1)r - m_2 r - m_1 r \in M_1$. Thus by Proposition 2.3.3,

$$(m_2 + m_1)r - m_2 r - m_1 r \in M_1 \cap M_2 = \{0\}.$$

Assume that if $m = \sum_{i=1}^{n-1} m_i$ where $m_i \in M_i$, then $mr = (\sum_{i=1}^{n-1} m_i)r = \sum_{i=1}^{n-1}(m_i r)$. Let $m \in M_R$, $r \in R$ and suppose $m = m_1 + \ldots + m_n$ where $m_i \in M_i$. We have, by Proposition 2.3.3,

$$(m_1 + \ldots + m_n)r - m_1 r - m_2 r - \ldots - m_n r =$$
$$(m_2 + \ldots + m_n + m_1)r - (m_2 + m_3 + \ldots + m_n)r - m_1 r \in M_1.$$

Also,

$$(m_1 + m_3 + \ldots + m_n + m_2)r - (m_1 + m_3 + \ldots + m_n)r - m_2r \in M_2.$$

By the same process, we also have

$$(m_1 + m_2 + \ldots + m_{n-1} + m_n)r - (m_1 + m_2 + \ldots + m_{n-1})r - m_nr \in M_n.$$

It follows that,

$$(m_1 + \ldots + m_n)r - m_1r - m_2r - \ldots - m_nr \in \bigcap_{j=1}^{n} M_j \subseteq M_1 \cap \sum_{j=2}^{n} M_j = \{0\}.$$

Thus,

$$mr = (\sum_{i=1}^{n} m_i)r = \sum_{i=1}^{n}(m_ir).$$

Furthermore, if I is infinite then we will consider all except finitely many of the m_i's to be zero. □

Lemma 2.3.5. *([5]) Let M_R be a unitary nearring module over the nearfield R. If $m \neq 0$ then $mr = 0$ implies that $r = 0$.*

Proof. If $mr = 0$ and $r \neq 0$ then $0 = 0r^{-1} = (mr)r^{-1} = m(rr^{-1}) = m1 = m$. □

Suppose that R is field, then an R-vector space is a ring module. Furthermore, we deduce the following result.

Theorem 2.3.6. *Let $M_R = \bigoplus_{i=1}^{n} M_i$ be a unitary nearring module where $\{M_i : i = 1, \ldots, n\}$ is a family of irreducible submodules of M_R and R is a nearfield. If $(m + m')r = mr + m'r$ and $m + m' = m' + m$ for all $m, m' \in M_i$ and $r \in R$ then M_R is a R-vector space.*

Proof. We need to check all the axioms of vector space.

- Let $m, m' \in M_R$. There exists $m_i \in M_i$ and $m_i' \in M_i$ for $i = 1, \ldots, n$ such that $m = m_1 + m_2 + \ldots + m_n$ and $m' = m_1' + m_2' + \ldots + m_n'$. We have,

$$\begin{aligned} m + m' &= (m_1 + m_2 + \ldots + m_n) + (m_1' + m_2' + \ldots + m_n') \\ &= (m_1 + m_1') + m_2 + \ldots + m_n + m_2' + \ldots + m_n' \text{ by Proposition 2.3.3} \\ &\vdots \\ &= (m_1' + m_2' + \ldots + m_n') + (m_1 + m_2 + \ldots + m_n) \\ &= m' + m. \end{aligned}$$

So $(M_R, +)$ is abelian.

- Let $m, m' \in M_R$ and $r \in R$.

$$\begin{aligned}(m+m')r &= (m_1 + m_2 + \ldots + m_n + m'_1 + m'_2 + \ldots + m'_n)r \\ &= \big((m_1 + m'_1) + \ldots + (m_n + m'_n)\big)r \text{ by Proposition 2.3.3,} \\ &= (m_1 + m'_1)r + \ldots + (m_n + m'_n)r \text{ by Lemma 2.3.4,} \\ &= m_1 r + m'_1 r + \ldots + m_n r + m'_n r \\ &= (m_1 r + m_2 r + \ldots + m_n r) + (m'_1 r + m'2r + \ldots + m'_n r) \\ &= mr + m'r.\end{aligned}$$

- Since M_R is a unitary nearring module, for $m \in M_R$, we have $m \cdot 1 = m$.

- We now need to show that R is a skewfield. By assumption R is a division nearing (with the left distributivity). Let $p, q, r \in R$ and $m \in M_R$ such that $m \neq 0$. We have,

$$\begin{aligned}\big(m(p+q)\big)r &= (mp + mq)r \\ &= (mp)r + (mq)r \\ &= m(pr) + m(qr) \\ &= m(pr + qr).\end{aligned}$$

  It follows that $m(p+q)r - m(pr - qr) = 0$, so $m\big((p+q)r - (pr + qr)\big) = 0$. Since $m \neq 0$, $(p+q)r - (pr+qr) = 0$. Hence $(p+q)r = pr + qr$. So the right distributivity holds. Furthermore since R is a nearfield, $(R, +)$ is abelian. Therefore R is a skewfield.

- We have $m(p+q) = mp + mq$ for all $m \in M_R$ and $p, q \in R$.

- Also $m(pq) = (mp)q$ for $m \in M_R$ and $p, q \in R$.

□

2.4 Preliminary material on Beidleman near-vector spaces

In [3], the concept of a vector space (or linear space) is generalised by J. André to a less linear structure which he called a near-vector space. André

near-vector spaces use automorphisms in the construction, resulting in the right distributive law holding. However, for Beidleman near-vector spaces, we have the left distributive law holding and right nearring modules are used in the construction. In this section we introduce the basic theory of Beidleman near-vector spaces.

Definition 2.4.1. *([5]) A nearring module M_R is called strictly semi-simple if M_R is a direct sum of irreducible submodules.*

We now have,

Definition 2.4.2. *([5]) Let R be a nearfield and M_R be a nearring module. M_R is called a Beidleman near-vector space if M_R is a strictly semi-simple nearring module.*

It is well known in [5] that if M_R is Beidleman near-vector space then M_R is unitary. The simplest example of a Beidleman near-vector space is obtained when M_R itself is an irreducible nearring module.

Lemma 2.4.3. *([5]) Let R be a nearfield and M_R an irreducible nearring module. Then M_R is a Beidleman near-vector space. Moreover,*

$$M_R \cong R_R.$$

As with vector spaces, we have the same notion of "linear combination".

Definition 2.4.4. *([5]) Let M_R be a Beidleman near-vector space over a nearfield R, and let $\{m_1, \ldots, m_n\}$ be a finite set of elements from M_R. An element $m \in M_R$ is said to be a linear combination of the elements $\{m_1, \ldots, m_n\}$ if and only if, there exist elements $r_1, \ldots, r_n$ of R such that $m = \sum_{i=1}^{n} m_i r_i$.*

But, in difference with vector spaces the notion of "spanning set" of a Beidleman near-vector space has a certain restriction.

Definition 2.4.5. *([5]) A non-empty subset X of a Beidleman near-vector space M_R is called a spanning set for M_R if and only if,*

- *Every element of X is contained in an irreducible submodule,*
- *Every element of M_R can be written as a linear combination of a finite set of elements from X.*

Now, the notion of basis and dimension are defined as the following.

Definition 2.4.6. *([5]) A non-empty subset X of a near-vector space M_R is called a basis if X is a spanning set for M_R and the representation of the elements of M_R as linear combinations of the elements of X is unique.*

Theorem 2.4.7. *([5]) If M_R is a Beidleman near-vector space, then M_R has a basis.*

Let M_R be a Beidleman near-vector space. If X is a non-empty subset of M_R, then we denote the cardinal number of X by $|X|$.

Theorem 2.4.8. *([5]) Let X_1 and X_2 be two bases of the Beidleman near-vector space M_R. Then $|X_1| = |X_2|$*

Finally we have,

Definition 2.4.9. *([5]) If M_R is a near-vector space over R, then the cardinality of any basis is called the dimension of M_R and is denoted by* $\dim M_R$.

2.5 Finite dimensional Beidleman near-vector spaces

In [27] A.P. van der Walt characterized finite dimensional André near-vector spaces. In this section we do the same for finite dimensional Beidleman near-vector spaces. We will see that finite dimensional Beidleman near-vector spaces are close (in terms of structure) to traditional finite dimensional vector spaces.

Definition 2.5.1. *([5]) Suppose M_R and N_R are nearring modules. The map ϕ from M_R into N_R is called an R-homomorphism if $\phi(xr) = \phi(x)r$ and $\phi(x+y) = \phi(x) + \phi(y)$ for all $x, y \in M_R$ and $r \in R$. If ϕ is bijective then ϕ is called an R-isomorphism.*

Theorem 2.5.2. *Let R be a (left) nearfield and M_R be a right nearring module. M_R is a finite dimensional near-vector space if and only if $M_R \cong R^n$ for some positive integer $n = \dim M_R$.*

Proof. Let us consider the nearring module M_R with the action given as $M \times R \to M$ such that $(m, r) \mapsto mr$. Since M_R is a Beidleman near-vector space, $M_R = \bigoplus_{i=1}^{n} M_i$ where M_i for $i \in \{1, \ldots, n\}$ are non-zero irreducible

submodules of M_R. Then by Corollary 2.2.11, there exists $0 \neq m_i \in M_i$ such that $m_iR = M_i$ for $i \in \{1,\ldots,n\}$. Hence $M_R = \bigoplus_{i=1}^{n} m_iR$. Then it is not difficult to see that $B = \{m_1,\ldots,m_n\}$ is a basis of M_R. Let us consider the map

$$\begin{aligned}\phi : R^n &\to M\\ (r_1,\ldots,r_n) &\mapsto \sum_{i=1}^{n} m_i r_i.\end{aligned}$$

Let $(r_1,\ldots,r_n),(r'_1,\ldots,r'_n) \in R^n$. We have

$$\begin{aligned}\phi\big((r_1,\ldots,r_n)+(r'_1,\ldots,r'_n)\big) &= \sum_{i=1}^{n} m_i(r_i+r'_i)\\ &= \sum_{i=1}^{n}(m_ir_i+m_ir'_i)\\ &= \sum_{i=1}^{n} m_ir_i + \sum_{i=1}^{n} m_ir'_i\\ &= \phi\big((r_1,\ldots,r_n)\big)+\phi\big((r'_1,\ldots,r'_n)\big).\end{aligned}$$

Let $r \in R$ and $(r_1,\ldots,r_n) \in R^n$. Using Lemma 2.3.4, we obtain

$$\phi\big((r_1,\ldots,r_n)r\big) = \sum_{i=1}^{n}(m_ir_i)r = \big(\sum_{i=1}^{n} m_ir_i\big)r = \phi\big((r_1,\ldots,r_n)\big)r.$$

Since B is a basis of M_R,

$$\begin{aligned}\phi\big((r_1,\ldots,r_n)\big) = 0 \Rightarrow \sum_{i=1}^{n} m_ir_i &= 0\\ \Rightarrow r_1 = r_2 = \ldots = r_n &= 0.\end{aligned}$$

We deduce that,

$$Ker\phi = \big\{(r_1,\ldots,r_n) \in R^n : \phi(r_1,\ldots,r_n) = 0\big\} = \big\{(0,\ldots,0)\big\}.$$

It follows that ϕ is injective. Let $m \in M_R$. Since B is a basis of M_R, there exists $r_1,\ldots,r_n \in R$ such that $m = \sum_{i=1}^{n} m_ir_i = \phi(r_1,\ldots,r_n)$. It follows that ϕ is surjective. Hence ϕ is a bijective map and an isomorphism.

□

André also generalized the concept of a vector space to a non-linear structure.

Definition 2.5.3. *([3]) The pair (M, R) is called an André near-vector space if*

- *$(M, +)$ is a group and R is a set of endomorphisms of M,*
- *R contains the endomorphisms $0, id$ and $-id$,*
- *$(R^*, \cdot)$ is a subgroup of the group $\big(Aut(M), \circ\big)$,*
- *R acts fixed point free on M, (i.e, for $x \in M, \alpha, \beta \in R, x\alpha = x\beta \Rightarrow x = 0$ or $\alpha = \beta$),*
- *the quasi-kernel $Q(M)$ of M (i.e, the set of all $m \in M$ such that, for each pair $\alpha, \beta \in R$, there exists $\gamma \in R$ for which $m\alpha + m\beta = m\gamma$) generates M additively as a group.*

The elements of M are called vectors and the members of R scalars (here R is seen as right nearfield). The action of R on M is called scalar multiplication. In his article [27] van der Walt characterised finite dimensional André near-vector spaces using nearrings and nearfields.

Theorem 2.5.4. *[27] Let M be a group and let $A := D \cup \{0\}$, where D is a fixed point free group of automorphisms of M. The pair (M, A) is a finite dimensional André near-vector space if and only if there exists a finite number of (right) nearfields, $R_1, R_2, \ldots, R_n$, semigroup isomorphisms $\psi_i : A \to R_i$ and a group isomorphism $\Phi : M \to R_1 \oplus R_2 \oplus \cdots \oplus R_n$ such that if*

$$\Phi(v) = (x_1, \ldots, x_n), \quad (x_i \in R_i)$$

then

$$\Phi(v\alpha) = (x_1\psi_1(\alpha), \ldots, x_n\psi_n(\alpha)),$$

for all $v \in M$ and $\alpha \in A$.

According to this theorem we can specify a finite dimensional André near-vector space by taking n copies of a (right) nearfield R for which there are semigroup isomorphisms $\vartheta_i : (R, \cdot) \to (R, \cdot)$, $i \in \{1, \ldots, n\}$. We then take $M := R^n$, n a positive integer, as the additive group of the near-vector space and define

$$(x_1, \ldots, x_n)\alpha := (x_1\vartheta_1(\alpha), \ldots, x_n\vartheta_n(\alpha)),$$

for all $\alpha \in R$.

Remark 2.5.5. *Let R be a (right) nearfield.*

- *By van der Walt's theorem [27], (R^n, R) is an André near-vector space with the scalar multiplication defined by*

$$(x_1, \ldots, x_n)\alpha = \big(x_1\psi_1(\alpha), \ldots, x_n\psi_n(\alpha)\big)$$

for all $\alpha \in R$ and $(x_1, \ldots, x_n) \in R^n$ where the ψ_i for $i \in \{1, \ldots, n\}$ are multiplicative automorphisms of R. Note that the action of the scalars on the vectors is on the right, whereas for Beidleman the action of the scalars on the vectors is on the left (when we use the right nearfield). Also by van der Walt's construction theorem [27] we can take different nearfields to construct finite dimensional André near-vector spaces, as long as the nearfields are multiplicatively isomorphic. For Beidleman near-vector spaces, n copies of the same nearfield are used in the construction and we can take the automorphism of nearfields, i.e, define

$$(x_1, \ldots, x_n)\alpha := (x_1\psi_1(\alpha), \ldots, x_n\psi_n(\alpha)),$$

for all $\alpha \in R$ where ψ_i are automorphisms of R.

- *If R is a field then (R^n, R) is both an André and Beidleman near-vector space, and both coincide to a vector space. Here we are taking all the $\psi_i = id$ for $i \in \{1, \ldots, n\}$.*

Remark 2.5.6. *Let M_R be a Beidleman near-vector space. Then $M_R = \bigoplus_{i\in I} M_i$, where the M_i are irreducible submodules of M_R. By Corollary 2.2.11 there exists $0 \neq m_i \in M_i$ such that $M_R = \bigoplus_{i\in I} m_i R$. Hence $\{m_i : i \in I\}$ is a basis for M_R. If I is infinite then M_R has infinite dimension and we can use the same procedure as in the proof of Theorem 2.5.2 to show that $M \cong R^{\dim M_R}$.*

In the next theorem we will show that two Beidleman near-vector spaces over the same nearfield R are R-isomorphic if and only if they have the same dimension.

Theorem 2.5.7. *([5]) Let M_R and M'_R be two finite dimensional Beidleman near-vector spaces. We have M_R is R-isomorphic to M'_R if and only if* $\dim(M_R) = \dim(M'_R)$.

Proof. Suppose $M_R \cong M'_R$. By Theorem 2.5.2 we have $M_R \cong R^{\dim(M_R)}$ and $M'_R \cong R^{\dim(M'_R)}$. It follows that $R^{\dim(M_R)} \cong R^{\dim(M'_R)}$. Thus $\dim(M_R) = \dim(M'_R)$. The converse is straight forward. □

Furthermore, we deduce the following.

Lemma 2.5.8. *We have that M_R is an André and Beidleman near-vector space if and only if M_R is an R-vector space.*

Proof. Assume that M_R is an André and Beidleman near-vector space. Since M_R is a Beidleman near-vector space, M_R is a nearring module and we have, $m(r_1 + r_2) = mr_1 + mr_2$, $m(r_1r_2) = (mr_1)r_2$ and $m1 = m$ for all $m \in M_R$ and $r_1, r_2 \in R$. Also since M_R is an André near-vector space, R is a set of endomorphisms of $(M_R, +)$ i.e., $(m_1 + m_2)r = m_1r + m_2r$ for all $m_1, m_2 \in M$ and $r \in R$. Let $r_1, r_2, r \in R$. If $0 \neq m \in M$ then,

$$\begin{aligned}\big(m(r_1 + r_2)\big)r &= \big(mr_1 + mr_2\big)r \\ &= (mr_1)r + (mr_2)r \\ &= m(r_1r) + m(r_1r) \\ &= m(r_1r + r_2r)\end{aligned}$$

By the fixed point free property, it follows that $(r_1 + r_2)r = r_1r + r_2r$. Furthermore since R is a nearfield, $(R, +)$ is abelian. Then R is a skewfield. Thus M_R is an R-vector space.
Conversely assume that M_R is R-vector space.

- Let $B = \{b_i : i \in I\}$ be a basis of M_R. Then $M_R \cong \oplus_{i\in I} R_i$ where $R_i = R$. But R_i is an irreducible nearring module over R. Hence M_R is a direct sum of irreducible nearring modules. Thus M_R is a Beidleman near-vector space.

- We check the following.

  – Clearly $(M, +)$ is a group. There is a map:

  $$h : R \to End(M),\ \alpha \mapsto f_\alpha \text{ where}$$

  $$f_\alpha : M \to M,\ m \mapsto m\alpha.$$

  We have that f_α is an endomorphism of M and h is injective. It follows that R is embedded into $End(M)$. So R can be considered as a set of endomorphism of M.

– Consider the endomorphism

$$f_0 : M \to M,\ m \mapsto m0.$$

We have $f_0(m) = m0 = m(0+0) = m0 + m0$. It follows that $m0 = 0$. Hence $f_0 = 0$. Also $h(0_R) = f_0 = 0 \in h(R)$. It follows that f_0 is element of R. Let us consider the endomorphism

$$f_1 : M \to M, m \mapsto m1.$$

We have $f_1(m) = m1 = m$. It follows that $f_1 = id$ (the identity endormophism). Let us also consider the endomorphism

$$f_{-1} : M \to M,\ m \mapsto m(-1).$$

We have $m + (-m) = 0_M = m0_R = m(1 + (-1)) = m1 + m(-1) = m + m(-1)$. It follows that $-m = m(-1)$. So $f_{-1}(m) = m(-1) = -m$. It follows that $f_{-1} = -id$.

– Let $\alpha \in R^*$ acts as endomorphism f_α of M. Let $m, m' \in M$. Suppose $f_\alpha(m) = f_\alpha(m')$. So $m\alpha = m'\alpha$. It follows that $(m - m')\alpha = 0$. Hence $m - m' = 0$ since $\alpha \neq 0$. Thus f_α is injective. Let $m \in M$. Then there exists $n = m\alpha^{-1} \in M$ such that $f_\alpha(n) = m$. We have $f_\alpha(m\alpha^{-1}) = m\alpha^{-1}\alpha = m$. Thus f_α is surjective. Let $\alpha, \beta \in R^*$. So $h(\alpha\beta) = f_{\alpha\beta}$. For all $m \in M$,

$$f_{\alpha\beta}(m) = m(\alpha\beta) = (m\beta)\alpha = f_\beta(m)\alpha = f_\alpha\big(f_\beta(m)\big).$$

It follows that $f_{\alpha\beta} = f_\alpha \circ f_\beta$. Hence $h(\alpha\beta) = h(\alpha)h(\beta)$ and since $(R^*, \cdot)$ is a group, $h(R^*)$ is a subgroup of $\big(Aut(M), \circ\big)$. Thus R^* can be considered as subgroup of $\big(Aut(M), \circ\big)$.

– Let $m \in M$ and $\alpha, \beta \in R$. Suppose that $m\alpha = m\beta$. So $m(\alpha - \beta) = 0$. Assume that $\alpha - \beta \neq 0$. So there exists $\gamma^{-1} = \alpha - \beta$. It follows that $m(\alpha - \beta)\gamma = 0\gamma = (0+0)\gamma = 0\gamma + 0\gamma$. So $0\gamma = 0$. Hence $m = 0$. This means that $m(\alpha - \beta) = 0$ implies $m = 0$ or $\alpha - \beta = 0$.

– $Q(M) = M$. It follows that $Q(M)$ generates M as a group.

□

2.6 Concluding comments

In later chapters we will study finite dimensional Beildleman near-vector spaces of the form R^m where R is a finite nearfield and m a positive integer and find some interesting results. For this reason the next chapter will be focused on finite nearfields.

Chapter 3

On finite Dickson nearfields

3.1 Introduction

The aim of this chapter is to introduce the basic notion of a finite Dickson nearfield and give some details on how to construct them. We will use Hull and Dobell's theorems [20] to prove some important results in the construction of a finite Dickson nearfield. As a result we found that a Dickson pair (See Definition 3.2.11) can be used in an area of random number generation. Furthermore in Proposition 3.2.17, we deduce that every Dickson pair (q, n), where $n > 1$, will always induce a proper finite nearfield. Let g be such that the multiplicative group of the finite field $\mathbb{F}_{q^n}$ (of order q^n) is generated by g. Let H be the subgroup of the multiplicative group of $\mathbb{F}_{q^n}$ generated by g^n. In Lemma 3.2.21 we deduce a condition on (q, n) for which any H-coset (see Definition 5.2.5) can be simplified. We also show in Theorem 3.2.24 that the multiplicative group of the distributive elements of a finite Dickson nearfield is always a subgroup of $(H, \cdot)$. In Section 3, building on some existing results from [10, 29], we present the additive and multiplicative group of a finite Dickson nearfield. In the last section, we provide by ourselves an alternative proof of the result originally done by H. Karzel and E. Ellers about the presentation of the center of a finite Dickson nearfield (see Theorem 3.4.6 and Theorem 3.4.9). Furthermore, we worked out by ourselves the proofs of the known results in Theorem 3.2.24 and Theorem 3.2.15. Later on, we will use some of the results of this chapter to describe the *"generalized distributive set"* of a finite Dickson nearfield.

3.2 Construction of finite Dickson nearfields

3.2.1 Coupling maps

In this subsection we introduce maps that are useful to define a new multiplication.

Definition 3.2.1. *([26]) Let R be a nearfield and $Aut(R,+,\cdot)$ the set of all automorphisms of R. A map*

$$\begin{aligned}\phi: \quad & R^* \to Aut(R,+,\cdot)\\ & a \mapsto \phi_a\end{aligned}$$

is called a coupling map if for all $a,b \in R^*, \phi_a \circ \phi_b = \phi_{\phi_a(b)\cdot a}$.

Example 3.2.2. *Let us consider*

$$\begin{aligned}\phi: \quad & R^* \to Aut(R,+,\cdot)\\ & a \mapsto id_R\end{aligned}$$

ϕ is a coupling map because for all $a,b \in R^*$, we have $\phi_a \circ \phi_b = id_R \circ id_R = id_R$ and $\phi_a(b) = b$, so $\phi_{\phi_a(b)\cdot a} = \phi_{ba} = id_R$. Therefore $\phi_a \circ \phi_b = \phi_{\phi_a(b)\cdot a}$.

Example 3.2.3. *([6]) Let $(\mathbb{H},+,\cdot)$ be the skew-field of real quaternions (with the the standard basis $\{1,i,j,k\}$) and $t \in \mathbb{R}$. The map*

$$\begin{aligned}\phi: \quad & \mathbb{H} \to Aut(\mathbb{H},+,\cdot)\\ & b \mapsto \phi_b\end{aligned}$$

is a coupling map, where

$$\begin{aligned}\phi_b: \quad & \mathbb{H} \to \mathbb{H}\\ & a \mapsto |b|^{it} a |b|^{-it}\end{aligned}$$

and $|a|$ is the Euclidean norm of $a \in \mathbb{H}$.

Proof. We need to check that $\phi_a \circ \phi_b = \phi_{\phi_a(b)\cdot a}$, for all $a,b \in \mathbb{H}$.
Let $s \in \mathbb{H}$, then

$$\begin{aligned}(\phi_a \circ \phi_b)(s) &= \phi_a(\phi_b(s))\\ &= \phi_a\left(|b|^{it} s |b|^{-it}\right)\\ &= |a|^{it}|b|^{it} s |b|^{-it}|a|^{-it}.\end{aligned}$$

Moreover,

$$\phi_{\phi_a(b)\cdot a}(s) = \left|\phi_a(b)\cdot a\right|^{it} s \left|\phi_a(b)\cdot a\right|^{-it}.$$

But

$$\begin{aligned}\left|\phi_a(b)\cdot a\right| &= \left||a|^{it}b|a|^{-it}a\right| \\ &= \left||a|^{it}\right||b|\left||a|^{-it}\right||a| \\ &= |b||a|\end{aligned}$$

because $|a|^{it} = e^{it\ln|a|}$ and $\left||a|^{it}\right| = |e^{it\ln|a|}| = 1$. Similarly $\left||a|^{-it}\right| = 1$. Therefore

$$\begin{aligned}\phi_{\phi_a(b)\cdot a}(s) &= \left|\phi_a(b)\cdot a\right|^{it} s \left|\phi_a(b)\cdot a\right|^{-it} \\ &= \left||b||a|\right|^{it} s \left||b||a|\right|^{-it} \\ &= |a|^{it}|b|^{it}s|b|^{-it}|a|^{-it}.\end{aligned}$$

Thus ϕ a coupling map. □

Definition 3.2.4. *([26]) Let R be a nearfield and ϕ a coupling map on R. Then one defines a new binary operation on R by*

$$a \circ_\phi b = \begin{cases} a\cdot\phi_a(b) & \text{if } a \neq 0 \\ 0 & \text{if } a = 0. \end{cases}$$

Lemma 3.2.5. *([26]) Let R be a nearfield and ϕ be a coupling map. Then the set*

$$G = \{\phi_a : a \in R^*\}$$

is a group under composition of maps.

Remark 3.2.6.

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

Theorem 3.2.7. *([26]) Let R be a nearfield and ϕ be a coupling map on R. Then $(R, +, \circ_\phi)$ is again a nearfield where $\circ_\phi$ is defined as in Definition 3.2.4.*

3.2.2 Dickson construction

The first finite proper nearfield was discovered by J.E. Dickson [10]. His technique was to "distort" the multiplication of a finite field.

Definition 3.2.8. *([26]) Let $(R,+,\cdot)$ be a nearfield and ϕ a coupling map on R^*. Then $(R,+,\circ_\phi)$ is called the ϕ-derivation of $(R,+,\cdot)$ and is denoted by R^ϕ. The group $(G,\circ)$ is called the Dickson group of ϕ with G defined as in Lemma 3.2.5. R is said to be a Dickson nearfield if R is the ϕ-derivation of some field F, i.e., $R = F^\phi$.*

Remark 3.2.9. *Let $(R,+,\cdot)$ be a nearfield. Let us consider the coupling map $\phi : a \mapsto id$. In this case*

$$a \circ_\phi b = \begin{cases} a \cdot \phi_a(b) = a \cdot id(b) = a \cdot b & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}$$

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

- *If $(R,+,\cdot)$ is a nearfield, then the ϕ-derivation of $(R,+,\cdot)$ is $(R,+,\circ_\phi)$ i.e., $R^\phi = R$ is also a nearfield but not necessarily a Dickson nearfield.*
- *If $(F,+,\cdot)$ is a field, then the ϕ-derivation of $(F,+,\cdot)$ is $(F,+,\circ_\phi)$ i.e., $F^\phi = F$. It follows that every field is a Dickson nearfield.*

Example 3.2.10. *([6]) Let $(\mathbb{H},+,\cdot)$ be the skew-field of real quaternions (with the the standard basis $\{1,i,j,k\}$) and $t \in \mathbb{R}$. We define a new multiplication $\circ$ on $\mathbb{H}$ by*

$$a \circ b = \begin{cases} |b|^{it} a |b|^{-it} b & \text{if } b \neq 0 \\ 0 & \text{if } b = 0 \end{cases}$$

Then $\mathbb{H}_t := (\mathbb{H},+,\circ)$ is a nearfield, but not a Dickson nearfield. In fact $\mathbb{H}_t = \mathbb{H}^\phi$ where

$$\begin{aligned} \phi : \mathbb{H} &\to Aut(\mathbb{H},+,\cdot) \\ b &\mapsto \phi_b \end{aligned}$$

is a coupling map, with the automorphism

$$\begin{aligned} \phi_b : \mathbb{H} &\to \mathbb{H} \\ a &\mapsto |b|^{it} a |b|^{-it}. \end{aligned}$$

Finally, to construct finite Dickson nearfields, we need the following:

Definition 3.2.11. *([26]) A pair of positive numbers (q, n) (where $q > 1$) is called a Dickson pair if*

(i) *q is some power p^l of some prime p where l is a positive integer,*

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

(iii) *if $q \equiv 3$ mod 4 then 4 does not divide n.*

Example 3.2.12. *The following are Dickson pairs:* $(7,9), (3,2), (4,3), (5,4)$ *and* $(5,8)$.

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

To generate a sequence of numbers which at least appear to be drawn at random from a certain probability distribution (uniform, normal, Poisson, or some other), we begin with a positive integer m, called the modulus, a positive integer x_0, called the starting value such that $0 \leq x_0 < m$, an integer a, called the multiplier such that $0 < a < m$ and another integer c, called the increment such that $0 \leq c < m$. We then define a sequence $\{x_i\}$ of non-negative integers, each less than m, by means of the congruence relation

$$x_i \equiv (ax_{i-1} + c) \mod m. \tag{3.2.1}$$

A sequence $\{x_i\}$ has full period m if $\{x_i\}$ forms a complete set of different residues modulo m. For the case $c \neq 0$, an important number theoretic property has been discovered by T.E. Hull and A.R. Dobell in 1962 and is stated as the following:

Theorem 3.2.13. *([20]) The sequence defined by the congruence relation (3.2.1) has full period m, provided that*

(i) *c is relatively prime to m,*

(ii) *$a \equiv 1 \mod p$ if p is a prime factor of m,*

(iii) *$a \equiv 1 \mod 4$ if 4 is a factor of m.*

We now deduce the following known result, which is a special case of Hull-Dobell's theorem.

Lemma 3.2.14. *Let (q,n) be a Dickson pair. For all $k,j \in \{1,\ldots,n\}$, if $k \neq j$ then $[k]_q$ is not congruent to $[j]_q$ modulo n.*

Proof. We put $x_0 = 1, a = q, m = n$ and $c = 1$ into the relation (3.2.1) and apply Theorem 3.2.13. Thus we have the following: $x_0 \equiv 1 \mod n$, $x_1 \equiv (q+1) \mod n$, $x_2 \equiv (q^2+q+1) \mod n, \ldots, x_{n-1} \equiv (q^{n-1}+q^{n-2}+\ldots+1) \mod n$. Hence the sequence $\{x_i\}_{i=0,\ldots,n-1}$ has full period n and is a family of different residues modulo n.

□

We will see in the next theorem that for each Dickson pair, we will be able to construct a finite Dickson nearfield containing q^n elements. From now on we will 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 a generator g by $DN_g(q,n)$. Note that g is a generator of the multiplicative group of the finite field of order q^n.

Theorem 3.2.15. *([10, 26]) For all Dickson pairs (q,n), there exist some associated finite nearfields, of order q^n which arise by taking the finite field $\mathbb{F}_{q^n}$ and changing the multiplication such that $\mathbb{F}_{q^n}^{\phi} = (\mathbb{F}_{q^n}, +, \circ)$ for some coupling map ϕ on $\mathbb{F}_{q^n}$ where " $\circ$ " is the new multiplication.*

Proof. Let (q,n) be a Dickson pair where $q = p^l$ where l is a positive integer. Let $(\mathbb{F}_{q^n}, +, \cdot)$ be a finite field with characteristic p, where p is prime, containing q^n elements. The multiplicative group $(\mathbb{F}_{q^n}^*, \cdot)$ is cyclic. So $\mathbb{F}_{q^n}^*$ is generated by an element denoted g. Let us consider H, the subgroup of $(\mathbb{F}_{q^n}^*, \cdot)$ generated by g^n. So $\mathbb{F}_{q^n}^*/H$ is the group of all left cosets of H. Each coset is of the form $g^jH = \{g^jh : h \in H\}$ where $j = 0,\ldots,n-1$. Since H is a subgroup of $\mathbb{F}_{q^n}^*$, the number of left cosets of H in $\mathbb{F}_{q^n}^*$ is the index $(\mathbb{F}_{q^n}^* : H)$ of H in $\mathbb{F}_{q^n}^*$. Since $\mathbb{F}_{q^n}^*$ is finite $(\mathbb{F}_{q^n}^* : H)$ is finite and by Lagrange's Theorem $(\mathbb{F}_{q^n}^* : H) = |\mathbb{F}_{q^n}^*/H| = n = \frac{|\mathbb{F}_{q^n}^*|}{|H|}$. Thus

$$\mathbb{F}_{q^n}^*/H = \{g^0H, g^1H, \ldots, g^{n-1}H\}.$$

By Lemma 3.2.14 the set $\{[1]_q, [2]_q, \ldots, [n]_q\}$ gives a complete set of residues modulo n and

$$\{g^{[1]_q}H, g^{[2]_q}H, \ldots, g^{[n]_q}H\} = \{g^0H, g^1H, \ldots, g^{n-1}H\}.$$

Therefore $\mathbb{F}_{q^n}^*/H$ can also be represented as follows

$$\mathbb{F}_{q^n}^*/H = \{g^{[1]_q}H, g^{[2]_q}H, \ldots, g^{[n]_q}H\}.$$

Now let us consider the maps:

$$\begin{aligned} \varphi: \quad & \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \\ & t \mapsto t^q \end{aligned}$$

which is a power of the Frobenius automorphism, i.e, $\varphi = \psi^l$. Define the map λ such that

$$\begin{aligned} \lambda: \quad & \mathbb{F}_{q^n}^*/H \to Aut(\mathbb{F}_{q^n}, +, \cdot) \\ & g^{[k]_q}H \mapsto \varphi^k. \end{aligned}$$

Suppose $g^{[k_1]_q}H, g^{[k_2]_q}H \in \mathbb{F}_{q^n}^*/H$ such that $g^{[k_1]_q}H = g^{[k_2]_q}H$. Then

$$\begin{aligned} g^{[k_1]_q}H = g^{[k_2]_q}H &\Rightarrow g^{[k_1]_q} = g^{[k_2]_q} \\ &\Rightarrow [k_1]_q = [k_2]_q \\ &\Rightarrow k_1 = k_2 \\ &\Rightarrow \varphi^{k_1} = \varphi^{k_2} \\ &\Rightarrow \lambda\left(g^{[k_1]_q}H\right) = \lambda\left(g^{[k_2]_q}H\right). \end{aligned}$$

So λ is well-defined. Let us consider the quotient map

$$\begin{aligned} \pi: \mathbb{F}_{q^n}^* &\to \mathbb{F}_{q^n}^*/H \\ f &\mapsto g^{[k]_q}H. \end{aligned}$$

Define the map ϕ such that

$$\begin{aligned} \phi = \lambda \circ \pi: \mathbb{F}_{q^n}^* &\to Aut(\mathbb{F}_{q^n}, +, \cdot) \\ t &\mapsto \varphi^k \text{ for } t \in g^{[k]_q}H. \end{aligned}$$

Claim: ϕ is a coupling map on $\mathbb{F}_{q^n}^*$.

To see this, we need to check that $\phi_a \circ \phi_b = \phi_{\phi_a(b)a}$ for all $a, b \in \mathbb{F}_{q^n}^*$. Since $\mathbb{F}_{q^n}^*/H$ can be presented as

$$\mathbb{F}_{q^n}^*/H = \{g^{[1]_q}H, g^{[2]_q}H, \ldots, g^{[n]_q}H\}$$

then

$$\mathbb{F}_{q^n}^* = g^{[1]_q}H \cup g^{[2]_q}H \cup \cdots \cup g^{[n]_q}H.$$

Therefore every element of $\mathbb{F}_{q^n}^*$ can be written as $g^{[k]_q+n\delta}$ for $\delta \in \mathbb{N}$ and $1 \leq k \leq n$. It follows that if $a = g^{[k_1]_q+n\delta_1}$ and $b = g^{[k_2]_q+n\delta_2}$, then $\pi(a) = g^{[k_1]_q}H$, $\pi(b) = g^{[k_2]_q}H$. So $\phi_a = (\lambda \circ \pi)(a) = \varphi^{k_1}$ and $\phi_b = (\lambda \circ \pi)(b) = \varphi^{k_2}$. It follows that

$$\phi_a \circ \phi_b = \varphi^{k_1} \circ \varphi^{k_2} = \varphi^{k_1+k_2}.$$

Also

$$\begin{aligned}
\phi_a(b) \cdot a &= \varphi^{k_1}(b) \cdot a \\
&= b^{q^{k_1}} a \\
&= g^{\left([k_2]_q+n\delta_2\right)q^{k_1}} g^{[k_1]_q+n\delta_1} \\
&= g^{\frac{q^{k_1+k_2}-q^{k_1}+q^{k_1}-1}{q-1}+n\delta_2 q^{k_1}+n\delta_1} \\
&= g^{\frac{q^{k_1+k_2}-1}{q-1}+n(\delta_1+q^{k_1}\delta_2)}.
\end{aligned}$$

It follows that

$$\phi_{\phi_a(b)\cdot a} = \varphi^{k_1+k_2}.$$

So $\phi_a \circ \phi_b = \phi_{\phi_a(b)\cdot a}$. Thus if we consider the finite field $(\mathbb{F}_{q^n}, +, \cdot)$ and the coupling map ϕ, then $\mathbb{F}_{q^n}^{\phi} = (\mathbb{F}_{q^n}, +, \circ_\phi)$ is the ϕ-derivation of the finite field $\mathbb{F}_{q^n}$. Thus $(\mathbb{F}_{q^n}, +, \circ_\phi)$ is a finite Dickson nearfield containing q^n elements denoted by $DN_g(q, n)$.

□

We will refer to the following example in later chapters.

Example 3.2.16. *Consider the field* $(\mathbb{F}_{3^2}, +, \cdot)$ *with*

$$\mathbb{F}_{3^2} := \{0, 1, 2, x, 1+x, 2+x, 2x, 1+2x, 2+2x\},$$

where x is a zero of $x^2 + x + 2 \in \mathbb{Z}_3[x]$. In ([26] p. 257), it is observed that $(\mathbb{F}_{3^2}, +, \cdot)$ with the following new multiplication

$$a \circ b := \begin{cases} a \cdot b & \text{if } b \text{ is a square in } (\mathbb{F}_{3^2}, +, \cdot) \\ a^3 \cdot b & \text{otherwise} \end{cases}$$

is a (right) nearfield but not a field. However when the new multiplication is defined as follows

$$a \circ b := \begin{cases} a \cdot b & \text{if } a \text{ is a square in } (\mathbb{F}_{3^2}, +, \cdot) \\ a \cdot b^3 & \text{otherwise} \end{cases}$$

then this gives the smallest finite Dickson (left) nearfield $DN_g(3,2) := (\mathbb{F}_{3^2}, +, \circ)$ which is not a field, where $\mathbb{F}_{3^2}^* = \langle g \rangle$. The table of the new operation " $\circ$ " for the (left) $DN_g(3,2)$ is presented as follows:

Table 3.1: The multiplication for $DN_g(3,2)$.

$\circ$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$2x+1$	2	x	$x+2$	$2x$	1
$x+2$	0	$x+2$	$2x+1$	$x+1$	$2x$	2	$2x+2$	1	x
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$2x+2$	x	1	$x+1$	2	$2x$
$2x+2$	0	$2x+2$	$x+1$	$x+2$	1	$2x$	$2x+1$	x	2

Let (q,n) be a Dickson pair, in the following lemma, we wish to prove the known result for which the finite Dickson nearfields $DN(q,n)$ are proper nearfields.

Lemma 3.2.17. *Let (q,n) be a Dickson pair where $n>1$. Let g be a generator of $\mathbb{F}_{q^n}^*$ and R the finite nearfield constructed with $H=\langle g^n\rangle$. Then R is a proper finite nearfield.*

Proof. Let $(q=p^l,n)$ be a Dickson pair, $\mathbb{F}_{q^n}^*=\langle g\rangle$ and $H=\langle g^n\rangle$. The quotient group is given by

$$\mathbb{F}_{q^n}^*/H=\{g^{[1]_q}H,g^{[2]_q}H,\ldots,g^{[n]_q}H\}.$$

The coupling map ϕ is defined as

$$\begin{array}{lcl}\mathbb{F}_{q^n}^* & \to & Aut(\mathbb{F}_{q^n},+,\cdot)\\ \alpha & \mapsto & \phi_\alpha=\varphi^k\end{array}$$

where φ is the appropriate power of the Frobenius automorphism of $\mathbb{F}_{q^n}$(i.e, $\varphi=\psi^l$ where ψ is the Frobenius autormorphism) and $k\in\{1,\ldots,n\}$ such that $\alpha\in g^{[k]_q}H$. We would like to show that $R=(\mathbb{F}_{q^n},+,\circ)$ is not a field by showing that there exist $a,b\in\mathbb{F}_{q^n}$ such that $a\circ b\neq b\circ a$. Let $a,b\in\mathbb{F}_{q^n}$. We have

$$\begin{aligned}a\circ b&=\begin{cases}a\cdot\phi_a(b) & \text{if } a\neq 0\\ 0 & \text{if } a=0\end{cases}\\ &=\begin{cases}a\cdot\varphi^k(b) & \text{if } a\in g^{[k]_q}H\\ 0 & \text{if } a=0\end{cases}\\ &=\begin{cases}a\cdot b^{q^k} & \text{if } a\in g^{[k]_q}H\\ 0 & \text{if } a=0\end{cases}\end{aligned}$$

for $k\in\{1,\ldots,n\}$. Thus $DN_g(q,n):=(\mathbb{F}_{q^n},+,\circ)$ is the finite Dickson nearfield constructed by $H=\langle g^n\rangle$. Suppose $n>1$ and let $a=g^n\in g^{[n]_q}H$ and $b=g\in g^{[1]_q}H$. We have

$$g\circ g^n=g\varphi^1(g^n)=g(g^n)^q=g^{nq+1}.$$

Also, since $\varphi^n=id$ then

$$g^n\circ g=g^n\varphi^n(g)=g^{n+1}.$$

Assume that $g^{nq+1} = g^{n+1}$, then $g^{n(q-1)} = 1$. But since $\mathbb{F}_{q^n}^* = \langle g \rangle$, then $|g| = q^n - 1$. It follows that if $g^t = 1 \Rightarrow q^n - 1 | t$. Moreover since $g^{n(q-1)} = 1$, then

$$q^n - 1 | n(q-1) \Rightarrow 1 + q + \ldots + q^{n-1} | n.$$

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

Theorem 3.2.18. *([10, 26]) By taking all Dickson pairs, all finite Dickson nearfields arise in the way described in Theorem 3.2.15.*

Furthermore,

Lemma 3.2.19. *([29]) Let (q, n) be a Dickson pair. Then n divides $[n]_q$.*

Proof. Suppose that (q, n) is a Dickson pair Let us consider $x_0 = 1, a = q, m = n$ and $c = 1$. By Theorem 3.2.13 the period of the sequence $\{x_i\}$ is exactly n. Thus $1 = x_0$ and is equivalent to x_n. But we have $x_{n-1} \equiv [n]_q \mod n$ satisfies the recurrence

$$\begin{aligned} x_n \equiv q x_{n-1} + 1 \mod n &\Leftrightarrow 1 \equiv q x_{n-1} + 1 \mod n \\ &\Leftrightarrow q x_{n-1} \equiv 0 \mod n. \end{aligned}$$

Since every prime divisor of n divides $q - 1$, then $\text{GCD}(q, n) = 1$. Thus

$$q x_{n-1} \equiv 0 \mod n \Leftrightarrow x_{n-1} \equiv 0 \mod n.$$

□

By Lemma 3.2.19 we deduce the following.

Corollary 3.2.20. *([29]) 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 $\mathbb{F}_{q^n}^*$ and R the finite nearfield constructed with $H = \langle g^n \rangle$. Then $g^{[n]_q} H = H$.*

Also we have the following.

Lemma 3.2.21. *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 $\mathbb{F}_{q^n}^*$ and R the finite nearfield constructed with $H = \langle g^n \rangle$. If n divides $q-1$ then $g^{[i]_q}H = g^iH$ for all $i = 1, \ldots, n$.*

Proof. Suppose that n divides $q-1$. We need to show that $[i]_q \equiv i \mod n$. We proceed by induction on i. For $i = 1$, we have $[1]_q \equiv 1 \mod n$. Suppose that $[i]_q \equiv i \mod n$. Since n divides $q-1$, $q^i \equiv 1 \mod n$. So $[i+1]_q \equiv i+1 \mod n$. □

Remark 3.2.22.

- *Lemma 3.2.21 is not always true for any Dickson pair, for example, take $(q,n) = (7,9)$. We have $[2]_7 = 8$ but $8 \ncong 2 \mod 9$.*
- *For $n = 1$, we have that $\mathbb{F}_{q^n}^* = \langle g \rangle$ and $H = \langle g \rangle$. It follows that $\mathbb{F}_{q^n}^*/H = \{H\}$ and then the coupling map is the identity since $\phi : \alpha \mapsto \varphi$ where $\varphi : t \mapsto t^q = t$ for all $t \in \mathbb{F}_q$. Thus all finite fields arise from the Dickson pair of the form $(q,1)$.*
- *Note that for all pairs (q,n) where $n = 1$ there exists a unique finite Dickson nearfield of order $q = p^l$ which is also a finite field.*
- *For $n \neq 1$ there exist finite proper nearfields of order q^n. In this case, they are not necessarily unique finite Dickson nearfields of this order. The number of non-isomorphic Dickson nearfields derived by this construction (for different choices of g) is given by $\frac{\varphi(n)}{i}$, where φ is the Euler-function and i is the order of $p(\mod n)$ (see [26])*
- *In general Dickson nearfields can be either finite or infinite.*

The authors in [13] determined the set of all distributive elements of R denoted by $D(R)$ where $R \in DN(q,n)$.

Theorem 3.2.23. *([13]) Let R be a finite Dickson nearfield that arises from the Dickson pair (q,n). Then $D(R) = C(R) = \mathbb{F}_q$.*

Now we deduce a proof of the following known result.

Theorem 3.2.24. *Let (q,n) be a Dickson pair and g a generator of $\mathbb{F}_{q^n}^*$. Let R be the finite nearfield constructed with $H = \langle g^n \rangle$. Then $(D(R)^*, \cdot)$ is a subgroup of $(H, \cdot)$.*

Proof. Let g and β be respectively the generators of $\mathbb{F}_{q^n}^*$ and $\mathbb{F}_q^*$. Since (q,n) is a Dickson pair, by Corollary 3.2.20 we have $H = g^{[n]_q}H$. So if we are able to show that $\beta = g^{[n]_q}$, then $\beta \in H$ and the subgroup generated by β, which is $\mathbb{F}_q^*$, will be a subgroup of the group H. Since $\mathbb{F}_{q^n}^* =< g >$ and $\mathbb{F}_q^* =< \beta >$, we have $|g| = q^n - 1$ and $|\beta| = q - 1$ where $|g|$ is denoted as the order of g. Also, since $\beta \in \mathbb{F}_{q^n}^*$, there is $i \in \mathbb{N}$ such that $\beta = g^i$. We have that

$$q - 1 = |\beta| = |g^i| = \frac{q^n - 1}{\text{GCD}(i, q^n - 1)}.$$

Hence

$$\text{GCD}(i, q^n - 1) = [n]_q.$$

We have

$$1 = \beta^{q-1} = g^{i(q-1)} = g^{[n]_q(q-1)} = g^{q^n-1} = 1.$$

It follows that $i = [n]_q$ is the smallest integer such that $\text{GCD}(i, q^n - 1) = [n]_q$ and $g^{i(q-1)} = 1$. Hence $\beta = g^{[n]_q}$. It follows that $\beta \in g^{[n]_q}H$. Therefore $< \beta > = \mathbb{F}_q^* = D(R)^*$ is a subgroup of H. □

3.2.3 The multiplicative group of a finite nearfield

In this subsection we will see a particular difference between a finite field and a finite nearfield.

Definition 3.2.25. *([26]) A metacyclic group is a group G such that both its commutator subgroup $G' = [G, G]$ and the quotient group G/G' are cyclic.*

Assume that (q,n) is a Dickson pair. We have seen in the previous section that for all (q,n) we can construct an associated Dickson nearfield $DN_g(q,n)$ with a generator g. Let $G_{q,n}$ denote the multiplicative group of $DN_g(q,n)$. In [29], Wahling gave a description of $G_{q,n}$. It is generated by two elements and can be presented as follows:

Theorem 3.2.26. *([29]) Let (q,n) be a Dickson pair, let g a generator of $\mathbb{F}_{q^n}^*$ and let R be the nearfield constructed with $H = \langle g^n \rangle$. The multiplicative group of R can be presented as*

$$G_{q,n} = \langle a, b : a^m = 1, b^n = a^t, ab = ba^q \rangle$$

where $m = \frac{q^n-1}{n}$ and $t = \frac{m}{q-1}$.

Example 3.2.27. *Let g be a generator of $\mathbb{F}_{3^2}^*$ and R be the nearfield constructed with $H = \langle g^2 \rangle$. Then*

$$(R^*, \circ) \cong (G_{3,2}, \cdot)$$

where

$$G_{3,2} = \langle a, b : a^4 = 1,\ b^2 = a^2,\ ab = ba^3 \rangle,$$

because $q = 3, m = 4$ and $t = 2$. Note $ab = ba^3 \Leftrightarrow aba = ba^4 \Leftrightarrow aba = b$. Thus

$$G_{3,2} = \langle a, b : a^4 = 1,\ b^2 = a^2,\ aba = b \rangle.$$

Moreover a presentation of the quaternion group of order 8 is given by

$$\begin{aligned} Q_8 &= \langle x, y : x^4 = 1,\ x^2 = y^2,\ y^{-1}xy = x^{-1} \rangle \\ &= \langle x, y : x^4 = 1,\ x^2 = y^2,\ xyx = y \rangle. \end{aligned}$$

Therefore $G_{3,2}$ and Q_8 have identical representations. It follows that $G_{3,2} \cong Q_8$. Thus

$$(R^*, \circ) \cong (Q_8, \cdot).$$

In contrast to field theory (knowing that the multiplication group of a finite field is always cyclic), we have the following:

Theorem 3.2.28. *[30, 26] A finite nearfield R is a Dickson nearfield if and only if $(R^*, \cdot)$ is metacyclic.*

3.2.4 Exceptional nearfields

Thirty years after Dickson's work, H. Zassenhauss fundamentally determined all finite nearfields.

Theorem 3.2.29. *[30, 26] A finite nearfield is either a finite Dickson nearfield or it is one of the 7 exceptional nearfields of order $5^2, 7^2, 11^2, 23^2, 29^2, 59^2$.*

Note that there exist two exceptional nearfields of order 11^2 (see [30] for more details). He denoted these seven exceptional nearfields as $R_i, i = 1, \ldots, 7$ with orders $5^2, 7^2, 11^2, 11^2, 23^2, 29^2, 59^2$ respectively.

Table 3.2: The 7 exceptional nearfields [30, 26].

i	p	Order of R_i	$(R_i^*, \cdot)$ is generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and
1	5	5^2	$\begin{pmatrix} 1 & -2 \\ -1 & -2 \end{pmatrix}$
2	11	11^2	$\begin{pmatrix} 1 & 5 \\ -5 & -2 \end{pmatrix}$ and $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$
3	7	7^2	$\begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$
4	23	23^2	$\begin{pmatrix} 1 & -6 \\ 12 & -2 \end{pmatrix}$ and $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$
5	11	11^2	$\begin{pmatrix} 2 & 4 \\ 1 & -3 \end{pmatrix}$
6	29	29^2	$\begin{pmatrix} 1 & -7 \\ -12 & -2 \end{pmatrix}$ and $\begin{pmatrix} -13 & 0 \\ 0 & -13 \end{pmatrix}$
7	59	59^2	$\begin{pmatrix} 9 & 15 \\ -10 & -10 \end{pmatrix}$ and $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$

3.3 The additive group of a nearfield

In this subsection one of our aims is to show that the additive group of a nearfield is always abelian. The authors of [30] first showed that the additive group of a finite nearfield is abelian. Also the author of [25] proved it for the infinite case. The author of [31] gave a new proof which differs considerably from Neuman's proof. There exists several different proofs. We will look at the simplest way to prove the additive group of a finite nearfield is abelian.

Definition 3.3.1. *([22])*

- *A p-group is a group whose order is some power of a prime p.*
- *A non-trivial p-group is one whose order is p^n for some $n \in \mathbb{N}$ and p is a prime.*

The following is well known.

Theorem 3.3.2. *([22]) Let p be a prime number. The center of any non-trivial p-group is non-trivial.*

Using Theorem 3.3.2 and based on Dickson's proof (see [10]) we have the following.

Theorem 3.3.3. *([10]) Let R be a finite nearfield. The additive group $(R,+)$ is abelian.*

Proof. It is not difficult to see that if R is a finite nearfield then $|R| = p^k$ for some $k \in \mathbb{N}$ where p is prime. It follows that $(R,+)$ is a p-group. This means that $(R,+)$ has non-trivial center by Theorem 3.3.2. It follows that there exists $y \neq 0$ such that for all $x \in R$, $y + x = x + y$. Moreover given $a, b \in R^*$, let $a' = -b + a + b$. We would like to show $a' = a$. Now

$$\begin{aligned} a' = -b + a + b &\Rightarrow b + a' = a + b \\ &\Rightarrow (b + a') \cdot (b^{-1}y) = (a + b) \cdot (b^{-1}y) \\ &\Rightarrow bb^{-1}y + a'b^{-1}y = ab^{-1}y + bb^{-1}y \\ &\Rightarrow y + a'b^{-1}y = ab^{-1}y + y. \end{aligned}$$

Since y is in the center, $y + a'b^{-1}y = ab^{-1}y + y = y + ab^{-1}y$. So

$$\begin{aligned} y + a'b^{-1}y = y + ab^{-1}y &\Rightarrow a'b^{-1}y = ab^{-1}y \\ &\Rightarrow a'b^{-1} = ab^{-1} \\ &\Rightarrow a' = a \\ &\Rightarrow -b + a + b = a \\ &\Rightarrow (b - b) + a + b = b + a \\ &\Rightarrow a + b = b + a. \end{aligned}$$

Thus $(R,+)$ is abelian. □

3.4 The center of a finite Dickson nearfield

In 1964 E. Ellers and H. Karzel showed that $C(R) = D(R) \cong \mathbb{F}_q$ where R is a finite Dickson nearfield that arises from the Dickson pair (q, n) (see Theorem 3.2.23). 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 $C(R) = \mathbb{F}_q$.

The following is well known.

Theorem 3.4.1. *([22]) If $K \subseteq F$ is a field extension (i.e., K is a subfield of F), then F is a vector space over K.*

Corollary 3.4.2. *([22]) If $K \subseteq F$ is a field extension and F is finite, then $|F| = |K|^n$ for some $n \in \mathbb{N}$.*

Lemma 3.4.3. *([22]) A polynomial equation of degree n has at most n roots over any field.*

Furthermore,

Lemma 3.4.4. *([22]) The set of elements fixed by a field automorphism is a field.*

Lemma 3.4.5. *([22]) The subfields of $\mathbb{F}_{p^m}$ are precisely those $\mathbb{F}_{p^t}$ where $t \mid m$ and they are unique. Furthermore, they are the fields fixed by the automorphism $\psi^t : x \mapsto x^{p^t}$.*

Given a Dickson pair $(q = p^l, n)$, let φ denote the appropriate power of the Frobenius automorphism of $\mathbb{F}_{q^n}$ i.e, $\varphi = \psi^l$ where ψ is the Frobenius autormorphism of $\mathbb{F}_{p^{ln}}$. We now deduce the following:

Theorem 3.4.6. *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 $\mathbb{F}_{q^n}^*$ 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*

$$\mathbb{F}_q \subseteq C(R).$$

Proof. By Lemma 3.4.5, $\mathbb{F}_q$ is the solution set to the equation $x^q - x = 0$ in $\mathbb{F}_{q^n}$. Let g be a generator of $\mathbb{F}_{q^n}^*$ and take $x \in \mathbb{F}_q^*$ and write $x = g^j$. Since $x \in \mathbb{F}_q$, $x^q = x$, i.e., $x^{q-1} = 1$. Then $\left(g^j\right)^{q-1} = 1$, i.e., $g^{j(q-1)} = 1$. Thus $|g| = q^n - 1$ divides $j(q-1)$, i.e., $[n]_q \mid j$. Thus $\mathbb{F}_q^* \subseteq \langle g^{[n]_q} \rangle$ (see in the proof of Theorem 3.2.24). Since $n \mid [n]_q$ then $\langle g^{[n]_q} \rangle$ is a subset of $\langle g^n \rangle$. Thus we have $\mathbb{F}_q^* \subseteq H$. Note that we also see this by Theorem 3.2.24. Furthermore for $x \in \mathbb{F}_q^*$, $x \in H = g^{[n]_q} H$. So 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 $x \in \mathbb{F}_q$ then $\varphi(x) = x^q = x$. Thus $\varphi^l(x) = x$ and

$$t \circ x = t \cdot \phi_t(x) = t \cdot \varphi^l(x) = t \cdot x = x \cdot t.$$

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 3.4.7. *([22]) Let F be a finite field of order p^n with characteristic p where p is prime. We have $(a+b)^{p^m} = a^{p^m} + b^{p^m}$ for all $a, b \in F$ and $m \in \mathbb{N}$.*

We have the following.

Lemma 3.4.8. *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 $\mathbb{F}_{q^n}^*$. 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 $\left(g^n\right)^{p^f} = g^n$. 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

$$\begin{aligned} x^{p^f} &= \Big(\sum_{i\in I} a_i g^{nb_i}\Big)^{p^f} \\ &= \sum_{i\in I} (a_i g^{nb_i})^{p^f} \quad \text{by Theorem 3.4.7} \\ &= \sum_{i\in I} a_i^{p^f} \left((g^n)^{p^f}\right)^{b_i} \\ &= \sum_{i\in I} a_i g^{nb_i} \\ &= x. \end{aligned}$$

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,

$$g^{n(p^f-1)} = 1,$$

hence

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

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

$$p^{ln} - 1 \mid n(p^f - 1) \Rightarrow p^{ln} - 1 \leq n(p^f - 1) \leq n(p^{\frac{ln}{2}} - 1).$$

Dividing by $p^{\frac{ln}{2}} - 1$, we get

$$p^{\frac{ln}{2}} + 1 \leq n,$$

but

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

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

Theorem 3.4.9. *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 $\mathbb{F}_{q^n}^*$ 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 ψ, the Frobenius map, ϕ_x fixes $\mathbb{F}_p$. Therefore ϕ_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 3.4.8, ϕ_x fixes $\mathbb{F}_{q^n}$. Thus $\phi_x = id$. Now take $t = g \in g^{[1]_q}H$, 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 $t \circ x = x \circ t \Leftrightarrow g \cdot \varphi(x) = x \cdot g \Leftrightarrow \varphi(x) = x \Leftrightarrow x^q = x$. So $x \in \mathbb{F}_q$.

□

By Theorem 3.4.6 and Theorem 3.4.9, we have shown that $C(R) = \mathbb{F}_q$ where $R \in DN(q, n)$.

3.5 Concluding comments

We suggest as future work to investigate all the automorphisms of a finite Dickson nearfield.

Chapter 4

The R-subgroups and subspaces of Beidleman near-vector spaces

4.1 Introduction

The first notion of near-vector spaces was introduced by J.C. Beidleman in 1966 [5]. Subsequently, several researchers like H. Wähling, J. André, and H. Karzel introduced a similar notion in different ways. André near-vector spaces have been studied in many papers (for example [3, 16, 17]). In this Chapter, we add to the theory of near-vector spaces originally defined by J.C. Beidleman. As in [17] for André near-vector spaces, we investigate the subspace structure of Beidleman near-vector spaces and highlight differences and similarities between these two types of near-vector spaces. In Section 4.3 we introduce the concepts of $gen(v_1, \ldots, v_k)$, which is the smallest R-subgroup containing the vectors $v_1, \ldots, v_k \in R^m$, the R-row space of a matrix, R-linear combinations of a finite set of vectors. Our goal is to describe the R-subgroups of R^m where m is a positive integer. We develop an algorithm (*EGE*), which is explained in the proof of Theorem 4.3.14. In Section 4.4 we give a further algorithm called the *Adjustment of the EGE algorithm (AEGE)*. The proofs of Theorem 4.4.1 and Corollary 4.4.4 explain the classification of the subspaces of R^m. In Section 4.5 we introduce the notions of R-dimension, R-basis, seed set and seed number of an R-subgroup. We investigate these new concepts and find some properties. We find the possible value of R-dimension for a given value of seed number.

4.2 The subspace structure of Beidleman near-vector spaces

In this section we investigate some properties of the subspace structure of Beidleman near-vector spaces. We find that with regard to subspace structure, André near-vector spaces are closest to traditional vector spaces.
As with André near-vector spaces, we deduce the following.

Lemma 4.2.1. *Let M_R be a Beidleman near-vector space. Then $(M,+)$ is abelian.*

Proof. If M_R is of finite dimension then by Theorem 2.5.2, $M_R \cong R^n$ where $\dim M_R = n$. Since R is a nearfield, by Theorem 2.2.4 $(R,+)$ is abelian. It follows that $(R^n,+)$ is abelian. Hence $(M,+)$ is abelian. If M is of infinite dimension, $M \cong R^{dimM}$. So $(M,+)$ is abelian. □

Definition 4.2.2. *([5]) Let M_R be a Beidleman near-vector space. A non-empty subset N of M_R is a subspace of M_R if and only if N is a submodule of M_R.*

Appealing to Lemma 4.2.1, Definition 4.2.2 is equivalent to the following.

Definition 4.2.3. *Let M_R be a Beidleman near-vector space. $\emptyset \neq N \subset M$ is a subspace of M_R if*

(i) $(N,+)$ *is a subgroup of* $(M_R,+)$,

(ii) $(m+n)r - mr \in N$ *for all* $m \in M, n \in N$ *and* $r \in R$.

Remark 4.2.4. *Let M_R be a Beidleman near-vector space.*

- *According to [5], $(N,+)$ should be a normal subgroup of $(M,+)$. But since $(M,+)$ is abelian, we do not need the normality again.*
- *A non-empty subset of M_R which is itself a Beidleman near-vector space is either a subspace or an R-subgroup of M_R. In the next section we will see that in the case of finite-dimensional Beidleman near-vector spaces, every R-subgroup of R^m is itself a Beidleman near-vector space (see Corollary 4.3.16).*

Lemma 4.2.5. *Let M_R be a Beidleman near-vector space. Let M_1 and M_2 be subspaces of M. Then $M_1 \cap M_2$ is also subspace of M.*

Proof. It is not difficult to see that $(M_1 \cap M_2, +)$ is a subgroup of $(M, +)$. Let $m \in M, n \in M_1 \cap M_2$ and $r \in R$. Then $(m+n)r - mr \in M_1$ and $(m+n)r - mr \in M_2$. Thus $(m+n)r - mr \in M_1 \cap M_2$. □

By Lemma 4.2.1, we now deduce the following.

Lemma 4.2.6. *Let M_R be a Beidleman near-vector space. Let M_1 and M_2 be subspaces of M. Then $M_1 + M_2$ is also a subspace of M where $M_1 + M_2 = \{m_1 + m_2 : m_1 \in M_1, m_2 \in M_2\}$.*

Proof.

i. Let $l, l' \in M_1 + M_2$ such that $l = m_1 + m_2$ and $l' = m_1' + m_2'$ for some $m_1, m_1' \in M_1, m_2, m_2' \in M_2$. We have $l - l' = (m_1 - m_2) + (m_1' - m_2') \in M_1 + M_2$. So $(M_1 + M_2, +)$ is a subgroup of $(M, +)$.

ii. Let $m \in M, l \in M_1 + M_2$ and $r \in R$. Then $l = m_1 + m_2$ for some $m_1 \in M_1$ and $m_2 \in M_2$. We have

$$\begin{aligned}(m+l)r - mr &= (m + m_1 + m_2)r - mr \\ &= \big((m + m_1) + m_2\big)r - mr \\ &= \big((m + m_1) + m_2\big)r - (m + m_1)r + (m + m_1)r - mr.\end{aligned}$$

Since $\big((m + m_1) + m_2\big)r - (m + m_1)r \in M_2$, $(m + m_1)r - mr \in M_1$ and $(M, +)$ is abelian it follows that $(m+l)r - mr \in M_1 + M_2$.

□

For vector spaces and André near-vector spaces, a non-empty subset is a subspace if and only if it is closed under addition and scalar multiplication [17]. For a Beidleman near-vector space we only have

Lemma 4.2.7. *If $\emptyset \neq N_R$ is a subspace of M_R then N_R is closed under addition and scalar multiplication.*

Proof. If N_R is a subspace of M_R, then $(N_R, +)$ is a subgroup of $(M_R, +)$ and for all $m \in M, r \in R, n \in N$ we have $(m+n)r - mr \in N$. In particular for $m = 0$, we obtain that $nr \in R$. □

By Definition 2.2.8 an R-subgroup S of R^m is a subgroup of $(R^m, +)$ that is closed under scalar multiplication. Note that every subspace is an R-subgroup but being closed under addition and scalar multiplication does not in general give a subspace. We now provide a counter example.

Example 4.2.8. *Appealing to Example 3.2.16 and Table 3.1, let us consider* $R \in DN(3,2)$ *to be a finite Dickson nearfield that arises from the Dickson pair* $(3,2)$. *Then* (R^2, R) *is a Beidleman near-vector space. Let us consider*

$$T = \{(1,x)r \ : \ r \in R\} = \langle (1,x) \rangle.$$

Note that T *is an* R*-subgroup of* R^2 *but not a subspace of* R^2. *Indeed by Example 3.2.16, we have* $(1, x+1) \in R^2, (1,x) \in T$ *and* $x \in R$. *We have*

$$\begin{aligned}((1,x+1)+(1,x)) \circ x - (1,x+1) \circ x &= (x, (2x+1) \circ x - (x+1) \circ x) \\ &= (x,1) \notin T,\end{aligned}$$

where " $\circ$ *" is the multiplication for* $DN(3,2)$. *Hence* T *is not a subspace of* R^2.

4.3 Classification of the R-subgroups of R^m

Let R be a nearfield. In particular if $(R, +, \circ, 0, 1)$ is a finite Dickson nearfield for the Dickson pair (q,n) with $n > 1$ then we know that the distributive elements of R form a subfield of size q. Also, not all elements are distributive, thus there are elements $\lambda \in R$ such that $(\alpha+\beta) \circ \lambda \neq \alpha \circ \lambda + \beta \circ \lambda$ for some $\alpha, \beta \in R$. From now on, we shall simply use concatenation instead of $\circ$.
Consider the nearring module R^m over R (for some fixed $m \in \mathbb{N}$) with component-wise addition and scalar multiplication $R^m \times R \to R^m$ given by $(x_1, x_2, \ldots, x_m)r = (x_1 r, x_2 r, \ldots, x_m r)$ for $(x_1, x_2, \ldots, x_m) \in R^m$.
Let $v_1, v_2, \ldots, v_k \in R^m$ be a finite number of vectors. The smallest subspace of R^m containing $\{v_1, v_2, \ldots, v_k\}$ is called the *span* of $v_1, v_2, \ldots, v_k$ and is denoted by $span(v_1, \ldots, v_k)$. In analogy to span, we introduce the notion of *gen*.

Definition 4.3.1. *Let* R *be a nearfield and* $v_1, v_2, \ldots, v_k \in R^m$ *(for some* $k \in \mathbb{N}$*) be a finite number of vectors. We define* $gen(v_1, \ldots, v_k)$ *to be the smallest* R*-subgroup of* R^m *containing* $\{v_1, v_2, \ldots, v_k\}$.

Our first aim is to find an explicit description of $gen(v_1, \ldots, v_k)$.
Let $LC_0(v_1, v_2, \ldots, v_k) := \{v_1, v_2, ..., v_k\}$ and for $n \geq 0$, let LC_{n+1} be the set of all linear combinations of elements in $LC_n(v_1, v_2, \ldots, v_k)$, i.e.

$$LC_{n+1}(v_1, v_2, \ldots, v_k) = \left\{ \sum_{w \in LC_n} w\lambda_w : \lambda_w \in R \ \forall w \in LC_n \right\}.$$

We will denote $LC_n(v_1, v_2, \ldots, v_k)$ by LC_n for short when there is no ambiguity with regard to the initial set of vectors.

Theorem 4.3.2. *Let R be a finite nearfield and $v_1, v_2, \ldots, v_k \in R^m$. We have*

$$gen(v_1, \ldots, v_k) = \bigcup_{i=0}^{\infty} LC_i.$$

Proof. We need to show that $\bigcup_{i=0}^{\infty} LC_i$ is an R-subgroup of R^m and for any R-subgroup S containing $v_1, v_2, ..., v_k$, we have $\bigcup_{i=0}^{\infty} LC_i \subseteq S$.
The zero vector 0_{R^m} of $(R^m, +)$ is an element of $\bigcup_{i=0}^{\infty} LC_i$. Let $x, y \in \bigcup_{i=0}^{\infty} LC_i$. We distinguish three cases:

- Case 1: $x, y \in LC_n$ for some $n \in \mathbb{N}$. So $x - y \in LC_{n+1}$.
- Case 2: $x \in LC_k$ and $y \in LC_n$ for some $k < n$. Since $k < n$, we have $LC_k \subseteq LC_n$ by definition. Hence $x - y \in LC_n$.
- Case 3: $x \in LC_k$ and $y \in LC_n$ for some $k > n$. We have $LC_n \subseteq LC_k$. Hence $x - y \in LC_k$.

  So $x - y \in \bigcup_{i=0}^{\infty} LC_i$.

Therefore $\left(\bigcup_{i=0}^{\infty} LC_i, +\right)$ is a subgroup of $\left(R^n, +\right)$. Let $x \in \bigcup_{i=0}^{\infty} LC_i$ and $r \in R$. Then $x \in LC_n$ for some $n \in \mathbb{N}$. For $n = 0$, $x = v_i$ for some $i \in \{1, \ldots, k\}$, so $v_i r \in LC_1$. For $n \geq 1$, we have $x = \sum_{w \in LC_{n-1}} w\lambda_w$, and thus

$$xr = \Big(\sum_{w \in LC_{n-1}} w\lambda_w\Big)r \in LC_n$$

It remains to show that for any R-subgroup S containing $v_1, \ldots, v_k$ we have $\bigcup_{i=0}^{\infty} LC_i \subseteq S$. It is sufficient to show that for all $n \in \mathbb{N}$, $LC_n \subseteq S$. We use induction on n. For $n = 0$ we have $LC_0 \subseteq S$. Assume that $LC_k \subseteq S$ for $k \in \mathbb{N}$. Let $x \in LC_{k+1}$. Then $x = \sum_{w \in LC_k} w\lambda_w$, where $\lambda_w \in R$. But $w \in LC_k \subseteq S$. So $w\lambda_w \in S$ since S is a R-subgroup (closed under addition and scalar multiplication). Therefore $\sum_{w \in LC_n} w\lambda_w \in S$. Hence $x \in S$. □

In the following propositions we give some basic properties of *gen*.

Proposition 4.3.3. *Let R be a finite nearfield, $k \in \mathbb{N}$ and T be a finite set of vectors in R^m. We have,*

$$LC_n\big(LC_k(T)\big) = LC_{n+k}(T) \text{ for all } n \in \mathbb{N}.$$

The proof is not difficult and uses induction on the positive integer n.

Proposition 4.3.4. *Let R be a finite nearfield. Let S and T be finite sets of vectors of R^m. The following hold:*

(1) $S \subseteq gen(S)$,

(2) If $S \subseteq T$ *then* $gen(S) \subseteq gen(T)$,

(3) $gen(S \cap T) \subseteq gen(S) \cap gen(T)$,

(4) $gen(S) \cup gen(T) \subseteq gen(S \cup T)$,

(5) $gen\big(gen(T)\big) = gen(T)$.

Proof. (1), (2), (3) and (4) are straightforward. Indeed $gen(T) \subseteq gen\big(gen(T)\big)$. Also for all $n \in \mathbb{N}$, we have that $LC_n\big(gen(T)\big) \subseteq gen(T)$. Hence

$$gen\big(gen(T)\big) \subseteq gen(T).$$

□

We want to give a description of $gen(v_1, \ldots, v_n)$ in terms of the basis elements (which we will define later in Definition 4.5.4). In the following lemmas, we first derive analogous results of row-reduction in vector spaces. The first lemma follows directly from Theorem 4.3.2 and we state it without proof.

Lemma 4.3.5. *Let R be a finite nearfield and $v_1, \ldots, v_k \in R^m$. For any permutation σ of the indices $1, 2, ..., k$, we have*

$$gen(v_1, \ldots, v_k) = gen(v_{\sigma(1)}, \ldots, v_{\sigma(k)}).$$

We can also show that

Lemma 4.3.6. *Let R be a finite nearfield and $v_1, \ldots, v_k \in R^m$. If $\lambda \in R^*$, then*

$$gen(v_1, \ldots, v_k) = gen(v_1\lambda, \ldots, v_k).$$

Proof. Let $gen(v_1, \ldots, v_k) = \bigcup_{i=0}^{\infty} LC_i$ and $gen(v_1\lambda, \ldots, v_k) = \bigcup_{i=0}^{\infty} LC_i'$. Let $x \in \bigcup_{i=0}^{\infty} LC_i$. Then $x \in LC_n$ for some $n \in \mathbb{N}$. Clearly $LC_0 \subseteq LC_1'$ and $LC_1 = \{v_1\alpha_1 + v_2\alpha_2 + \ldots + v_k\alpha_k : \alpha_1, \ldots, \alpha_k \in R\}$. Say $x \in LC_1$. Since $\lambda \neq 0$ there exists $\lambda' \in R$ such that $\lambda\lambda' = 1$. So

$$\begin{aligned} x &= v_1\alpha_1 + v_2\alpha_2 + \ldots + v_k\alpha_k \\ &= v_1(\lambda\lambda')\alpha_1 + v_2\alpha_2 + \ldots + v_k\alpha_k \\ &= (v_1\lambda)\lambda'\alpha_1 + v_2\alpha_2 + \ldots + v_k\alpha_k. \end{aligned}$$

Then $x \in LC_1'$. Thus we see if $x \in LC_n$ for some $n \neq 0$ in the expression of x we have

$$v_1\alpha_1 = v_1 1\alpha_1 = v_1(\lambda\lambda')\alpha_1 = (v_1\lambda)(\lambda'\alpha_1).$$

Thus $x \in LC_n'$. So $x \in \bigcup_{i=0}^{\infty} LC_i'$. Thus $x \in gen(v_1\lambda, \ldots, v_k)$. Let $x \in \bigcup_{i=0}^{\infty} LC_i'$. Then $x \in LC_n'$ for some $n \in \mathbb{N}$. In fact $LC_0' = \{v_1\lambda, v_2, \ldots, v_k\}$ and we have that $LC_0' \subseteq LC_1$. Also $LC_1' = \{(v_1\lambda)\alpha_1 + v_2\alpha_2 + \ldots + v_k\alpha_k : \alpha_1, \ldots, \alpha_k \in R\}$. Let $x \in LC_1'$ then

$$\begin{aligned} x &= (v_1\lambda)\alpha_1 + v_2\alpha + \ldots + v_k\alpha_k \\ &= v_1(\lambda\alpha_1) + v_2\alpha_2 + \ldots + v_k\alpha_k. \end{aligned}$$

It follows that $x \in LC_1$. Thus we see that if $x \in LC_n'$ for some $n \neq 0$ in the expression of x we have,

$(v_1\lambda)\alpha_1 = v_1(\lambda\alpha_1)$ by the associativity of the multiplication.

It follows that $x \in LC_n$. Thus $x \in \bigcup_{i=0}^{\infty} LC_i$. Hence $x \in gen(v_1, \ldots, v_k)$. □

Lemma 4.3.7. *Let R be a finite nearfield and $v_1, \ldots, v_k \in R^m$. For any scalars $\lambda_2, \lambda_3, \ldots, \lambda_k \in R$, we have*

$$gen(v_1, \ldots, v_k) = gen(v_1 + \sum_{i=2}^{k} v_i\lambda_i, v_2, \ldots, v_k).$$

Proof. By Theorem 4.3.2 we can write

$$gen(v_1,\dots,v_k)=\bigcup_{i=0}^{\infty} LC_i \text{ and } gen(v_1+\sum_{i=2}^{k} v_i\lambda_i, v_2,\dots,v_k)=\bigcup_{i=0}^{\infty} LC_i'.$$

We have $LC_0=\{v_1,\dots,v_k\}$ and $LC_1=\{\sum_{i=1}^{k} v_i\alpha_i : \alpha_i \in R\}$. Also

$$LC_0'=\{v_1+\sum_{i=2}^{k} v_i\lambda_i, v_2,\dots,v_k\},$$
$$LC_1'=\{(v_1+\sum_{i=2}^{k} v_i\lambda_i)\beta_1+\sum_{i=2}^{k} v_i\beta_i : \lambda_i,\beta_i \in R\}.$$

We proceed by induction on i. Clearly $v_2,\dots,v_k \in LC_0' \subseteq LC_1'$. Since

$$v_1=\big(v_1+\sum_{i=2}^{k} v_i\lambda_i\big)-\sum_{i=2}^{k} v_i\lambda_i,$$

we have $v_1 \in LC_1'$. So $LC_0 \subseteq LC_1'$. Assume that $LC_m \subseteq LC_{m+1}'$ for some $m \in \mathbb{N}$. We show that $LC_{m+1} \subseteq LC_{m+2}'$. Let $x \in LC_{m+1}$. Then

$$x=\sum_{w\in LC_m} w\lambda_w=\sum_{w\in LC_{m+1}'} w\lambda_w \text{ where } \lambda_w=0\ \forall w \in LC_{m+1}'\backslash LC_m.$$

It follows that $x \in LC_{m+2}'$. For the other inclusion, we also argue by induction. Clearly $v_2,\dots,v_k \in LC_1$ and $v_1+\sum_{i=2}^{k} v_i\lambda_i \in LC_1$, so $LC_0' \subseteq LC_1$. Let $x \in LC_1'$. Then $x=\big(v_1+\sum_{i=2}^{k} v_i\lambda_i\big)\beta_1+\sum_{i=2}^{k} v_i\beta_i$. Then $x \in LC_2$. Assume that $LC_m' \subseteq LC_{m+1}$ for some $m \in \mathbb{N}$. We need to show that $LC_{m+1}' \subseteq LC_{m+2}$. Let $x \in LC_{m+1}'$. So $x=\sum_{w\in LC_m'} w\lambda_w=\sum_{w\in LC_{m+1}} w\lambda_w$. Hence $x \in LC_{m+2}$. □

We need one more lemma which follows directly from Theorem 4.3.2.

Lemma 4.3.8. *Let R be a finite nearfield and $v_1,\dots,v_k \in R^m$. If $w \in gen(v_1,\dots,v_k)$, then*

$$gen(v_1,\dots,v_k)=gen(w,v_1,v_2,\dots,v_k).$$

Proof. By Theorem 4.3.2, let us assume that

$$gen(v_1,\dots,v_k)=\bigcup_{i=0}^{\infty} LC_i \text{ and } gen(w,v_1,v_2,\dots,v_k)=\bigcup_{i=0}^{\infty} LC_i'.$$

We have $LC_0 = \{v_1, \ldots, v_k\}$ and $LC_1 = \{\sum_{i=1}^{k} v_i\alpha_i | \alpha_i \in R\}$.
Also $LC_0' = \{w, v_1, v_2, \ldots, v_k\}$ and $LC_1' = \{w\alpha + \sum_{i=1}^{k} v_i\alpha_i | \alpha, \alpha_i \in R\}$.
Let $x \in LC_0$. Clearly $x \in LC_0'$. Assume that $LC_p \subseteq LC_p'$ for $p \in \mathbb{N}$. It is not difficult to show that $LC_{p+1} \subseteq LC_{p+1}'$.
For the other inclusion, let $x \in LC_0'$. Then $x \in LC_n$ because $w \in LC_n$ and $v_1, \ldots, v_k \in LC_1 \subseteq LC_n$. Let $x \in LC_1'$. Then $x = w\alpha + \sum_{i=1}^{k} v_i\alpha_i$. But $w \in LC_n, w\alpha \in LC_{n+1}$ and $\sum_{i=1}^{k} v_i\alpha_i \in LC_1 \subseteq LC_{n+1}$. So $x \in LC_{n+1}$. Thus we see that if $x \in LC_n'$ then $x \in LC_{n+n}$. □

By Lemmas 4.3.5, 4.3.6, 4.3.7 and 4.3.8, we deduce that, given a set of row vectors $v_1, \ldots, v_k$ in R^m, arranged in a matrix V of size $k \times m$, $gen(v_1, \ldots, v_k)$ constructed from the matrix V does not change under elementary row operations (swopping rows, scaling rows, adding multiples of a row to another). Recall that two matrices are said to be row equivalent if one can be changed to the other by a sequence of elementary row operations.

Lemma 4.3.9. *Suppose that $k \times m$ matrices $V = \begin{bmatrix} v_1 \\ \vdots \\ v_k \end{bmatrix}$ and $W = \begin{bmatrix} w_1 \\ \vdots \\ w_k \end{bmatrix}$ are row equivalent (with the rows $v_1, \ldots, v_k, w_1, \ldots, w_k \in R^m$). Then*

$$gen(v_1, \ldots, v_k) = gen(w_1, \ldots, w_k)$$

Proof. This proof follows from Lemmas 4.3.5, 4.3.6, 4.3.7 and 4.3.8. □

We will use $\{v_1, \ldots, \hat{v_i}, \ldots, v_k\}$ to indicate that the vector v_i has been removed from the set of vectors $\{v_1, \ldots, v_k\}$.

Definition 4.3.10. *Let M_R be a Beidleman near-vector space and $V = \{v_1, \ldots, v_k\}$ be a finite set of vectors of M_R. We say V is R-linearly dependent if there exists $v_i \in V$ such that $v_i \in gen(v_1, \ldots, \hat{v_i}, \ldots, v_k)$. We say that V is R-linearly independent if it is not R-linearly dependent.*

Definition 4.3.11. *Let $v_1, \ldots, v_k, v \in R^m$. Then v is called an R-linear combination of $v_1, \ldots, v_k \in R^m$ if $v \in gen(v_1, \ldots, v_k)$. Furthermore, v is called an p-linear combination of $v_1, \ldots, v_k \in R^m$ if $v \in LC_p(v_1, \ldots, v_k)$.*

Remark 4.3.12.

- *Let $w \in R^m$. We know that w is a linear combination of some finite set of vectors $v_1, \ldots, v_k \in R^m$ if $w \in LC_1(v_1, \ldots, v_k)$. However an R-linear combination is defined to make a difference to the traditional notion of linear combination.*

- *A matrix V consisting of the rows $v_1, \ldots, v_k \in R^m$ will be denoted by $V = (v_i^j)_{\substack{1 \leq i \leq k \\ 1 \leq j \leq m}}$ where v_i^j is always the j-th entry of v_i.*

Definition 4.3.13. *The R-row space of a matrix is the set of all possible R-linear combinations of its row vectors.*

Thus the R-row space of a given matrix M is the same as the *gen* of the rows of M. We now turn to the classification of the smallest R-subgroup containing a given set of vectors in R^m, the main result of this section.

Theorem 4.3.14. *Let R be a proper nearfield and $v_1, \ldots, v_k$ be vectors in R^m. Then*

$$gen(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} u_i R,$$

where the u_i (obtained from v_i by an explicit procedure) for $i \in \{1, \ldots, k'\}$ are the rows of a matrix $U = (u_i^j) \in R^{k' \times m}$ each of whose columns has at most one non-zero entry.

Proof. Given a set of vectors $v_1, \ldots, v_k \in R^m$, arrange them in a matrix V whose i-th row is v_i. Say $V = (v_i^j)_{\substack{1 \leq i \leq k \\ 1 \leq j \leq m}}$. Then $gen(v_1, \ldots, v_k)$ is the R-row space of V, which is an R-subgroup of R^m. We can then do the usual Gaussian elimination on the rows. According to Lemma 4.3.9, the *gen* of the rows of V will remain unchanged under each row operation (swapping rows, scaling rows, adding multiples of a row to another). When the algorithm terminates, we obtain a matrix $W \in R^{k \times m}$ in reduced row-echelon form. Let the non-zero rows of W be denoted by $w_1, w_2, \ldots, w_t$ where $t \leq k$.
Case 1: Suppose that every column has at most one non-zero entry. Then

$$gen(v_1, \ldots, v_k) = gen(w_1, \ldots, w_t) = w_1 R + w_2 R + \cdots + w_t R,$$

where the sum is direct. In this case we are done.
Case 2: Suppose that the j-th column is the first column that has at least 2 non-zero entries. Let p be the number of non-zero entries it has, say $w_r^j \neq$

$0 \neq w_s^j$, with $r < s$, are the first two non-zero entries (we necessarily have $r, s \leq j$) where w_r^j is the j-th entry of row w_r and w_s^j the j-th entry of row w_s. Let

$$(\alpha, \beta, \lambda) \in R^3 \text{ such that } (\alpha + \beta)\lambda \neq \alpha\lambda + \beta\lambda. \tag{4.3.1}$$

We apply what we will call the *distributivity trick*:
Let $\alpha' = (w_r^j)^{-1}\alpha$ and $\beta' = (w_s^j)^{-1}\beta$. Then form a new row

$$\theta = (w_r\alpha' + w_s\beta')\lambda - w_r(\alpha'\lambda) - w_s(\beta'\lambda).$$

Since $\theta \in LC_2(w_r, w_s)$ we have $\theta \in gen(w_1, \ldots, w_t)$.
For $1 \leq l < j$, either w_r^l or w_s^l is zero because the j-th column is the first column that has two non-zero entries, thus $\theta^l = 0$. Note that by the choice of α, β, λ, we have

$$\begin{aligned}\theta^j &= (w_r^j\alpha' + w_s^j\beta')\lambda - (w_r^j\alpha')\lambda - (w_s^j\beta')\lambda \\ &= \big(w_r^j(w_r^j)^{-1}\alpha + w_s^j(w_s^j)^{-1}\beta\big)\lambda - \big(w_r^j(w_r^j)^{-1}\alpha\big)\lambda - \big(w_s^j(w_s^j)^{-1}\beta\big)\lambda \\ &= (\alpha + \beta)\lambda - \alpha\lambda - \beta\lambda \neq 0.\end{aligned}$$

It follows that $\theta^j \neq 0$. Hence $\theta = (0, \ldots, 0, \theta^j, \theta^{j+1}, \ldots, \theta^n)$. We now multiply the row θ by $(\theta^j)^{-1}$, obtaining the row

$$\phi = (0, \ldots, 0, 1, \theta^{j+1}(\theta^j)^{-1}, \ldots, \theta^n(\theta^j)^{-1}) \in gen(w_1, \ldots, w_k)$$

where $\phi^j = 1$ is the pivot that we have created.
As a next step, we form a new matrix of size $(t+1) \times m$ by adding ϕ to the rows $w_1, \ldots, w_t$ (just after the row w_s). In this augmented matrix we replace the rows w_r, w_s with $y_r = w_r - (w_r^j)\phi, y_s = w_r - (w_s^j)\phi$, respectively. This yields another new matrix composed of the rows

$$w_1, \ldots, w_{r-1}, y_r, \ldots, y_s, \phi, w_{s+1}, \ldots, w_t$$

which has $p - 1$ non-zero entries in the j-th column. By Lemma 4.3.9, the *gen* of the rows of the augmented matrix is the *gen* of the rows of W (which in turn is $gen(v_1, \ldots, v_k)$). Hence,

$$\begin{aligned}gen(v_1, \ldots, v_k) &= gen(w_1, \ldots, w_r, \ldots, w_s, \ldots, w_t) \\ &= gen(w_1, \ldots, y_r, \ldots, y_s, \phi, \ldots, w_t).\end{aligned}$$

We keep repeating the *distributivity trick* on the j-th column until we form another new matrix which has only one non-zero entry in the j-th column. By continuing this process, we can eliminate all columns with more than one non-zero entry. Let the final matrix have rows $u_1, u_2, \ldots, u_{k'}$. Then

$$\begin{aligned} gen(v_1, \ldots, v_k) &= gen(w_1, \ldots, w_t) \\ &= gen(u_1, \ldots, u_{k'}) \\ &= u_1R + u_2R + \ldots + u_{k'}R, \end{aligned}$$

where the sum is direct.

□

Remark 4.3.15. *The procedure described in the proof of Theorem 4.3.14 will be called Expanded Gaussian Elimination (EGE algorithm).*

Corollary 4.3.16. *Let R be a proper nearfield. Every R-subgroup of R^m is a Beidleman near-vector space.*

Proof. By Theorem 4.3.14 every R-subgroup of R^m is isomorphic to R^k for some k. Note that R^k is a strictly semi-simple nearring module over R. □

Example 4.3.17. *Appealing to Example 3.2.16 and Table 3.1, let us consider $R \in DN(3,2)$ to be the finite Dickson nearfield that arises from the pair $(3,2)$ and $v_1 = (1, x, 1, 2x+2, 1), v_2 = (x, 2x, x, 0, x), v_3 = (1, x+1, 1, 0, 2) \in R^5$. By Theorem 4.3.14, we have*

$$gen(v_1, v_2, v_3) = \bigoplus_{i=1}^{4} u_i R,$$

where $u_1 = (1,0,1,0,0), u_2 = (0,1,0,0,0), u_3 = (0,0,0,1,0)$ and $u_4 = (0,0,0,0,1)$. Note that $gen(v_1, v_2, v_3) = \{ (x, y, x, z, t) : \ x, y, z, t \in R \}$. Appealing to Example 4.2.8, the smallest R-subgroup containing v_1, v_2 and v_3 is not always a subspace of R^5.

One fundamental property of *gen* is the following.

Theorem 4.3.18. *Let R be a proper nearfield and $m \in \mathbb{N}$. There exists vectors $v_1, \ldots, v_{m-1}$ of R^m such that*

$$gen(v_1, \ldots, v_{m-1}) = R^m.$$

Proof. Suppose R is proper nearfield. Then there exist $\alpha_1, \alpha_2, \ldots, \alpha_{m-1} \in R$ (note that the α_i's don't necessarily need to be distinct) and $\lambda \in R$ such that $\left(\sum_{i=1}^{m-1} \alpha_i\right)\lambda \neq \sum_{i=1}^{m-1} \alpha_i\lambda$. We choose

$$v_1 = (1,1,0,0,\ldots,0), v_2 = (1,0,1,0,\ldots,0), \ldots, v_{n-1} = (1,0,0,\ldots,0,1) \in R^m.$$

Then

$$\begin{aligned} v = ((1,1,0,0,\ldots,0)\alpha_1 + (1,0,1,0,\ldots,0)\alpha_2 + \ldots + (1,0,0,\ldots,0,1)\alpha_{m-1})\,\lambda - \\ (1,1,0,0,\ldots,0)\alpha_1\lambda - (1,0,1,0,\ldots,0)\alpha_2\lambda - \ldots - (1,0,0,\ldots,0,1)\alpha_{m-1}\lambda \\ = ((\alpha_1 + \alpha_2 + \ldots + \alpha_{m-1})\lambda - \alpha_1\lambda - \alpha_2\lambda - \ldots - \alpha_{m-1}\lambda, 0, 0, \ldots, 0) \\ = (\gamma, 0, 0, \ldots, 0) \end{aligned}$$

where $\gamma = (\alpha_1 + \alpha_2 + \ldots + \alpha_{m-1})\lambda - \alpha_1\lambda - \alpha_2\lambda - \cdots - \alpha_{m-1}\lambda$. So

$$v\gamma^{-1} = (1,0,0,0,\ldots,0) \in gen(v_1, v_2, \ldots, v_{m-1}).$$

Let $(x_1, x_2, x_3, \ldots, x_m) \in R^m$. Then

$$\begin{aligned} (x_1, x_2, x_3, \ldots, x_m) = v_1x_2 + v_2x_3 + \ldots + v_{m-1}x_m - v\gamma^{-1}(x_m + x_{m-1} \\ + x_{m-2} + \ldots + x_2 - x_1) \\ = v_1x_2 + v_2x_3 + \ldots v_{m-1}x_m - \\ \big((v_1\alpha_1 + v_2\alpha_2 + \ldots v_{m-1}\alpha_{m-1})\lambda \\ -v_1\alpha_1\lambda - v_2\alpha_2\lambda - \ldots - v_{m-1}\alpha_{m-1}\lambda\big)\gamma^{-1}(x_m + x_{m-1} + x_{m-2} + \ldots + x_2 - x_1). \end{aligned}$$

It follows that $(x_1, x_2, x_3, \ldots, x_m) \in LC_2(v_1, \ldots, v_{m-1})$, so $(x_1, x_2, x_3, \ldots, x_m) \in gen(v_1, \ldots, v_{m-1})$. Thus $gen(v_1, \ldots, v_{m-1}) = R^m$. □

Corollary 4.3.19. *Suppose that $gen(V) = R^m$. There exists some positive integer p such that $LC_p(V) = R^m$.*

Remark 4.3.20. *Suppose that R is a finite nearfield. By Theorem 4.3.18 there exist two vectors v_1 and v_2 such that $gen(v_1, v_2) = R^3$. By experimental computations there exist no two vectors v_1 and v_2 such that $gen(v_1, v_2)$ is the whole space R^m where $m > |R| + 1$.*

The following gives the description of $gen(v)$ for $v \in M_R$.

Lemma 4.3.21. *Let R be a nearfield and M_R be a Beidleman near-vector space. Let $v \in M$. Then $gen(v) = vR$.*

Proof. $LC_p(v) = vR$ for all positive integers p. Using Theorem 4.3.2 we have that $gen(v) = vR$. □

4.4 Classification of the subspaces of R^m

Let R be a proper nearfield. The Extended Gaussian Elimination algorithm can be used to determine the *span* of a given set of vectors, which is defined as the smallest submodule containing all the given vectors. From Example 4.2.8, we know that some R-subgroups are not necessarily subspaces of Beidleman near-vector spaces R^m. In Theorem 4.4.1 we describe the smallest subspace of R^m containing a given set of vectors. This allows us to classify all the subspaces of R^m in Corollary 4.4.4.

Theorem 4.4.1. *Let R be a proper nearfield and $v_1, \ldots, v_k$ be vectors of R^m. Then*

$$span(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k''} e_i R,$$

where e_i is a row vector with only one non-zero entry obtained from v_i by an explicit procedure.

Proof. Let $v_1, \ldots, v_k \in R^n$. Since a submodule is an R-subgroup, we have

$$gen(v_1, \ldots, v_k) \subseteq span(v_1, \ldots, v_k).$$

Note that $gen(v_1, \ldots, v_k)$ will be a subspace if $gen(v_1, \ldots, v_k) = span(v_1, \ldots, v_k)$. Let $u_1, \ldots, u_{k'}$ be determined as before in Theorem 4.3.14.

Case 1: Suppose that u_i for all $i \in \{1, \ldots, k'\}$ has only one non-zero component. Then

$$u_1R + u_2R + \ldots + u_{k'}R = R^{k'} \times \underbrace{\{0\} \times \ldots \times \{0\}}_{(m-k)\ times}$$

(up to reordering of coordinates) is a submodule of R^m, hence it is the desired span. So

$$\begin{aligned} span(v_1, \ldots, v_k) &= gen(v_1, \ldots, v_k) \\ &= \bigoplus_{i=1}^{k'} u_i R. \end{aligned}$$

Case 2: Suppose that no row has more than two non-zero entries and u_i is the first i-th row that has entries $u_i^{j_1} \neq 0 \neq u_i^{j_2}$ i.e.,

$$u_i = \left(0, \ldots, 0, u_i^{j_1}, 0, \ldots, 0, u_i^{j_2}, 0, \ldots, 0\right).$$

We apply what we will call the *"adjustment trick"*. Let $\alpha, \beta, \lambda \in R$ such that $(\alpha+\beta)\lambda \neq \alpha\lambda + \beta\lambda$. Define $\varpi \in R^m$ by $\varpi^j = \alpha\delta_{jj_2}$ for $1 \leq j \leq m$ where δ_{ij} is the Kronecker function. So

$$\varpi^j = \begin{cases} 0 \text{ if } j \neq j_2 \\ \alpha \text{ if } j = j_2 \end{cases}.$$

It follows that $\varpi = (0, \ldots, 0, \alpha, 0, \ldots, 0)$.

Define $a = u_i((u_i^{j_2})^{-1}\beta) = \big(0, \ldots, 0, u_i^{j_1}(u_i^{j_2})^{-1}\beta, 0, \ldots, 0, \beta, 0, \ldots, 0\big)$, so that $a^{j_2} = \beta$.

Then let $v \in R^m$ be defined as

$$\begin{aligned} v &= (\varpi + a)\lambda - \varpi\lambda \\ &= \big(0, \ldots, 0, u_i^{j_1}(u_i^{j_2})^{-1}\beta\lambda, 0, \ldots, 0, (\alpha+\beta)\lambda - \alpha\lambda, 0, \ldots, 0\big). \end{aligned}$$

By the additional condition on submodules, we must have

$$v \in span(u_1, \ldots, u_{k'}).$$

Hence we may add v without changing the span (it strictly increases the gen though). Note that by construction, $v \neq a\lambda$. In fact, the only non-zero entry of $v - a\lambda$ is the j_2 component. Hence we may reduce the j_2 entry of u_i to zero. Since $a \in span(u_1, \ldots, u_{k'})$,

$$\begin{aligned} v - a\lambda &= \big(0, \ldots, 0, (\alpha+\beta)\lambda - \alpha\lambda - \beta\lambda, 0, \ldots, 0\big) \\ &= \big(0, 0, \ldots, 0, \gamma, 0, \ldots, 0\big) \in span(u_1, \ldots, u_{k'}) \end{aligned}$$

where $\gamma = (\alpha+\beta)\lambda - \alpha\lambda - \beta\lambda$ is in the j_2-th position of $v - a\lambda$.

So $(v - a\lambda)\gamma^{-1} = (0, \ldots, 0, 1, 0 \ldots, 0)$ is denoted by e_{j_2} (the row that only has a non-zero entry "1" in its j_2-th column) and $e_{j_2} \in span(u_1, \ldots, u_{k'})$. Also

$$\big(u_i(u_i^{j_2})^{-1} - e_{j_2}\big)\big(u_i^{j_1}(u_i^{j_2})^{-1}\big)^{-1} = (0, \ldots, 0, u_i^{j_1}(u_i^{j_2})^{-1}, 0, \ldots, 0)\big(u_i^{j_1}(u_i^{j_2})^{-1}\big)^{-1}$$

is denoted as e_{j_1} (the row that only has a non-zero entry "1" in its j_1-th column) and $e_{j_1} \in span(u_1, \ldots, u_{k'})$. We now add the new rows e_{j_1}, e_{j_2} to the rows $u_1, \ldots, u_i, \ldots, u_{k'}$ and remove the row u_i (the span is

unchanged). We have that

$$\begin{aligned} span(v_1,\ldots,v_k) &= span(u_1,\ldots,u_i,\ldots,u_{k'}) \\ &= span(u_1,\ldots,e_{j_1},e_{j_2},u_i,\ldots,u_{k'}) \\ &= span(u_1,\ldots,e_{j_1},e_{j_2},\ldots,u_{k'}). \end{aligned}$$

Continuing the implementations of the *"adjustment trick"* on the other rows u_t (which has also two non-zero entries) where $t > i$, we may eliminate occurrences of multiple non-zero entries in the u_t while appending new vectors with only one non-zero entry to make up for them. Thus

$$\begin{aligned} span(v_1,\ldots,v_k) &= span(u_1,\ldots,u_i,\ldots,u_{k'}) \\ &= span(e_1,e_2,e_3,\ldots,e_{k''}) \\ &= \bigoplus_{i=1}^{k''} e_iR, \end{aligned}$$

where e_i is the i-th row that has a non-zero entry ″1″ in its i-th position only.

Case 3: Suppose that there exists at least one row which has more than two non-zero entries and u_i is the first i-th row with l non-zero entries where $l \geq 2$. Then continuing with the procedure in Case 2, we must apply the *"adjustment trick"* on the first two non-zero entries of u_i and repeat the procedure on the other non-zero entries. Thus we may eliminate occurrences of multiple non-zero entries in the u_i while appending new vectors with only one non-zero entry to make up for them. Hence

$$\begin{aligned} span(v_1,\ldots,v_k) &= span(u_1,\ldots,u_i,\ldots,u_{k'}) \\ &= span(u_1,\ldots,u_i,e_{j_1},e_{j_2},\ldots,e_{j_l},\ldots,u_{k'}) \\ &= span(u_1,\ldots,e_{j_1},e_{j_2},\ldots,e_{j_l},\ldots,u_{k'}) \\ &= span(e_1,e_2,e_3,\ldots,e_{k''}) \\ &= \bigoplus_{i=1}^{k''} e_iR, \end{aligned}$$

where e_i is the i-th row that has a non-zero entry ″1″ in column i only.

Thus we have proved that the span can always be written as a direct sum of vectors with only one non-zero entry.

□

Definition 4.4.2. *The row space of a given matrix M is the span of the rows of M.*

Remark 4.4.3. *Let $V \in R^{k\times m}$ be a matrix and $v_1,\ldots,v_k$ be vectors in R^m arranged in V. The smallest subspace containing $v_1,\ldots,v_k$ denoted as $span(v_1,\ldots,v_k)$ is the row space of the matrix V. Let k'' be determined as in Theorem 4.4.1. Thus the dimension of $span(v_1,\ldots,v_k)$ is k''.*

From the description of subspaces of R^m in Theorem 4.4.1 we deduce the following.

Corollary 4.4.4. *Let R be a proper nearfield. The subspaces of R^m are all of the form $S_1 \times S_2 \times \ldots \times S_m$ where $S_i = \{0\}$ or $S_i = R$ for $i = 1,\ldots,m$.*

Proof. Let S be a subspace of R^m. If $S = \{0\}$ or $S = R^m$ then S is a trivial subspace of R^m. Let $v_1 \in S \setminus \{0\}$ then $span(v_1) \subseteq S$. Let $v_2 \in S \setminus span(v_1)$ then $span(v_1, v_2) \subseteq S$. Continue this process until for $v_k \in S \setminus span(v_1,\ldots,v_{k-1})$ we have $span(v_1,\ldots,v_k) = S$. Thus by Theorem 4.4.1 S is equal to $R^{k''}$ (up to the reordering of coordinates) for $k'' \leq m$. It follows that S is of the form $S_1 \times S_2 \times \cdots \times S_m$ where $S_i = R$ for $i = 1,\ldots,k''$ and $S_i = \{0\}$ for $i = k''+1,\ldots,m$. □

Remark 4.4.5. *Let us consider $T = \{(r,r,\ldots,r) \in R^m : r \in R\}$. T is not of the form prescribed in Corollary 4.4.4. To see that T is not a subspace, let*

$$(r_1,0,\ldots,0),(r,r,\ldots,r) \in R^m \text{ and } \alpha \notin D(R).$$

Then

$$\begin{aligned}((r_1,0,\ldots,0) + (r,r,\ldots,r))\,\alpha - ((r_1,0,\ldots,0))\,\alpha \\ = \big((r_1+r)\alpha + r_1\alpha, r\alpha,\ldots,r\alpha\big).\end{aligned}$$

Since $\alpha \notin D(R)$, there exists $x,y \in R$ such that $(x+y)\alpha \neq x\alpha + y\alpha$. We choose $r_1 = x$ and $r = y$. So $(r_1+r)\alpha \neq r_1\alpha + r\alpha$ from which it follows that $(r_1+r)\alpha - r_1\alpha \neq r\alpha$. Observe that $(r_1+r)\alpha - r_1\alpha \neq r\alpha$ shows that $((r_1,0,\ldots,0) + (r,r,\ldots,r))\,\alpha - ((r_1,0,\ldots,0))\,\alpha \notin T$ and so T cannot be a subspace of R^m.

Let us illustrate Theorem 4.4.1 with the following two examples.

Example 4.4.6. *Appealing to Example 3.2.16 and Table 3.1, let us consider* $R \in DN(3,2)$ *and* $v_1, v_2, v_3 \in R^5$ *such that* $v_1 = (0,1,1,0,0), v_2 = (0, x+1, 2, 0, x+1)$ *and* $v_3 = (1, x+1, 1, 0, x)$. *By Theorem 4.3.14,*

$$gen(v_1, v_2, v_3) = u_1R \oplus u_2R \oplus u_3R \oplus u_4R,$$

where $u_1 = (1,0,0,0,0), u_2 = (0,1,0,0,0), u_3 = (0,0,1,0,0)$ *and* $u_4 = (0,0,0,0,1)$. *By Theorem 4.4.1, case 1, we have*

$$\begin{aligned} gen(v_1, v_2, v_3) &= span(v_1, v_2, v_3) \\ &= e_1R \oplus e_2R \oplus e_3R \oplus e_5R \text{ where } e_i = u_i, \text{ for } i \in \{1,2,3,5\}, \end{aligned}$$

is a subspace of R^5.

Example 4.4.7. *Appealing to Example 3.2.16 and Table 3.1, let us consider* $R \in DN(3,2)$ *and* $v_1, v_2, v_3 \in R^5$ *such that* $v_1 = (1,1,2,x+1,1), v_2 = (0,0,0,2x+2,1)$ *and* $v_3 = (1,1,1,x+2,1)$. *By Theorem 4.3.14,*

$$gen(v_1, v_2, v_3) = u_1R \oplus u_2R \oplus u_3R \oplus u_4R,$$

where $u_1 = (1,1,0,0,0), u_2 = (0,0,1,0,0), u_3 = (0,0,0,1,0)$ *and* $u_4 = (0,0,0,0,1)$. *We wish to determine* $span(v_1, v_2, v_3)$. *By Theorem 4.4.1, case 2, we may apply the "adjusted trick" to reduce* u_1. *Define* $\varpi \in R^5$ *such that*

$$\varpi^j = \begin{cases} 0 \text{ if } j \neq 1 \\ \alpha \text{ if } j = 1. \end{cases}.$$

Note that ϖ^j *denotes the j-th entry of the row* ϖ. *Let* $\alpha, \beta, \lambda \in R$ *such that* $(\alpha + \beta)\lambda \neq \alpha\lambda + \beta\lambda$. *Let* $a = u_1((u_1^1)^{-1})\beta = u_1\beta$ *and* $S = span(u_1, u_2, u_3, u_4)$. *We have*

$$\begin{aligned} (\varpi + a)\lambda - \varpi\lambda &= ((1,0,0,0,0)\alpha + (1,1,0,0,0)\beta)\,\lambda - ((1,0,0,0,0))\,\alpha\lambda \\ &= ((\alpha+\beta)\lambda - \alpha\lambda, \beta\lambda, 0, 0, 0) \in S \end{aligned}$$

and

$$\begin{aligned} ((\alpha+\beta)\lambda - \alpha\lambda, \beta\lambda, 0, 0, 0) - (\beta\lambda, \beta\lambda, 0, 0, 0) &= ((\alpha+\beta)\lambda - \alpha\lambda - \beta\lambda, 0, 0, 0, 0)) \\ &= (\gamma, 0, 0, 0, 0) \in S, \end{aligned}$$

where $\gamma = (\alpha + \beta)\lambda - \alpha\lambda - \beta\lambda$. *It follows that*

$$(\gamma, 0, 0, 0, 0)\gamma^{-1} = (1, 0, 0, 0, 0) = e_1 \in S.$$

Also

$$u_1 - e_1 = e_2 \in S.$$

Therefore

$$\begin{aligned} span(v_1, v_2, v_3) &= span(e_1, e_2, u_1, u_2, u_3, u_4) \\ &= span(e_1, e_2, u_2, u_3, u_4) \\ &= span(e_1, e_2, e_3, e_4, e_5) \\ &= \bigoplus_{i=1}^{5} e_i R \\ &= R^5 \text{ (up to the reordering of coordinates)}, \end{aligned}$$

where $u_2 = e_3, u_3 = e_4$ *and* $u_4 = e_5$.

Surprisingly, unlike traditional vector spaces, $span(v)$ for $v \in R^m$ can be the whole space.

Proposition 4.4.8. *Let* R *be a proper nearfield and* $v \in R^m$ *and* $k \leqslant m$. *Then* $span(v)$ *is* k*-dimensional if and only if* v *contains* k *non-zero entries.*

Proof. Let $V \in R^{1\times m}$ be a matrix of size $1 \times m$ whose only row is v. Suppose $span(v)$ is k-dimensional. Then after reordering the row space of the matrix V has a standard basis $\{e_1, \ldots, e_k\}$. So $span(v) = \bigoplus_{i=1}^{k} e_i R$. Then $v = \sum_{i=1}^{k} e_i r_i$ where $r_i \in R$. Thus v contains at most k non-zero entries. Conversely suppose v contains k non-zero entries. We now implement the *"adjustment trick"* (see case 3, proof of Theorem 4.4.1). Hence we eliminate occurrences of multiple non-zero entries in v while obtaining k new vectors with each containing only one non-zero entry. Thus $span(v) = \bigoplus_{i=1}^{k} e_i R$. Therefore $span(v)$ is k-dimensional. □

Corollary 4.4.9. *Let* R *be a proper nearfield and* $v \in R^m$. *Then* $span(v) = vR$ *if and only if* v *has at most one non-zero entry.*

Proof. If $span(v) = vR$ then $span(v)$ is one dimensional or zero dimensional. By Proposition 4.4.8 v must contain only one non-zero entry. Suppose v has at most one non-zero entry. By Lemma 4.3.21 $gen(v) = vR$. Thus $span(v) = gen(v) = vR$. □

In [15] the authors derived an expression that evaluates the number of k-dimensional subspaces of the finite dimensional vector space (F^m, F) where F is a finite field. In the case of the finite dimensional Beidleman near-vector space (R^m, R), where R is a finite nearfield we have that:

Proposition 4.4.10. *Let R be a proper nearfield. The number of subspaces of dimension k of R^m is* $\begin{pmatrix} m \\ k \end{pmatrix}$.

Proof. By Corollary 4.4.4 a k-dimensional subspace is equal to R^k (up to the reordering of coordinates) and $m-k$ is the number of zeros appearing in the m coordinates. Now the number of subspaces of dimension k corresponds to choosing k out of the m coordinates, hence it is $\begin{pmatrix} m \\ k \end{pmatrix}$. □

Corollary 4.4.11. *Let R be a proper nearfield. There are 2^m subspaces of R^m.*

4.5 R-dimension and seed number of R-subgroups

In this section, we will consider R to be a finite nearfield. All the results in this section make use of Theorem 4.3.14 where at each *"distributivity trick"*, a triple $(\alpha, \beta, \lambda) \in R^3$ such that

$$(\alpha + \beta) \circ \lambda \neq \alpha \circ \lambda + \beta \circ \lambda$$

is chosen within an application of the *EGE algorithm*.

4.5.1 Some properties

In this subsection, we study the notion of R-dimension and R-basis of R-subgroups.

Definition 4.5.1. *A finite set $V = \{v_1, \ldots, v_k\}$ of non-zero vectors in R^m is R-linearly dependent if there exists $v_i \in V$ such that $v_i \in gen(v_1, \ldots, \hat{v_i}, \ldots, v_k)$.*

Note that we use $\{v_1, \ldots, \hat{v_i}, \ldots, v_k\}$ to denote the fact that the vector v_i has been removed from the set of vectors $\{v_1, \ldots, v_k\}$.

Lemma 4.5.2. *Let R be a finite nearfield and $v_1, \ldots, v_k \in R^m$. Then*

$$|gen(v_1, \ldots, v_k)| = |R|^{k'}$$

where k' is the number of non-zero rows obtained after performing the EGE algorithm on the vectors $v_1, \ldots, v_k$.

Proof. By Theorem 4.3.14, we have $gen(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} u_i R$ where $U = (u_i^j) \in R^{k' \times m}$ is the final matrix after the expanded Gaussian elimination with the property that all its columns have at most one non-zero entry. Hence $|gen(v_1, \ldots, v_k)| = |\bigoplus_{i=1}^{k'} u_i R| = |u_1 R| \times |u_2 R| \times \cdots \times |u_{k'} R| = |R|^{k'}$. □

In particular, we obtain:

Corollary 4.5.3. *Let R be a finite nearfield and T an R-subgroup of R^m. Then $|T| = |R|^k$ for some $k \leq m$.*

In analogy to the notion of a basis of a subspace in the theory of vector spaces, we introduce what we will call R-basis and R-dimension of an R-subgroup of the finite dimensional Beidleman near-vector space R^m.

Definition 4.5.4. *Let R be a finite nearfield and T an R-subgroup of R^m. There exist some vectors $v_1, \ldots, v_k \in R^m$ such that $gen(v_1, \ldots, v_k) = T$. By the EGE algorithm, the finite set of non-zero row vectors $\{u_1, \ldots, u_{k'}\}$ obtained will be called an R-basis of T and the number k' will be called the R-dimension of T.*

Remark 4.5.5. *Let R be a finite nearfield. Suppose there exist $v_1, \ldots, v_k \in R^m$ and $w_1, \ldots, w_l \in R^m$ such that $gen(v_1, \ldots, v_k) = gen(w_1, \ldots, w_l) = T$. By Theorem 4.3.14 we have $gen(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} \mu_i R$ and $gen(w_1, \ldots, w_l) = \bigoplus_{i=1}^{l'} \nu_i R$ such that $(\mu_i^j)_{\substack{1 \leq i \leq k' \\ 1 \leq j \leq m}}$ and $(\nu_i^j)_{\substack{1 \leq i \leq l' \\ 1 \leq j \leq m}}$ are some matrices that have at most one non-zero entry in each column. We have, $|gen(v_1, \ldots, v_k)| = |gen(w_1, \ldots, w_l)|$. Then $|R|^{k'} = |R|^{l'}$. Thus $k' = l'$. Thus the R-dimension of T is well-defined.*

Definition 4.5.6. *Let R be a finite nearfield and T an R-subgroup of R^m. The set V generates T if $V \subseteq T$ and $gen(V) = T$.*

Definition 4.5.7. *Let R be a finite nearfield and T an R-subgroup of R^m. The set V is a seed set for T if V is R-linearly independent and V generates T.*

Definition 4.5.8. *Let R be a finite nearfield and T an R-subgroup of R^m. The seed number of T is the minimal cardinality of all the seed sets, i.e., $s(T) = \min_{V\in\mathcal{B}}\{|V|\}$, where $\mathcal{B}$ is the set of seed sets for T.*

Remark 4.5.9. *Let R be a finite nearfield and T an R-subgroup of R^m. Then the seed number $s(T)$ is well-defined. Note that for every R-subgroup T, $gen(T) = T$ (i.e., T is generated by all its elements), then $s(T) \leq |T|$. Thus $s(T)$ is well-defined.*

Lemma 4.5.10. *Let R be a finite nearfield and T an R-subgroup of R^m. Then*

$$R\text{-}\dim(T) = \max\{|V| : V \in \mathcal{B}\},$$

where $\mathcal{B}$ is the set of seed sets for T.

Proof. Let T be an R-subgroup of R^m. Suppose V is a seed set for T containing k vectors. Then $gen(V) = T$. By the *EGE algorithm* we have $gen(V) = \bigoplus_{i=1}^{k'} u_i R$ where $\left(u_i^j\right)_{\substack{1\leq i\leq k'\\ 1\leq j\leq m}}$ is a matrix that has at most one non-zero entry in each column. Knowing that V is R-linearly independent, we have the following cases:

- Case 1 : The matrix constituted by the vectors in V has exactly one non-zero entry in each column. Then $k' = k$.
- Case 2 : The matrix constituted by the vectors in V has more than one non-zero entry in some columns. So in the process of the *EGE algorithm*, we will create some additional rows. Then $k' > k$.

It follows that $k' \geq k$. Thus $R\text{-}\dim(T) \geq |V|$ and note that $R\text{-}\dim(T) \in \{|V| : V \in \mathcal{B}\}$. □

Example 4.5.11. *Let us consider the finite dimensional Beidleman near-vector space R^m over R where R is a proper finite nearfield. Suppose $m = 1$. Then $s(R) = 1$. Suppose $n = 2$. Since $gen(v) = vR$ for all $v \in R^2$, we have $s(R^2) \neq 1$. Thus $s(R^2) = 2$. Suppose $m = 3$. Let $v_1 = (1,1,0)$ and $v_2 = (1,0,1)$ in R^3 such that $gen(v_1, v_2) = gen(e_1, e_2, e_3) = R^3$ where $e_1 = (1,0,0), e_2 = (0,1,0)$ and $e_3 = (0,0,1)$. So $\{e_1, e_2, e_3\}$ and $\{v_1, v_2\}$ are some seed sets for R^3. A seed set of maximum size is $\{e_1, e_2, e_3\}$ and a seed set of minimum size is $\{v_1, v_2\}$. Thus $s(R^3) = 2$ and $R\text{-}\dim(R^3) = 3$.*

Lemma 4.5.12. *Let R be a finite nearfield and V a finite set of vectors in R^m. If $gen(V) = T$, then V contains a seed set for T.*

Proof. Let $V = \{v_1, \ldots, v_k\}$ such that $gen(V) = T$. Using Lemma 4.3.9, keep removing elements from V that do not contribute to $gen(V)$ until we find a seed set for T. Note that the order in which we remove elements matters, in the sense that the seed sets we get at the end may have different sizes. □

Lemma 4.5.13. *Let R be a finite nearfield and V a finite set of vectors in R^m such that $gen(V) = T$. Assume that the vectors in V are arranged in a matrix M of size $k \times m$. Then $s(T)$ is less than or equal to the number of pivots that we get in the reduced row echelon form of M.*

Proof. Let V be a seed set for T. Suppose V contains the vectors $v_1, \ldots, v_k \in R^m$ arranged in a matrix $M \in R^{k\times m}$. The reduced row echelon form of M gives another matrix $M' \in R^{k\times m}$ whose set of non-zero row vectors is $W = \{w_1, \ldots, w_t\}$ where $t \leq k$. By Lemma 4.3.9, we have $T = gen(V) = gen(W)$ and W is R-linearly independent. So W is also a seed set for T. If W is of minimum size then $s(T)$ is the number of elements in W which correspond to the number of pivots of $M' = RREF(M)$. Else $s(T)$ is less than the number of elements in W. □

4.5.2 Seed number of R^m

Let R be a finite nearfield and T an R-subgroup of R^m where m is a positive integer. By definition $s(T)$ is the minimum size of all seed sets of T. In the theory of vector spaces, the dimension of a subspace is at most the dimension of the entire space. Similarly, the R-dimension of an R-subgroup of R^m is at most the R-dimension of the entire space. Thus $s(T) \leq R\text{-dim}(T) \leq m$. In analogy to the theory of vector spaces we have the following.

Lemma 4.5.14. *Let $v = (v_i)_{1\leq i\leq m}, w = (w_i)_{1\leq i\leq m} \in R^m$. Suppose there exists $(v_j, w_j) = \rho(v_i, w_i)$ where $i \neq j$ and $\rho \in R$. Then by elimination of one of the pairs (v_i, w_i) or (v_j, w_j) from v and w, we obtain the new vectors $v' = (v_1, \ldots, \hat{v_i}, \ldots, v_m) \in R^{m-1}, w' = (w_1, \ldots, \hat{w_i}, \ldots, w_m) \in R^{m-1}$ or $v' = (v_1, \ldots, \hat{v_j}, \ldots, v_m) \in R^{m-1}, w' = (w_1, \ldots, \hat{w_j}, \ldots, w_m) \in R^{m-1}$ with*

$$R\text{-dim}\left(gen(v, w)\right) = R\text{-dim}\left(gen(v', w')\right).$$

Proof. Let $v = (v_i)_{1\leq i\leq m}, w = (w_i)_{1\leq i\leq m} \in R^m$ arranged in a matrix

$$V = \begin{bmatrix} v_1 & v_2 & v_3 & \dots & v_m \\ w_1 & w_2 & w_3 & \dots & w_m \end{bmatrix} \in R^{2\times m}.$$

Suppose for simplicity that

$$(v_2, w_2) = \rho(v_1, w_1) = (\rho v_1, \rho w_1) \text{ where } v_1, v_2, w_1, w_2, \rho \in R.$$

We apply the *EGE algorithm* on the set $\{v, w\}$. Note that eliminating the non-zero entries in the first column of V will also automatically eliminate the non-zero entries in the second column of V. Hence, the number of additional rows created as we apply *EGE algorithm* on $\{v, w\}$ is the same as the number of additional rows we will create when we apply the *EGE algorithm* on $\{v', w'\}$ where $v' = (v_2, \dots, v_m) \in R^{m-1}, w' = (w_2, \dots, w_m) \in R^{m-1}$. □

We now deduce the following:

Theorem 4.5.15. *Let R be a finite Dickson nearfield that arises from the Dickson pair (q, n) and T be an R-subgroup of R^m. If $s(T) = 2$, then*

$$2 \leq R\text{-}\dim(T) \leq q^n + 1.$$

Proof. Suppose T is an R-subgroup of R^m and $s(T) = 2$. Then there exist minimal generators of T denoted as $v_1 = (v_1^1, \dots, v_1^m), v_2 = (v_2^1, \dots, v_2^m)$, i.e., $gen(v_1, v_2) = T$. We arrange v_1 and v_2 in a matrix $V \in R^{2\times m}$.
Consider the pairs (v_1^i, v_2^i) with $v_1^i \neq 0 \neq v_2^i$ where $1 \leq i \leq m$. Assume there are two such pairs such that

$$v_1^j = \rho v_1^i,\ v_2^j = \rho v_2^i \text{ for } i \neq j \text{ and } \rho \in R. \tag{4.5.1}$$

Note that we may think of (v_1^j, v_2^j) as a multiple of (v_1^i, v_2^i). For simplicity, assume $i = 1, j = 2$. Thus we can write $v_1^2 = \rho v_1^1$ and $v_2^2 = \rho v_2^1$.
Now the *EGE algorithm* (in the proof of Theorem 4.3.14) returns a seed set $\{u_1, \dots, u_k\}$ (where $k = R\text{-}\dim(T)$) for T such that every column of the matrix with rows $u_1, \dots, u_k$ has at most one non-zero entry. In this process, we take R-linear combinations of the rows to form new rows, e.g., suppose we have $\alpha, \beta, \lambda \in R$ and we consider the vector $z_1 = (v_1\alpha + v_2\beta)\lambda$. So $z_1 \in LC_2(v_1, v_2)$. Then $z_1^1 = (v_1^1\alpha + v_2^1\beta)\lambda$ and

$$z_1^2 = (v_1^2\alpha + v_2^2\beta)\lambda = (\rho v_1^1\alpha + \rho v_2^1\beta)\lambda = \rho(v_1^1\alpha + v_2^1\beta)\lambda = \rho z_1^1.$$

Thus every vector created in this manner satisfies $z_1^2 = \rho z_1^1$. In fact for $z_1 \in LC_m(v_1, v_2)$ where m is a positive integer, we will still have that $z_1^2 = \rho z_1^1$. At the end of the expanded Gaussian elimination, u_1 is an R-linear combination of v_1 and v_2, so we will have $u_1^1 = 1, u_1^2 = \rho$ where the column is indicated by the super-script.
Furthermore, if $v_1^i = 0$ or $v_2^i = 0$ then the pair $(v_1^i, v_2^i) = (0, v_2^i) = v_2^i(0,1)$ or $(v_1^i, v_2^i) = (v_1^i, 0) = v_1^i(1,0)$. Else $v_1^i \neq 0 \neq v_2^i$ then
$(v_1^i, v_2^i) = v_1^i(1, (v_1^i)^{-1} v_2^i) = v_1^i(1, r)$ where $r = (v_1^i)^{-1} v_2^i$. So we can write any pair as a multiple of one of the following pairs : $(1,0), (0,1)$ or $(1,r)$ for $r \in R^*$. Using Lemma 4.5.14, we note that

$$R\text{-dim}\left(gen(v_1, v_2)\right) = R\text{-dim}\left(gen(w_1, w_2)\right)$$

for some pairs (v_1^i, v_2^i) and (w_1^i, w_2^i) not satisfying the above condition (4.5.1), and

$$(w_1^i, w_2^i) = \rho(v_1^j, v_2^j) \text{ for some } i, j \text{ and } \rho \in R.$$

Furthermore, also by Lemma 4.5.14, for any two pairs (v_1^i, v_2^i) and (v_1^j, v_2^j) for $i \neq j$ satisfying the above condition (4.5.1), we may eliminate one of them without changing the R-dimension of the R-subgroup generated by v_1, v_2. Hence the R-dimension of T cannot exceed the maximal number of pairs where we can not eliminate any other pairs of the form $(1,0), (0,1)$ or $(1,r)$ for $r \in R^*$. Thus

$$\max_{v_1, v_2 \in R^m} \left\{R\text{-dim}\left(gen(v_1, v_2)\right)\right\} = 2 + (|R| - 1) = 1 + |R| = q^n + 1.$$

□

Example 4.5.16. *Appealing to Example 3.2.16 and Table 3.1, let us consider $R \in DN(3,2)$ to be the finite Dickson nearfield that arises from the pair $(3,2)$. Let $v = (x+2, x+1, 1, 1, 2x+1, x+1, 2, 0, 2x+1, 2x+2, x+2, 2x, 2x+1, 2x+2, x+1, x+2, 2x+1, 2x+2, x+1)$ and $w = (2x, 2, 1, 2x+2, 0, 2x, 2, 2x, 2x+1, x+1, 0, 2x+1, 1, x+1, 2x+2, 2x+2, 2x+2, 2x+2, x+1) \in R^{19}$. Then $T = gen(v, w)$ is an R-subgroup of R^{19} and we have $R\text{-dim}(T) = 10$.*

Remark 4.5.17. *In contrast to the theory of vector spaces, the following does not always hold: $R\text{-dim}\left(gen(v_1, \ldots, v_k)\right) = R\text{-dim}\left(gen(w_1, \ldots, w_m)\right)$ where a matrix $V \in R^{k \times m}$ contains the rows $v_1, \ldots, v_k$ and the columns $w_1, \ldots, w_m$. To see*

this, suppose $R \in DN(3,2)$ *(from Example 3.2.16). Let* $v_1 = (1,2,x,0,0), v_2 = (0,0,0,1,0), v_3 = (1,0,0,0,1)$ *and* $w_1 = \begin{bmatrix}1\\0\\1\end{bmatrix}, w_2 = \begin{bmatrix}2\\0\\0\end{bmatrix}, w_3 = \begin{bmatrix}x\\0\\0\end{bmatrix}$, $w_4 = \begin{bmatrix}0\\1\\0\end{bmatrix}, w_5 = \begin{bmatrix}0\\0\\1\end{bmatrix}$. *In fact*

$$R\text{-dim}\left(gen(v_1,v_2,v_3)\right) = 4 \text{ and } R\text{-dim}\left(gen(w_1,w_2,w_3,w_4,w_5)\right) = 3.$$

In the next theorem we shall determine the seed number of the finite dimensional Beidleman near-vector space R^m where R is a finite Dickson nearfield and m is not too large. This is accomplished by finding two vectors $v, w \in R^m$ such that $gen(v,w) = R^m$ and assuming $m \leq |R| + 1$. The result is the converse of Theorem 4.5.15.

Theorem 4.5.18. *Let* R *be a finite Dickson nearfield that arises from the Dickson pair* (q,n). *For every value* m *satisfying* $2 \leq m \leq q^n + 1$, *we have* $s(R^m) = 2$.

Proof. For $2 \leq m \leq |R| + 1$, we choose

$$v = (1,0,1,\ldots,1) \text{ and } w = (0,1,w^3,\ldots,w^m) \in R^m$$

arranged in a matrix

$$V = \begin{bmatrix}1 & 0 & 1 & \ldots & 1\\ 0 & 1 & w^3 & \ldots & w^m\end{bmatrix} \in R^{2\times m},$$

where each element $w^j \neq 1$ for $j \in \{3,\ldots,m\}$ is a non-zero distinct element (i.e, $w^j \in R^* \setminus \{1\}$). Note that all the pairs

$$(1,0),(0,1),(1,w^3),\ldots,(1,w^j),\ldots,(1,w^m)$$

satisfy the following condition

$$(v_j,w_j) \neq \alpha(v_i,w_i) \text{ for all } i,j \text{ where } i \neq j \text{ and } \alpha \in R^*. \tag{4.5.2}$$

Thus by implementing the *EGE algorithm* (the explicit procedure in the proof of Theorem 4.3.14) on the initial matrix V, we create at least $m-2$ additional rows (since the first two columns each have exactly one non-zero

entry and the pairs $(1, w^j)$ are all non multiples of each other). Hence we may apply the "distributivity trick" on the third column and so on. Note that the process will stop after creating exactly $m-2$ new rows so that at the end of *the EGE algorithm*, we will get in total m rows so that $gen(v,w) = \bigoplus_{i=1}^{m} e_i R = R^m$ where $\{e_i\}_{i=1,\ldots,m}$ is the standard basis. Thus $s(R^m) = 2$. □

Example 4.5.19. *Appealing to Example 3.2.16 and Table 3.1, let us consider* $R \in DN(3,2)$. *There exist* $v = (1, 2x+2, x, 0, x)$ *and* $w = (2, 2x, 1, 2, x) \in R^5$ *such that* $gen(v,w) = R^5$. *Thus* $s(R^5) = 2$.

We have seen that it takes two vectors that belong to R^m under the condition that $m \leq |R| + 1$ to generate the whole space.

4.6 Concluding comments

All the results in the subsection 4.3 and 4.4 are true for any proper nearfield R, however those in subsection 4.5 are true for any finite nearfield R.
In future work, we suggest investigating the following questions.

- Given a matrix M in extended reduced row echelon form with non-zero rows, can we determine the minimal sets of non-zero row vectors that form a matrix N such that gen(rows of M)= gen(rows of N)?
- Let T be an R-subgroup of R^m. In the more general setting if $s(T) = k$, what are the possible R-dimensions for T?
- Let T be an R-subgroup of R^m. Suppose that $R\text{-dim}(T) = k$. What are the possible seed numbers for T?
- By experimental computations, there exist no two vectors v_1 and v_2 such that $gen(v_1, v_2)$ is the whole space R^m when the dimension is high enough, for instance $R^{m^{m^2}}$. Let R be finite nearfield, what is $s(R^m)$ for $m > |R| + 1$?

Chapter 5

On the generalized distributive set of a finite nearfield

5.1 Introduction

Let R be a finite Dickson nearfield that arises from the Dickson pair (q, n). For a given pair $(\alpha, \beta) \in R^2$ we introduce the generalized distributive set

$$D(\alpha, \beta) = \{\lambda \in R \ : \ (\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda\}$$

where " $\circ$ " is the multiplication of the Dickson nearfield (see Definition 5.2.10). We find that $D(\alpha, \beta)$ is not in general a subfield of the finite field $\mathbb{F}_{q^n}$ (see Example 5.4.4). Nor is it in general a subnearfield of R. We obtain sufficient conditions on α, β for $D(\alpha, \beta)$ to be a subfield of $\mathbb{F}_{q^n}$ (see Theorem 5.3.2). Also in the case where $\alpha, \beta, \alpha + \beta$ belong to different H-cosets, we construct a subfield of $\mathbb{F}_{q^n}$ using $D(\alpha, \beta)$ (see Theorem 5.3.4). In Section 4 by Lemma 5.4.1 we show that $D(\alpha, \beta)$ can be presented as a vector space and we derive an algorithm that tests whether $D(\alpha, \beta)$ is a subfield of $\mathbb{F}_{q^n}$ or not.

5.2 Some properties

Let $(R, +, \circ)$ be a nearfield. By Definition 2.2.5, $D(R)$ denotes the set of all distributive elements and $C(R)$ the center of R.

Theorem 5.2.1. *([32]) Let R be a nearfield. Then $D(R)$ under the operations of R is a skewfield and $D(R)$ is a subnearfield of R.*

Note that it is shown in [2] that for any nearring R the multiplicative center of R is not always a subnearring of R. Later the authors in [7] introduced the concept of generalized center and have shown that for certain classes of nearrings, $C(R)$ is a subnearring of R if and only if the generalized center of R is the center of R.

Definition 5.2.2. *([7]) Let R be a nearring and $D(R)$ be the distributive elements of R. Then the generalized center of R is the set*

$$GC(R) = \{x \in R : \ x \circ y = y \circ x \text{ for all } y \in D(R)\}.$$

Lemma 5.2.3. *([7]) Let R be a nearring. Then $GC(R)$ under the operations of R is a subnearring of R containing $C(R)$. In particular, if R is a nearfield, then $GC(R)$ is a subnearfield of R.*

Now consider a finite Dickson nearfield $(R, +, \circ)$ for the Dickson pair (q, n) with $n > 1$.

Theorem 5.2.4. *([13]) Let R be a finite Dickson nearfield that arises from the Dickson pair (q, n). Then $D(R) = C(R) = \mathbb{F}_q$.*

So the distributive elements of a finite Dickson nearfield R under the operations of R form a subnearfield of the nearfield and under the operations of the field $\mathbb{F}_{q^n}$ form a subfield of size q. Thus there are elements $(\alpha, \beta, \lambda) \in R^3$ such that $(\alpha + \beta) \circ \lambda \neq \alpha \circ \lambda + \beta \circ \lambda$. In the *EGE algorithm* described in the proof of Theorem 4.3.14, the *"distributivity trick"* requires that a triple of non-distributive elements (see Equation (4.3.1)) be chosen at each step and used in the creation of new rows. This leads us to investigate the distributive elements of finite Dickson nearfields.

Definition 5.2.5. *Given $k \in \{1, \ldots, n\}$, an H-coset is a coset of the form $g^{[k]_q}H$.*

We have the following:

Lemma 5.2.6. *Let $R \in DN(q, n)$ where (q, n) is a Dickson pair. Let $(\alpha, \beta) \in R^2$. If $\alpha, \beta, \alpha + \beta$ belong to the same H-coset, then $(\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda$ for all $\lambda \in R$.*

Proof. Let g be such that $\mathbb{F}_{q^n}^* = \langle g \rangle$ and $H = \langle g^n \rangle$. By the finite Dickson nearfield construction, the set of all H-cosets is presented as $\mathbb{F}_{q^n}^*/H =$

$\{H, g^{[1]_q}H, \ldots, g^{[n]_q}H\}$. Assume that $\alpha, \beta, \alpha+\beta \in g^{[k]_q}H$ for some $1 \leq k \leq n$. Then

$$(\alpha+\beta)\circ\lambda = (\alpha+\beta)\lambda^{q^k} = \alpha\lambda^{q^k} + \beta\lambda^{q^k} = \alpha\circ\lambda + \beta\circ\lambda,$$

for all $\lambda \in R$. □

Now let us look at the case for Dickson pairs (q, n) where $n = 2$. We have the following.

Lemma 5.2.7. *Let $(q, n) = (p^l, 2)$ where p is prime and $R \in DN(q, 2)$. Let $(\alpha, \beta) \in R^2$ and assume that $\alpha, \beta, \alpha+\beta$ don't all belong to the same H-coset. We have $(\alpha+\beta)\circ\lambda = \alpha\circ\lambda + \beta\circ\lambda$ if and only if $\lambda \in D(R)$.*

Proof. Suppose $\alpha, \beta, \alpha+\beta$ belong to different H-cosets which means $\alpha, \beta, \alpha+\beta$ are not all square and not all non-square. We consider the case where $\alpha+\beta \in H$ and $\alpha, \beta \in gH$ (note that the other cases are similar). If $(\alpha+\beta)\circ\lambda = \alpha\circ\lambda + \beta\circ\lambda$ then we have $(\alpha+\beta)\lambda = \alpha\lambda^q + \beta\lambda^q$. Thus $\lambda^{p^l} - \lambda = 0$ and since every $\lambda \in \mathbb{F}_q$ is a solution of this equation, they are all the solutions. By Theorem 5.2.4 we have $\lambda \in D(R)$. The converse is straightforward. □

By Lemma 5.2.7 we deduce the following.

Corollary 5.2.8. *Let $(q, 2)$ be a Dickson pair with $q = p^l$. Let g be a generator of $\mathbb{F}^*_{q^2}$ and R the finite nearfield constructed with $H = \langle g^2 \rangle$. For all pairs $(\alpha, \beta) \in R^2$ and $\lambda \in R$, $(\alpha+\beta)\circ\lambda = \alpha\circ\lambda + \beta\circ\lambda$ if and only if either all $\alpha, \beta, \alpha+\beta$ belong to the same H-coset or $\lambda \in D(R)$.*

Lemma 5.2.7 does not hold in general for any finite Dickson nearfield $DN_g(q, n)$ where (q, n) is a Dickson pair. The following example gives an illustration.

Example 5.2.9. *Let $R \in DN(q, 2)$ and $(\alpha, \beta) \in R^2$ where $\alpha, \beta, \alpha+\beta$ belong to different H-cosets. Then by Lemma 5.2.7 and Corollary 5.2.8, $(\alpha+\beta)\circ\lambda = \alpha\circ\lambda + \beta\circ\lambda$ will always lead to the equation $\lambda^q - \lambda = 0$ and all the solutions will be in $\mathbb{F}_q$. But Lemma 5.2.7 can fail for a positive integer $n > 2$. For instance given $R = DN_g(5, 4) = (\mathbb{F}_{5^4}, +, \circ)$ where $\mathbb{F}_{5^4} = \{0, 1, 2, 3, 4, x, x^2+1, x^4+x^2, 3+x^2+2, \ldots\}$ is the finite field of order 5^4. Here we take the irreducible polynomial X^4+2 of degree 4 over $\mathbb{F}_5$ where x is a root of X^4+2. Let g be such that $\mathbb{F}^*_{5^4} = \langle g \rangle$ and $H = \langle g^4 \rangle$. The quotient group is represented by*

$$\mathbb{F}^*_{5^4}/H = \{gH, g^6H, g^{31}H, g^{156}H\} = \{H, gH, g^2H, g^3H\}.$$

Let $\alpha, \beta \in \mathbb{F}_{5^4}$. We have

$$\alpha \circ \beta = \begin{cases} \alpha \cdot \beta \text{ if } \alpha \in H \\ \alpha \cdot \beta^5 \text{ if } \alpha \in gH \\ \alpha \cdot \beta^{25} \text{ if } \alpha \in g^2H \\ \alpha \cdot \beta^{125} \text{ if } \alpha \in g^3H. \end{cases}$$

We consider $g = x + 2$. Let $\alpha = 3 \in H, \beta = x^2 + 2 \in H$. Then $\alpha + \beta \in g^2H$. In fact $\lambda = x^2 + 1 \in g^2H$ distributes over the pair (α, β). To see this, $(\alpha + \beta) \circ \lambda = (3 + x^2 + 2) \circ (x^2 + 1) = x^2 + x^4$. Also $\alpha \circ \lambda + \beta \circ \lambda = 3 \circ (x^2 + 1) + (x^2 + 2) \circ (x^2 + 1) = x^4 + x^2$. But $\lambda \notin D(R) = \mathbb{F}_5$. Note that $\lambda \notin D(R)$ but distributes over the pair (α, β).

We now introduce the generalized distributive set for a given pair in a nearfield.

Definition 5.2.10. *Let R be a nearfield. Given a pair $(\alpha, \beta) \in R^2$, the generalized distributive set*

$$D(\alpha, \beta) = \{\lambda \in R : (\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda\}$$

is the set of elements in R that distribute over the pair (α, β).

Note that in the *EGE algorithm*, we have to choose at every step of the creation of a new row a triple $(\alpha, \beta, \lambda) \in R^3$ such that $\lambda \notin D(\alpha, \beta)$ for the implementation of the *"distributivity trick"*. It is not difficult to see the following.

Lemma 5.2.11. *Let R be a nearfield. We have*

$$\bigcap_{\alpha,\beta \in R} D(\alpha, \beta) = D(R).$$

Suppose $R \in DN(q, n)$ and $(\alpha, \beta) \in R^2$ such that $\alpha, \beta, \alpha + \beta$ belong to the same H-coset. Then $D(\alpha, \beta)$ is always a subnearfield of R because it is R. We define $C(D(\alpha, \beta))$ to be the center of $D(\alpha, \beta)$. The following is an immediate consequence of Lemma 5.2.6.

Corollary 5.2.12. *Let $R \in DN(q, n)$ and $(\alpha, \beta) \in R^2$ such that $\alpha, \beta, \alpha + \beta$ belong to the same H-coset. Then $C(D(\alpha, \beta)) = C(R) = D(R)$.*

5.3 Some results on $D(\alpha, \beta)$ where $\alpha, \beta \in DN_g(q, n)$

We remind the reader that by definition a subset $S \subseteq \mathbb{F}_{p^n}$ that is a field (when equipped with the operations of $\mathbb{F}_{p^n}$) is a subfield of the finite field $\mathbb{F}_{p^n}$. Also the subfields of $\mathbb{F}_{p^n}$ are the fields $\mathbb{F}_{p^k}$ where k divides n.
Our aim is to determine $D(\alpha, \beta)$ where $(\alpha, \beta) \in R^2$ for R a finite Dickson nearfield that arises from the Dickson pair (q, n). Note that if $n = 1$ then $DN(q, 1)$ is the set of all finite fields of order q. Hence in this case $D(\alpha, \beta) = \mathbb{F}_q$ and also $C\big(D(\alpha, \beta)\big) = \mathbb{F}_q$.
From Lemma 5.2.6, Lemma 5.2.7 and Theorem 5.2.1, we deduce the following when $n = 2$.

Lemma 5.3.1. *Let $(q, 2)$ be a Dickson pair with $q = p^l$ for some prime p and integer l. Let g be a generator of $\mathbb{F}_{q^2}^*$ and let R be the nearfield constructed with $H = \langle g^2 \rangle$. Let $(\alpha, \beta) \in R^2$. Then*

(i) $D(\alpha, \beta)$ is a subnearfield of R.

(ii) $C\big(D(\alpha, \beta)\big)$ is a subnearfield of R.

Proof.

(i) Let $R \in DN(q, 2)$ and $\alpha, \beta \in R$. We have $D(\alpha, \beta) = R$ or $D(\alpha, \beta) = D(R)$. So $D(\alpha, \beta)$ is a subnearfield of R.

(ii) Suppose $\alpha, \beta, \alpha + \beta$ all belong to the same H-coset. Then by Corollary 5.2.12 we have $C\big(D(\alpha, \beta)\big) = C(R) = D(R)$ and by Theorem 5.2.1 $C\big(D(\alpha, \beta)\big)$ is a subnearfield of R. Suppose $\alpha, \beta, \alpha + \beta$ don't all belong to the same H-coset. We have $D(\alpha, \beta) = D(R)$. Hence by Lemma 5.2.3,

$$C\big(D(\alpha, \beta)\big) = C\big(D(R)\big) = D(R) \cap GC(R)$$

is a subnearfield of R.

□

Furthermore it is not difficult to see the following. Let (q, n) be a Dickson pair with $q = p^l$ for some prime p and integers l, n. Let g be a generator

of $\mathbb{F}_{q^n}^*$ and let R be the nearfield constructed with $H = \langle g^n \rangle$. Then for each positive integer h (dividing ln) there exists a unique subfield of $\mathbb{F}_{q^n}$ of order p^h such that $g^{\frac{q^n-1}{p^h-1}}$ generates its multiplicative group. In the next theorem we shall give a sufficient condition on α, β for which $D(\alpha, \beta)$ is a subfield of $\mathbb{F}_{q^n}$.

Theorem 5.3.2. *Let (q, n) be a Dickson pair with $q = p^l$ for some prime p and positive integers l, n such that $n > 2$. Let g be a generator of $\mathbb{F}_{q^n}^*$ and R the finite nearfield constructed with $H = \langle g^n \rangle$. Let $\alpha, \beta \in R^*$. If at least two of $\alpha, \beta, \alpha + \beta$ are in the same H-coset then $D(\alpha, \beta)$ is a subfield of $\mathbb{F}_{q^n}$ of order p^h for some h dividing ln.*

Proof.
Assume that $\alpha, \beta, \alpha + \beta$ are all in the same H-coset. Then By Lemma 5.2.6, $(\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda$ for all $\lambda \in R$. Hence $D(\alpha, \beta)$ coincides with $\mathbb{F}_{q^n}$. Assume now that exactly two of $\alpha, \beta, \alpha + \beta$ are in the same H-coset. We consider the case where $\alpha, \beta \in g^{[s]_q} H$ and $\alpha + \beta \in g^{[t]_q} H$ for $s \neq t$ (note that the other cases are similar). Then $(\alpha + \beta) \circ \lambda = (\alpha + \beta)\lambda^{q^t} = \alpha\lambda^{q^t} + \beta\lambda^{q^t}$. Also $\alpha \circ \lambda + \beta \circ \lambda = \alpha\lambda^{q^s} + \beta\lambda^{q^s}$. Hence

$$(\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda \Rightarrow (\alpha + \beta)(\lambda^{q^t} - \lambda^{q^s}) = 0$$

and then $\lambda = 0$ is solution of the equation. Now suppose $\lambda \neq 0$, so

$$(\alpha + \beta)(\lambda^{q^t} - \lambda^{q^s}) = 0 \Rightarrow \lambda^{q^t - q^s} - 1 = 0.$$

It follows that

$$(\lambda^{q^t - q^s} - 1)^q = 0 \Rightarrow \lambda^{q^{t+1} - q^{s+1}} - 1 = 0.$$

Continuing this procedure (raising to the power q^ϵ such that $n = s + \epsilon$) we obtain

$$\lambda^{q^{t+\epsilon} - q^{s+\epsilon}} - 1 = 0.$$

Hence, we have $\lambda^{q^r - q^n} - 1 = 0$ where $r = t + \epsilon$ and since $\lambda^{q^n} = \lambda$, we get $\lambda^{q^r} - \lambda = 0$. We know that $q = p^l$ where p is a prime number and l, n are positive integers. Hence we get the following equation

$$(\Sigma) : \lambda^{p^k} - \lambda = 0 \text{ where } \lambda \in \mathbb{F}_{p^m} \tag{5.3.1}$$

for some positive integers $k = lr$ and $m = ln$.

(i) Suppose k divides m. Then there exists exactly one subfield of $\mathbb{F}_{p^m}$ which is isomorphic to $\mathbb{F}_{p^k}$. So all the solutions of (Σ) are in $\mathbb{F}_{p^m}$. Hence $D(\alpha, \beta)$ coincides with $\mathbb{F}_{p^k}$ which is a subfield of $\mathbb{F}_{p^m}$.

(ii) Suppose k does not divide m. Note that $\lambda = 0$ is a solution of (Σ). Set $\delta = \text{GCD}(m, k)$. Now let $\lambda \in \mathbb{F}_{p^m}^*$ be a solution of (Σ). So $\lambda = g^a$ for some $0 \leq a < p^m - 1$ and $g^{a(p^k)} - g^a = 0$. Then $g^{a(p^k-1)} = 1$. We have,

$$(p^m - 1) \text{ divides } a(p^k - 1).$$

So there exists an integer t such that $a(p^k - 1) = t(p^m - 1)$. Since δ divides m there exists $\theta \in \mathbb{N}$ such that $m = \delta\theta$. Also since δ divides k there exists $\theta' \in \mathbb{N}$ such that $k = \delta\theta'$. So we have $p^m - 1 = (p^\delta - 1)\big((p^\delta)^{\theta-1} + \ldots + p^\delta + 1\big)$ and $p^k - 1 = (p^\delta - 1)\big((p^\delta)^{\theta'-1} + \ldots + p^\delta + 1\big)$. Furthermore, since

$$\text{GCD}(p^m - 1, p^k - 1) = p^\delta - 1,$$

by Bezout's identity there exists some integers u and v such that

$$u(p^m - 1) + v(p^k - 1) = p^\delta - 1.$$

Hence substituting $a(p^k - 1) = t(p^m - 1)$ we get

$$au(p^m - 1) + vt(p^m - 1) = a(p^\delta - 1).$$

Thus $(p^m - 1)$ divides $a(p^\delta - 1)$. It follows that $\frac{p^m-1}{p^\delta-1}$ divides a. So $a = \frac{p^m-1}{p^\delta-1}b$ where $b \in \mathbb{N}$. Now,

$$0 \leq a < p^m - 1 \Leftrightarrow 0 \leq b < p^\delta - 1.$$

Reciprocally, let $0 \leq b < p^\delta - 1$ and $\lambda_0 = g^a$. We know that $a = \frac{p^m-1}{p^\delta-1}b$ and $p^k - 1 = t'(p^\delta - 1)$ for some integer t'. We have,

$$\begin{aligned} \lambda_0^{p^k-1} - 1 &= (g^a)^{t'(p^\delta-1)} - 1 \\ &= g^{(p^m-1)t'b} - 1 \\ &= 1^{t'b} - 1 = 0. \end{aligned}$$

It follows that λ_0 is a solution of the equation $\lambda^{p^k} - \lambda = 0$. Hence the set of solutions (denoted as $S(\Sigma)$) of the equation (Σ) for $\lambda \in \mathbb{F}_{p^m}$ are

presented as

$$S(\Sigma) = \{0\} \cup \left\{ g^{\frac{p^m-1}{p^\delta-1}b} : 0 \leq b < p^\delta - 1 \right\}.$$

The elements of $S(\Sigma)$ are all distinct since $g^{\frac{p^m-1}{p^\delta-1}}$ is a generator of the multiplicative group of the subfield $\mathbb{F}_{p^\delta}$ of $\mathbb{F}_{p^m}$ (since δ divides m). Hence

$$|S(\Sigma)| = p^\delta - 1 + 1 = p^\delta = p^{l \cdot \mathrm{GCD}(t+n-s,n)}.$$

So all the solutions of (Σ) are in the finite field of order p^δ. Hence $D(\alpha, \beta)$ coincides with $S(\Sigma) = \mathbb{F}_{p^\delta}$.

□

Example 5.3.3. *Suppose $R = DN_g(5,4)$ with the generator $g = x + 2$ (see Example 5.2.9 regarding the construction of $DN_g(5,4)$). Let $\alpha, \beta \in R$ such that $\alpha = x + 2 \in gH$ and $\beta = x^3 + x^2 + 2x + 3 \in g^2H$ where x is a root of the irreducible polynomial $X^4 + 2 \in \mathbb{Z}_5[X]$. Then $\alpha + \beta \in gH$. There exist $\lambda_1 = x^2 + 3$, $\lambda_2 = 3x^2 + 2 \in D(\alpha, \beta)$ such that $\lambda_1 \in H$ and $\lambda_2 \in g^2H$. So the distributive elements λ_1 and λ_2 don't necessarily belong to the same H-coset.*

We now look at $D(\alpha, \beta)$ where $\alpha, \beta, \alpha + \beta$ are all in distinct H-cosets. We deduce the following construction of a subfield of $\mathbb{F}_{q^n}$ by making use of $D(\alpha, \beta)$.

Theorem 5.3.4. *Let (q, n) be a Dickson pair with $q = p^l$ for some prime p and integers l, n such that $n > 2$. Let g be a generator of $\mathbb{F}_{q^n}^*$ and R the finite nearfield constructed with $H = \langle g^n \rangle$. Suppose $(r, s, t) \in \mathbb{N}^3$ such that $0 < t < s < r \leq n$ where $r - s$ divides n and $r - t$ divides n. Let $(\alpha, \beta, \alpha + \beta) \in g^{[r]_q}H \times g^{[s]_q}H \times g^{[t]_q}H$. Let $F_{r,s,t}(\alpha, \beta)$ be the subset of $\mathbb{F}_{q^n}$ defined by*

$$F_{r,s,t}(\alpha, \beta) = D(\alpha, \beta) \cap \mathbb{F}_{q^{r-s}} \cap \mathbb{F}_{q^{r-t}}.$$

Then $F_{r,s,t}(\alpha, \beta)$ is a subfield of $\mathbb{F}_{q^n}$.

Proof. Let $(\alpha, \beta, \alpha + \beta) \in g^{[r]_q}H \times g^{[s]_q}H \times g^{[t]_q}H$ such that $0 < t < s < r \leq n$. Let $\lambda \in D(\alpha, \beta)$, so we have $\alpha(\lambda^{q^t} - \lambda^{q^r}) = \beta(\lambda^{q^s} - \lambda^{q^t})$. Suppose $r - s$ divides n and $r - t$ divides n. Then $\mathbb{F}_{q^{r-s}} \cap \mathbb{F}_{q^{r-t}}$ is a subfield of $\mathbb{F}_{q^n}$. Note that

$\lambda \in \mathbb{F}_{q^{r-s}} \cap \mathbb{F}_{q^{r-t}} \Leftrightarrow \lambda^{q^{r-s}} = \lambda$ and $\lambda^{q^{r-t}} = \lambda$. It follows that $(\lambda^{q^{r-s}} - \lambda)^{q^s} = 0$ and $(\lambda^{q^{r-t}} - \lambda)^{q^t} = 0$. Thus $\lambda^{q^r} = \lambda^{q^s}$ and $\lambda^{q^r} = \lambda^{q^t}$. Also $F_{r,s,t}(\alpha, \beta) \neq \emptyset$ since $0, 1 \in F_{r,s,t}(\alpha, \beta)$. Suppose $\lambda_1, \lambda_2 \in F_{r,s,t}(\alpha, \beta)$. We have

$$\begin{aligned}
\alpha\big((\lambda_1 + \lambda_2)^{q^t} - (\lambda_1 + \lambda_2)^{q^r}\big) &= \alpha(\lambda_1^{q^t} + \lambda_2^{q^t} - \lambda_1^{q^r} - \lambda_2^{q^r}) \\
&= \alpha(\lambda_1^{q^t} - \lambda_1^{q^r}) + \alpha(\lambda_2^{q^t} - \lambda_2^{q^r}) \\
&= \beta(\lambda_1^{q^s} - \lambda_1^{q^t}) + \beta(\lambda_2^{q^s} - \lambda_2^{q^t}) \\
&= \beta\big((\lambda_1 + \lambda_2)^{q^s} - (\lambda_1 + \lambda_2)^{q^t}\big).
\end{aligned}$$

It follows that $\lambda_1 + \lambda_2 \in D(\alpha, \beta)$. Also $\lambda_1 + \lambda_2 \in \mathbb{F}_{q^{r-s}} \cap \mathbb{F}_{q^{r-t}}$. Hence $\lambda_1 + \lambda_2 \in F_{r,s,t}(\alpha, \beta)$. Furthermore,

$$\begin{aligned}
\alpha\big((\lambda_1\lambda_2)^{q^t} - (\lambda_1\lambda_2)^{q^r}\big) &= \alpha(\lambda_1^{q^t}\lambda_2^{q^t} - \lambda_1^{q^r}\lambda_2^{q^r}) \\
&= \alpha(\lambda_1^{q^r}\lambda_2^{q^t} - \lambda_1^{q^r}\lambda_2^{q^r}) \\
&= \alpha\lambda_1^{q^r}(\lambda_2^{q^t} - \lambda_2^{q^r}) \\
&= \lambda_1^{q^r}\beta(\lambda_2^{q^s} - \lambda_2^{q^t}) \\
&= \beta(\lambda_1^{q^r}\lambda_2^{q^s} - \lambda_1^{q^r}\lambda_2^{q^t}) \\
&= \beta(\lambda_1^{q^s}\lambda_2^{q^s} - \lambda_1^{q^t}\lambda_2^{q^t}) \\
&= \beta\big((\lambda_1\lambda_2)^{q^s} - (\lambda_1\lambda_2)^{q^t}\big).
\end{aligned}$$

It follows that $\lambda_1\lambda_2 \in D(\alpha, \beta)$. Also $\lambda_1\lambda_2 \in \mathbb{F}_{q^{r-s}} \cap \mathbb{F}_{q^{r-t}}$. Hence $\lambda_1\lambda_2 \in F_{r,s,t}(\alpha, \beta)$. We also have $\lambda_1 - \lambda_2 \in F_{r,s,t}(\alpha, \beta)$. So $\big(F_{r,s,t}(\alpha, \beta), +\big)$ is a subgroup of $(\mathbb{F}_{q^n}, +)$. Suppose $\lambda \in \mathbb{F}_{q^{r-s}} \cap \mathbb{F}_{q^{r-t}}$. We know that if $\lambda \in D(\alpha, \beta)$ then assuming $\lambda \neq 0$, we have

$$\alpha(\lambda^{q^t} - \lambda^{q^r}) = \beta(\lambda^{q^s} - \lambda^{q^t}) \Leftrightarrow \alpha(\lambda^{q^r - q^t} - 1) = -\lambda^{-q^t}\beta(\lambda^{q^s} - \lambda^{q^t}).$$

Thus

$$\begin{aligned}
\alpha(\lambda^{-q^t} - \lambda^{-q^r}) &= \alpha\lambda^{-q^r}(\lambda^{q^r - q^t} - 1) \\
&= \alpha\lambda^{-q^s}(\lambda^{q^r - q^t} - 1) \\
&= -\lambda^{-q^s}\lambda^{-q^t}\beta(\lambda^{q^s} - \lambda^{q^t}) \\
&= \beta(\lambda^{-q^s} - \lambda^{-q^t}).
\end{aligned}$$

Thus $\lambda^{-1} \in D(\alpha, \beta)$. Hence $\lambda_1\lambda_2^{-1} \in F_{r,s,t}(\alpha, \beta)$. So $\big(F_{r,s,t}(\alpha, \beta), \cdot\big)$ is a subgroup of $(\mathbb{F}_{q^n}^*, \cdot)$. □

Remark 5.3.5. *Only the case where $0 < t < s < r \leq n$ is considered in Theorem 5.3.4. However the other cases can be deduced in a similar way.*

5.4 $D(\alpha, \beta)$ presented as a vector space where $\alpha, \beta \in DN_g(q, n)$

In this subsection it is shown that $D(\alpha, \beta)$ has a vector space structure. We have the following:

Lemma 5.4.1. *Let (q, n) be a Dickson pair with $q = p^l$ for some prime p and integers l, n. Let g be a generator of $\mathbb{F}_{q^n}^*$ and R the finite nearfield constructed with $H = \langle g^n \rangle$. Let $(\alpha, \beta) \in R^2$. Then $D(\alpha, \beta)$ is an $\mathbb{F}$-vector space for some finite field $\mathbb{F}$.*

Proof. We have:

- Suppose that $\alpha, \beta, \alpha + \beta$ are all in the same H-coset. Then $D(\alpha, \beta) = \mathbb{F}_{q^n}$. Thus $D(\alpha, \beta)$ is an $\mathbb{F}$-vector space where $\mathbb{F} = \mathbb{F}_{q^n}$.
- Suppose that exactly two of $\alpha, \beta, \alpha + \beta$ belong to the same H-coset. We consider the case where $\alpha, \beta \in g^{[s]_q} H$ and $\alpha + \beta \in g^{[t]_q} H$ for $s \neq t$ (note that the other cases are similar). By the proof of Theorem 5.3.2, we have $D(\alpha, \beta) = \mathbb{F}_{q^{\mathrm{GCD}(t+n-s,n)}}$. Thus $D(\alpha, \beta)$ is an $\mathbb{F}$-vector space where $\mathbb{F} = \mathbb{F}_{q^{\mathrm{GCD}(t+n-s,n)}}$.
- Suppose that $\alpha \in g^{[r]_q} H$ and $\beta \in g^{[s]_q} H$ and $\alpha + \beta \in g^{[t]_q} H$ where r, s and t are all distinct. We define

$$\mathbb{F} = \{k \in \mathbb{F}_{q^n} : k^{q^t} = k^{q^r} = k^{q^s} = k\} = \mathbb{F}_{q^t} \cap \mathbb{F}_{q^r} \cap \mathbb{F}_{q^s}.$$

  Let $\lambda_1, \lambda_2 \in D(\alpha, \beta)$. Using the Frobenius identity, we have $\lambda_1 + \lambda_2 \in D(\alpha, \beta)$. Let $k \in \mathbb{F}$ and $\lambda \in D(\alpha, \beta)$. We have,

$$\begin{aligned} \alpha\big((k\lambda)^{q^t} - (k\lambda)^{q^r}\big) &= \alpha k^{q^t}(\lambda^{q^t} - \lambda^{q^r}) \\ &= \beta k^{q^t}(\lambda^{q^s} - \lambda^{q^t}) \\ &= \beta(k^{q^t}\lambda^{q^s} - k^{q^t}\lambda^{q^t}) \\ &= \beta\big((k\lambda)^{q^s} - (k\lambda)^{q^t}\big). \end{aligned}$$

  It follows that $k\lambda \in D(\alpha, \beta)$. Thus $D(\alpha, \beta)$ is an $\mathbb{F}$-vector space where $\mathbb{F} = \mathbb{F}_{q^t} \cap \mathbb{F}_{q^r} \cap \mathbb{F}_{q^s}$.

□

Remark 5.4.2. *It is not difficult to see that $D(\alpha,\beta)$ is also an $\mathbb{F}_q$-vector space.*

Lemma 5.4.3. *Let (q,n) be a Dickson pair with $q = p^l$ for some prime p and integers l,n. Let g be a generator of $\mathbb{F}_{q^n}^*$ and R the nearfield constructed with $H = \langle g^n \rangle$. Let $(\alpha,\beta) \in R^2$. Then there exists a positive integer k such that $|D(\alpha,\beta)| = q^k$.*

Proof. $D(\alpha,\beta)$ is a finite dimensional vector space over $\mathbb{F}_q$. Then $D(\alpha,\beta)$ has a basis over $\mathbb{F}_q$ consisting of say k elements. Thus $D(\alpha,\beta)$ has exactly q^k elements. □

Our next goal is to find a basis for $D(\alpha,\beta)$.

Computational aspect

Let $\alpha,\beta,\alpha+\beta \in DN_g(q,n)$ such that $\alpha \in g^{[r]_q}H$, $\beta \in g^{[s]_q}H$ and $\alpha+\beta \in g^{[t]_q}H$ where r,s and t are all different. We have

$$(\alpha+\beta)\circ\lambda = \alpha\circ\lambda + \beta\circ\lambda \Leftrightarrow \alpha(\lambda^{q^t}-\lambda^{q^r}) = \beta(\lambda^{q^s}-\lambda^{q^t})$$

for all $\lambda \in \mathbb{F}_{q^n}$. We resort to computational methods in order to check the nature of the distributive elements $D(\alpha,\beta)$. We derive an algorithm called *"DSS"* (Distributive Set Subfields) which tests whether $D(\alpha,\beta)$ is a finite field.
We construct a function ϕ from $\mathbb{F}_{q^n}$ to itself that maps λ to $\alpha(\lambda^{q^t}-\lambda^{q^r}) - \beta(\lambda^{q^s}-\lambda^{q^t})$. This function will be zero if and only if λ is a solution to the equation $\alpha(\lambda^{q^t}-\lambda^{q^r}) = \beta(\lambda^{q^s}-\lambda^{q^t})$. Moreover, ϕ is an $\mathbb{F}_q$-linear map, so it suffices to compute it on a basis. A basis of $\mathbb{F}_{q^n}$ is $\{1,g,g^2,\ldots,g^{n-1}\}$. The function ϕ is entirely determined by the vectors $\phi(1),\phi(g),\ldots,\phi(g^{n-1})$. We can represent each vector $\phi(g^j)$ for $0 \le j \le n-1$ as

$$\phi(g^j) = m_0^j 1 + m_1^j g + \ldots + m_{(n-1)}^j g^{n-1} \text{ where } m_i^j \in \mathbb{F}_q \text{ with } 0 \le i \le n-1.$$

Thus ϕ is entirely determined by the values of the matrix of size $n \times n$ defined by $M = (m_i^j)_{\substack{0\le i\le n-1\\ 0\le j\le n-1}}$. Let $\lambda \in \mathbb{F}_{q^n}$. There exist $\lambda_0,\ldots,\lambda_{n-1} \in \mathbb{F}_q$ such that $\lambda = \lambda_0 1 + \ldots + \lambda_{n-1}g^{n-1}$. So λ can be represented by $\begin{bmatrix} \lambda_0 \\ \vdots \\ \lambda_{n-1} \end{bmatrix}$. Thus

for all $\lambda \in \mathbb{F}_{q^n}$ we have $\phi(\lambda) = M \begin{bmatrix} \lambda_0 \\ \vdots \\ \lambda_{n-1} \end{bmatrix}$ where $\lambda = \lambda_0 1 + \ldots + \lambda_{n-1} g^{n-1}$.

We have

$$\begin{aligned} D(\alpha,\beta) &= ker\phi \\ &= Nullspace(M) \\ &= \left\{ \lambda \in \mathbb{F}_{q^n} : M \begin{bmatrix} \lambda_0 \\ \vdots \\ \lambda_{n-1} \end{bmatrix} = 0 \right\}. \end{aligned}$$

We give the details of the full algorithm in the appendix (see Algorithm C.0.1). After the implementation of the DSS algorithm, we have the following examples.

Example 5.4.4.

1. *Suppose that* $(q,n) = (4,3)$. *Let* g *be such that* $\mathbb{F}_{4^3}^* = \langle g \rangle$ *and* $H = \langle g^3 \rangle$. *We know by Theorem 5.3.2, that if at least two of* $\alpha, \beta, \alpha+\beta$ *belong to the same* H*-coset then* $D(\alpha,\beta)$ *is a subfield of* $\mathbb{F}_{q^n}$. *Furthermore for every* α, β *and* $(\alpha+\beta)$ *all belong to distinct* H*-cosets,* $D(\alpha,\beta)$ *is a finite field.*

2. *Suppose that* $(q,n) = (5,4)$. *Then* $D(\alpha,\beta)$ *is also a finite field for every* $\alpha, \beta \in DN_g(5,4)$ *where* $\mathbb{F}_{5^4}^* = \langle g \rangle$ *and* $H = \langle g^4 \rangle$.

3. *Suppose that* $(q,n) = (7,9)$. *Let* g *be such that* $\mathbb{F}_{7^9}^* = \langle g \rangle$ *and* $H = \langle g^9 \rangle$. *We know that* $D(\alpha,\beta)$ *is an* $\mathbb{F}_7$*-vector space. Also* $\mathbb{F}_{7^9}$ *is an* $\mathbb{F}_7$*-vector space with a basis* $\{1, g^2, \ldots, g^8\}$. *We take some elements*

$$\alpha = 4g^8 + 5g^7 + 3g^4 + 6g^3 + 6g^2 + 6g + 4 \in \mathbb{F}_{7^9}^*$$

and

$$\beta = 5g^8 + 3g^7 + g^6 + 3g^5 + 3g^4 + g^3 + 3g^2 + 6g + 6 \in \mathbb{F}_{7^9}^*$$

such that $\alpha, \beta, \alpha+\beta$ *are in distinct* H*-cosets. Then it turns out that a basis of* $D(\alpha,\beta)$ *is* $\{1, g + 2g^2 + 6g^5 + 6g^6 + 5g^7 + 6g^8\}$ *and has dimension* 2. *Then*

$$D(\alpha,\beta) = \left\{ \sum_{i=1}^{2} v_i \alpha_i \mid \alpha_i \in \mathbb{F}_7 \right\}$$

where $v_1 = 1$ *and* $v_2 = g + 2g^2 + 6g^5 + 6g^6 + 5g^7 + 6g^8$. *Hence* $|D(\alpha, \beta)| = 7^2$ *and* 2 *does not divide* 9. *Thus* $D(\alpha, \beta)$ *is not a finite field.*

4. *We also consider the Dickson pair* $(q, n) = (5, 8)$. *Let* g *be such that* $\mathbb{F}_{5^8}^* = \langle g \rangle$ *and* $H = \langle g^8 \rangle$. *We know that* $D(\alpha, \beta)$ *is an* $\mathbb{F}_5$*-vector space. Also* $\mathbb{F}_{5^8}$ *is an* $\mathbb{F}_5$*-vector space with a basis* $\{1, g^2, \ldots, g^7\}$. *We take a pair of elements in* $\mathbb{F}_{5^8}^*$

$$\alpha = 3g^6 + 4g^4 + 3g^3 + 3g^2 + 2g + 2$$

and

$$\beta = 4g^7 + g^6 + g^5 + 3g^4 + 4g^2 + 3g + 2$$

such that $\alpha, \beta, \alpha + \beta$ *are in distinct* H*-cosets. Then*

$$D(\alpha, \beta) = \left\{ \sum_{i=1}^{2} v_i \alpha_i \mid \alpha_i \in \mathbb{F}_5 \right\}$$

where $v_1 = 1$ *and* $v_2 = 2g^7 + 3g^6 + g$ *and* $D(\alpha, \beta)$ *has dimension* 2. *Hence* $|D(\alpha, \beta)| = 5^2$. *Note that* 2 *divides* 8. *But* $D(\alpha, \beta)$ *is not closed under the finite field multiplication. To see this,*

$$v_2^2 = v_2 \cdot v_2 = 4g^7 + g^6 + 2g^5 + g^4 + 2g^3 + 3g^2 + 2g + 4.$$

In fact

$$v_2^2 \notin D(\alpha, \beta).$$

Hence $D(\alpha, \beta)$ *is not a finite field.*

Example 5.4.4 leads us to deduce that if α, β and $\alpha + \beta$ belong to distinct H-cosets then $D(\alpha, \beta)$ is not in general a subfield of the finite field $\mathbb{F}_{q^n}$. During 1971 and 1972, Dancs showed in [8, 9] that the subnearfield structure of a finite nearfield is analogous to the subfield structure of finite fields.

Theorem 5.4.5. *([8, 9]) Let* R *be a finite nearfield of order* q^n, *where* $q = p^l$ *for some prime* p.

(i) If K *is a subnearfield of* R, *then* $|K| = p^h$ *with* h *dividing* ln.

(ii) Conversely, if h *divides* ln, *then* R *has a unique subnearfield* K *of order* p^h.

Let $R \in DN(q,n)$ where $n > 2$. Let $(\alpha,\beta) \in R^2$. Looking at $D(\alpha,\beta)$ where $\alpha,\beta,\alpha+\beta$ are all in distinct H-cosets, assume that $(\alpha,\beta,\alpha+\beta) \in g^{[r]_q}H \times g^{[s]_q}H \times g^{[t]_q}H$ such that r,s,t are all distinct. Then

$$D(\alpha,\beta) = \left\{\lambda \in R \ : \ \alpha(\lambda^{q^t} - \lambda^{q^r}) = \beta(\lambda^{q^s} - \lambda^{q^t})\right\}.$$

By Example 5.4.4 and appealing to Theorem 5.4.5, if we take the Dickson pair $(7,9)$ we see that there exist some pairs (α,β) such that $D(\alpha,\beta)$ is not a subnearfield of $DN_g(7,9)$.
Furthermore by proof of Theorem 5.3.2 the following is an immediate consequence:

Corollary 5.4.6. *Let (q,n) be a Dickson pair with $q = p^l$ for some prime p and positive integers l,n such that $n > 2$. Let g be a generator of $\mathbb{F}_{q^n}^*$ and let R be the nearfield constructed with $H = \langle g^n \rangle$. Let $(\alpha,\beta) \in R^2$. We have the following:*

(i) If all $\alpha,\beta,\alpha+\beta$ belong to the same H-coset then $D(\alpha,\beta) = R$ and so is also a subnearfield of R.

(ii) If two of $\alpha,\beta,\alpha+\beta$ belong to $g^{[s]_q}H$ and the third to $g^{[t]_q}H$ such that $\mathrm{GCD}(t+n-s,n) = 1$ where $s \neq t$ then by the proof in Theorem 5.3.2 and Theorem 5.2.1 $D(\alpha,\beta) = D(R)$ is a subnearfield of R. Furthermore $C\big(D(\alpha,\beta)\big) = C\big(D(R)\big) = D(R) \cap GC(R)$.

Remark 5.4.7. *Let $(q = p^l, n)$ be a Dickson pair and $R = DN_g(q,n)$ where g is a generator of $\mathbb{F}_{q^n}^*$ and R the finite nearfield constructed with $H = \langle g^n \rangle$. Every $\mathbb{F}_{p^k}$ with k dividing l is a subnearfield of $DN_g(q,n)$. To see this, by Theorem 5.2.1 $D(R)$ is a subnearfield of R. Also by Theorem 5.2.4 $D(R)$ is a finite field, so isomorphic to $\mathbb{F}_{p^l}$. It is known that $\mathbb{F}_{p^k}$ can be embedded into $\mathbb{F}_{p^l}$ if and only if k divides l. So every $\mathbb{F}_{p^k}$ with k dividing l can be embedded into $DN_g(q,n)$. Note that inside $\mathbb{F}_{p^k}$ the multiplication is different, but $\mathbb{F}_{p^k}$ is isomorphic to a subfield of $\mathbb{F}_{p^l}$ which is a subnearfield of $DN_g(q,n)$. Hence $\mathbb{F}_{p^k}$ is a subnearfield of $DN_g(q,n)$. Observe that k must divide l, dividing ln is not enough.*

Furthermore, if two of $\alpha,\beta,\alpha+\beta$ belong to $g^{[s]_q}H$ and the third to $g^{[t]_q}H$ such that $\mathrm{GCD}(t+n-s,n) = 1$ where $s \neq t$ then by proof of Theorem 5.3.2 $D(\alpha,\beta) = \mathbb{F}_{p^{l\cdot\mathrm{GCD}(t+n-s,n)}}$. Suppose $\mathrm{GCD}(t+n-s,n) \neq 1$. Then $l \cdot \mathrm{GCD}(t+n-s,n)$ cannot divide l. Hence by Theorem 5.4.5 $D(\alpha,\beta)$ cannot be a subnearfield of $D(R) = \mathbb{F}_{p^l}$.

5.5 Concluding comments

We have determined $D(\alpha, \beta)$ for a given $(\alpha, \beta) \in R^2$ and showed that it is used in the determination of $s(R^m)$ by the implementation of the *EGE algorithm*. Some computational methods have been implemented in Sage. It shouldn't be too hard to use the characterization of the 7 exceptional finite nearfields to determine their generalized distributive sets. Furthermore, the proof of Theorem 5.3.2 can be shortened because every $\lambda \in \mathbb{F}_{p^k}$ is a solution of Equation (5.3.1) if and only if λ is fixed by the automorphism $\phi : \lambda \mapsto \lambda^{p^k}$. It is known that the set of all elements of a fixed field F left fixed by a given automorphism ϕ of F is a subfield of F. Note that we include our proof of determining explicitly the solutions of Equation (5.3.1) because it was later used in Lemma 5.4.1 and Corollary 5.4.6. It seems appropriate to close with further problems on the set of distributive elements and seed number.

- Let (q, n) be a Dickson pair with $q = p^l$ for some prime p and integers l, n such that $n > 2$. Let g be a generator of $\mathbb{F}_{q^n}^*$ and R the nearfield constructed with $H = \langle g^n \rangle$. Let $(\alpha, \beta, \alpha + \beta) \in g^{\frac{q^r-1}{q-1}} H \times g^{\frac{q^s-1}{q-1}} H \times g^{\frac{q^t-1}{q-1}} H$ such that r, s, t are all distinct. Can we find a condition on (q, n) such that $D(\alpha, \beta)$ is a always subfield of $\mathbb{F}_{q^n}$? To answer this question, from some computational methods, we suggest the following:

  Conjecture 5.5.1. *If n divides $q - 1$ then $D(\alpha, \beta)$ is always a subfield of $\mathbb{F}_{q^n}$.*

- Can we find a sufficient condition on the Dickson pair (q, n) such that $D(\alpha, \beta)$ is a subnearfield of $DN_g(q, n)$?

Chapter 6

Conclusion and perspectives

This thesis has as its main motivation to add to the body of nearfield theory, especially with regard to finite dimensional Beidleman near-vector spaces. In contrast to vector spaces, there do not exist k vectors that span the whole finite dimensional vector space F^m where $k < m$ and F is a field. However for the case of finite dimensional Beidleman near-vector spaces there exist such vectors that yield the whole space of R^m where R is a proper nearfield (see Theorem 4.3.18 in Chapter 4). In Chapter 4 we showed the classification of the R-subgroups of R^m from a finite set of vectors. In the process of finding an explicit description of the smallest R-subgroup containing a given set of vectors, Theorem 4.3.2 illustrated that the union of p-linear combinations of these vectors will be used. Suppose that there exists a finite set of vectors in R^m such that the smallest R-subgroup containing these vectors is the whole space R^m, then there exists a smallest positive integer p for which the p-linear combinations of these vectors will yield the whole space R^m. An interesting question is to find a tight bound on positive integers p for which the p-linear combinations of a finite set of vectors yield the whole space. We now introduce the following concepts.

Definition 6.0.1. *Let R be a finite nearfield. A finite set of vectors $V = \{v_1, \ldots, v_k\}$ in R^m is called γ-linearly dependent for some positive integer γ if there exists $v_i \in V$ such that $v_i \in LC_\gamma(v_1, \ldots, v_{i-1}, \widehat{v_i}, v_{i+1}, \ldots, v_k)$. We define V to be γ-linearly independent if V is not γ-linearly dependent.*

Definition 6.0.2. *Let R be a finite nearfield and $v_1, \ldots, v_k \in R^m$ be a finite set of vectors such that $k \geq 2$. Suppose that $gen(v_1, \ldots, v_k) = R^m$. We define the index*

of R-linearity of $v_1, \ldots, v_k \in R^m$ *to be*

$$I(v_1, \ldots, v_k) = \min\{p \in \mathbb{N} \ : \ LC_p(v_1, \ldots, v_k) = R^m\}$$

the smallest positive integer for which the p-linear combinations of the vectors $v_1, \ldots, v_k$ *yields the whole space* R^m.

Suppose that there exists $V = \{v_1, \ldots, v_k\}$ a finite set of vectors in R^m such that $gen(V) = R^m$. Since $\mathbb{N}$ is an ordered set then $I(V)$ is well-defined.

Example 6.0.3. *Taking* $n = 3$, *it has been shown by Theorem 4.3.18 that there exists* $v_1 = (1,0,1)$ *and* $v_2 = (1,1,0)$ *in* R^3 *such that* $gen(v_1, v_2) = R^3$. *Note that* $LC_2(v_1, v_2) = R^3$ *and* $LC_1(v_1, v_2) \neq R^3$. *Hence* $I(v_1, v_2) = 2$.

Lemma 6.0.4. *Let R be a finite nearfield and* $V = \{v_1, \ldots, v_k\}$ *be a finite set of vectors in* R^m *and* $|R| = t$. *Then* $|LC_1(V)| \leq t^k$. *Furthermore, if V is 2-linearly independent every element of* $LC_1(V)$ *is unique,* $|LC_1(V)| = t^k$ *and* $k \leq m$.

Proof. Let $u, v \in LC_1(V)$ such that $u = \sum_{i=1}^{k} v_i\alpha_i$ and $v = \sum_{j=1}^{k} v_i\beta_j$ where $(\alpha_1, \ldots, \alpha_k) \neq (\beta_1, \ldots, \beta_k)$. Without loss of generality we can assume that $\alpha_1 \neq \beta_1$. Suppose that $u = v$. Then $v_1\alpha_1 - v_1\beta_1 = \sum_{i=2}^{k} v_i\alpha_i - \sum_{j=2}^{k} v_i\beta_j$. It follows that

$$v_1 = \Big(\sum_{j=2}^{k} v_i(\beta_i - \alpha_i)\Big)(\alpha_1 - \beta_1)^{-1}.$$

Thus $v_1 \in LC_2(v_2, \ldots, v_k)$, so V is 2-linearly dependent, a contradiction. Therefore if V is 2-linearly independent then $|LC_1(V)| = t^k$. Suppose that V is 2-linearly independent and $k > m$, we have $|LC_1(V)| = t^k > t^m$ and all the t^k are distinct. This contradicts the fact that we have at most t^m vectors in the space. Hence $t \leq m$. □

It might be interesting to investigate the notions of index of R-linearity. Suppose the vectors $v_1, \ldots, v_k \in R^m$ which are γ-linearly independent for some positive integer γ and $gen(v_1, \ldots, v_k) = R^m$.

- Can we find a tight bound on $I(v_1, \ldots, v_k)$?
- Can we find an explicit algebraic expression of $I(v_1, \ldots, v_k)$ as a function of $k, |R|, m$?

In Chapter 5 the generalized distributive set $D(\alpha, \beta)$, for $\alpha, \beta \in R$, was central topic of investigation. We primarily focused on the case where R is a finite Dickson nearfield. It might also be interesting to investigate $D(\alpha, \beta)$ for the case of infinite nearfields. However, some years ago, there were some attempts to study infinite nearfields with some sort of finiteness conditions imposed on them ("locally finite" and "pseudo-finite" are two, but perhaps there are more). We don't know if there are any results on their centers, but for us that seems like a reasonable way to start thinking about the infinite case. It might be fruitful to classify nearfields according to when their multiplicative centers are subnearfields.

Appendices

Appendix A

The EGE algorithm

A.1 The smallest R-subgroup containing a given set of vectors

Algorithm A.1.1. *The Expanded Gaussian Elimination (EGE) computes the smallest R-subgroup containing a given set of vectors in R^m. The algorithm implements the normal Gaussian elimination plus the distributivity trick.*

Input: $v_1, v_2, \ldots, v_k \in R^n$ *for* $R \in DN(q,n)$ *where* $n > 1$, *arranged in a matrix* $V = (v_i^j)_{1\leq i\leq k, 1\leq j\leq m} \in R^{k\times m}$.

Step 1 $W = RREF(V)$ *(reduced row echelon form of V by Gaussian elimination operations).*

Step 2

Case 1 *Suppose that every column of W has at most one non-zero entry. Then* $gen(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k} w_i R$.

Case 2 *Suppose that j-th column is the first and the only column of W that has at least two non-zero entries denoted by* $w_r^j, w_s^j, w_t^j, \ldots$ *where* $r < s < t < \cdots$

Subcase 1 *Consider the first two non-zero entries say* $w_r^j \neq 0 \neq w_s^j$ *with* $r < s$.
Apply the first 'distributivity trick' by creating the new row ϕ.

Subcase 2 *Consider the first two non-zero entries say* $\phi^j \neq 0 \neq w_t^j$.
Apply the second 'distributivity trick'.

$\vdots$

Continue this manner until in the j-th column we have only one non-zero entry.

Case 3 *Suppose that there exists at least one non-zero entries at j-th, $(j+1)$-th, $(j+2)$-th, ..., m-th columns of W. Then apply the 'distributivity trick' on the columns where there is more than one non-zero entries until we have only one non-zero entry in every column.*

Output: *The final matrix $U = (u_i^j)_{1\leq i\leq k', 1\leq j\leq m} \in R^{k'\times m}$ which has at most one non-zero entry in every column. Let $u_1, \ldots, u_{k'}$ be the rows of U. We have, $gen(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} u_i R$.*

A.2 Classification of all R-subgroups of R^m

Algorithm A.2.1. *Let H be an R-subgroup of R^m*
If $H = \{0\}$ then done
Let $x_1 \in H \setminus \{0\}$ then $gen(x_1) \subseteq H$
Elseif $H = gen(x_1)$
Let $x_2 \in H \setminus gen(x_1)$ then $gen(x_1, x_2) \subseteq H$
Elseif $H = gen(x_1, x_2)$
Let $x_3 \in H \setminus gen(x_1, x_2)$ then $gen(x_1, x_2, x_3) \subseteq H$
$\ddots\ \ddots$

Let $x_k \in H \setminus gen(x_1, x_2, \ldots, x_{k-1})$ then $gen(x_1, x_2, x_3, \ldots, x_k) = H$.

Appendix B

The AEGE algorithm

Algorithm B.0.1. *The Adjustment Expanded Gaussian Elimination (AEGE) computes the smallest subspace containing a given set of vectors in R^m. The algorithm implements the expanded Gaussian elimination plus the adjustment trick.*

Input: *$v_1, v_2, \ldots, v_k \in R^m$ for $R \in DN(q,n)$ where $n > 1$ arranged in a matrix $V = (v_i^j)_{1 \leq i \leq k, 1 \leq j \leq n} \in R^{k \times m}$.*

Step 1 *Apply EGE and we get $gen(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} u_i R$.*

Step 2

Case 1 *Suppose that u_i for $i = 1, \ldots, k'$ has exactly one non-zero entry. Then $span(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} u_i R$.*

Case 2 *Suppose that u_i is the only row that has more than one non-zero entries, say $u_i^{j_1}, u_i^{j_2}, u_i^{j_3}, \ldots$. Apply the "adjustment trick" (see in the proof of Theorem 4.4.1) on the row u_i until we eliminate occurrences of multiple non-zero entries while appending new vectors with only one non-zero entry.*

Case 3 *Suppose that the rows $u_i, u_{i+1}, u_{i+7}, \ldots, u_{k'}$ have each more than one non-zero entry. Apply on each row the "adjustment trick".*

Output: *The final matrix $E = (e_i^j)_{1 \leq i \leq k'', 1 \leq j \leq n} \in R^{k'' \times n}$ which has at most one non-zero entry in every row and column. Let $e_1, \ldots, e_{k'}$ be the rows of E. We have, $span(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k''} e_i R$.*

Appendix C

The DSS Algorithm

Algorithm C.0.1. *Let R be a finite Dickson nearfield that arises from the Dickson pair (q,n). In this section we give more details about the pseudo-code that we have implemented in Sage for some tests on $D(\alpha,\beta)$ for a given $(\alpha,\beta) \in R^2$. The algorithm called "DSS" (Distributive Set Subfields) tests if $D(\alpha,\beta)$ for a given pair $(\alpha,\beta) \in g^{[r]_q}H \times g^{[s]_q}H$ for some positive integers r,s, is a subfield of $\mathbb{F}_{q^n}$. The algorithm is described as follows:*
Step 1: Dickson pair

We define the ***function isDicksonpair***(q,n). *Note that isDicksonpair(q,n) returns True if (q,n) is a Dickson pair, false if it is not and list all Dickson pairs (p^l,n) such that $(p,n,l) \in \{1,\ldots,x\} \times \{1,\ldots,y\} \times \{1,\ldots,z\}$ where x,y and z are three positive integers.*

Denote by H a subgroup of $\mathbb{F}_{q^n}^*$ generated by g^n. Each non-zero element α of $\mathbb{F}_{q^n}^*$ is then in an H-coset of the form $g^{\frac{q^j-1}{q-1}}H$. The next function computes the value of j in $\{0,1,...,n-1\}$ for α to be in $g^{\frac{q^j-1}{q-1}}H$.
Step 2: Index of** H**-coset

Input: *An element α in $\mathbb{F}_{q^n}^*$.*
Output: *The index j of α if it exists, false if it doesn't.*

---

define ***function isDicksonpair***(q,n)

1. $\mathbb{F}_{q^n}^* = \langle g \rangle$

2. *define* ***function associatedcoset***(α)
3. ***if*** $\alpha \neq 0$
4. $idx = \log(\alpha, g)$ *(return the logarithm of* α *to the base of* g*).*
5. ***else return*** *False*
6. $idx = idx \mod (n)$

   (since $H =< g^n >$ *we only care about idx modulo n).*
7. ***for*** $j \in \{0, \ldots, n\}$ ***do***
8. $k = \frac{q^j - 1}{q - 1}$
9. $k = k \mod (n)$
10. ***if*** $idx = k$ ***then***
11. ***return*** j

Step 3: Matrix basis

Input: $\alpha, \beta \in \mathbb{F}_{q^n}$.
Output: *Basis for the space of solutions* λ *to the equation* $\phi(\lambda) = 0$*. The idea is to perform this test on various randomly chosen* $\alpha, \beta \in \mathbb{F}_{q^n}^*$.

---

1. *define* ***function*** $\phi(\alpha, \beta, \lambda, r, s, t)$
2. ***return*** $\alpha(\lambda^{q^t} - \lambda^{q^r}) - \beta(\lambda^{q^s} - \lambda^{q^t})$
3. *define* ***function performtest***(α, β)
4. $r = associatedcoset(\alpha)$
5. $s = associatedcoset(\beta)$
6. $t = associatedcoset(\alpha + \beta)$
7. ***if*** $r = s$ *or* $r = t$ *or* $s = t$ ***then***
8. ***return*** *"* $D(\alpha, \beta)$ *is finite field"*
9. ***else***

10. ***for*** $j \in \{0, \ldots, n-1\}$ ***do***
11. $M \longleftarrow$ *matrix associated to* $\phi(\alpha, \beta, g^j, r, s, t)$
12. $K \longleftarrow$ *kernel* (M)
13. ***if*** $\dim(K) > 1$ ***then***
14. ***return*** K
15. ***if*** *isDicksonpair*(q, n) ***then***
16. ***for*** $r_1 \in \{1, \ldots, q^n - 1\}$ ***do***
17. ***for*** $r_2 \in \{1, \ldots, q^n - 1\}$ ***do***
18. $\alpha \leftarrow g^{r_1}$
19. $\beta \leftarrow g^{r_2}$
20. *performtest*(α, β)

Step 4: Row vector to field element

Input: *A row vector from the matrix basis K of* $D(\alpha, \beta)$ *over* $\mathbb{F}_q$.
Output: *Field element of* $D(\alpha, \beta)$.

---

1. *define* ***function rowvectortofieldelement***(v)
2. $a \longleftarrow 0$
3. $k \longleftarrow$ *number of column in v (length* (v)*).*
4. ***for*** $i \in \{1, \ldots k\}$
5. $a \longleftarrow \sum_{i=1}^{k} v[i] * g^{i-1}$
6. ***return*** a

Step 5: Field test

1. *define* ***function isfield***(K)
2. ***if*** $\dim(K) = 1$ ***then***

3. ***return*** *True*
4. ***else***
5. $B \longleftarrow$ *set constituted by rows vectors in K.*
6. ***for*** $i \in B$ ***do***
7. ***for*** $j \in B$ ***do***
8. $b_1 \leftarrow rowvectortofieldelement(i)$
9. $b_2 \leftarrow rowvectortofieldelement(j)$
10. $b \leftarrow b_1 b_2^{-1}$
11. ***if*** *row vector*$(b) \notin K$ ***then***
12. ***return*** *False*

Input: *The matrix* $K = Kernel(M)$.
Output: $D(\alpha, \beta)$ *is a finite field or not.*

---

1. ***if*** *isfield(K)* ***then***
2. ***write*** *"*$D(\alpha, \beta)$ *is a finite field".*
3. ***else***
4. ***write*** *"*$D(\alpha, \beta)$ *is not a finite field".*

List of References

[1] E. Aichinger, F. Binder, J. Ecker, P. Mayr, and C. Nöbauer. Sonata–system of near-rings and their applications. *GAP package*, 2, 2012.

[2] E. Aichinger and M. Farag. On when the multiplicative center of a near-ring is a subnear-ring. *Aequationes mathematicae*, 68(1-2):46–59, 2004.

[3] J. André. Lineare algebra über fastkörpern. *Mathematische Zeitschrift*, 136(4):295–313, 1974.

[4] J. A. Beachy. *Introductory lectures on rings and modules*, volume 47. Cambridge University Press, 1999.

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

[6] G. Betsch. *Near-rings and near-fields*, volume 137. Elsevier, 2011.

[7] G. A. Cannon, M. Farag, and L. Kabza. Centers and generalized centers of near-rings. *Communications in Algebra*, 35(2):443–453, 2007.

[8] S. Dancs. The sub-near-field structure of finite near-fields. *Bulletin of the Australian Mathematical Society*, 5(02):275–280, 1971.

[9] S. Dancs. On finite dickson near-fields. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 37, pages 254–257. Springer, 1972.

[10] L. E. Dickson. On finite algebras. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1905:358–393, 1905.

[11] P. Djagba. On the generalized distributive set of a finite nearfield. *Journal of Algebra*, 542:130–161, 2020.

[12] P. Djagba and K.-T. Howell. The subspace structure of finite dimensional beidleman near-vector spaces. *Linear and Multilinear Algebra, accepted to appear*, 2019.

[13] E. Ellers and H. Karzel. Endliche inzidenzgruppen. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 27, pages 250–264. Springer, 1964.

[14] M. Farag. Hill ciphers over near-fields. *Mathematics and Computer Education*, 41(1):46, 2007.

[15] J. Goldman and G.-C. Rota. On the foundations of combinatorial theory iv finite vector spaces and eulerian generating functions. *Studies in Applied Mathematics*, 49(3):239–258, 1970.

[16] K.-T. Howell. *Contributions to the theory of near vector spaces*. PhD thesis, University of the Free State, 2007.

[17] K.-T. Howell. On subspaces and mappings of near-vector spaces. *Communications in Algebra*, 43(6):2524–2540, 2015.

[18] K.-T. Howell and J. Meyer. Finite-dimensional near-vector spaces over fields of prime order. *Communications in Algebra*, 38(1):86–93, 2009.

[19] K.-T. Howell and J. Meyer. Near-vector spaces determined by finite fields. *Journal of Algebra*, 398:55–62, 2014.

[20] T. E. Hull and A. R. Dobell. Random number generators. *SIAM review*, 4(3):230–254, 1962.

[21] D. E. Knuth. Subspaces, subsets, and partitions. *Journal of Combinatorial Theory, Series A*, 10(2):178–180, 1971.

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

[23] J. Malone Jr and H. Heatherly. Some near-ring embeddings. *The Quarterly Journal of Mathematics*, 20(1):81–85, 1969.

[24] J. D. Meldrum. *Near rings and their links with groups*. Number 134. Pitman Advanced Publishing Program, 1985.

[25] B. H. Neumann. On the commutativity of addition. *Journal of the London Mathematical Society*, 1(3):203–208, 1940.

[26] G. Pilz. *Near-rings: the theory and its applications*, volume 23. Elsevier, 2011.

[27] A. P. van der Walt. Matrix near-rings contained in 2-primitive near-rings with minimal subgroups. *Journal of Algebra*, 148(2):296–304, 1992.

[28] O. Veblen and J. Maclagan-Wedderburn. Non-desarguesian and non-pascalian geometries. *Transactions of the American Mathematical Society*, 8(3):379–388, 1907.

[29] H. Wähling. *Theorie der Fastkörper*, volume 1. Thales Verlag, 1987.

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

[31] J. Zemmer. The additive group of an infinite near-field is abelian. *Journal of the London Mathematical Society*, 1(1):65–67, 1969.

[32] J. L. Zemmer. Near-fields, planar and non-planar. *Math. Student*, 31:145–150, 1964.