Contributions to the theory of Near-vector spaces

by

Sogo Pierre Sanon

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

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

Supervisor: Dr. Karin-Therese Howell

December 2017

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.

Signature: ....Sogo Pierre Sanon....

Date: ....December 2017....

Abstract

Contribution to the theory of Near-vector spaces

Sogo Pierre Sanon

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

Thesis: MSc

December 2017

The purpose of this thesis is to give an exposition and expand the theory of near-vector spaces. Near-vector space theory is a new and rich field of mathematics and has been used in several applications, including in secret sharing schemes in cryptography and to construct interesting new examples of planar near-rings. There are two type of near-vector spaces, we focus on the near-vector space defined by André in [2]. After giving several elementary definitions and properties in Chapter 2, we present the theory of near-vector spaces in Chapter 3. In [13] van der Walt showed how to construct an arbitrary finite-dimensional near-vector space, using a finite number of near-fields, all having isomorphic multiplicative semigroups. The majority of the results did not contain complete proofs and explanation. Chapter 4 is dedicated to the proofs and explanations of these results. In Chapter 5 we investigate the linear mappings of near-vector spaces. New results are presented in this section which have been accepted for publication.

Uittreksel

Contribution to the theory of Near-vector spaces

("Contribution to the theory of Near-vector spaces")

Sogo Pierre Sanon

Departement Wiskuudige Wetenskappe,
Universiteit van Stellenbosch,
Privaatsak X1, Matieland 7602, Suid Afrika.

Tesis: MSc

Desember 2017

Die doel van hierdie tesis is om 'n uiteensetting en uitbreiding van die teorie van byna-vektorruimtes te gee. Die teorie van byna-vektorruimtes is 'n nuwe en ryk veld van wiskunde wat al in verskeie toepassings gebruik is, insluitend geheimdelingskemas in kriptografie en om nuwe interessante voorbeelde van planêre bynaringe te konstruktueer. Daar is twee tipes byna-vektorruimtes, ons fokus op die een gedefinieer deur André in [2]. Na ons in Hoofstuk 2 verskeie elementêre definisies en eienskappe gegee het, bied ons die teorie van byna-vektorruimtes in Hoofstuk 3 aan. In [13] het van der Walt gewys hoe om 'n arbitrêre eindig-dimensionele byna-vektorruimte te konstrueer deur gebruik te maak van 'n eindige aantal byna-liggame, met isomorfe vermenigvuldings semi-groepe. Die meerderheid van die resultate het nie volledige bewyse en verduidelikings bevat nie. Hoofstuk 4 is toegewy aan die bewyse en verduidelikings van hierdie resultate. In Hoofstuk 5 ondersoek ons die lineêre afbeeldings van byna-vektorruimtes. Nuwe resultate wat reeds vir publikasie goedgekeur is, word in hierdie afdeling aangebied.

Acknowledgements

Foremost, I wish to thank my supervisor Dr Karin-Therese Howell (Stellenbosch University) for her constructive criticism and patience with me. Her guidance and friendliness helped me to get the best out of this thesis.
To my family, I say thank you for your encouragement, continuous prayers. I record my gratitude to you for believing in me and for standing by me. You have always supported me and I will always be proud to have you as family. I sincerely appreciate you.

Dedications

To my family

Contents

Nomenclature

Symbols

$\subseteq$	Inclusion.
$\subsetneq$	Strict inclusion.
$(R, +, \cdot)$	Near-ring.
R_0	Zero-symmetric part of R.
R_c	Constant part of R.
$S \leqslant R$	S is a sub-near-ring of R
R_d	The set of distributive elements of R.
$Hom(R, R')$	the set of all near-rings homomorphisms from R to R'.
$End(R) = Hom(R, R)$	.
Id_R	Identity homomorphism of R.
$I \trianglelefteq R$	I is an Ideal of R.
$I \trianglelefteq_l R$	I is a left ideal of R.
$I \trianglelefteq_r R$	I is a right ideal of R.
$Hom_R(G_1, G_2)$	The set of all R-homomorphisms from G_1 to G_2.
$End_R(G) = Hom_R(G, G)$	.
Id_R	Identity R-homomorphism of G.
$Ann_R(X)$	The annihilator of X.
$H \leqslant_R G$	H is an R-submodule of G.
$G' \trianglelefteq_R G$	G' is an R-ideal of G.
$\ker f$	The kernel of f.
$S \cong S'$	S isomorphic to S'.
$GF(p^n)$	The Galois field of order p^n, with p a prime.
(V, F)	F-group.

$Q(V)$ The quasi-kernel of (V, F).

$\lhd$ A dependence relation.

$\overline{S}$ The algebraic closure of S.

cl A closure operator.

$C := End_R(G)$ The R-centrilizer of G.

$D^0 = D \cup \{0\}$.

cp Compatibility relation.

$G^* = G \setminus \{0\}$.

$St_A(g)$ The stabilizer of $g \in G$ in A.

$rk(r)$ The rank of r.

$A \oplus B$ The direct sum of A and B.

$F^n = \underbrace{F \oplus \cdots \oplus F}_{ntimes}$.

$L_A(V)$ The set of all linear mappings from V to itself.

$M_A(V)$ The set of all homogeneous functions of V into itself.

$\mathcal{L}(V, W)$ The set of all linear mappings from V to W.

Chapter 1

Introduction

Near-rings are generalized rings. A near-ring is an algebraic structure which satisfies all the axioms of a ring except for commutativity of addition and one of the two distributive laws. They arise in a natural way. The set $M(G)$ of all mappings of a group $(G,+)$ into itself, with the usual addition and composition of mappings is, a near-ring.

For near-rings it is proven in ([12], Theorem 1.86) that every near-ring can be embedded into $M(\Gamma)$ for some group Γ. There is the analogous result from ring theory which says that every ring can be embedded into the ring $E(\Gamma)$ of all endomorphisms of some abelian group Γ. Hence one might view ring theory as the “linear theory of group mappings", while near-rings provide the “non-linear theory". Surprisingly, a lot of “linear" results can be transferred to the general case after suitable changes.

Historically, the first step toward near-rings was an axiomatic research done by the American mathematician Leonard Eugene Dickson in 1905. Some years later these near-fields showed up again and proved to be useful in coordinatizing certain important classes of geometric planes (see [12]). It was Zassenhaus who was able to determine all finite near-fields ([12], Theorem 8.34).

Near-rings might also be the appropriate tool to develop a “non-abelian homological algebra" and show up again in algebraic topology, functional analysis and categories with groups objects ([12]). Near-rings and near-ring modules are useful for a number of theories which try to generalize “linear" results to the "non-linear case", for instance in the theory of near-vector spaces.

The concept of a vector space, i.e., linear space, can be generalized to a structure comprising a bit more non-linearity, the so-called near-vector space. There are two types of near-vector spaces, those studied by André and those studied by Beidleman ([3]). The André near-vector space uses automorphisms in the construction, resulting in the right distributive law holding. However, for the Beidleman near-vector space, we have the left distributive law and near-ring modules are used in the construction.

In [13] van der Walt showed how to construct an arbitrary finite dimensional André near-vector space, using a finite number of near-fields, all having isomorphic multiplicative semigroups. In [8] this construction is used to characterize all finite dimensional near-vector spaces over $\mathbb{Z}_p$, for p a prime. In [9] these results were extended to all finite-dimensional near-vector spaces over arbitrary finite fields. In [7] various constructions, ranging from those closest to vector spaces to those further away, were considered and discussed in terms of their quasi-kernel and regularity.

Regularity is a central notion in the study of near-vector spaces. An important theorem of André [2], the Decomposition Theorem, states that every near-vector space can be written as the direct sum of maximal regular subspaces. Moreover, this decomposition is unique. As a result, André wrote in his paper that the regular subspaces are the building blocks of near-vector spaces. We focus on André near-vector spaces.

Near-vector space theory is far from being a mere collection of trivial results without any application to other branches of mathematics. It is worth noting that recently near-vector spaces have been used in several applications, including in secret sharing schemes in cryptography [5] and to construct interesting examples of families of planar near-rings [4]. In addition, they have proved interesting from a model theory perspective too. The main purpose of this thesis is to give an exposition and expand the theory of near-vector spaces. We begin, in Chapter 2, with some preliminary material.

Chapter 3 is dedicated to the presentation of the theory of near-vector spaces. We study the concept of regularity which, as already mentioned, is a central notion in the study of near-vector spaces. In fact it largely reduces the theory of near-vector spaces to the theory of regular near-vector spaces. We also prove regularity for certain constructions of near-vector spaces.

In Chapter 4 we turn our attention to the work done by van der Walt [13]. He showed how to construct an arbitrary finite-dimensional near-vector space, using a finite number of near-fields, all having isomorphic multiplicative semigroups. We give a complete proof and explanation of his result (Theorem 4.1.43).

For vector spaces over fields it is well-known that every linear transformation between finite dimensional vector spaces can be represented as a matrix transformation. In addition, the set of all linear transformations between two vector spaces is itself a vector space over the same field. In Chapter 5 we investigate how the weakening of one of the distributive laws affects the set of all linear mappings between two near-vector spaces. This is my original work and it has been accepted for publication ([10]).

Chapter 2

Basic Definitions and Examples

This chapter introduces the basic theory of nearrings and nearfields, as given in Pilz ([12]). We do not include any proofs.

2.1 Nearrings

We start with elementary definitions and examples.

Definition 2.1.1. *([12], Definition 1.1) A right nearring is a set R together with two binary operations " $+$ " and " $\cdot$ " such that:*

1. *$(R, +)$ is a group (not necessarily abelian),*
2. *$(R, \cdot)$ is a semigroup,*
3. *$(r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$, for all $r_1, r_2, r_3 \in R$.*

We abbreviate $(R, +, \cdot)$ by R when the operations are clearly understood and omit the symbol " $\cdot$ " for multiplication if no confusion is possible.
We have the following examples :

Example 2.1.2.

1. *Let $(G, +)$ be a group. Then $(M(G), +, \circ)$ is a nearring under pointwise addition and composition, where*

$$M(G) := \{f : G \to G\}$$

the set of all mappings on G.

It is straightforward to see that $(M(G), +)$ is a group, and composition, "$\circ$", is an associative binary operation on $M(G)$. We also have that

$$(f+g)\circ h = f\circ h + g\circ h, \quad \forall f, g, h \in M(G).$$

So the right distributive law is satisfied.

2. *Let R be a commutative ring with unity. Then $(R[x], +, \circ)$ is a nearring, under pointwise addition and composition, where $R[x]$ is the set of all polynomials with coefficients in R.*

Similar to right nearrings we have the following definition for left nearrings:

Definition 2.1.3. *A left nearring is a set R together with two binary operations "$+$" and "$\cdot$" such that:*

1. *$(R, +)$ is a group (not necessarily abelian),*
2. *$(R, \cdot)$ is a semigroup,*
3. *$r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$, for all $r_1, r_2, r_3 \in R$.*

Although many authors prefer left nearrings, we use right nearrings. The theory runs completely parallel in both cases and unless stated otherwise by a nearring we mean a right nearring.
We now give some basic properties of a right nearring.

Proposition 2.1.4. *([12], Proposition 1.5) Let R be a nearring, and $r, r' \in R$. Then we have*

- $0r = 0$,
- $(-r)r' = -rr'$.

In general it is not true that $r(-r') = -rr'$ and $r0 = 0$ for all $r, r' \in R$. For example, in $M(\mathbb{R})$ we have $f \circ 0 = c$, with $f = c$, c a nonzero constant. This leads to the following definition:

Definition 2.1.5. *([12], Definition 1.7) Let R be a nearring.*

1. *The set $R_0 = \{r \in R | r0 = 0\}$ is called the zero-symmetric part of R.*
2. *The set $R_c = \{r \in R | r0 = r\}$ is called the constant part of R.*

A nearring R in which $r0 = 0$ for all $r \in R$ is called a zero-symmetric nearring.

We now turn our attention to the substructures of nearrings.

Definition 2.1.6. *([12], Definition 1.21) Let R be a nearring. A subset S of $(R, +, \cdot)$ is called a subnearring if $(S, +, \cdot)$ is a nearring. If S is a subnearring of R, then we write $S \leq R$.*

Example 2.1.7. *Let R be a nearring. R_0 and R_c are subnearrings of R.*

In the following definition we formally introduce the concept of a homomorphism of nearrings.

Definition 2.1.8. *([12], Definition 1.25) Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be two nearrings.*
A nearring homomorphism from R to R' is a mapping $h : R \rightarrow R'$ such that for all $r, s \in R$ we have

- $h(r + s) = h(r) + h(s)$,
- $h(rs) = h(r)h(s)$.

An epimorphism is a surjective homomorphism and a monomorphism is an injective homomorphism. If a homomorphism is bijective, i.e. surjective and injective, it is called an isomorphism. A homomorphism g from a set to itself is called an endomorphism. If g is bijective, it is called an automorphism. We say that R is embedded in R' if there exists a monomorphism from R to R'.
The set of all nearring homomorphisms from R to R' is denoted by $Hom(R, R')$.

Definition 2.1.9. *([12], Definition 1.11) Let R be a nearring. An element $r \in R$ is said to be*

1. *a left identity element if for all $r' \in R$, $rr' = r'$, a right identity element if $r'r = r'$ and a two-sided identity element, or an identity element, if it is both left and right identity,*

2. *left invertible if there is $r' \in R$ such that $rr' = 1$, right invertible if $r'r = 1$ and invertible if it is left and right invertible,*

3. *left cancellable if for all $r_1, r_2 \in R$ such that $rr_1 = rr_2$ then $r_1 = r_2$, right cancellable if $r_1r = r_2r$ then $r_1 = r_2$ and it is cancellable if it is left and right cancellable,*

4. *a left divisor of zero if* $r \neq 0$ *and there is* $r' \in R \setminus \{0\}$ *such that* $rr' = 0$*, a right divisor of zero if* $r'r = 0$ *and two-sided divisor of zero, of simply divisor of zero, if it is left and right divisor of zero,*

5. *idempotent if* $rr = r$ *and nilpotent if there is* $k \in \mathbb{N}$ *such that* $r^k = 0$*,*

6. *distributive if for all* $r_1, r_2 \in R$ *we have that* $r(r_1 + r_2) = rr_1 + rr_2$*.*

We now define some important types of nearrings.

Definition 2.1.10. *([12], Definition* 1.14*) A nearring R is said to be*

1. *abelian if* $(R, +)$ *is an abelian group,*

2. *commutative if* $(R, \cdot)$ *is a commutative semigroup,*

3. *distributive if* $R = R_d = \{d \in R | \forall r, r' \in R : d(r + r') = dr + dr'\}$*,*

4. *satisfying the left cancellation law if all non-zero elements of R are left cancellable, and the right cancellation law if all non-zero elements of R are right cancellable.*

5. *integral if R has no non-zero divisors of zero,*

6. *a nearfield if* $(R \setminus \{0\}, \cdot)$ *is a group.*

Example 2.1.11. *Let* $(G, +)$ *be a group.*

1. *The nearring* $M(G)$ *is abelian if G is abelian.*

2. *Let* $\circ$ *be the binary operation on G defined for all* $r, r' \in G$ *by*

$$r \circ r' = 0.$$

   Then $(G, +, \circ)$ *is a commutative nearring, because* $\circ$ *is commutative.*

3. *Let* $*$ *be the binary operation on G defined for all* $r, r' \in G$ *by*

$$r * r' = r.$$

   The nearring $(G, +, *)$ *is an integral nearring.*

   We note that if $r * r' = 0$*, then* $r = 0$*.*

Next we define the concept of ideals for nearrings.

Definition 2.1.12. *([12], Definition 1.27) Let $(R, +, \cdot)$ be a nearring. An ideal of R is a subset I of R such that*

1. $(I, +)$ *is a normal subgroup of* $(R, +)$,
2. $IR \subseteq I$, *i.e. for all* $r \in R, i \in I$ *we have* $ir \in I$,
3. $r(r' + i) - rr' \in I$ *for all* $r, r' \in R, i \in I$.

If I is an ideal of R, we write $I \trianglelefteq R$.

A right ideal is a normal subgroup of $(R, +)$ which satisfies 2. If a normal subgroup of $(R, +)$ satisfies 3, it is called a left ideal of R. The nearring R is called simple if its only ideals are $\{0\}$ and R. The symbols $\trianglelefteq_r$ and $\trianglelefteq_l$ are used to mean "right ideal" and "left ideal" respectively.

2.2 Nearfields

In this section we give some basic properties of nearfields.

Theorem 2.2.1. *([12], Theorem 8.11) If $(F, +, \cdot)$ is a nearfield, then $(F, +)$ is an abelian group.*

Example 2.2.2.

- *Every field and division ring is a nearfield.*
- *Consider the field $(GF(3^2), +, \cdot)$ with*

$$GF(3^2) := \{0, 1, 2, \gamma, 1 + \gamma, 2 + \gamma, 2\gamma, 1 + 2\gamma, 2 + 2\gamma\},$$

where γ is a zero of $x^2 + 1 \in \mathbb{Z}_3[x]$.
The operations on $GF(3^2)$ can be defined as follows:

$$+ : (a + b\gamma) + (c + d\gamma) = (a + c) mod3 \ + ((b + d) mod3 \ )\gamma,$$

$\cdot$	0	1	2	γ	$1+\gamma$	$2+\gamma$	2γ	$1+2\gamma$	$2+2\gamma$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	γ	$1+\gamma$	$2+\gamma$	2γ	$1+2\gamma$	$2+2\gamma$
2	0	2	1	2γ	$2+2\gamma$	$1+2\gamma$	γ	$2+\gamma$	$1+\gamma$
γ	0	γ	2γ	2	$2+\gamma$	$2+2\gamma$	1	$1+\gamma$	$1+2\gamma$
$1+\gamma$	0	$1+\gamma$	$2+2\gamma$	$2+\gamma$	2γ	1	$1+2\gamma$	2	γ
$2+\gamma$	0	$2+\gamma$	$1+2\gamma$	$2+2\gamma$	1	γ	$1+\gamma$	2γ	2
2γ	0	2γ	γ	1	$1+2\gamma$	$1+\gamma$	2	$2+2\gamma$	$2+\gamma$
$1+2\gamma$	0	$1+2\gamma$	$2+\gamma$	$1+\gamma$	2	2γ	$2+2\gamma$	γ	1
$2+2\gamma$	0	$2+2\gamma$	$1+\gamma$	$1+2\gamma$	γ	2	$2+\gamma$	1	2γ

We have that $(GF(3^2), +, \circ)$*, with*

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

is a (right) nearfield, but not a field.

$\circ$	0	1	2	γ	$1+\gamma$	$2+\gamma$	2γ	$1+2\gamma$	$2+2\gamma$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	γ	$1+\gamma$	$2+\gamma$	2γ	$1+2\gamma$	$2+2\gamma$
2	0	2	1	2γ	$2+2\gamma$	$1+2\gamma$	γ	$2+\gamma$	$1+\gamma$
γ	0	γ	2γ	2	$1+2\gamma$	$1+\gamma$	1	$2+2\gamma$	$2+\gamma$
$1+\gamma$	0	$1+\gamma$	$2+2\gamma$	$2+\gamma$	2	2γ	$1+2\gamma$	γ	1
$2+\gamma$	0	$2+\gamma$	$1+2\gamma$	$2+2\gamma$	γ	2	$1+\gamma$	1	2γ
2γ	0	2γ	γ	1	$2+\gamma$	$2+2\gamma$	2	$1+\gamma$	$1+2\gamma$
$1+2\gamma$	0	$1+2\gamma$	$2+\gamma$	$1+\gamma$	2γ	1	$2+2\gamma$	2	γ
$2+2\gamma$	0	$2+2\gamma$	$1+\gamma$	$1+2\gamma$	1	γ	$2+\gamma$	2γ	2

The nearfield $(GF(3^2), +, \circ)$ *is called a Dickson nearfield and it is the smallest nearfield that is not a field. See [12].*

Proposition 2.2.3. *([6], Theorem 2.5.5) Let* F *be a nearfield and* F_d *be the set of all distributive elements. Then*

- F_d *is a division ring.*
- F *can be considered as a right vector space over* F_d*.*

2.3 Nearring Modules

Definition 2.3.1. *([11], Definition 2.1) Let $(G,+)$ be a group, and $(R,+,\cdot)$ be a nearring. G is an R-module if there is a map μ defined by*

$$\begin{aligned} \mu : R \times G &\to G \\ (r,g) &\mapsto rg \end{aligned}$$

such that for all $r, r' \in R$ and $g \in G$,

- $(r + r')g = rg + r'g$,
- $(rr')g = r(r'g)$.

The following definition also holds for nearring modules.

Definition 2.3.2. *([11]) Let $(G,+)$ be a group, $(R,+,\cdot)$ be a nearring. Then G is a R-module if there is a nearring homomorphism $\theta : (R,+,\cdot) \to (M(G),+,\circ)$. The homomorphism θ is called a representation of R and θ is called faithful if $\ker\theta = 0$. If θ is faithful then G is said to be a faithful R-module.*
If G is an R-module, we write rg for $\theta(r)g$, for all $g \in G$ and $r \in R$.

Example 2.3.3. *([11], Definition 2.1) Let $(G,+)$ be a group, and let S be a sub-semigroup of endomorphisms of G. Then $M_S(G)$ defined by*

$$M_S(G) := \{\alpha \in M(G) | \alpha(s(g)) = s(\alpha(g)) \text{ for all } s \in S, g \in G\}$$

is a nearring and G is a faithful $M_S(G)$-module.

It is not difficult to verify that.

Proposition 2.3.4. *If G is abelian, $M_S(G)$ is abelian.*

Definition 2.3.5. *([12], Definition 1.25) Let G_1, G_2 be two R-modules. A mapping $f : G_1 \to G_2$ is called an R-homomorphism if for all $g, g' \in G_1$ and $r \in R$:*

- $f(g + g') = f(g) + f(g')$
- $f(rg) = rf(g)$.

The set of all R-homomorphisms from G_1 to G_2 is denoted $Hom_R(G_1, G_2)$ and the identity R-homomorphism from G to G is denoted by Id_G.

Example 2.3.6. *Let R be a nearring, and G be a R-module. Let $g \in G$. The mapping*

$$\begin{aligned} h_g : R &\to G \\ r &\mapsto rg \end{aligned}$$

is a R-homomorphism.
For $r, r_1, r_2 \in R$, we have
$h_g(r_1 + r_2) = (r_1 + r_2)g = r_1 g + r_2 g = h_g(r_1) + h_g(r_2)$ and
$h_g(rr_1) = (rr_1)g = r(r_1 g) = rh_g(r_1)$.

We now define the concept of annihilator.

Definition 2.3.7. *([12], Definition 1.41) Let R be a nearring and G an R-module. Let X, Y be subsets of G. We define the set $(X : Y)$ as follows*

$$(X : Y) = \{r \in R | ry \in X \text{ for all } y \in Y\}.$$

If $X = \{a\}$, we write $(a : Y)$ instead of $(\{a\} : Y)$.
Furthermore, for a subset X of G, the annihilator of X is the set $(0_G : X)$ and it is denoted by $Ann_R(X)$.

Remark 2.3.8. *If G is a faithful R-module of a nearring R, then $Ann_R(G) = \{0\}$.*

Proposition 2.3.9. *([12], Corollary 1.43) For all $g \in G$, $Ann_R(g)$ is a left ideal of R.*

Definition 2.3.10. *([12], Definition 1.21) Let R be a nearring and G an R-module. A subgroup H of G is called an R-submodule of G if H is an R-module. So H is an R-submodule of G if*

$$rh \in H, \text{ for all } r \in R \text{ and } h \in H.$$

We write $H \leq_R G$ if H is an R-submodule of G.

Definition 2.3.11. *([12], Definition 1.27) Let $(R, +, \cdot)$ be a nearring and G an R-module. A normal submodule G' of G is called an ideal of G or R-ideal of G if for all $g \in G$, $g' \in G'$ and $r \in R$,*

$$r(g + g') - rg \in G'.$$

If G' is an ideal of G, we write $G' \trianglelefteq_R G$.

Example 2.3.12. *Let R be a nearring and G, G' be R-modules and $f : G \to G'$ be an R-homomorphism. Then* $\ker f$ *is an R-submodule of G and in addition an R-ideal of G. We have* $(\ker f, +)$ *is a normal subgroup of* $(G, +)$. *It follows from the following, let $r \in R, g \in G$ and $g' \in \ker f$. Then*

$$f(r(g+g') - rg) = r\left(f(g) + f(g')\right) - rf(g) = rf(g) - rf(g) = 0,$$

since $f(g') = 0$. Hence $r(g+g') - rg \in \ker f$ and $\ker f$ is an R-ideal.
Also for $r \in R, g \in \ker f$, we have $f(rg) = rf(g) = 0$. Hence $R \ker f \subseteq \ker f$.

Remark 2.3.13. *If R is a nearring, then the R-ideals of R are the left ideals of R.*

Theorem 2.3.14. *([11], Lemma 2.27) Let R be a nearring, G an R-module and A, B be R-ideals of G. Then $A + B$ and $A \cap B$ are also R-ideals of G.*

Proposition 2.3.15. *([12], Remark 1.28) Let R be a nearring and G an R-module. A submodule I of R (H of G) is an ideal (R-ideal) if and only if $r_1 \equiv r_1'(\text{mod } I)$ and $r_2 \equiv r_2'(\text{mod } I)$ ($g_1 \equiv g_1'(\text{mod } H)$ and $g_2 \equiv g_2'(\text{mod } H)$) implies that*

$$r_1 + r_2 \equiv (r_1' + r_2')(\text{mod } I) \text{ and } r_1 r_2 \equiv (r_1' r_2')(\text{mod } I),$$

$$\left(g_1 + g_2 \equiv (g_1' + g_2')(\text{mod } H) \text{ and } rg_1 \equiv rg_1'(\text{mod } H)\right), \text{ respectively.}$$

We also say $\equiv (\text{mod } I)$ ($\equiv (\text{mod } H)$) is a congruence relation on R (on G).

Definition 2.3.16. *([12], Remark 1.28) Let R be a nearring and I an ideal of R. On the set R/I we define $+$ and $\cdot$ where $R/I = \{I + r | r \in R\}$ by*

$$\begin{aligned}(I + r_1) + (I + r_2) &= I + r_1 + r_2 \quad \text{and} \\ (I + r_1) \cdot (I + r_2) &= I + r_1 r_2.\end{aligned}$$

for all $r_1, r_2 \in R$. Then $(R/I, +, \cdot)$ is a nearring, called the quotient nearring of R.

Definition 2.3.17. *([12], Remark 1.28) Let R be a nearring, G an R-module and H an R-ideal of G. On the set $G/H = \{H + g | g \in G\}$ we have*

$$\begin{aligned}(H + g_1) + (H + g_2) &= H + g_1 + g_2 \quad \text{and} \\ r(H + g_1) &= H + rg_1.\end{aligned}$$

for all $g_1, g_2 \in G$. Then G/H is an R-module, called the quotient R-module of G.

Lemma 2.3.18. *([12], Theorem 1.29) Let R be a nearring and I an ideal of R. Then the canonical map*

$$\begin{aligned}\pi: R &\to R/I\\ r &\mapsto I+r\end{aligned}$$

is a nearring epimorphism and $\ker\pi = I$.

Lemma 2.3.18 remains true if we replace "nearring" by "R-module".
This prompts the First Isomorphism Theorem.

Theorem 2.3.19. *([12], Theorem 1.29) Let h be an epimorphism from R to R' where R and R' are nearrings. Then $R/\ker h \cong R'$.*

The theorem above also holds for an epimorphism of R-modules.

Definition 2.3.20. *([12], Definition 1.36) Let R be a nearring and G an R-module. Then*

1. *R is simple if it has no non-trivial ideals,*

2. *G is simple if it has no non-trivial R-ideals.*

Proposition 2.3.21. *([12], Proposition 1.37) Let R be a simple nearring and G be a simple R-module. Then all homomorphic images are isomorphic to either $\{0_R\}$ or to R. Also all R-homomorphic images are isomorphic to either $\{0_G\}$ or G.*

Definition 2.3.22. *([11], Definition 2.10) Let R be a nearring. A two-sided R-subgroup of R is a subset H of R that satisfies:*

1. *$(H, +)$ is a subgroup of $(R, +)$,*

2. *$RH \subseteq H$,*

3. *$HR \subseteq H$.*

H is called a right R-subgroup of R when it satisfies (1) and (2) and is called a left R-subgroup if it satisfies (1) and (3).

It is not difficult to see that

Lemma 2.3.23. *The R-submodules of R are just the left R-subgroups of R.*

Definition 2.3.24. *([12], Definition 1.39) Let R be a nearring.*

1. *I is a minimal ideal of R if it is minimal in the set of all non-zero ideals of R. Similarly, one defines minimal right ideal, left ideal, R-subgroup, left R-subgroup and right R-subgroup.*

2. *I is a maximal ideal of R if $I \neq R$ and if J is an ideal of R such that $I \subseteq J$, then $I = J$ or $J = R$. Similarly, one defines maximal right ideal, left ideal, R-subgroup, left R-subgroup and right R-subgroup.*

Definition 2.3.25. *Let R be a nearring and G an R-module.*

1. *H is a minimal R-ideal of G if it is minimal in the set of all non-zero R-ideals of G.*

2. *H is a maximal R-ideal G if $H \neq G$ and if H' is an R-ideal of G such that $H \subseteq H'$, then $H = H'$ or $H' = G$.*

Proposition 2.3.26. *([12], Proposition 1.40) Let R be a nearring and I an ideal of R. I is maximal if and only if R/I is simple.*

We have a similar result for the ideals of an R-module.

Definition 2.3.27. *([11], Definition 3.1) Let R be a nearring and let G be an R-module. The R-module G is called monogenic if there exists a $g \in G$ such that $Rg = G$ and g is called a generator of G.*

Definition 2.3.28. *([11], Definition 3.4) A nearring R is called 2-primitive on G if G is a faithful R-module of type 2. We say that G is of type 2 if G is monogenic and has no proper nontrivial R-submodules.*

We list some properties of 2-primitive nearrrings.

Theorem 2.3.29. *([11], Theorem 3.2) Let G be a monogenic R-module, and g be a generator of G. Then the map*

$$\begin{aligned} f_g : R &\to G \\ r &\mapsto rg \end{aligned}$$

is an R-epimorphism from R_R to G.

Theorem 2.3.30. *([11], Corollary 3.3) Let G be a monogenic R-module, and let g be a generator of G. Then there is an R-isomorphism between G and $R/Ann_R(g)$.*

Lemma 2.3.31. *If G is of type 2, $Ann_R(g)$ is a maximal R-ideal.*

Lemma 2.3.32. *([11], Lemma 3.7) Let G be an R-module with the properties:*

- *G is faithful as an R-module,*
- *$(G, +)$ is an abelian group,*
- *for all $r \in R$, the map $\rho_r : G \to G$ given by $\rho_r : g \mapsto rg$ is an endomorphism of G.*

Then R is a ring.

From now on we consider only 2-primitive nearrings.

Chapter 3

The Theory of Near-Vector Spaces

In this section, we give the basic theory of near-vector spaces.

We start this chapter by introducing what we call an F-group.

3.1 F-groups

Definition 3.1.1. *([2], Definition* 1.1*) An F-group is a pair (V, F) which satisfies the following conditions:*

1. *$(V, +)$ is a group and F is a set of endomorphisms of V;*
2. *F contains the endomorphisms 0, id and $-id$;*
3. *$F^* = F \setminus \{0\}$ is a subgroup of the group $Aut(V)$;*
4. *If $x\alpha = x\beta$ with $x \in V$ and $\alpha, \beta \in F$, then $\alpha = \beta$ or $x = 0$, i.e. F acts fixed point free on V.*

Remark 3.1.2. *Since $-id \in F$, we have*

$$x + y = (-x)(-id) + (-y)(-id) = (-x - y)(-id) = (-(y + x))(-id) = y + x.$$

So $(V, +)$ is abelian.

Example 3.1.3.

- *We consider the finite field $GF(p^n)$, p a prime number, n a positive integer and $p > 3$. Let $(V_1, +) = (GF(p^n), +)$ and $F_1 = \{id, -id, 0\}$. Then (V_1, F_1) is an F-group. In fact F_1^* is a subgroup of the group $Aut(V)$, and F_1 acts fixed point free on V_1.*

- *For the second example we still consider $GF(p^n)$, for any prime p and n a positive integer and $(V_2, +) = (GF(p^n), +)$. Let*

  $$F_2 = \{\phi_\alpha : V_2 \to V_2 | \alpha \in GF(p^n) \text{ and } x\phi_\alpha = x\alpha^q\},$$

  with $gcd(p^n - 1, q) = 1$.

  Then (V_2, F_2) is an F-group.

Lemma 3.1.4. *([1]) Let $F = GF(p^n)$, the field with p^n elements. Then each element of F has a q-th root in F if and only if $gcd(q, p^n - 1) = 1$.*

Definition 3.1.5. *([2], Definition 2.1) Let (V, F) be an F-group. The set*

$$\{x \in V | \forall \alpha, \beta \in F, \exists \gamma \in F \text{ such that } x\alpha + x\beta = x\gamma\}$$

is called the quasi-kernel of (V, F). We write $Q(V)$ or just Q to denote the quasi-kernel.

Example 3.1.6.

- *For the F-group (V_1, A_1) in Example 3.1.3 we have $Q(V_1) = \{0\}$. If $x \in Q(V_1)$, then there is $\psi \in \{id, -id, 0\}$ such that $xid + xid = x\psi$. We have the following three cases:*

  $$\begin{cases} x + x = x \\ x + x = -x \\ x + x = 0 \end{cases}$$

  But since the characteristic of $GF(p^n)$ is greater than 3, we have that $x = 0$.

- *For the second F-group we have $Q(V_2) = V_2$. To see this, let $x \in V_2$ and $\phi_\alpha, \phi_\beta \in A_2$. Then we have that*

  $$x\phi_\alpha + x\phi_\beta = x\alpha^q + x\beta^q = x(\alpha^q + \beta^q).$$

  Since $gcd(p^n - 1, q) = 1$, by Lemma 3.1.4 there is $\gamma \in GF(p^n)$ such that $\alpha^q + \beta^q = \gamma^q$. Hence

  $$x\phi_\alpha + x\phi_\beta = x\gamma^q = x\phi_\gamma.$$

  Therefore $Q(V_2) = V_2$.

We have the following for any nonzero element of the quasi-kernel.

Theorem 3.1.7. *([2], Theorem 2.4) Let (V, F) be an F-group and let $u \neq 0$ be an element of the quasi-kernel $Q(V)$. Then $(F, +_u, \cdot)$ is a near-field with the operation $+_u$ on F defined by*

$$u(\alpha +_u \beta) := u\alpha + u\beta,$$

for all $\alpha, \beta \in F$.

A proof can be found in [2], Theorem 2.4 or in [6] Theorem 2.3.5.

Definition 3.1.8. *([2], Definition 2.6) Let (V, F) be an F-group and let $u \neq 0$ be an element of the quasi-kernel $Q(V)$. The kernel $R_u(V)$ or just R_u of (V, F) is the set*

$$R_u := \{v \in V | v(\alpha +_u \beta) = v\alpha + v\beta, \text{ for every } \alpha, \beta \in F\}.$$

We now look at a relation that is foundational in the structure of near-vector spaces.

3.2 Dependence Relation

Definition 3.2.1. *([2], Definition 3.1) A relation between a set S and its power set 2^S, denoted by $v \lhd M$, with $v \in S$ and $M \subseteq S$, is a dependence relation if for all $u, v, w \in S$ and $M, N \subseteq S$ we have:*

1. *$v \in M$ implies that $v \lhd M$,*
2. *$w \lhd M$ and $v \lhd N$ for each $v \in M$, implies that $w \lhd N$,*
3. *$v \lhd M$ and $v \ntriangleleft M \setminus \{u\}$, implies that $u \lhd (M \setminus \{u\}) \cup \{v\}$.*

Example 3.2.2.

1. *Let K be a field extension of a field F such that K is algebraically closed. Define $\lhd$ by $\alpha \lhd S$ if α is algebraic over $F(S)$. Then $\lhd$ is a dependence relation.*

   Let $\alpha, \beta \in K$ and $S, T \subseteq K$. Then

   - *If $\alpha \in S$, then α is algebraic over $F(S)$. Hence $\alpha \lhd S$.*
   - *We assume that α is algebraic over $F(S)$ and that for all $\beta \in S$, β is algebraic over $F(T)$. Then the algebraic closure of $F(T)$, $\overline{F(T)}$, contains $F(S)$. Hence $\overline{F(S)} \subseteq \overline{F(T)}$. Therefore α is algebraic over $F(T)$.*

- *Suppose that $\alpha \lhd S$ and $\alpha \ntriangleleft S \setminus \{\beta\}$. Since $\alpha \lhd S$, there are $a_i \in F(S)$, $i \in \{0, \ldots, n\}, a_n \neq 0$, such that $a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0$. But the fact that $\alpha \ntriangleleft S \setminus \{\beta\}$ implies that $a_n x^n + \ldots + a_1 x + a_0 \notin F(S \setminus \{\beta\})[x]$. So there is $i_0 \in \{0, \ldots, n\}$ such that $a_{i_0} = b_m\beta^m + \ldots + b_1\beta + b_0$, with $b_i \in F(S \setminus \{\beta\}), i \in \{0, \ldots, m\}$. Hence β is algebraic over $F((S \setminus \{\beta\}) \cup \{\alpha\})$.*

2. *Let $Q = Q(V)$ be the quasi-kernel of an F-group V. Define a relation between Q and 2^Q as follows:*

   (i) $v \lhd \emptyset$ if $v = 0$;

   (ii) $v \lhd M, \emptyset \neq M \subseteq Q$, if and only if there exists $u_i \in M$ and $\lambda_i \in F(i = 1, 2, ..., n)$ such that
$$v = \sum_{i=1}^{n} u_i \lambda_i. \tag{3.1}$$

The proof that this is a dependence relation is given in [6] Theorem 2.4.1.

We now introduce the notion of closure operators

Definition 3.2.3. *A closure operator on a set S is a function $cl : 2^S \to 2^S$ satisfying the following conditions for all $X, Y \subseteq S$:*

- *$X \subseteq cl(X)$. We say that cl is extensive.*
- *If $X \subseteq Y$, then $cl(X) \subseteq cl(Y)$. The function cl is increasing.*
- *$cl(cl(X)) = cl(X)$. cl is said to be idempotent.*

Remark 3.2.4.

1. *For a set X, $cl(X)$ is called a closed set and it is the smallest closed set containing X.*

2. *We can define a closure operator from a dependence relation. If A is a set, $cl(A)$ will be the set of all elements related to A.*

In the following theorem we explicitly define a closure operator from a dependence relation.

Theorem 3.2.5. *Let $\lhd$ be a dependence relation between a set S and its power set 2^S. The function cl defined by*

$$cl : 2^S \to 2^S$$
$$A \mapsto cl(A) = \bigcup_{P \in \mathcal{P}} P,$$

where $\mathcal{P} = \{P \subseteq S | \forall v \in P, v \lhd A\}$ is a closure operator on S.

Proof. The map is well defined since for all $A \subseteq S$, $cl(A) \subseteq S$. Let $A, B \in 2^S$. We have

- For all $v \in A$, $v \lhd A$, so $A \subseteq cl(A)$.
- If $A \subseteq B$, then $cl(A) \subseteq cl(B)$. Since $v \lhd A$ implies that $v \lhd B$.
- Let $v \in cl(cl(A))$. Then $v \lhd cl(A)$. But for all $u \in cl(A)$, $u \lhd A$. It follows that $v \lhd A$. Hence $cl(cl(A)) \subseteq cl(A)$. Therefore $cl(cl(A)) = cl(A)$, since $cl(A) \subseteq cl(cl(A))$. Thus cl is idempotent.

□

Remark 3.2.6. *For the first dependence relation in Example 3.2.2, we have $cl(S) = \overline{F(S)}$ and for the second one we have $cl(A) = span(A)$. We define what span is in Definition 3.3.8.*

3.3 Near-Vector Spaces

Definition 3.3.1. *([2], Definition 4.1) An F-group (V, F) is called a near-vector space over F if the following condition holds:*

The quasi-kernel $Q = Q(V)$ of V generates the group $(V, +)$.

So we have

Definition 3.3.2. *A near-vector space is a pair (V, F) which satisfies the following conditions:*

1. *$(V, +)$ is a group and F is a set of endomorphisms of V;*
2. *F contains the endomorphisms 0, id and $-id$;*
3. *$F^* = F \setminus \{0\}$ is a subgroup of the group $Aut(V)$;*

4. *If $x\alpha = x\beta$ with $x \in V$ and $\alpha, \beta \in F$, then $\alpha = \beta$ or $x = 0$, i.e. F acts fixed point free on V;*

5. *The quasi-kernel $Q(V)$ of V, generates V as a group. Here, $Q(V) = \{x \in V | \forall \alpha, \beta \in F, \exists \gamma \in F$ such that $x\alpha + x\beta = x\gamma\}$.*

We sometimes refer to V as a near-vector space over F. The elements of V are called vectors and the members of F scalars.

Remark 3.3.3. *If V is a vector space over a division ring F, we can consider F as a set of endomorphisms of V. For $\alpha \in F$ we have the endomorphism f_α of V defined for all $x \in V$ by $f_\alpha x = x\alpha$. Also the quasi-kernel $Q(V) = V$. But the converse is not true in general, as we will see i.e $Q(V) = V$ is not sufficient for V to be a vector space over F.*

Example 3.3.4.

1. *Every (right) vector space V over a division ring F is a near-vector space.*

   In fact F can be regarded as a set of endomorphisms of V (for $\alpha \in F$, the endomorphism f_α of V is defined by $f_\alpha x := x\alpha$ for each $x \in V$). For every $\alpha, \beta \in F$ and for each $x \in V$, there is a $\gamma \in F$ (via, $\gamma = \alpha + \beta$) such that $x\alpha + x\beta = x\gamma$.

   A vector space is a special instance of a near vector space

2. *In Example 3.1.3 the F-group (V_2, F_2) is a near-vector space, since $Q(V_2) = V_2$. But (V_1, F_1) is not a near-vector space, since $Q(V_1) = \{0\}$ and cannot generate V_1.*

3. *Let F be a near-field. Then F is a near-vector space over itself.*

4. *Let F be a near-field, θ an automorphism of $(F, \cdot)$ and let I be a nonempty index set. Then the set*

   $$F^{(I)} := \{(n_i)_{i \in I} | n_i \in F, n_i \neq 0 \text{ for at most a finite number of } i \in I\},$$

   with the scalar multiplication defined by

   $$(n_i)\lambda := (n_i\theta(\lambda)),$$

   gives that $(F^{(I)}, F)$ is a near-vector space.

5. *Consider the pair* $(V, F) = (\mathbb{R}^2, \mathbb{R})$ *with the scalar multiplication defined by* $(x_1, x_2)\alpha = (x_1\alpha^3, x_2\alpha^3)$. *Then* (V, F) *is a near-vector space.*

Remark 3.3.5. *The near-vector space* (V, F) *in Example 3.3.4* (5) *is not a vector space over* $\mathbb{R}$, *but* $Q(V) = V$.
To see this, let $(x, y) \in \mathbb{R}^2$. *Then for* $\alpha, \beta \in \mathbb{R}$, *we have that*

$$\begin{aligned} (x,y)(\alpha+\beta) &= (x(\alpha+\beta)^3, y(\alpha+\beta)^3) \quad \textit{and} \\ (x,y)\alpha + (x,y)\beta &= (x\alpha^3 + x\beta^3, y\alpha^3 + y\beta^3). \end{aligned}$$

In general $(x,y)(\alpha+\beta) \neq (x,y)\alpha + (x,y)\beta$. *Therefore* V *is not a vector space over* $\mathbb{R}$.

Lemma 3.3.6. *([2], Lemma* 2.2*) The quasi-kernel* Q *of an* F*-group has the following properties:*

- $0 \in Q$.
- *If* $u \in Q$ *and* $\lambda \in F$, *then* $u\lambda \in Q$, *i.e.* $uF \subseteq Q$.
- *If* $u \in Q \setminus \{0\}$ *and* $\alpha, \beta \in F$, *then there exists a* $\gamma \in F$ *such that* $u\alpha - u\beta = u\gamma$.

The proofs of these properties are given in [2] Lemma 2.2 or [6] Lemma 2.3.2. The following theorem describes the quasi-kernel of the near-vector space $(F^{(I)}, F)$ in Example 3.3.4. Recall that F_d denotes all the distributive elements of F.

Theorem 3.3.7. *The quasi-kernel of the near-vector space* $(F^{(I)}, F)$ *is given by*

$$Q(F^{(I)}) = \{(d_i)\lambda | \lambda \in F, d_i \in F_d \textit{ for all } i \in I\}.$$

Proof. Let $d_i \in F_d$ for $i \in I$ and $\alpha, \beta \in F$. We have

$$\begin{aligned} (d_i)\alpha + (d_i)\beta &= (d_i\theta(\alpha) + d_i\theta(\beta)) \\ &= (d_i(\theta(\alpha) + \theta(\beta))), \text{ since } d_i \text{ is distributive} \\ &= (d_i\theta(\gamma)) \text{ with } \gamma = \theta^{-1}(\theta(\alpha) + \theta(\beta)) \in F. \\ &= (d_i)\gamma. \end{aligned}$$

Hence $(d_i) \in Q(V)$. Since $Q(V)$ is closed under scalar multiplication (Lemma 3.3.6), we have

$$Q(V) \supseteq \{(d_i)\lambda | \lambda \in F, d_i \in F_d \text{ for all } i \in I\}.$$

Now suppose that $(x_i) \in Q(V)$. If $(x_i) = 0$ then $(x_i) \in \{(d_i)\lambda | \lambda \in F, d_i \in F_d \text{ for all } i \in I\}$. Suppose that $(x_i) \neq 0$. Then there is $i_0 \in I$ such that $x_{i_0} \neq 0$. Let $d_i = x_i x_{i_0}^{-1}$ for $i \in I$. Then $(d_i) = (x_i)\theta^{-1}(x_{i_0}^{-1})$. Since $(x_i) \in Q(V)$ and $Q(V)$ is closed under scalar multiplication, $(d_i) \in Q(V)$. Then for all $\alpha, \beta \in F$ there is $\gamma \in F$ such that $(d_i)\alpha + (d_i)\beta = (d_i)\gamma$. It follows that $d_i\theta(\alpha) + d_i\theta(\beta) = d_i\theta(\gamma)$ for all $i \in I$. Since θ is an automorphism, there are $\alpha_1, \beta_1 \in F$ such that $\alpha = \theta^{-1}(\alpha_1)$ and $\beta = \theta^{-1}(\beta_1)$. So $d_i\alpha_1 + d_i\beta_1 = d_i\theta(\gamma)$ for all $i \in I$. But $d_{i_0} = 1$. So $\alpha_1 + \beta_1 = \theta(\gamma)$. Hence $d_i\alpha_1 + d_i\beta_1 = d_i(\alpha_1 + \beta_1)$, and this is satisfied for all $\alpha_1, \beta_1 \in F$ because θ is an automorphism of $(F, \cdot)$. Therefore d_i is distributive and

$$Q(V) = \{(d_i)\lambda | \lambda \in F, d_i \in F_d \text{ for all } i \in I\}.$$

□

For a near-vector space we have the following definitions of linear independence and spanning set.

Definition 3.3.8. *([2], Lemma 4.4) Let (V, F) be a near-vector space. A subset B of $Q(V)$ is said to be linearly independent if for all $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ and $v_1, \ldots, v_n \in B$, $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$ implies that $\alpha_1 = \ldots = \alpha_n = 0$.*
A subset B of $Q(V)$ is a generating subset of $Q(V)$, if for all $v \in Q(V)$ there exist $\alpha_1, \ldots, \alpha_n \in F$ and $v_1, \ldots, v_n \in B$ such that $v = \alpha_1 v_1 + \ldots + \alpha_n v_n$. We then write that $Q(V) = span(B)$.
Finally, a basis B of $Q(V)$ is a linearly independent subset of $Q(V)$ that generates $Q(V)$.

Lemma 3.3.9. *([2], Lemma 4.5) Let V be a near-vector space and let $B = \{u_i | i \in I\}$ be a basis of $Q(V)$. Then each $x \in V$ is a unique linear combination of elements of B, i.e. there exists $x_i \in F$, with $x_i \neq 0$ for at most a finite number of $i \in I$, which are uniquely determined by x and B, such that*

$$x = \sum_{i \in I} u_i x_i.$$

Definition 3.3.10. *([2], Definition 4.4) Let (V, F) be a near-vector space. A basis of V is a basis of $Q(V)$. The dimension of (V, F), denoted by $dim(V)$, is the cardinality of a basis of $Q(V)$.*

Example 3.3.11.

- *We consider the near-vector space* (F, F), *F a near-field. We have* $Q(F) = F$ *and for any* $x \in F^*$ *we have* $y = xx^{-1}y = x(x^{-1}y)$ *for all* $y \in F$*. Thus* $\{x\}$ *is a basis for* $Q(V)$ *and so a basis of* (F, F)*. Thus dim* $F = 1$*.*

- *The near-vector space* $(\mathbb{R}^2, \mathbb{R})$ *in Example 3.3.4* (5) *has basis* $B = \{(1, 0), (0, 1)\}$ *and so its dimension is* 2*.*

Mathematical structures of a given type usually come equipped with the corresponding notion of a "substructure". In the case of near-vector spaces, we have the following:

Definition 3.3.12. *([7], Definition* 2.3*) Let* (V, F) *be a near-vector space and* V' *a subset of* V*, such that* $V' \neq \emptyset$*.* (V', F) *is said to be a subspace of* (V, F) *if* $(V', +)$ *is a subgroup of* $(V, +)$ *generated by* $XF = \{xa | x \in X, a \in F\}$*, where* X *is an independent subset of* $Q(V)$*.*

Remark 3.3.13.

1. *X is a basis of* (V', F)*.*

2. *If* (V', F) *is a subspace of* (V, F)*, then it is closed under addition and scalar multiplication.*

Another characterization of subspaces is the following proposition.

Proposition 3.3.14. *([7], Proposition* 2.4*) Let* (V, F) *be a near-vector space and* V' *a subset of* V*, such that* $V' \neq \emptyset$*. Then* V' *is a subspace of* V *if and only if* V' *is closed under addition and scalar multiplication.*

Example 3.3.15.

1. *If* (V, F) *is a near-vector space, then it is a subspace of itself.*

2. *Let us consider the near-vector space* (V, F) *in Example 3.3.4* (5)*. Then the subset* $V' = \{(x, y) \in \mathbb{R}^2 | x = y\}$ *of* V *is a subspace of* (V, F)*.*

To see this let $\alpha \in F$ and $(x,y),(x',y') \in V'$, then we have that $x = y$ and $x' = y'$. So

$$\begin{aligned}
(x,y) + (x',y') &= (y,y) + (y',y') \\
&= (y + y', y + y') \\
&= (y + y', y + y') \in (V', F). \\
(x,y)\alpha &= (y,y)\alpha \\
&= (y\alpha^3, y\alpha^3) \in (V', F).
\end{aligned}$$

Therefore V' is closed under addition and scalar multiplication. Thus (V', F) is a subspace of (V, F).

Proposition 3.3.16. *([7]) Let (V, F) be a near-vector space and (V_1, F), (V_2, F) two subspaces of V. Then $(V_1 \cap V_2, F)$ is a subspace of V.*

Proposition 3.3.17. *If W is a subspace of V , then $Q(W) = W \cap Q(V)$.*

Definition 3.3.18. *([7]) Two near-vector spaces, (V, F) and (W, F) are isomorphic if there is a bijection $f : V \to W$ such that for all $v_1, v_2, v \in V$ and $\alpha \in F$ we have*

$$\begin{aligned}
f(v_1 + v_2) &= f(v_1) + f(v_2) \\
f(v\alpha) &= f(v)\alpha.
\end{aligned}$$

We now introduce the concept of regularity which is a central notion in the theory of near-vector spaces. We start by defining the concept of compatibility.

Definition 3.3.19. *([2], Definition 4.7) Let (V, F) be a near-vector space such that $Q(V) \neq \{0\}$. Two elements u and v of $Q(V) \setminus \{0\}$ are called compatible (u cp v), if there is a $\lambda \in F \setminus \{0\}$ such that $u + v\lambda \in Q(V)$.*

Remark 3.3.20.

- *The compatibility relation cp is an equivalence relation on $Q(V) \setminus \{0\}$.*
- *The elements u and v of $Q(V) \setminus \{0\}$ are compatible if and only if there exists a $\lambda \in F \setminus \{0\}$ such that $+_u = +_{v\lambda}$.*

Definition 3.3.21. *([2], Definition 4.11) A near-vector space V is called a regular near-vector space if any two vectors of $Q(V) \setminus \{0\}$ are compatible.*

Theorem 3.3.22. *The near-vector space $(F^{(I)}, F)$ in Example 3.3.4 is regular.*

Proof. To show that V is regular we prove that we just have one equivalence class, under the compatibility relation. We consider $d_i \in F_d$ for $i \in I$. Then from Theorem 3.3.7 above we have that $(d_i) \in Q(V)$. It turns out that every element in $Q(V)$ is related to (d_i). In fact let $(a_i) = (d_i')\lambda_1 \in Q(V)$, where $d_i' \in F_d$ of all $i \in I$ and $\lambda_i \in F$. If $\lambda_1 = 0$ then $(d_i) + (a_i) \in Q(V)$. Suppose $\lambda_1 \neq 0$ and let $\lambda = \lambda_1^{-1}$. We show that $(d_i) + (a_i)\lambda \in Q(V)$. We have

$$\begin{aligned}
(d_i) + (a_i)\lambda &= (d_i) + ((d_i')\lambda_1)\lambda \\
&= (d_i) + (d_i'\theta(\lambda_1))\lambda \\
&= (d_i) + (d_i'\theta(\lambda_1\lambda)) \\
&= (d_i) + (d_i'\theta(\lambda_1\lambda_1^{-1})) \\
&= (d_i) + (d_i'), \text{ since } \theta(1) = 1 \\
&= (d_i + d_i').
\end{aligned}$$

We know that F_d, with the operations of F, is a division ring. Hence $d_i + d_i' \in F_d$ for all $i \in I$. Therefore $(d_i) + (a_i)\lambda \in Q(V)$. Thus (d_i) and every element of $Q(V)$ are compatible. So V is regular. □

Remark 3.3.23. *The near-vector space $(F^{(I)}, F)$ is regular but we do not have $Q(F^{(I)}) = F^{(I)}$ in general.*

Here is an example.

Example 3.3.24. *Let F be a near-field which is not a field and $V = F \oplus F$. Then V with the scalar multiplication $(x, y)\alpha = (x\alpha, y\alpha)$ is such that $Q(V) \subsetneq V$.*
Since F is a not a field, we have $F_d \subsetneq F$. From Theorem 3.3.7 we know that $Q(V) = \{(d_1, d_2)F | d_1, d_2 \in F_d\}$. Let $x \in F \setminus F_d$. We show that $(1, x) \notin Q(V)$. Suppose that $(1, x) \in Q(V)$. Then there is $\alpha \in F, d_1, d_2 \in F_d$ such that $(1, x) = (d_1\alpha, d_2\alpha)$. It follows that $\alpha = d_1^{-1}$ and $x = d_2 d_1^{-1}$. Since F_d with the operations of F is a division ring, $x \in F_d$ (Proposition 2.2.3), a contradiction. Hence $(1, x) \notin Q(V)$. Therefore $Q(V) \subsetneq V$.

We now list some properties related to compatibility.

Proposition 3.3.25. *([2], Proposition 4.10) Let u, v and $u + v$ be elements of $Q \setminus \{0\}$. Then*

- *u cp v, and*

- u *cp* $u + v$.

Theorem 3.3.26. *([2], Theorem 4.12) A near-vector space V is regular if and only if there exists a basis which consists of mutually pairwise compatible vectors.*

Next we give the main theorem of this chapter. It is from André ([2]).

Theorem 3.3.27. *([2], Theorem 4.13) (The Decomposition Theorem) Every near-vector space V is the direct sum of regular near-vector spaces $V_j (j \in J)$ such that each $u \in Q(V) \setminus \{0\}$ lies in precisely one direct summand V_j . The subspaces V_j are maximal regular near-vector spaces.*

The proof can be found in [2] or in [6], Theorem 2.5.17.
The following theorems are consequences of this theorem. We do not repeat the proofs here.

Theorem 3.3.28. *([2], Theorem 4.14) (The Uniqueness Theorem) There exists only one direct decomposition of a near-vector space into maximal regular near subspaces.*

Definition 3.3.29. *([2], Definition 4.15) The uniquely determined direct decomposition of a near-vector space V into maximal regular subspaces, is called the canonical direct decomposition of V.*

Theorem 3.3.30. *([2], Theorem 4.17) Let (V, F) be a near-vector space with quasi-kernel $Q(V)$. If $u \in Q(V) \setminus \{0\}, x \in V \setminus uF$ and $u\alpha + x\beta = u\alpha' + x\beta'$ $(\alpha, \beta, \alpha', \beta' \in F)$, then $\alpha = \alpha'$ and $\beta = \beta'$.*

Theorem 3.3.31. *([2], Theorem 5.1) A near-vector space (V, F) is regular if and only if*

$$Q(V) = \{v\lambda | \lambda \in F, v \in R_u\} =: R_u F,$$

where $R_u(V) = R_u$ is the kernel of a $u \in Q(V) \setminus \{0\} = Q(V) \setminus \{0\}$. In this case $Q = R_u F$ for all $u \in Q(V) \setminus \{0\}$.

If we consider the near-vector space $F^{(I)}$ in Example 3.3.4 with $\theta = id$ we have the following:

Theorem 3.3.32. *([2], Theorem 5.2) (The Structure Theorem for Regular Near-Vector Spaces)*
An F-group (V, F), with $V \neq \{0\}$, is a regular near-vector space if and only if F is a near-field and V is isomorphic to $F^{(I)}$, for some index set I.

Chapter 4

Finite dimensional near-vector spaces

We now turn our attention to finite dimensional near-vector spaces.

4.1 Finite dimensional near-vector spaces

Definition 4.1.1. *Let (V, F) be a near-vector space. (V, F) is said to be a finite dimensional near-vector space if its dimension is finite.*

Example 4.1.2. *Let us consider the near-vector space $(\mathbb{R}^2, \mathbb{R})$ in Example 3.3.4 (5), and the elements $(1, 0)$ and $(0, 1)$. Let $\alpha, \beta \in \mathbb{R}$. We have $(1, 0)\alpha + (0, 1)\beta = (\alpha^3, \beta^3)$. So, if $(1, 0)\alpha + (0, 1)\beta = 0$, then $\alpha = 0$ and $\beta = 0$. Hence the set $\{(1, 0), (0, 1)\}$ is an independent set of $Q(\mathbb{R}^2) = \mathbb{R}^2$. Now let $(x, y) \in (\mathbb{R}^2, \mathbb{R})$. We have $x^{1/3}, y^{1/3} \in \mathbb{R}$, and $(x, y) = (1, 0)x^{1/3} + (0, 1)y^{1/3}$. Therefore $\{(1, 0), (0, 1)\}$ is a generating set of $Q(\mathbb{R}^2)$. Thus $(\mathbb{R}^2, \mathbb{R})$ is a finite dimensional near-vector space and its dimension is 2.*

The main objective of this chapter is to study finite dimensional near-vector spaces and we need more tools for 2 primitive near-rings.
From now on we suppose all near-rings are zero-symmetric. The theorems in Meldrum ([11]) have been adapted for the 2-primitive case.

Proposition 4.1.3. *([11], Corollary 2.16) Let R be a near-ring, G an R-module. Then every R-ideal of G is an R-submodule.*

Proof. Since R is zero-symmetric, $r0_R = 0_R$ for all $r \in R$. Let I be an R-ideal of G. Then for all $r \in R, g \in G, i \in I$ we have $r(g + i) - rg \in I$. For $g = 0$ we have

$$ri - r0_G = ri + r(0_R 0_G) = ri - (r0_R)0_G = ri - 0_R 0_G = ri - 0_G = ri \in I.$$

Hence for all $r \in R, i \in I$ we have $ri \in I$. Therefore I is an R-submodule. □

Definition 4.1.4. *([11], Definition 3.8) Let R be a near-ring and G an R-module. The semigroup, $C := End_R(G)$, of all endomorphisms of G is called the R-centralizer of G. Its subset, the group of units of C, is denoted by $D := Aut_R(G)$.*

Remark 4.1.5. *Let 0 be the zero endomorphism of G. We write D^0 for $D \cup \{0\}$. We are interested in the situation in which $C = D^0$, which is not always the case. So we consider the following two subsets of G*

$$\begin{aligned} G_0 &:= \{g \in G | Rg = \{0\}\} \\ G_1 &:= \{g \in G | Rg = G\}. \end{aligned}$$

This leads to the following lemma.

Lemma 4.1.6. *([11], Lemma 3.12) Let G be an R-module. We have*

- *$G_1 \neq \emptyset$ if and only if G is monogenic.*
- *If R is 2-primitive on G, then $G = G_0 \cup G_1$. Furthermore if R has an identity and $G \neq \{0\}$, then $G_1 = G \setminus \{0\}$ and $G_0 = \{0\}$.*
- *$DG_0 = G_0$ and $DG_1 = G_1$.*

Proof. Let G be an R-module.

- G is monogenic if and only if there is $g \in G$ such that $Rg = G$. So G is monogenic if and only if $G_1 \neq \emptyset$.
- If R is 2-primitive on G, then G has no nontrivial proper R-submodules. Since Rg is an R-submodule of G, $Rg = \{0\}$ or $Rg = G$ for all $g \in G$. Therefore for all $g \in G$, $g \in G_0$ or $g \in G_1$. So $G = G_0 \cup G_1$. Furthermore if R has an identity and $g \neq 0$, then $Rg \neq \{0\}$ since $g = 1g \in Rg$. Hence $Rg = G$ and so for all $g \in G$, such that $g \neq 0$, $g \in G_1$. Thus $G_0 = \{0\}$ and $G_1 = G \setminus \{0\}$.
- Let $g \in DG_0$. Then there is a $\alpha \in D$ and $g_0 \in G_0$ such that $g = \alpha(g_0)$. Since $g_0 \in G_0$, $Rg_0 = \{0\}$. We have $Rg = R[\alpha(g_0)] = \alpha(Rg_0) = \{0\}$. Hence $g \in G_0$ and $DG_0 \subseteq G_0$. Therefore $DG_0 = G_0$, since $id \in D$. We also have $DG_1 = G_1$ using the same technique.

□

We assume, unless otherwise stated, that if the near-ring R has an identity, then all R-modules are unitary. We have the following theorem.

Theorem 4.1.7. *([11], Theorem* 3.13*) Let R be* 2*-primitive on an R-module $G \neq \{0\}$. Then*

- *D acts fixed point free on G_1.*
- *$C = D^0$.*

Proof. Let R be 2-primitive on the R-module $G \neq \{0\}$.

- D acts fixed point free on G_1 if for all $g_1 \in G_1$ and $d \in D$, $d(g_1) = g_1$ implies that d is the identity map of G. So let $d \in D$ and $g_1 \in G_1$ such that $d(g_1) = g_1$. Since $g_1 \in G_1$, $Rg_1 = G$. Then for any $g \in G$ there is $r \in R$ such that $rg_1 = g$. It follows that $d(g) = rd(g_1) = rg_1 = g$. Hence $d = 1$. Therefore D acts fixed point free on G_1.

- Since R is a 2-primitive near-ring on G, the only R-submodules of G are $\{0\}$ and G. Let $c \in C \setminus \{0\}$. Then $\ker c \neq G$. But we know that $\ker c$ is an R-ideal of G, by Example 2.3.12, and since R is a zero-symmetric near-ring, R-ideals of G are R-submodules of G, by Proposition 4.1.3. Hence $\ker c = \{0\}$ and c is injective. Likewise $c(G)$ is an R-submodule of G. It follows that $c(G) = G$, since $c(G) \neq \{0\}$. Hence c is surjective. Therefore $c \in D$.

□

From the previous theorem comes the following corollary.

Corollary 4.1.8. *([11], Corollary* 3.15*) Let R be a* 2*-primitive near-ring with identity on an R-module G. Then $C = D^0$ and D is a fix point free group of automorphisms of G.*

Proof. Since R has an identity, by Lemma 4.1.6 $G_1 = G \setminus \{0\}$. But Theorem 4.1.7 tells us that D acts fixed point free on G_1. Hence D acts fixed point free on $G \setminus \{0\}$. Therefore D is a fix point free group of automorphisms of G. □

The following theorem gives a correspondence between D, the set of all R-automorphisms of G, and the concept of an annihilator that we introduced in 2.3.7.

Theorem 4.1.9. *([11], Theorem 3.20) Let R be a 2-primitive near-ring, with identity, on an R-module G. Then for all $g, h \in G_1$ we have*

$$Dg = Dh \quad \textit{if and only if} \quad Ann_R(g) = Ann_R(h).$$

Proof. Let $g, h \in G$.

- Suppose that $Dg = Dh$. We have to show that $Ann_R(g) = \{r \in R | rg = 0_G\} = Ann_R(h) = \{r \in R | rh = 0_G\}$. Since $Ann_r(g) \neq \emptyset$, let $r \in Ann_R(g)$. Then $rg = 0$. Using the fact that $Dg = Dh$, we have $d \in D$ such that $dg = h$. It follows that $rh = r(dg) = d(rg) = 0$, since $d \in D = Aut_R(G)$ and $rg = 0$. Therefore $r \in Ann_R(h)$ and $Ann_R(g) \subseteq Ann_R(h)$. We similarly have that $Ann_R(h) \subseteq Ann_R(g)$. Hence $Ann_R(g) = Ann_R(h)$.

- Now, we assume that $Ann_R(g) = Ann_R(h)$. We want to show that $Dg = Dh$. To do this, we define the following map

$$\begin{aligned} \rho : Rg &\to Rh \\ rg &\mapsto rh. \end{aligned}$$

  Since $g, h \in G_1$, $Rg = Rh = G$. Let $r_1g, r_2g \in G$ such that $r_1g = r_2g$. Then $(r_1 - r_2)g = 0$. It follows that $r_1 - r_2 \in Ann_R(g) = Ann_R(h)$. Hence $r_1h = r_2h$. Therefore the map ρ is well-defined. For $r_1, r_2 \in R$ we have

$$\rho(r_1g + r_2g) = \rho((r_1 + r_2)g) = (r_1 + r_2)h = r_1h + r_2h = \rho(r_1g) + \rho(r_2g)$$
$$\rho(r_1(r_2g)) = \rho((r_1r_2)g) = (r_1r_2)h = r_1(r_2h) = r_1\rho(r_2g)$$

  Hence $\rho \in C$. Since $\rho(g) = \rho(1g) = 1h = h \neq 0$, $\rho \in C \setminus \{0\}$. We know from Theorem 4.1.7 that $C = D^0$. So $\rho \in D$ and $D\rho = D$. Since $\rho(g) = h$, $Dh = D\rho(g) = Dg$.

□

In order to prove Theorem 4.1.13 below, we need the following lemmas.

Lemma 4.1.10. *([11], Lemma 3.22) Let R be a near-ring and G an R-module. If A, B, C are R-ideals of G, then we have*

$$H = [(A + C) \cap (B + C)] \, / \, [(A \cap B) + C]$$

is an abelian group and for all $r \in R$ the mapping

$$\begin{aligned} \rho : H &\to H \\ h &\mapsto rh \end{aligned}$$

is an endomorphism of $(H, +)$.

Proof. Let $I = (A \cap B) + C$ and $N = (A + C) \cap (B + C)$.

- From Theorem 2.3.14 we have that I and N are R-ideals of G and since $I \subseteq N$, I is an R-ideal of N. It follows that N/I is a group. We want to show that $H = N/I$ is abelian. But H is abelian if for any $n_1, n_2 \in N$, we have $n_1 + n_2 - n_1 - n_2 \in I$ which is the same as proving that $n_1 + n_2 \equiv n_2 + n_1 \mod I$. Since $N \subseteq A + C$ and $C \subseteq I$, there is an $a \in A, c \in C$ such that $n_1 = a + c$. So $n_1 \equiv a \mod I$. Likewise we have $N \subseteq B + C$ and so there is a $b \in B$ such that $n_2 \equiv b \mod I$. Therefore $n_1 + n_2 \equiv a + b \mod I$. Since A, B are normal subgroups of G (A, B are R-ideals) and $(a + b - a) - b = a + b - a - b = a + (b - a - b)$, we have $a + b - a - b \in A \cap B$. Hence $a + b \equiv b + a \mod A \cap B$. But $A \cap B \subseteq I$. It follows that $a + b \equiv b + a \mod I$. Hence $n_1 + n_2 \equiv a + b \equiv b + a \equiv n_2 + n_1 \mod I$. Therefore H is abelian.

- We now show that the map ρ is an endomorphism of $(H, +)$. To prove it, we show that $r(n_1 + n_2) \equiv rn_1 + rn_2 \mod I$. From the first part we know that for all $n_1, n_2 \in N$ there are $a \in A$ and $b \in B$ such that $n_1 \equiv a \mod I, n_2 \equiv b \mod I$. It follows that $rn_1 \equiv ra \mod I, rn_2 \equiv rb \mod I$. Also since A is an R-ideal, we have $r(b + a) - rb \in A$. It follows that $r(b + a) \equiv rb \mod A$. From the first part we have that $r(a + b) \equiv r(b + a) \mod A$ and so $r(a + b) \equiv rb \mod A$. Hence $r(a + b) \equiv ra + rb \mod A$, since $r(b + a) - rb, ra \in A$ and $(r(b + a) - rb) - ra \in A$. Likewise we have $r(a + b) \equiv ra + rb \mod B$. Hence $r(a + b) \equiv ra + rb \mod A \cap B$. Since $A \cap B \subseteq I$, $r(a + b) \equiv ra + rb \mod I$. Therefore $r(n_1 + n_2) \equiv r(a + b) \equiv ra + rb \equiv rn_1 + rn_2 \mod I$, so ρ is an endomorphism of $(H, +)$.

$\square$

Lemma 4.1.11. *([11], Lemma 3.25) Let R be a 2-primitive near-ring on the R-module G, and let g be its generator. If B, C are left ideals of R such that*

$$B + Ann_R(g) = C + Ann_R(g) = R, \quad B \cap C \subseteq Ann_R(g),$$

then R is a ring.

Proof. By Remark 2.3.13 the left ideals of R are also R-ideals of R, by considering R as an R-module. Also $Ann_R(g)$ is an R-ideal of R by Proposition 2.3.9. From Lemma 4.1.10

$$H = [(B + Ann_R(g)) \cap (C + Ann_R(g))] \,/\, [(B \cap C) + Ann_R(g)]$$

is abelian and the map ρ is an endomorphism of $(H, +)$. But $H = R/Ann_R(g)$, since $B + Ann_R(g) = C + Ann_R(g) = R$ and $B \cap C \subsetneq Ann_R(g)$, and so H is R-isomorphic to G, by Corollary 2.3.30. Hence G is abelian and for all $r \in R$, the map $\rho_r : G \to G$ given by $\rho_r : g \mapsto rg$ is an endomorphism of G. Therefore from Lemma 2.3.32 we have R is a ring, since G is a faithful R-module. □

From now on we will write G^* for $G \setminus \{0\}$.

Lemma 4.1.12. *([11], Lemma 3.26) Let R be a 2-primitive near-ring on the R-module G, such that R has an identity and it is not a ring, and let $\{g_1, g_2 \ldots, g_n\} \subseteq G_1$, $n > 1$, such that $Ann_R(g_i) \neq Ann_R(g_j)$ if $i \neq j$. Then for all $t = 1, \ldots, n-1$*

$$\bigcap_{i=1}^{t} Ann_R(g_i) \nsubseteq Ann_R(g_k)$$

for $t < k \leq n$.

Proof. We use induction on t to prove the lemma. Since R is 2-primitive on G with identity, $G_1 = G^*$ by Lemma 4.1.6 and G has no nontrivial proper R-submodules. So if $g \in G^*$, then by Lemma 2.3.31 we have $Ann_R(g)$ is a maximal R-ideal of R. Hence $Ann_R(g_i) \subseteq Ann_R(g_j)$ implies $Ann_R(g_i) = Ann_R(g_j)$. Thus $i = j$. So for all $k > 1$ we have $Ann_R(g_1) \nsubseteq Ann_R(g_k)$. Now we assume that for $t > 2$, $\bigcap_{i=1}^{t} Ann_R(g_i) \nsubseteq Ann_R(g_k)$ for $t < k \leq n$. Let $B = \bigcap_{i=1}^{t} Ann_R(g_i)$. We want to show that $\bigcap_{i=1}^{t+1} Ann_R(g_i) \nsubseteq Ann_R(g_k)$ for $t + 1 < k \leq n$. We know that $Ann_R(g_{t+1}) \nsubseteq Ann_R(g_k)$ for $t + 1 < k \leq n$. Let $C = Ann_R(g_{t+1})$. We have by Theorem 2.3.14 that $B + Ann_R(g_k)$ and $C + Ann_R(g_k)$ are R-ideals of R. Also by Theorem 2.3.31 $Ann_R(g_{k+1})$ is a maximal R-ideal of R. Since $B \neq \{0\}, C \neq \{0\}$,

$$R = B + Ann_R(g_k) = C + Ann_R(g_k).$$

We assumed that R is not a ring. So from Lemma 4.1.11 $B \cap C \not\subseteq Ann_R(g_k)$ for $t+1 < k \leq n$. Hence $\bigcap_{i=1}^{t+1} Ann_R(g_i) \not\subseteq Ann_R(g_k)$ for $t+1 < k \leq n$. $\square$

Theorem 4.1.13. *([11], Theorem 3.21) Let R be a 2-primitive near-ring with identity on the R-module G, such that R is not a ring. Let $\{g_1, g_2 \ldots, g_n\} \subseteq G_1$, $n \geqslant 1$, such that for $i \neq j$, $Ann_R(g_i) \neq Ann_R(g_j)$. Let $\{h_1, h_2, \ldots, h_n\} \subseteq G$, where the h_i are not necessarily all distinct for $i \in \{1, \ldots, n\}$. Then there exists an element $r \in R$ such that $rg_i = h_i$ for $1 \leq i \leq n$.*

Proof. We use induction on n, the number of $g_i's$, to prove the theorem. By Lemma 4.1.6, $G_1 = G^*$. For $g_1 \in G^*$ we have $Rg_1 = G$ and so for $h_1 \in G$ there is $r \in R$ such that $rg_1 = h_1$.
So we assume that there is $r_m \in R$ such that $r_m g_i = h_i$ for $1 \leq i \leq m < n$. Let $I = \bigcap_{i=1}^{m} Ann_R(g_i)$. By Lemma 4.1.12 we have $I \not\subseteq Ann_R(g_{m+1})$. So $Ig_{m+1} \neq \{0\}$, otherwise $I \subseteq Ann_R(g_{m+1})$. By Proposition 2.3.9 we have that I is a left ideal of R. We want to show that Ig_{m+1} is an R-ideal of G. Let $sg_{m+1} \in Ig_{m+1}, r \in R, g \in G$. Since $g_{m+1} \in G_1$, $Rg_{m+1} = G$. So there is $r_1 \in R$ such that $g = r_1 g_{m+1}$. So we have

$$\begin{aligned} r(g + sg_{m+1}) - rg &= r(r_1 g_{m+1} + sg_{m+1}) - (rr_1)g_{m+1} \\ &= [r(r_1 + s) - rr_1]\, g_{m+1}. \end{aligned}$$

Since I is a left ideal of R and $s \in I, r(r_1+s) - rr_1 \in I$. Hence $r(g + sg_{m+1}) - rg \in Ig_{m+1}$. Also Ig_{m+1} is normal since I is normal. Therefore Ig_{m+1} is an R-ideal of G. Since R is a zero-symmetric near-ring, by Proposition 4.1.3 R-ideals of G are R-submodules of G. So Ig_{m+1} is an R-submodule of G. Since R is a 2-primitive near-ring on G, G has no nontrivial proper R-submodules. It follows that $Ig_{m+1} = G$, because $Ig_{m+1} \neq \{0\}$. So there is $s \in I$ such that $sg_{m+1} = h_{m+1} - r_m g_{m+1}$. Let $r_{m+1} = s + r_m$. We now verify that r_{m+1} is the required element. We have for all i, $1 \leq i \leq m$, $sg_m = 0$, since $s \in I = \bigcap_{i=1}^{m} Ann_R(g_i)$. So

$$\begin{aligned} r_{m+1} g_i &= (s + r_m)g_i = sg_i + r_m g_i = r_m g_i, \forall 1 \leq i \leq m \\ r_{m+1} g_{m+1} &= (s + r_m)g_{m+1} = sg_{m+1} + r_m g_{m+1} = h_{m+1} - r_m g_{m+1} + r_m g_{m+1} \\ &= h_{m+1}. \end{aligned}$$

Thus we have proved the theorem. □

We need the following material in order to prove two important theorems, namely Theorem 4.1.21 and Theorem 4.1.22.

Definition 4.1.14. *([11]) Let $(G,+)$ be a group and A a set of automorphisms of G. Then G consists of a disjoint union of orbits of A, under the action of A on G. A subset $\{g_i | i \in I\}$ of G, where I is some index set, is called a set of orbit representatives if*

$$G^* = \bullet_{i \in I} A g_i.$$

where "$\bullet$" means disjoint union.

Lemma 4.1.15. *([11], Lemma 3.28) Let $(G,+)$ be a group, A a group of automorphisms of G. Let $f \in M_A(G)$ and $G^* = \bullet_{i \in I} A g_i$. Then f uniquely determines and is determined uniquely by the set $\{h_i | i \in I\}$, where $h_i = f(g_i)$.*

Lemma 4.1.16. *([11], Lemma 3.28) Let $(G,+)$ be a group, A a group of automorphisms of G. Let $f \in M_A(G)$. Then f induces a map from the orbits of A on G to themselves.*

Proof. We have $f(Ag) = A(f(g))$. So the result follows. □

Lemma 4.1.17. *([11], Lemma 3.30) Let $(G,+)$ be a group, A a group of automorphisms of G. Let $g \in G^*$ and $h \in G$. Then there exists $f \in M_A(G)$ such that $f(g) = h$ if and only if $St_A(g) \subseteq St_A(h)$, where $St_A(g) := \{a \in A | a(g) = g\}$ is the stabilizer of $g \in G$ in A.*

Proof. Suppose that there exists $f \in M_A(G)$ such that $f(g) = h$. Let $a \in St_A(g) = \{a \in A | a(g) = g\}$. We have $a(h) = af(g) = f(a(g)) = f(g) = h$. Hence $a \in St_A(h)$. Thus $St_A(g) \subseteq St_A(h)$. Now we assume that $St_A(g) \subseteq St_A(h)$. We have to find $f \in M_A(G)$ such that $f(g) = h$. We define f as follows:

$$\begin{aligned} f(a(g)) &= a(h) \quad \text{for all } a \in A \\ f(x) &= 0 \qquad \text{for all } x \in G \setminus Ag. \end{aligned}$$

We have to show that f is well-defined on Ag. So let $a_1, a_2 \in A$, such that $a_1(g) = a_2(g)$. Then $(a_2^{-1} \circ a_1)(g) = g$. It follows that $(a_2^{-1} \circ a_1) \in St_A(g)$. But by hypothesis $St_A(g) \subseteq St_A(h)$ and so $a_2^{-1} \circ a_1 \in St_A(h)$. Hence $a_1(h) =$

$a_2(h)$. Therefore f is well-defined. We now show that $f \in M_A(G)$. Let $x \in G$ and $\alpha \in A$. If $x \notin Ag$, then $\alpha(x) \notin Ag$. So $0 = \alpha f(x) = f(\alpha(x)) = 0$. Now if $x \in Ag$, then $x = a(g)$ for some $a \in A$. We have $f(\alpha(x)) = f(\alpha(a(g)) = f((\alpha \circ a)(g)) = (\alpha \circ a)(h) = \alpha(f(x))$. Thus $f \in M_A(G)$. Finally we have $f(g) = h$. □

Theorem 4.1.18. *([11], Theorem 3.31) Let $(G, +)$ be a group, A a fix point free group of automorphisms of G. Let $\{g_i | i \in I\}$ be a set of orbit representatives of G, and let $\{h_i | i \in I\} \subseteq G$, where the h_i are not necessarily distinct for $i \in I$. Then there is a unique $f \in M_A(G)$ such that $f(g_i) = h_i$, for all $i \in I$.*

Proof. Since $\{g_i | i \in I\}$ is a set of orbit representatives, $G^* = \bullet_{i \in I} Ag_i$. So any nonzero element can be written as $a(g_j)$ for some $a \in A$ and $g_j \in \{g_i | i \in I\}$. We define f as follows

$$f(a(g_i)) = a(h_i), \text{ for all } a \in A, i \in I,$$
$$f(0) = 0.$$

We prove that f is well-defined. Let $a_1, a_2 \in A, i \in I$ such that $a_1(g_i) = a_2(g_i)$. So $(a_2^{-1} \circ a_1)(g_i) = g_i$. Since A is a fix point free group of automorphisms of G, $a_2^{-1} \circ a_1 = Id_G$. Hence f is well-defined. It remains to show that $f \in M_A(G)$ since we already have $f(g_i) = h_i$ by construction. Let $\alpha \in A, g \in G$. If $g = 0$, then $\alpha(f(0)) = 0 = f(\alpha(0))$. So let $g \in G^*$. Then there is $a \in A, i \in I$ such that $g = a(g_i)$. So $f(\alpha(g)) = f(\alpha(a(g_i))) = f((\alpha \circ a)(g_i)) = (\alpha \circ a)(h_i) = \alpha(f(g))$. Therefore $f \in M_A(G)$. By Lemma 4.1.15 f is unique. □

Definition 4.1.19. *([11], Definition 3.32) Let S be a subnear-ring of the near-ring R with a natural faithful representation on the R-module V. Then S is said to be dense in R if given any finite subset $\{v_1, v_2, \dots, v_k\}$, $k \geqslant 1$, of V and any element r of R, there exists an $s \in S$ such that $sv_i = rv_i$, for $1 \leq i \leq k$.*

Proposition 4.1.20. *([11], Theorem 3.33) Let $(G, +)$ be a group, A a group of automorphisms of G. Let R be a subnear-ring of $M_A(G)$. Then*

- *R is dense in $M_A(G)$ if and only if for all $\{g_1, g_2, \dots, g_n\} \subseteq G$, $n > 0$, and $f \in M_A(G)$, there is $r \in R$ such that $r(g_i) = f(g_i)$ for $1 \leq i \leq n$.*
- *If A is a fix point free group, then R is dense in $M_A(G)$ if and only if for $\{g_1, g_2, \dots, g_n\} \subseteq G^*$ such that $Ag_i \neq Ag_j$ if $i \neq j$ and $\{g'_1, g'_2, \dots, g'_n\} \subseteq G$, there exists $r \in R$ such that $r(g_i) = g'_i$, for $1 \leq i \leq n$.*

Proof.

- This follows directly from the definition.
- Since A is a fix point free group and $Ag_i \neq Ag_j$ if $i \neq j$, by Theorem 4.1.18 there is $f \in M_A(G)$ such that $f(g_i) = g_i'$ for all $i \in \{1, \ldots, n\}$. Since R is dense, there is $r \in R$ such that $r(g_i) = f(g_i) = g_i'$, for $1 \leqslant i \leqslant n$.

□

Theorem 4.1.21. *([11], Theorem* 3.34*) Let $(G, +)$ be a group such that $G \neq \{0\}$, A a fix point free group of automorphisms of G. Then any dense subnear-ring of $M_A(G)$ is* 2*-primitive on G.*

Proof. Let R be a subnear-ring of $M_A(G)$. We know that G is a faithful $M_A(G)$-module by Example 2.3.3. So by restricting the representation of $M_A(G)$ on G to R, we have that G is a faithful R-module. Let $g^* \in G^*$ and R a dense subnear-ring of $M_A(G)$. From Proposition 4.1.20 we know that for all $g \in G$, there is $r \in R$ such that $rg^* = g$. Hence $Rg^* = G$ and so G is a monogenic R-module. Since for all $g^* \in G^*$ we have $Rg^* = G$, G has no nontrivial proper R-submodules. Therefore R is a 2-primitive near-ring on G. □

Theorem 4.1.22. *([11], Theorem* 3.35*) Let R be a near-ring with identity* 1*, which is* 2*-primitive on the R-module G. Let $C := End_R(G)$ and $D := Aut_R(G)$. Then $R \subseteq M_D(G)$, $C = D \cup \{0\}$, D is fix point free and if R is not a ring then is a dense subnear-ring of $M_D(G)$.*

Proof. We first show that $R \subseteq M_D(G)$. Since G is an R-module, we can define the following map for all $r \in R$:

$$\begin{aligned} f_r : G &\to G \\ g &\mapsto rg. \end{aligned}$$

We have $f_r \in M_D(G)$, since for all $\alpha \in D, g \in G$, $f_r(\alpha(g)) = r\alpha(g) = \alpha(rg) = \alpha(f_r(g))$. Hence $R \subseteq M_D(G)$. From Corollary 4.1.8 we have that $C = D \cup \{0\}$ and D is fix point free. It remains to show that R is a dense subnear-ring of $M_D(G)$. Let $\{g_1, \ldots, g_n\} \subseteq G^*$ such that $Dg_i \neq Dg_j$ if $i \neq j$ and let $\{g_1', \ldots, g_n'\} \subseteq G$. From Theorem 4.1.9 we have $Ann_R(g_i) \neq$

$Ann_R(g_j)$ for all $i \neq j$. Since R is not a ring, by Theorem 4.1.13 there is $r \in R$ such that $rg_i = g_i'$ for $1 \leqslant i \leqslant n$. Finally by Proposition 4.1.20 R is dense in $M_D(G)$. □

We now define the concept of rank.

Definition 4.1.23. *([11], Definition 4.3) Let A be a group of automorphisms, not necessarily fix point free, of the group $(G, +)$. Let $r \in M_A(G)$. The A-rank of r, denoted by $rk_A(r)$, is the cardinal of the set of nonzero orbits of A on rG. We speak of the rank of r and write $rk(r)$ if there is no possibility of confusion. Unless otherwise specified, $A = Aut_R(G)$, where R is a near-ring and G an R-module.*

In the rest of the thesis A is equal to $Aut_R(G)$.

Remark 4.1.24. *Let R be a near-ring and G an R-module. As in Theorem 4.1.22 $R \subseteq M_D(G), D := Aut_R(G)$, for an element $r \in R$ the rank is determined by the cardinality of the set of nonzero orbits of the following action:*

$$\begin{aligned} D \times rG &\to rG \\ (\alpha, rg) &\mapsto \alpha \cdot rg := r\alpha(g). \end{aligned}$$

If r is of rank 1 then according to the definition we have only one nonzero orbit. So for all $g \in G$, $g \neq 0$,

$$rG^* = \{r\alpha(g), \text{ for all } \alpha \in Aut_R(G)\}.$$

From now on R will denote a zero-symmetric right near-ring with identity 1. The following theorems are important in proving van der Walt's theorem.

Theorem 4.1.25. *([11], Theorem 4.2) Let R be a near-ring, G_1 and G_2 be R-modules such that θ is an R-isomorphism from G_1 to G_2. Let $C_i := End_R(G_i)$, $D_i := Aut_R(G_i)$ for $i = 1, 2$. We define*

$$\begin{aligned} \varphi : C_1 &\to C_2 \\ c &\mapsto \varphi(c) \end{aligned}$$

with $\varphi(c)(g_2) = \theta(c(g_1))$, where $g_2 = \theta(g_1)$. Then φ is an isomorphism and φ restricted to D_1 is an isomorphism from D_1 to D_2.

Proof. First we show that φ is well-defined. For φ to be well-defined we have to show that for all $c \in C_1$, $\varphi(c) \in C_2$. Since θ is an R-isomorphism from G_1 to G_2, for all $g_2 \in G_2$ there is a unique $g_1 \in G_1$ such that $\theta(g_1) = g_2$. We have for all $c \in C_1, g, h \in G_1, r \in R$

$$\begin{aligned}
\varphi(c)(r\theta(g)) &= \varphi(c)(\theta(rg)), \text{ since } \theta \text{ is an } R\text{-isomorphism,}\\
&= \theta(c(rg)),\\
&= \theta(rc(g)), \text{ since } c \in C_1,\\
&= r\theta(c(g)), \text{ since } \theta \text{ is an } R\text{-isomorphism,}\\
&= r\varphi(c)(\theta(g)),
\end{aligned}$$

and

$$\begin{aligned}
\varphi(c)(\theta(g)+\theta(h)) &= \varphi(c)(\theta(g+h)), \text{ since } \theta \text{ is an } R\text{-isomorphism,}\\
&= \theta(c(g+h)),\\
&= \theta(c(g)+c(h)), \text{ since } c \in C_1,\\
&= \theta(c(g))+\theta(c(h)), \text{ since } \theta \text{ is an } R\text{-isomorphism,}\\
&= \varphi(c)(\theta(g))+\varphi(c)(\theta(h)).
\end{aligned}$$

Hence $\varphi(c) \in C_2$ for all $c \in C_1$. Therefore φ is well-defined.
Now we show that φ is a semigroup homomorphism from C_1 to C_2. Let $c_1, c_1' \in C_1, g \in G_1$. we have

$$\begin{aligned}
\varphi(c_1 \circ c_1')(\theta(g)) &= \theta((c_1 \circ c_1')(g))\\
&= \theta(c_1(c_1'(g)))\\
&= \varphi(c_1)(\theta(c_1'(g)))\\
&= \varphi(c_1)(\varphi(c_1')(\theta(g)))\\
&= \left[\varphi(c_1) \circ \varphi(c_1')\right](\theta(g)).
\end{aligned}$$

Hence φ is a semigroup homomorphism. The homomorphism φ is bijective. In fact let $c_1, c_1' \in C_1$ such that $\varphi(c_1) = \varphi(c_1')$. So for all $g \in G_1$ we have $\varphi(c_1)(\theta(g)) = \varphi(c_1')(\theta(g))$. It follows that $\theta(c_1(g)) = \theta(c_1'(g))$. Since θ is injective, $c_1(g) = c_1'(g)$ for all $g \in G_1$. Hence φ is injective. Let $c_2 \in C_2$. We want to find $c_1 \in C_1$ such that $c_2 = \varphi(c_1)$. Let $c_1 = \theta^{-1} \circ c_2 \circ \theta$. We have for

$g \in G$

$$\begin{aligned}\varphi(c_1)(\theta(g)) &= \varphi(\theta^{-1} \circ c_2 \circ \theta)(\theta(g)) \\ &= \theta(\theta^{-1} \circ c_2 \circ \theta(g)) \\ &= c_2(\theta(g)).\end{aligned}$$

Hence $\varphi(c_1) = c_2$ and φ is surjective. Since φ is a semigroup homomorphism, it maps invertible elements of C_1 to invertible elements of C_2. Therefore φ restricted to D_1 is an isomorphism from D_1 to D_2. □

Theorem 4.1.26. *([11], Theorem 4.5) Let R be a 2-primitive near-ring, which is not a ring, on G which has a minimal left ideal K. Then we have:*

- *G is R-isomorphic to K.*
- *There is an idempotent $e \in K \setminus \{0\}$ such that*
  - *$K = Re = Ke$, and*
  - *$End_R(G)$ and eRe are isomorphic semigroups.*
- *Every nonzero element of K has rank 1.*

Proof.

- Since K is a left ideal of R, by Remark 2.3.13 it is also an R-ideal of R. It follows by Proposition 4.1.3 that K is an R-submodule of R. So it is possible to define an R-homomorphism from K to G.

  Since G is faithful, by Remark 2.3.8 $Ann_R(G) := \{r \in R | rg = 0, \forall g \in G\} = \{0\}$. It follows that $KG \neq \{0\}$ and there is $g \in G$ such that $Kg \neq \{0\}$. But Kg is an R-submodule of G. Since R is zerosymmetric and K is a left ideal of R, for all $r \in R, k \in K$ we have $rk = r(0 + k) + r0 \in K$. It follows that $RK \subseteq K$. Hence $RKg \subseteq Kg$. Since G is of type 2 and $Kg \neq \{0\}$, $Kg = G$. Then we define a mapping from K to G as follows:

  $$\begin{aligned} f : K &\to G \\ k &\mapsto kg.\end{aligned}$$

  The map f is an R-homomorphism. Also $f(K) = Kg = G$. So f is surjective. We have $\ker f = \{k \in K | kg = 0\} = K \cap Ann_R(g)$. So $\ker f$ is a left ideal of R, since by Proposition 2.3.9 $Ann_R(g)$ is a left ideal of

R. But K is minimal, so $\ker f = \{0\}$ or $\ker f = K$. If $\ker f = K$, then $Kg = \{0\}$, which is not possible. So $\ker f = \{0\}$. Hence f is injective. Therefore G is R-isomorphic to K.

- We now prove that there is an idempotent $e \in K \setminus \{0\}$ such that $K = Re = Ke$. From the first part we have that $Kg = G$. So there is $e \in K \setminus \{0\}$ such that $eg = g$. So $e^2 g = e(eg) = eg = g$, and $e^2 - e \in K \cap Ann_R(g)$=$\{0\}$. It follows that $e^2 = e$, and so e is idempotent. We have Ke is an R-submodule of K and K is of type 2, since it is isomorphic to G. Hence $K = Ke$ and $K = Ke \subseteq Re \subseteq RK \subseteq K$. Therefore $K = Ke = Re$.

  We have that Re is R-isomorphic to G. So by Theorem 4.1.25, $End_R(G)$ is isomorphic to $End_R(Re)$. We show that $End_R(Re) \cong eRe$. Let $f_r : Re \to Re$ be the mapping defined by $f_r(se) = sere$. We have $f_r(s_1e + s_2e) = f_r(s_1e) + f_r(s_2e)$ and $f_r(ss_1e) = sf(s_1e)$. So f_r is an endomorphism. Hence we can define a mapping from:

$$\begin{aligned} F : eRe &\to End_R(Re) \\ ere &\mapsto f_r \end{aligned}$$

  We have to show that F is well defined. If $er_1e = er_2e$, then for all $s \in R$ we have $ser_1e = ser_2e$. Hence $f_{r_1} = f_{r_2}$ and so F is well-defined. We also have for all $er_1e, er_2e \in eRe$, $F((er_1e)(er_2e)) = f_{r_2} \circ f_{r_1} = F(r_1) * F(r_2)$ with $f * g = g \circ f$. Hence F is a semigroup homomorphism from $(eRe, \cdot)$ to $(End_R(Re), *)$. We now show that F is a bijection. Let $er_1e, er_2e \in eRe$ such that $f_{r_1} = f_{r_2}$. Then $f_{r_1}(e) = f_{r_2}(e)$ and $er_1e = er_2e$, so F is injective. Let $g \in End_R(Re)$. We want to find $ere \in eRe$ such that $f_r = g$, i.e $g(se) = sere$ for all $s \in R$. We know that $e = e^2 \in Re$ and $g(e) \in Re$. So there is $r \in R$ such that $g(e) = re$. Then $ere = eg(e)$, and since g is an R-homomorphism, $ere = eg(e) = g(e^2) = g(e)$. So for all $s \in R$, we have $g(se) = sg(e) = sere = f_r(se)$. Hence F is surjective and therefore F is a semigroup isomorphism.

- We show that every element of $K \setminus \{0\}$ has rank 1. This means that for any nonzero element k, the following action of $D := Aut_R(G)$ on kG

by

$$\begin{aligned} D \times kG &\to kG \\ (\alpha, kg) &\mapsto k\alpha(g), \end{aligned}$$

has just one nonzero orbit. Let us suppose that there are two disjoint nonzero orbits $D(kg_1), D(kg_2)$, with $kg_1, kg_2 \neq 0$. Then by Theorem 4.1.13 for all $\{a_1, a_2\} \subseteq G$, there is $r \in R$ such that $rkg_1 = a_1$ and $rkg_2 = a_2$. So we can have $rkg_1 = 0$ and $rkg_2 \neq 0$. Then $rk \in K \cap Ann_R(g_1)$ and $rk \neq 0$ since otherwise $rkg_2 = 0$. It follows that $K \cap Ann_R(g_1)$ is a nonzero left ideal of R contained in K. Since K is minimal left ideal of R, $K = K \cap Ann_R(g_1)$ and so $K \subseteq Ann_R(g_1)$. It follows that $kg_1 = 0$ which is a contradiction. Therefore every element of $K \setminus \{0\}$ has rank 1.

$\square$

Remark 4.1.27. *According to the theorem above, the minimal left ideals of R are of the form Re for some idempotent element e in R and they are all isomorphic to G.*

We also have

Theorem 4.1.28. *([13]) Let R be a* 2*-primitive near-ring which has a minimal left R-subgroup K. Suppose G is a faithful R-module of type* 2*. Then we have:*

- *G is R-isomorphic to K.*
- *There is an idempotent $e \in K \setminus \{0\}$ such that*
  - *$K = Re = Ke$, and*
  - *$End_R(G)$ and eRe are isomorphic semigroups.*
- *Every nonzero element of K has rank* 1.

We now have a characterisation of minimal left R-subgroups for a given 2-primitive near-ring R.

Theorem 4.1.29. *([13], Theorem* 2.1*) Let R be a* 2*-primitive near-ring on the R-module G. Then R has a minimal left R-subgroup if and only if R contains an idempotent e of rank* 1.

Proof. If R has a minimal left R-subgroup by Theorem 4.1.28, R contains an idempotent e of rank 1.
Now we assume that R contains an idempotent e of rank 1. We have to construct a minimal left R-subgroup K of R. Let $K = Re$, then K is an R-submodule of R. The idea is to find an R-isomorphism between K and G and since G is of type 2, K will also be simple and will be a minimal left R-subgroup. Since G is faithful, there is $g_1 \in G$, such that $Kg_1 \neq \{0\}$. But G being of type 2 implies that $Rg_1 = G$. Let $g = eg_1$. We have $g \neq 0$, otherwise we will have $\{0\} = Rg = Reg_1 = Kg_1$, but $Kg_1 \neq \{0\}$. We have $eg = e(eg_1) = eg_1 = g$, since e is an idempotent. It follows that $Kg = Reg = Rg = G$, since by Theorem 4.1.6, for all $g \in G^*$, $Rg = G$. We define a mapping

$$\begin{aligned} f : K &\to G \\ k &\mapsto kg. \end{aligned}$$

The mapping f is an R-homomorphism and surjective, since $Kg = G$. We show that it is also one to one. We have $\ker f = K \cap Ann_R(g)$. It remains to prove that $\ker f = \{0\}$. Since $\ker f$ is an left R-subgroup of K (by Lemma 2.3.23, the R-submodules are left R-subgroups and by Example 2.3.12 $\ker f$ is an R-submodule) and also contained in $Ann_R(g)$, we will simply show that there is no nonzero left R-subgroup of K contained in $\ker f$. So let H be a nonzero left R-subgroup of K. Since $K = Re$, H will be of the form Ie. So $He = (Ie)e = Ie = H$. Since G is faithful, there is $g' \in G$, such that $Hg' \neq \{0\}$. Then $Heg' = Hg' = G$, since G is of type 2, and there is $h \in H$, such that $h(eg') = g \neq 0$. It follows that $h \notin Ann_R(eg')$. But since e is of rank 1, $eG = \{0\} \cup D(eg_1) = D(g)$. It follows that g and eg' are in the same orbit and so $D(eg') = D(g)$. By Theorem 4.1.9 we have that $Ann_R(g) = Ann_R(eg')$. Hence $h \notin Ann_R(g)$ and $H \not\subseteq Ann_R(g)$. Therefore f is injective and K is a minimal left R-subgroup of R. □

The theorems above have some very important consequences.

Corollary 4.1.30. *([13], Corollary 2.2) Let R be 2-primitive near-ring with identity on G and suppose K is a minimal left R-subgroup and that e is an idempotent of rank 1 such that $K = Re$. Then $(eRe, \cdot)$ is a group with zero, and the group $eRe \setminus \{0\}$ acts on Re by right multiplication as a fix point free group of automorphisms.*

Proof. Since R is 2-primitive on G, by Theorem 4.1.22

$$End_R(G) \setminus \{0\} = Aut_R(G).$$

It follows that $End_R(G)$ is a group with zero. From Theorem 4.1.28 $End_R(G)$ and eRe are isomorphic semigroups. It follows that $(eRe, \cdot)$ is also a group with zero. By Theorem 4.1.22 again we know that $Aut_R(G)$ is fix point free and by Theorem 4.1.28 G is R-isomorphic to K. Hence $eRe \setminus \{0\}$ acts on $K = Re$ as a fix point free group of automorphisms. □

Corollary 4.1.31. *([13], Corollary 2.3) Let R be a 2-primitive near-ring on G and let e be a distributive idempotent element of R of rank 1. Then $(eRe, +, \cdot)$ is a near-field.*

Proof. Since e is idempotent of rank 1, by Theorem 4.1.29 Re is a minimal left R-subgroup of R. So by Corollary 4.1.30 $(eRe, \cdot)$ is a group with zero. Moreover e being distributive implies that $(eRe, +)$ is a group. Therefore $(eRe, +, \cdot)$ is a near-field. □

Remark 4.1.32. *Since every near-field is abelian by Theorem 2.2.1, $(eRe, +)$ is abelian if R is 2-primitive on G and e is a distributive idempotent element of R of rank 1.*

Proposition 4.1.33. *([13], Corollary 2.6) Let $(G, +)$ be a group, A a group of automorphisms of G such that A acts fix point free on G. Then $M_A(G)$ is a near-field if G^* is an orbit, that is if there is $g \in G^*$ such that $Ag = G^*$.*

Proof. From Theorem 4.1.21 we know that $M_A(G)$ is 2-primitive on G. Also $Id_G \in M_A(G)$ is distributive and idempotent. We want to show that Id_G is of rank 1. By definition, the rank of Id_G is the cardinality of the set of nonzero orbits of the action of A on $Id_G G = G$. Since G^* is an orbit, we have only one nonzero orbit. So Id_G is of rank 1. Hence by Corollary 4.1.31 $M_A(G)$ is a near-field. □

We introduce a new class of near-rings.

Definition 4.1.34. *([13]) If the near-ring R contains a complete set of distributive idempotents, i.e. it contains a finite set $\{e_1, e_2, \ldots, e_n\}$ of idempotents such that*

1. $e_1 + e_2 + \cdots + e_n = 1$;

2. *$e_ie_j = 0$ if $i \neq j$;*

3. *each e_i is of rank 1;*

4. *each e_i is a distributive element of R;*

then R is called a CDI-near-ring.

Remark 4.1.35. *([13]) Let R be a CDI-near-ring and 2-primitive on G. Let $\{e_1, e_2, \ldots, e_n\}$ be the set of idempotents of rank 1. By Theorem 4.1.29 R has minimal left R-subgroups Re_i for all $i \in \{1, \ldots, n\}$. Moreover by Theorem 4.1.28 we have*

- *n R-isomorphisms $\phi_i : G \to Re_i$, and*
- *n semigroup isomorphisms $\psi_i : End_R(G) \to e_iRe_i$.*

By Corollary 4.1.30 $e_iRe_i \setminus \{0\}$ acts on Re_i by right multiplication for all $i \in \{1, \ldots, n\}$ and we now give the action explicitly. Any element of Re_i and e_iRe_i can be uniquely written as $\phi_i(g)$ and $\psi_i(\alpha)$ for some $g \in G, \alpha \in End_R(G)$, respectively. The action is defined by

$$\phi_i(g) \cdot \psi_i(\alpha) := \phi_i(\alpha(g)).$$

We simply write $\phi_i(g)\psi_i(\alpha) = \phi_i(\alpha(g))$ instead of $\phi_i(g) \cdot \psi_i(\alpha) = \phi_i(\alpha(g))$ when there is no room for confusion.
So for all $r \in R, g \in G, \alpha \in End_R(G)$, $r\phi_i(g)\psi_i(\alpha) = \phi_i(r\alpha(g))$.

Proposition 4.1.36. *([13]) Let R be 2-primitive on the R-module G and suppose that R is a CDI-near-ring with $\{e_1, \ldots, e_n\}$ as the set of idempotents. Then*

- *$(e_iRe_i, +)$ is isomorphic to $(e_iG, +)$ for all $i \in \{1, \ldots, n\}$.*
- *$G = e_1G + \cdots + e_nG$ and G is abelian.*
- *There is a group isomorphism Φ between G and $H := e_1Re_1 \oplus \cdots \oplus e_nRe_n$.*

Proof.

- For all $i \in \{1, \ldots, n\}$, $\phi_i : G \to Re_i$ is an R-isomorphism and $\phi_i(e_iG) = e_i\phi_i(G) = e_iRe_i$. So $(e_iG, +)$ and $(e_iRe_i, +)$ are isomorphic.

- By Remark 4.1.32 $(e_iRe_i, +)$ is abelian for all $i \in \{1, \dots, n\}$. It follows that $(e_iG, +)$ is also abelian. Since for all $i, j \in \{1, \dots, n\}$ we have $e_ie_j = 0$ if $i \neq j$ and $e_1 + \cdots + e_n = 1$, $G = e_1G + \cdots + e_nG$ is a direct decomposition, and so G is abelian. Where direct decomposition means each e_iG is a normal subgroup of G, $e_iG \cap e_jG = \{0\}$ for all $i \neq j$, $i, j \in \{1, \dots, n\}$ and $G = e_1G + \cdots + e_nG$. Since e_iG is abelian, it is a normal subgroup of G. We also have $e_iG \cap e_jG = \{0\}$, $i \neq j$, $i, j \in \{1, \dots, n\}$, since if $j \neq i$ and $e_ig = e_jg'$, we have

$$0 = 0g = (e_je_i)g = e_j(e_ig) = e_j(e_jg') = (e_je_j)g' = e_jg' = e_ig.$$

- Let Φ be the map defined by

$$\begin{aligned} \Phi : G &\to H \\ g &\mapsto \phi_1(e_1g) + \cdots + \phi_n(e_ng). \end{aligned}$$

  We show that Φ is a group isomorphism. Since $G = e_1G + \cdots + e_nG$ is a direct decomposition and $\phi_i : (e_iG, +) \to (e_iRe_i, +)$ is group isomorphism, for all $i \in \{1, \dots, n\}$, Φ is a group isomorphism.

$\square$

Corollary 4.1.37. *([13]) Let $H := e_1Re_1 \oplus \cdots \oplus e_nRe_n$. Then*

- *H is an R-module under the action defined by*

$$r \cdot h := \Phi(rg)$$

  with $h = \Phi(g) \in H$, where Φ is the group isomorphism defined in the proof of Proposition 4.1.36. We simply write rh instead of $r \cdot h$.

- *Φ is an R-isomorphism.*

Proof.

- Since Φ is a group isomorphism from G to H, for any $h \in H$ there is a unique $g \in G$ such that $h = \Phi(g)$. Hence the action is well-defined. It follows that H is an R-module.

- Let $g \in G$ an $r \in R$. We have $\Phi(rg) = r \cdot \Phi(g) = r\Phi(g)$, by the definition of the action. Since we already have that Φ is a group isomorphism, we now have that Φ is an R-isomorphism.

□

Corollary 4.1.38. *([13]) Let Φ be the R-isomorphism between G and $H := e_1Re_1 \oplus \cdots \oplus e_nRe_n$ defined in the proof of Proposition 4.1.36. Then:*

- *There is a semigroup isomorphism $\Psi : End_R(G) \to End_R(H)$ such that for all $g \in G, r \in R$ and $\alpha \in End_R(G)$ we have*

$$\Phi(g)\Psi(\alpha) := \Psi(\alpha)(\Phi(g)) = \phi_1(e_1g)\psi_1(\alpha) + \cdots + \phi_n(e_ng)\psi_n(\alpha)$$

  and $\Phi(r\alpha(g)) = r\Phi(g)\Psi(\alpha)$.

- *If R is not a ring, then R is a dense subnear-ring of $M_A(H)$, where $A := End_R(H)$.*

Proof.

- We have seen in Corollary 4.1.37 that G is R-isomorphic to H. So by Theorem 4.1.25 there is a semigroup isomorphism

$$\Psi : End_R(G) \to End_R(H)$$

  such that

$$\Phi(g)\Psi(\alpha) = \Psi(\alpha)(\Phi(g)) = \Phi(\alpha(g)),$$

  since

$$\Psi(\alpha)(h) = \Phi(\alpha(g)), \text{ with } \Phi(g) = h.$$

  But we know from Proposition 4.1.36 that

$$\Phi(\alpha(g)) = \phi_1(e_1\alpha(g)) + \cdots + \phi_n(e_n\alpha(g))$$

  and by Remark 4.1.35 we have $\phi_i(g)\psi_i(\alpha) = \phi_i(\alpha(g))$. Hence

$$\Phi(g)\Psi(\alpha) = \phi_1(e_1g)\psi_1(\alpha) + \cdots + \phi_n(e_ng)\psi_n(\alpha).$$

  We have

$$\begin{aligned} r\Phi(g)\Psi(\alpha) &= \Phi(rg)\Psi(\alpha) \\ &= \Phi(\alpha(rg)) \text{ since } \Phi(g_1)\Psi(\alpha_1) = \Phi(\alpha_1(g_1)) \\ &= \Phi(r\alpha(g)) \text{ since } \alpha \in End_R(G). \end{aligned}$$

- Suppose that R is not a ring. Since H is R-isomorphic to G, R is 2-primitive on H. By Theorem 4.1.22 R is a dense subnear-ring of $M_D(H)$, with $D := Aut_R(H)$, and $Aut_R(H) = A \setminus \{0\}$ by Corollary 4.1.8. Therefore R is a dense subnear-ring of $M_{A^*}(H)$. But we have $M_A(H) \subseteq M_{A^*}(H)$. Therefore R is a dense subnear-ring of $M_A(H)$.

$\square$

Lemma 4.1.39. *([13], Lemma 3.1) Let $H := e_1Re_1 \oplus \cdots \oplus e_nRe_n$ as defined in Proposition 4.1.36 and $A := End_R(H)$. Then (H, A) is a near-vector space.*

Proof. We have that

- $(H, +)$ is an abelian group and A is a set of endomorphism of $(H, +)$.
- We have $id, -id, 0 \in A$.
- Since R is 2-primitive on H (because $G \cong_R H$), by Corollary 4.1.8 $A \setminus \{0\} = Aut_R(H)$ and A acts fix point free on H. So A^* is a subgroup of $Aut(H)$.
- We now show that the quasi-kernel $Q(H)$ generates H additively. Since $H = e_1Re_1 \oplus \cdots \oplus e_nRe_n$, if we can show that $e_iRe_i \subset Q(H)$ then $Q(H)$ generates H additively. So let $i \in \{1, \ldots, n\}$, $e_ire_i \in e_iRe_i$, with $r \in R$, and $\alpha, \beta \in A$. Then there are unique $\alpha_1, \beta_1 \in A, g \in G$ such that $\alpha = \Psi(\alpha_1), \beta = \Psi(\beta_1), e_ire_i = \Phi(e_ig)$, since by Corollary 4.1.38 $\Psi : End_R(G) \to End_R(H)$ is an isomorphism and by Proposition 4.1.36 $\Phi : G \to H$ is also an isomorphism. Again by Corollary 4.1.38, for all $g \in G, \alpha \in End_R(G)$ we have $\Phi(g)\Psi(\alpha) = \phi_1(e_1g)\psi_1(\alpha) + \cdots + \phi_n(e_ng)\psi_n(\alpha)$. It follows that

$$\begin{aligned}\Phi(e_ig)\Psi(\alpha) &= \phi_1(e_1(e_ig))\psi_1(\alpha) + \cdots + \phi_n(e_n(e_ig))\psi_n(\alpha) \\ &= \phi_1((e_1e_i)g)\psi_1(\alpha) + \cdots + \phi_n((e_ne_i)g)\psi_n(\alpha) \\ &= \phi_i(e_ig)\psi_i(\alpha) \text{ since } e_ie_j = 0, \forall i \neq j \text{ and } e_ie_i = e_i.\end{aligned}$$

Hence

$$\begin{aligned} e_i r e_i \alpha + e_i r e_i \beta &= \Phi(e_i g)\Psi(\alpha_1) + \Phi(e_i g)\Psi(\beta_1) \\ &= \phi_i(e_i g)\psi_i(\alpha_1) + \phi_i(e_i g)\psi_i(\beta_1) \\ &= \phi_i(e_i g)\psi_i(\gamma_1) \\ &= \Phi(e_i g)\Psi(\gamma_1) \\ &= e_i r e_i \gamma \text{ with } \gamma = \Psi(\gamma_1), \end{aligned}$$

with $\gamma_1 = \psi_i^{-1}\left[(\phi_i(e_i g))^{-1}\left(\phi_i(e_i g)\psi_i(\alpha_1) + \phi_i(e_i g)\psi_i(\beta_1)\right)\right]$.

Therefore $e_i R e_i \subset Q(H)$. Thus $Q(H)$ generates H.

Thus (H, A) is a near-vector space. □

Corollary 4.1.40. *([13]) The near-vector space (H, A) in Lemma 4.1.39 is a finite dimensional near-vector space.*

Proof. The set $\{e_1, \ldots, e_n\}$ is a set of idempotents of rank 1. For each e_i we have one nonzero orbit of the action of A^* on $e_i H$, namely $e_i H \setminus \{0\}$. Since $e_1 + \cdots + e_n = 1$ and $1 \in R$ we have

$$\begin{aligned} 1 &= e_1 + \cdots + e_n \\ &= e_1 e_1 + \cdots + e_n e_n, \text{ since } e_i \text{ is idempotent for all } i \in \{1, \ldots, n\} \\ &= e_1 1 e_1 + \cdots + e_n 1 e_n \\ &\in H, \text{ where } H = e_1 R e_1 \oplus \cdots \oplus e_n R e_n. \end{aligned}$$

It follows that $e_i \in e_i H$. Hence the only non zero orbit is $e_i H \setminus \{0\} = \{e_i \alpha, \text{ for all } \alpha \in A^*\}$. But $e_i H = e_i R e_i$, since $e_i e_i = e_i$ and $e_i e_j = 0$ for $i \neq j$. Therefore $e_i R e_i \setminus \{0\} = \{e_i \alpha, \text{ for all } \alpha \in A^*\}$, and e_i generates $e_i R e_i$. But we have seen in the proof of Lemma 4.1.39 that $\bigcup_{i=1}^{n} e_i R e_i$ generates H. So $\{e_1, \ldots, e_n\}$ generates H. We now show that $\{e_1, \ldots, e_n\}$ is independent. Let $\alpha_1, \ldots, \alpha_n \in A$ such that $e_1 \alpha_1 + \cdots + e_n \alpha_n = 0$. Then for all $i \in \{1, \ldots, n\}$, we have

$$\begin{aligned} e_i(e_1 \alpha_1 + \cdots + e_n \alpha_n) &= e_i 0 \\ &= e_i \alpha_i, \text{ since } e_i e_i = e_i \text{ and } e_i e_j = 0, \forall j \neq i \\ &= 0. \end{aligned}$$

Hence $e_i\alpha_i = 0$. Since A acts fix point free on H and $e_i \neq 0$, $\alpha_i = 0$. Therefore $\{e_1, \ldots, e_n\}$ is independent. Thus $\{e_1, \ldots, e_n\}$ is a basis of (H, A) and so (H, A) is of dimension n. □

Theorem 4.1.41. *([13], Theorem 3.2) Let R be 2-primitive on an R-module G and suppose that R is a CDI-near-ring and not a ring. Then*

- *R is abelian and symmetric i.e. $a(-b) = -ab$.*
- *There is a finite dimensional near-vector space (H, A) such that R is isomorphic to a dense subnear-ring of $M_A(H)$.*

Proof.

- Since R is 2-primitive on G, by Theorem 4.1.22

  $$D := Aut_R(G) = End_R(G) \setminus \{0\}$$

  and R is a dense subnear-ring of $M_D(G)$. It suffices to show that $M_D(G)$ is abelian and symmetric. From Proposition 4.1.36, G is abelian, so by Proposition 2.3.4, $M_D(G)$ is also abelian. Also $-id \in D$. Hence for all $f, h \in M_D(G), g \in G$, $(f \circ (-h))(g) = f(-id(h(g))) = -id(f(h(g))) = -(f \circ h)(g)$. So for all $f, h \in M_D(G)$, $f \circ (-h) = -(f \circ h)$. Therefore R is abelian and symmetric.

- Since R is 2-primitive on G and R is a CDI-near-ring, by Lemma 4.1.39 and Corollary 4.1.40 there is a finite dimensional near-vector space (H, A). Since R is not ring, by Corollary 4.1.38, R is a dense subnear-ring of $M_A(H)$.

□

Theorem 4.1.42. *([13], Theorem 3.3) Let (G, A) be a finite dimensional near-vector space. Then $M_A(G)$ is a CDI-near-ring which is 2-primitive on G.*

Proof. We know from Theorem 4.1.21 that $M_A(G)$ is 2-primitive on G. We just have to show that $M_A(G)$ is a CDI-near-ring. Let $\{g_1, \ldots, g_n\}$ be a basis of (G, A) and define $f_i : G \to G$ by $f_i(x) = g_i\alpha_i$, with $x = g_1\alpha_1 + \cdots + g_n\alpha_n \in G$, $\alpha_1, \ldots, \alpha_n \in A$, for all $i \in \{1, \ldots, n\}$. For all $i \in \{1, \ldots, n\}$, f_i is well-defined, since x is uniquely written in terms of the basis $\{g_1, \ldots, g_n\}$ by Lemma 3.3.9. So for $\alpha \in A$, we have

$$f_i(x\alpha) = f_i(\sum_{j=1}^{n}(g_j\alpha_j)\alpha) = f_i(\sum_{j=1}^{n} g_j(\alpha_j\alpha)) = g_i(\alpha_i\alpha) = (g_i\alpha_i)\alpha = f_i(x)\alpha.$$

Hence $f_i \in M_A(G)$, for all $i \in \{1, \ldots, n\}$. Let $x = g_1\alpha_1 + \cdots + g_n\alpha_n$. We have

- for all $i \in \{1, \ldots, n\}$, $(f_i \circ f_i)(x) = f_i(g_i\alpha_i) = g_i\alpha_i = f_i(x)$. Hence f_i is idempotent.

- We have that for all $x \in G$,

  $$(f_1 + \cdots + f_n)(x) = f_1(x) + \cdots + f_n(x) = g_1\alpha_1 + \cdots + g_n\alpha_n = x.$$

  Hence $f_1 + \cdots + f_n = id$.

- Let $i \neq j$, we have that $(f_i \circ f_j)(x) = f_i(g_j\alpha_j) = 0$. So $f_i \circ f_j = 0$ if $i \neq j$.

- Let $h_1, h_2 \in M_A(G)$ such that $h_1(x) = g_1\beta_1 + \cdots g_n\beta_n, h_2(x) = g_1\beta_1' + \cdots + g_n\beta_n'$ and $i \in \{1, \ldots, n\}$. We have that

  $$\begin{aligned} f_i \circ (h_1 + h_2)(x) &= f_i(h_1(x) + h_2(x)) \\ &= g_i\beta_i + g_i\beta_i' \\ (f_i \circ h_1 + f_i \circ h_2)(x) &= f_i(h_1(x)) + f_i(h_2(x)) \\ &= g_i\beta_i + g_i\beta_i'. \end{aligned}$$

  Hence f_i is distributive for all $i \in \{1, \ldots, n\}$.

- For $i \in \{1 \ldots, n\}$, the rank of f_i is the cardinal of the set of nonzero orbits of A^* on f_iG, and the action is defined as follows

  $$\begin{aligned} &A^* \times f_iG \to f_iG \\ &(\alpha, f_i(x)) \mapsto \alpha \cdot f_i(x) := f_i(x\alpha). \end{aligned}$$

  For $x \in G$, we have $x = g_1\alpha_1 + \cdots + g_n\alpha_n$, for $\alpha_i \in A$ and $i \in \{1, \ldots, n\}$. Since $f_i(x) = g_i\alpha_i$ we have

  $$f_iG^* = \{g_i\alpha | \alpha \in A^*\}.$$

The orbit of $f_i(g_i)$ is given by

$$\{f_i(g_i)\alpha|\alpha \in A^*\} = \{g_i\alpha|\alpha \in A^*\} = f_iG^*.$$

Hence f_iG^* is an orbit of A on f_iG, and it is necessarily the only nonzero orbit. Hence f_i is of rank 1.

Therefore $M_A(G)$ is a CDI-near-ring which is 2-primitive on G. □

The materials above are sufficient to prove van der Walt's theorem (Theorem 4.1.43).
The following theorem characterizes finite dimensional near-vector spaces.

Theorem 4.1.43. *([13], Theorem 3.4) [van der Walt's theorem]*
Let $(G, +)$ be a group and let $A := D \cup \{0\}$, where D is a fixed point free group of automorphisms of $(G, +)$.

- *(G, A) is a finite dimensional near-vector space if and only if $M_A(G)$ is a CDI-near-ring.*

- *(G, A) is a finite dimensional near-vector space if and only if there exist a finite number of near-fields $F_1, \dots, F_m$, semigroup isomorphisms $\psi_i : (A, \circ) \to (F_i, \cdot)$, and an additive group isomorphism $\Phi : G \to F_1 \oplus \cdots \oplus F_m$ such that if $\Phi(g) = (x_1, \dots, x_m)$, then $\Phi(g\alpha) = (x_1\psi_1(\alpha), \dots, x_m\psi_m(\alpha))$ for all $g \in G$, $\alpha \in A$.*

Proof of van der Walt's theorem.
If $G = \{0\}$ there is nothing to show. Suppose $G \neq \{0\}$.

- Suppose that (G, A) is a finite dimensional near-vector space. Then by Theorem 4.1.42 $M_A(G)$ is a CDI-near-ring.

  To show the converse, we suppose that $M_A(G)$ is a CDI-near-ring. Let $R := M_A(G)$. By Theorem 4.1.21 we know that any dense subnear-ring of $M_A(G)$ is 2-primitive on G. In particular $R = M_A(G)$ is 2-primitive on G. We first prove that $A = End_R(G)$. Let $\alpha \in A$. Then for all $f \in M_A(G), g \in G$, $\alpha(f(g)) = f(\alpha(g))$. But $\alpha \in Aut(G, +)$, hence $\alpha \in End_{M_A(G)}(G) = End_R(G)$. Now let $\alpha \in End_R(G)$ and suppose that $\alpha \notin A$. Since

$$M_A(G) = \{h \in M(G)|\alpha(h(g)) = h(\alpha(g)), \forall \alpha \in A, g \in G\},$$

if $\alpha \notin A$ there is an $f \in M_A(G) = R$ or $g \in G$ such that $f(\alpha(g)) \neq \alpha(f(g))$. But this is contradiction since $\alpha \in End_R(G)$. Therefore $A = End_R(G)$. From Proposition 4.1.36, since R is a CDI-near-ring, there is a group H, such that H is R-isomorphic to G. By Corollary 4.1.38 $End_R(G)$ is isomorphic to $End_R(H)$ and by 4.1.39 $(H, End_R(H))$ is a near-vector space. Furthermore by Corollary 4.1.40 $(H, End_R(H))$ is a finite dimensional near-vector space. It follows that $(G, End_R(G))$ is isomorphic to $(H, End_R(H))$ as near-vector spaces. Hence $(G, End_R(G))$ is a finite dimensional near-vector space. But $End_R(G) = A$. Therefore (G, A) is a finite dimensional near-vector space.

- Suppose that there exist a finite number of near-fields $F_1, \ldots, F_m$, semi-group isomorphisms $\psi_i : (A, \circ) \to (F_i, \cdot), i \in \{1, \ldots, m\}$, and an additive group isomorphism $\Phi : G \to F_1 \oplus \cdots \oplus F_m$ such that if $\Phi(g) = (x_1, \ldots, x_m)$, then $\Phi(g\alpha) = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha))$ for all $g \in G, \alpha \in A$. We show that (G, A) is a finite dimensional near-vector space. We have that
  - $(G, +)$ is a group and A is a set of endomorphisms of $(G, +)$.
  - We have $0 \in A$ and $id \in A$. We show that $-id \in A$. The multiplicative group of a near-field has just one element of order 2, namely -1. So A also has just one element of order 2, say α_0. It follows that for all $i \in \{1, \ldots, m\}$, $\psi_i(\alpha_0) = -1$. We have for all $g \in G$

$$\begin{aligned}\Phi(g\alpha_0) &= (x_1\psi_1(\alpha_0), \ldots, x_m\psi_m(\alpha_0)) \\ &= (-x_1, \ldots, -x_m) \\ &= -\Phi(g) \\ &= \Phi(-g).\end{aligned}$$

Since $\Phi : (G, +) \to (F_1 \oplus \cdots \oplus F_m, +)$ is a group isomorphism, $\Phi(-g) = -\Phi(g)$. Hence

$$g\alpha_0 = \Phi^{-1}(\Phi(g\alpha_0)) = \Phi^{-1}(\Phi(-g)) = -g.$$

Therefore $\alpha_0 = -id$.

– $A \setminus \{0\} = D$ is a fixed point free group of automorphisms of $(G, +)$.
– We now show that there is a set $\{g_1, \ldots, g_m\} \in Q(G)$ that generates G. Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with $1 \in F_i$ and 1 in the i-th position. There is a unique $g_i \in G$ such that $\Phi(g_i) = e_i$, for all $i \in \{1, \ldots, m\}$. Let $\alpha, \beta \in A$. We have

$$\begin{aligned}\Phi(g_i\alpha + g_i\beta) &= \Phi(g_i\alpha) + \Phi(g_i\beta)\\ &= (0, \ldots, 0, \psi_i(\alpha), 0, \ldots, 0) + (0, \ldots, 0, \psi_i(\beta), 0, \ldots, 0)\\ &= (0, \ldots, 0, \psi_i(\alpha) + \psi_i(\beta), 0, \ldots, 0)\\ &= \Phi(g_i\psi_i^{-1}(\psi_i(\alpha) + \psi(\beta))).\end{aligned}$$

Since Φ is an isomorphism,

$$g_i\alpha + g_i\beta = g_i\psi_i^{-1}(\psi_i(\alpha) + \psi(\beta)),$$

and $\psi_i^{-1}(\psi_i(\alpha) + \psi(\beta)) \in A$. Hence $\{g_1, \ldots, g_m\} \subseteq Q(G)$. Let $g \in G$. Since G is isomorphic to $F_1 \oplus \cdots \oplus F_m$, there are unique $x_1 \in F_1, \ldots, x_m \in F_m$ such that $g = \Phi^{-1}(x_1, \ldots, x_m)$. Also for each of the x_i, there is a unique $\alpha_i \in A$ such that $\psi_i(\alpha_i) = x_i$. Hence $g = \Phi^{-1}(\psi_1(\alpha_1), \ldots, \psi_m(\alpha_m))$. It follows that

$$\begin{aligned}g &= \Phi^{-1}(\psi_1(\alpha_1), 0, \ldots, 0) + \cdots + \Phi^{-1}(0, \ldots, 0, \psi_m(\alpha_m))\\ &= g_1\alpha_1 + \cdots + g_m\alpha_m.\end{aligned}$$

Hence $\{g_1, \ldots, g_m\}$ generates G. Therefore (G, A) is a finite dimensional near-vector space.

Now assume that (G, A) is a finite dimensional near-vector space. Then by Theorem 4.1.42 $R := M_A(G)$ is a CDI-near-ring and 2-primitive on G. Let $\{e_1, \ldots, e_m\}$ be the set of idempotent elements. Then by Theorem 4.1.26 there are semigroup isomorphisms $\psi_i : A \to e_iRe_i$ and by Proposition 4.1.31 $(e_iRe_i, +, \cdot)$ is a near-field, for all $i \in \{1, \ldots, m\}$. So let $F_i = e_iRe_i$. By Proposition 4.1.36, there is a group isomorphism $\Phi : G \to F_1 \oplus \cdots \oplus F_m$ such that

$$\Phi(g) = (\phi_1(e_1g), \ldots, \phi_m(e_mg)) = (x_1, \ldots, x_m).$$

Finally by Corollary 4.1.38 we know that

$$\Phi(g\alpha) = \phi_1(e_1g)\psi_1(\alpha) + \cdots + \phi_m(e_mg)\psi_m(\alpha),$$

since $F_1 \oplus \cdots \oplus F_m$ is a direct sum we have

$$\Phi(g\alpha) = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)), \text{ for all } g \in G, \alpha \in A.$$

$\square$

The characterization of finite dimensional near-vector spaces is quite different from the one for vector spaces. In general we do not have one but a finite number of direct summands of near-fields, all having isomorphic multiplicative semigroup structures.

Chapter 5

Linear mappings of near-vector spaces

5.1 Linear mappings from a near-vector space $V = F^n$ to itself, where F is a near-field

The action of a field F on the vector space $V = F^n$, where $n > 1$, results in the creation of two well-known structures that depend very tightly on this action:

- There is the ring of linear transformations of V, also known as the ring of F-endomorphisms of the group V, which can be identified with the ring $\mathcal{M}_n(F)$ of $n \times n$ matrices over F.
- This ring is contained in the second structure, namely the nearring $M_F(V)$ of F-mappings of V into itself.

It turns out that $\mathcal{M}_n(F)$ is the smallest 2-primitive nearring on V which contains all the distributive elements of $M_F(V)$. In [13] van der Walt extended this result for V a near-vector space and F a near-field.

Definition 5.1.1. *([6], Definition* 4.1.1*) Let* (V, A) *be a near-vector space. A map* $g : V \to V$ *is called a homogeneous transformation of* V *if for each* $x \in V$ *and for each* $\alpha \in A$*,*

$$g(x\alpha) = (g(x))\alpha.$$

The set

$$M_A(V) := \{f : V \to V \mid f(x\alpha) = f(x)\alpha, \text{ for all } x \in V, \alpha \in A\}$$

of all homogeneous functions of V into itself is a nearring (See [6], Definition 4.1.1). It has the following subset

$$L_A(V) := \{f \in M_A(V) \mid f(v_1 + v_2) = f(v_1) + f(v_2) \text{ for all } v_1, v_2 \in V\},$$

i.e. the set of all linear mappings from V to itself. For vector spaces, these would be called the linear transformations of the vector space. In [6], Proposition 4.1.4, it is proved that $L_A(V)$ is a ring.

According to Theorem 4.1.43 we can specify a finite dimensional near-vector space by taking n near-fields $F_1, F_2, \ldots, F_n$ for which there are semigroup isomorphisms $\vartheta_{ij} : (F_j, \cdot) \to (F_i, \cdot)$ with $\vartheta_{ij}\vartheta_{jk} = \vartheta_{ik}$ for $1 \leq i, j, k \leq n$. We can then take $V := F_1 \oplus F_2 \oplus \cdots \oplus F_n$ as the additive group of the near-vector space and any one of the semigroups $(F_{i_0}, \cdot)$ as the semigroup of endomorphisms by defining

$$(x_1, x_2, \cdots, x_n)\alpha := x_1\vartheta_{1i_0}(\alpha) + x_2\vartheta_{2i_0}(\alpha) + \cdots + x_n\vartheta_{ni_0}(\alpha),$$

for all $x_j \in F_j$ and all $\alpha \in F_{i_0}$. We want to study the nearring $M_{F_{i_0}}(V)$ for a certain constructions.
In [13] van der Walt also defines

Definition 5.1.2. *([13]) The subnearring of $M_{F_{i_0}}(V)$ generated by the set of all square matrices, $C := (c_{ij})$, where $c_{ij} \in F_i$ with their action on V defined by*

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} c_{11}\vartheta_{11}(x_1) + \cdots + c_{1n}\vartheta_{1n}(x_n) \\ \vdots \\ c_{n1}\vartheta_{n1}(x_1) + \cdots + c_{nn}\vartheta_{nn}(x_n) \end{pmatrix}$$

is called the nearring of matrices determined by the near-fields $F_1, F_2, \ldots, F_n$ and the matrix of isomorphisms (ϑ_{ij}), and is denoted by $\mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$.

Note that the choice of i_0 does not figure in the definition of this nearring.

Corollary 5.1.3. *([13], Corollary 3.6) Suppose (V, A) is a finite near-vector space which is not a vector space. Then $M_A(V)$ is isomorphic to a nearring of matrices determined by a finite number of finite near-fields with isomorphic multiplicative semigroups.*

Thus in the finite case, if (V, A) is not a vector space, the elements of $M_A(V)$ are isomorphic to $\mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$, i.e. the homogeneous transformations are exactly the elements of $\mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$.

Throughout this section we look at constructions of the form $V = F \oplus \cdots \oplus F$ (n copies), where F is a near-field and the $\psi_i : (F, \cdot) \to (F, \cdot)$ multiplicative automorphisms for $i \in \{1, \ldots, n\}$. We put $A = F$ with the scalar multiplication defined for all $\alpha \in F$ and $(x_1, \ldots, x_n) \in V$ by

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

Then we have that $\mathcal{M}_n(\{F_i\}, (\vartheta_{ij})) = \mathcal{M}_n(F, (\vartheta_{ij}))$, with $\vartheta_{ij} = \psi_i\psi_j^{-1}$.
The set of all linear mappings $L_F(V)$ is a subset of $\mathcal{M}_n(F, (\vartheta_{ij}))$. We begin with an example:

Example 5.1.4. *([13], Example 3.7) Let $F_1 = F_2 := \mathbb{R}$, the field of real numbers, let ϑ_{11} be the identity function and let ϑ_{21} be defined by $\vartheta_{21}(x) := x^3$. Then $(F_1 \oplus F_2 = \mathbb{R}^2, \mathbb{R})$ is a near-vector space, with the action of the semigroup of endomorphisms given by $(x_1, x_2)\alpha = (x_1\alpha, x_2\alpha^3)$ for $\alpha \in \mathbb{R}$.*
Then the action of a matrix (c_{ij}) in $\mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$ on $F_1 \oplus F_2 = \mathbb{R}^2$ is given by

$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} := \begin{pmatrix} c_{11}x_1 + c_{12}x_2^{1/3} \\ c_{21}x_1^3 + c_{22}x_2 \end{pmatrix}.$$

Here

$$L_A(V) = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix}.$$

In the case where F is a field, we can characterize the elements of $L_F(V)$.

Theorem 5.1.5. *Let F be a field, $V = F^n$ and (V, F) be a near-vector space with the scalar multiplication defined by*

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

with $\alpha \in F$ and $(x_1, \ldots, x_n) \in V$, where $\psi_i : (F, \cdot) \to (F, \cdot)$ is a semigroup automorphism for all $i \in \{1, \ldots, n\}$. Then

$$L_F(V) = \{(c_{ij}) \in \mathcal{M}_n(F, (\vartheta_{ij})) | \text{ for all } i, j, c_{ij} = 0 \text{ or } \vartheta_{ij} \in Aut(F, +, \cdot)\}.$$

Proof. Let $(c_{ij}) \in L_F(V)$. Suppose that $c_{i_0j_0} \neq 0$ for some i_0, j_0. Then for all $(x_i), (y_i) \in V$, $(c_{ij})((x_i) + (y_i)) = (c_{ij})(x_i) + (c_{ij})(y_i)$. Let $(x_i) = (0, \ldots, x_{i_0}, \ldots, 0), (y_i) = (0, \ldots, y_{i_0}, \ldots, 0)$. We have

$$(c_{ij})((x_i) + (y_i)) = \begin{pmatrix} c_{1i_0}\vartheta_{1i_0}(x_{i_0} + y_{i_0}) \\ \vdots \\ c_{j_0i_0}\vartheta_{j_0i_0}(x_{i_0} + y_{i_0}) \\ \vdots \\ c_{ni_0}\vartheta_{ni_0}(x_{i_0} + y_{i_0}) \end{pmatrix},$$

and

$$(c_{ij})(x_i) + (c_{ij})(y_i) = \begin{pmatrix} c_{1i_0}\vartheta_{1i_0}(x_{i_0}) + c_{1i_0}\vartheta_{1i_0}(y_{i_0}) \\ \vdots \\ c_{j_0i_0}\vartheta_{j_0i_0}(x_{i_0}) + c_{j_0i_0}\vartheta_{j_0i_0}(y_{i_0}) \\ \vdots \\ c_{ni_0}\vartheta_{ni_0}(x_{i_0}) + c_{ni_0}\vartheta_{ni_0}(x_{i_0}) \end{pmatrix}.$$

Since $(c_{ij})((x_i)+(y_i)) = (c_{ij})(x_i)+(c_{ij})(y_i)$, $c_{j_0i_0}\vartheta_{j_0i_0}(x_{i_0}+y_{i_0}) = c_{j_0i_0}\vartheta_{j_0i_0}(x_{i_0}) + c_{j_0i_0}\vartheta_{j_0i_0}(y_{i_0})$. It follows that $\vartheta_{j_0i_0}(x_{i_0} + y_{i_0}) = \vartheta_{j_0i_0}(x_{i_0}) + \vartheta_{j_0i_0}(y_{i_0})$ for all $x_{i_0}, y_{i_0} \in F$. We know that the $\vartheta_{ji}{}'s$ are semigroup automorphisms of $(F, \cdot)$. Hence $\vartheta_{j_0i_0} \in Aut(F, +, \cdot)$. Therefore

$$L_F(V) \subseteq \{(c_{ij}) \in \mathcal{M}_n(F, (\vartheta_{ij}))| \text{ for all } i, j, c_{ij} = 0 \text{ or } \vartheta_{ij} \in Aut(F, +, \cdot)\}.$$

It is not difficult to check that

$$\{(c_{ij}) \in \mathcal{M}_n(F, (\vartheta_{ij}))| \text{ for all } i, j, c_{ij} = 0 \text{ or } \vartheta_{ij} \in Aut(F, +, \cdot)\} \subseteq L_F(V).$$

□

5.1.1 Linear mappings from a near-vector space $V = \mathbb{R}^n$ to itself

In this section we look at the construction where $V = F^n$ where $F = \mathbb{R}$, i.e. the near-vector space $(V, \mathbb{R})$ and prove some properties of $L_{\mathbb{R}}(V)$.
It is well known that

Lemma 5.1.6. *The only field automorphism of $\mathbb{R}$ is the identity.*

Theorem 5.1.7. *Let $(V, \mathbb{R})$ be a near-vector space where scalar multiplication is defined for all $\alpha \in \mathbb{R}$ and $(x_1, \ldots, x_n) \in \mathbb{R}^n$ by*

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

Then $\psi_i \neq \psi_j$ for all $i \neq j$ in $\{1, 2, \ldots, n\}$ if and only if

$$L_{\mathbb{R}}(V) = \begin{pmatrix} \mathbb{R} & 0 & 0 & \ldots & 0 \\ 0 & \mathbb{R} & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & 0 & \mathbb{R} & 0 \\ 0 & 0 & \ldots & 0 & \mathbb{R} \end{pmatrix}.$$

Proof. We have $\psi_i \neq \psi_j$ for all $i \neq j$ if and only if $\vartheta_{ij} \neq id_{\mathbb{R}}$ for all $i \neq j$, since $\vartheta_{ij} = \psi_i\psi_j^{-1}$. It follows from Lemma 5.1.6 that $\psi_i \neq \psi_j$ for all $i \neq j$ if and only if $\vartheta_{ij} \notin Aut(\mathbb{R}, +, \cdot)$ for all $i \neq j$. Therefore using Theorem 5.1.5, $(c_{ij}) \in L_{\mathbb{R}}(V)$ if and only if $c_{ij} = 0$ for all $i \neq j$. □

Theorem 5.1.8. *Let $(V, \mathbb{R})$ be a near-vector space where scalar multiplication is defined for all $\alpha \in \mathbb{R}$ and $(x_1, \ldots, x_n) \in \mathbb{R}^n$ by*

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

Then $\psi_i = \psi_j$ for all i, j in $\{1, 2, \ldots, n\}$ if and only if $L_{\mathbb{R}}(V) = \mathcal{M}_n(\mathbb{R})$.

Proof. Suppose that $\psi_i = \psi_j$ for all i, j in $\{1, 2, \ldots, n\}$. Then for all i, j $\vartheta_{ij} = id_{\mathbb{R}}$. Therefore $L_{\mathbb{R}}(V) = \mathcal{M}_n(\mathbb{R})$. We now assume that $L_{\mathbb{R}}(V) = \mathcal{M}_n(\mathbb{R})$. From Theorem 5.1.5, ϑ_{ij} is a field automorphism of $\mathbb{R}$ for all $i, j \in \{1, 2, \ldots, n\}$. Then from Lemma 5.1.6 $\vartheta_{ij} = id_{\mathbb{R}}$ for all $i, j \in \{1, 2, \ldots, n\}$. Since $\vartheta_{ij} = \psi_i\psi_j^{-1}$, we have $\psi_i = \psi_j$ for all i, j. □

Corollary 5.1.9. *Let $(V, \mathbb{R})$ be a near-vector space. Then V is regular if and only if $L_{\mathbb{R}}(V) = \mathcal{M}_n(\mathbb{R})$.*

Proof. By Theorem 3.3.32 V is regular if and only if it is isomorphic to a near-vector space $(V', \mathbb{R})$, with $(V, +) = (V', +)$ and the following scalar multiplication

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

with $\psi_1 = \ldots = \psi_n$. Hence V is regular if and only if $L_{\mathbb{R}}(V) = \mathcal{M}_n(\mathbb{R})$. □

Theorem 5.1.10. *Let $(V, \mathbb{R})$ be a near-vector space where scalar multiplication is defined for all $\alpha \in \mathbb{R}$ and $(x_1, \ldots, x_n) \in \mathbb{R}^n$ by*

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

and let $V = \bigoplus_{i=1}^{r} V_i$ be the canonical decomposition of V into maximal regular subspaces. Then $(V, \mathbb{R})$ is isomorphic to a near-vector space $(V', \mathbb{R})$ such that

$$L_{\mathbb{R}}(V') = \begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & 0 & A_{r-1} & 0 \\ 0 & 0 & \ldots & 0 & A_r \end{pmatrix},$$

where A_i is of the form

$$A_i = \begin{pmatrix} \mathbb{R} & \ldots & \mathbb{R} \\ \vdots & \ddots & \vdots \\ \mathbb{R} & \ldots & \mathbb{R} \end{pmatrix}.$$

Proof. Let us consider the following equivalence relation "$\sim$" on $\{\psi_1, \ldots, \psi_n\}$ defined for all i, j by $\psi_i \sim \psi_j$ if and only if $\psi_i = \psi_j$. Let $\Phi_1, \ldots, \Phi_r$ be the equivalence classes with $|\Phi_i| = n_i$. Put $V' = \mathbb{R}^n$ and consider the near-vector space $(V', \mathbb{R})$ with the scalar multiplication defined by $(x_1, \ldots, x_n)\alpha = (x_1\phi_1(\alpha), \ldots, x_n\phi_n(\alpha))$ such that $\phi_i \in \Phi_{k+1}$ for $n_1 + n_2 + \ldots + n_k + 1 \leq i \leq n_1 + n_2 + \ldots + n_k + n_{k+1}$, where $0 \leqslant k \leqslant r - 1$. Hence $(V, \mathbb{R})$ and $(V', \mathbb{R})$ are isomorphic, since they have the same dimension and $\{\psi_1, \ldots, \psi_n\} = \{\phi_1, \ldots, \phi_n\}$. We have

$$L_{\mathbb{R}}(V') = \begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & 0 & A_{r-1} & 0 \\ 0 & 0 & \ldots & 0 & A_r \end{pmatrix}$$

where A_i is of the form

$$A_i = \begin{pmatrix} \mathbb{R} & \ldots & \mathbb{R} \\ \vdots & \ddots & \vdots \\ \mathbb{R} & \ldots & \mathbb{R} \end{pmatrix}$$

since for any $n_1 + n_2 + \ldots + n_k + 1 \leq i, j \leq n_1 + n_2 + \ldots + n_k + n_{k+1}$, $\vartheta_{ij} = \phi_i \phi_j^{-1} = id$, for all $0 \leq k < r$ and

$$L_{\mathbb{R}}(V) = \{(c_{ij}) \in \mathcal{M}_n(\mathbb{R}, (\vartheta_{ij}))| \text{ for all } i, j, c_{ij} = 0 \text{ or } \vartheta_{ij} \in Aut(\mathbb{R}, +, \cdot)\}.$$

Indeed, for any $n_1 + n_2 + \ldots + n_k + 1 \leq i, j \leq n_1 + n_2 + \ldots + n_k + n_{k+1}$, $\phi_i = \phi_j$ $(\phi_i, \phi_j \in \Phi_{k+1})$ and $\vartheta_{ij} = \phi_i \phi_j^{-1} = id$, for all $0 \leq k < r$. □

Example 5.1.11. *Let us consider the near-vector space $V = \mathbb{R}^4$ with the scalar multiplication defined for $(x_1, x_2, x_3, x_4) \in V$ and $\alpha \in \mathbb{R}$ by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3).$$

The near-vector space $(V, \mathbb{R})$ is isomorphic to $(V', \mathbb{R})$ where $V' = \mathbb{R}^4$ with the scalar multiplication defined for $(x_1, x_2, x_3, x_4) \in V$ and $\alpha \in \mathbb{R}$ by $(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha, x_3\alpha^3, x_4\alpha^3)$. We have

$$L_{\mathbb{R}}(V') = \begin{pmatrix} \mathbb{R} & \mathbb{R} & 0 & 0 \\ \mathbb{R} & \mathbb{R} & 0 & 0 \\ 0 & 0 & \mathbb{R} & \mathbb{R} \\ 0 & 0 & \mathbb{R} & \mathbb{R} \end{pmatrix}.$$

In fact we have $\Phi_1 = \{\phi_1 = id, \phi_2 = id\}$ and $\Phi_2 = \{\phi_3, \phi_4\}$ with $\phi_3(x) = \phi_4(x) = x^3, \forall x \in \mathbb{R}$. Hence we have $\vartheta_{ij} = id$ for $1 \leqslant i, j \leqslant 2$ and $3 \leqslant i, j \leqslant 4$. But we have for example $\vartheta_{13} = \vartheta_{14} = \vartheta_{23} = \vartheta_{24} = \phi_3^{-1} \neq id$ and $\vartheta_{31} = \vartheta_{41} = \vartheta_{32} = \vartheta_{42} = \phi_3 \neq id$.

5.1.2 Linear mappings from a near-vector space $V = F^n$ to itself, where F is a finite field

Let $GF(p^m)$ denote the finite field of p^m elements, where m is a positive integer and p a prime. In this section we look at the near-vector space $(V, GF(p^m))$, where $V = (GF(p^m))^n$. We will write $GF(p^m)^*$ for $GF(p^m) \backslash \{0\}$ and $L_{GF(p^m)}(V)$ for $L_{GF(p^m)}((GF(p^m))^n)$.
We have that

Proposition 5.1.12. *([1]) Let ψ be an automorphism of the group $(GF(p^m)^*, \cdot)$. Then there exists $q \in \mathbb{Z}$ with $1 \leq q \leq p^m - 1$ and $gcd(p^m - 1, q) = 1$, such that $\psi(x) = x^q$ for all $x \in GF(p^m)^*$.*

Proposition 5.1.13. *The automorphisms of $(GF(p^m), \cdot)$ that are additive homomorphisms are the maps f defined by $f(x) = x^q$, with $gcd(p^m - 1, q) = 1$ and $q = p^l$ for some $l \in \{0, 1, \ldots, m-1\}$.*

Remark 5.1.14. *In fact, the field automorphisms of $GF(p^m)$ are exactly the polynomials $f(x) = x^{p^l}$, for $l = 0, 1, \ldots, m-1$. So we have exactly m field automorphisms of $GF(p^m)$ and the group $Aut(GF(p^m), +, \cdot)$ is cyclic and is generated by the Frobenius automorphism $f(x) = x^p$.*

Theorem 5.1.15. *Let $(V, GF(p^m))$ be a near-vector space with scalar multiplication defined for all $\alpha \in GF(p^m)$ and $(x_1, \ldots, x_n) \in V$ by*

$$(x_1, \ldots, x_n)\alpha = (x_1\alpha^{q_1}, \ldots, x_n\alpha^{q_n}),$$

where for $i \in \{1, \ldots, n\}$, $gcd(p^m - 1, q_i) = 1$ and $1 \leq q_i \leq p^m - 1$. Then $L_{GF(p^m)}(V) = \mathcal{M}_n(GF(p^m))$ if and only if for all $i, j \in \{1, \ldots, n\}$, $q_i = p^{l_{ij}} q_j$ for some $l_{ij} \in \{0, 1, \ldots, m-1\}$.

Proof. Suppose that $q_i = p^{l_{ij}} q_j$ for all $i, j \in \{1, \ldots, n\}$. Then for all i, j, $\vartheta_{ij}(x) = (\psi_i \psi_j^{-1})(x) = x^{\frac{q_i}{q_j}} = x^{p^{l_{ij}}}$ is a field automorphism. Therefore $L_{GF(p^m)}(V) = \mathcal{M}_n(GF(p^m))$. Now suppose that $L_{GF(p^m)}(V) = \mathcal{M}_n(GF(p^m))$. Then for all $i, j \in \{1, \ldots, n\}$ we have ϑ_{ij} is a field automorphism. So $\vartheta_{ij}(x) = x^{p^{l_{ij}}}$, but $\vartheta_{ij} = \psi_i \psi_j^{-1}$. It follows that $\vartheta_{ij}(x) = x^{\frac{q_i}{q_j}}$, for all $x \in GF(p^m)$. Hence $q_i = p^{l_{ij}} q_j$. ☐

Example 5.1.16. *We consider the finite field $F = GF(3^2)$ and the near-vector space $V = F^2$ with scalar multiplication defined for all $(x_1, x_2) \in V$ and $\alpha \in F$ by*

$$(x_1, x_2)\alpha = (x_1\alpha, x_2\alpha^3).$$

Then we have

$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} := \begin{pmatrix} c_{11}x_1 + c_{12}x_2^{1/3} \\ c_{21}x_1^3 + c_{22}x_2 \end{pmatrix}.$$

The maps $\vartheta_{21}, \vartheta_{12}$ from F to F defined by by $\vartheta_{21}(x) = x^3, \vartheta_{12}(x) = x^{\frac{1}{3}}$ are field automorphisms of F. So $L_F(V) = \begin{pmatrix} F & F \\ F & F \end{pmatrix}$.
In fact we have for $a, b \in F$, $(a+b)^3 = a^3 + b^3$ and $(ab)^3 = a^3b^3$. Also $(a+b)^{\frac{1}{3}} = a^{\frac{1}{3}} + b^{\frac{1}{3}}$ and $(ab)^{\frac{1}{3}} = a^{\frac{1}{3}}b^{\frac{1}{3}}$.

In the following lemma, since each ψ_i, $i \in \{1,\ldots,n\}$ is an automorphism of the group $(GF(p^m)^*,\cdot)$, by Proposition 5.1.12, for each one there exists $q_i \in \mathbb{Z}$ with $1 \leq q_i \leq p^m - 1$ and $gcd(p^m-1, q_i) = 1$ such that $\psi_i(x) = x^{q_i}$ for each $i \in \{1,\ldots,n\}$.

Lemma 5.1.17. *Let $(V, GF(p^m))$ be a near-vector space with scalar multiplication defined for $\alpha \in GF(p^m)$ and $(x_1,\ldots,x_n) \in V$ by*

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

The relation $\sim$ defined on $\Psi = \{\psi_1,\psi_2,\ldots,\psi_n\}$ by

$$\psi_i \sim \psi_j \text{ if and only if for all } \alpha \in GF(p^m)\backslash\{0\}, \psi_i(\alpha) = \psi_j(\alpha^{p^l}),$$

for some $l \in \{0,1,\ldots,m-1\}$, is an equivalence relation on Ψ.

Proof.

- It is not difficult to see that the relation $\sim$ is reflexive.
- Suppose that $\psi_i \sim \psi_j$ for some $i,j \in \{1,\ldots,n\}$. Then there is $l \in \{0,1,\ldots,m-1\}$ such that for all $\alpha \in GF(p^m)\backslash\{0\}$, $\alpha^{q_i} = \alpha^{p^l q_j} = (\alpha^{q_j})^{p^l}$. It follows that $\alpha^{q_j} = \alpha^{\frac{q_i}{p^l}}$. But we know that $\left(\alpha^{\frac{q_i}{p^l}}\right)^{p^m} = \alpha^{\frac{q_i}{p^l}}$, since for any $z \in GF(p^m)$ we have $z^{p^m} = z$. Hence $\alpha^{q_j} = \alpha^{p^{m-l}q_i}$. Therefore $\psi_j \sim \psi_i$, so the relation is symmetric.
- Suppose that $\psi_i \sim \psi_j$ and $\psi_j \sim \psi_k$ $i,j,k \in \{1,\ldots,n\}$. Then there are $l_1, l_2 \in \{0,1,\ldots,m-1\}$ such that $\alpha^{q_i} = \alpha^{q_j p^{l_1}}$ and $\alpha^{q_j} = \alpha^{q_k p^{l_2}}$ for all $\alpha \in GF(p^m)\backslash\{0\}$. So $\alpha^{q_i} = \alpha^{q_k p^{l_2} p^{l_1}} = \alpha^{q_k p^{l_1+l_2}}$. Hence the relation is transitive.

□

Theorem 5.1.18. *([9], Theorem 2.2) Let $F = GF(p^m)$, $q_1, q_2 \in \{1,2,\ldots,p^m-1\}$ with $gcd(q_i, p^m-1) = 1 (i = 1,2)$ and $q_1 < q_2$. Then $(a^{q_1} + b^{q_1})^{q_2} = (a^{q_2} + b^{q_2})^{q_1}$ for all $a, b \in F$ if and only if $q_1 \equiv q_2 p^l (\mod p^m - 1)$ for some $l \in \{0,1,\ldots,m-1\}$.*

Lemma 5.1.19. *Let $F = GF(p^m)$ and $V = F \oplus \cdots \oplus F$ be a near-vector space with the following scalar multiplication*

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

where ψ_i is an automorphism of $(F, \cdot)$, for all $i \in \{1, \ldots, n\}$. Then V is regular if and only if for all $\alpha \in GF(p^m)$, $\psi_i(\alpha) = \psi_j(\alpha^{p^l})$, for some $l \in \{0, 1, \ldots, m-1\}$.

Proof. Suppose that for all $\alpha \in GF(p^m)\backslash\{0\}$, $\psi_i(\alpha) = \psi_j(\alpha^{p^l})$, for some $l \in \{0, 1, \ldots, m-1\}$. Then $\psi_j(\psi_i^{-1}(\alpha)) = \psi_i(\psi_j^{-1}(\alpha)) = \alpha^{p^l}$, since for any $x \in F$ we have

$$\psi_i(\psi_j^{-1}(x)) = \psi_i(x^{\frac{1}{q_j}}) = x^{\frac{q_i}{q_j}} = \psi_j^{-1}(x^{q_i}) = \psi_j^{-1}(\psi_i(x)).$$

We show that there is a basis that consists of mutually pairwise compatible vectors. Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, 1 in the position i, for all $i \in \{1, \ldots, n\}$. Let $\alpha, \beta \in F$. We have

$$\begin{aligned}
(e_i + e_j)\alpha + (e_i + e_j)\beta &= (0, \ldots, \psi_i(\alpha) + \psi_i(\beta), 0, \ldots, \psi_j(\alpha) + \psi_j(\beta), \ldots, 0) \\
&= (0, \ldots, \psi_j(\alpha^{p^l}) + \psi_j(\beta^{p^l}), 0, \ldots, \psi_j(\alpha) + \psi_j(\beta), \ldots, 0) \\
&= (0, \ldots, \psi_j(\alpha)^{p^l} + \psi_j(\beta)^{p^l}, 0, \ldots, \psi_j(\alpha) + \psi_j(\beta), \ldots, 0) \\
&= (0, \ldots, (\psi_j(\alpha) + \psi_j(\beta))^{p^l}, 0, \ldots, \psi_j(\alpha) + \psi_j(\beta), \ldots, 0) \\
&= (0, \ldots, \psi_i(\psi_j^{-1}(\psi_j(\alpha) + \psi_j(\beta)), 0, \ldots, \psi_j(\alpha) + \psi_j(\beta), \ldots, 0) \\
&= (0, \ldots, 1, 0, \ldots, 1, \ldots, 0)\psi_j^{-1}(\psi_j(\alpha) + \psi_j(\beta)) \\
&= (e_i + e_j)\psi_j^{-1}(\psi_j(\alpha) + \psi_j(\beta))
\end{aligned}$$

Hence $\{e_1, \ldots, e_n\}$ is a basis of V that consists of mutually pairwise compatible vectors. Therefore V is regular.
Now suppose that V is regular and $\psi_i(x) = x^{q_i}, \forall x \in F$ and for $i \in \{1, \ldots, n\}$, with $gcd(q_i, p^m - 1) = 1$ and $1 \leqslant q_i < p^m$. Then we have $(x_1, \ldots, x_n)\alpha := (x_1\alpha^{q_1}, x_2\alpha^{q_2}, \ldots, x_n\alpha^{q_n})$. The set $\{e_1, \ldots, e_n\}$ is a basis of V and it consists of mutually pairwise compatible vectors. Then there is $a \in F^*$ such that $e_i + e_j a \in Q(V)$, for all $i, j \in \{1, \ldots, n\}$. Then for all $\alpha, \beta \in F$, there is $\gamma \in F$ such that $(e_i + e_j a)\alpha + (e_i + e_j a)\beta = (e_i + e_j a)\gamma$. We have

$$\begin{aligned}
(e_i + e_j a)\alpha + (e_i + e_j a)\beta &= (0, \ldots, \alpha^{q_i} + \beta^{q_i}, 0, \ldots, a^{q_j}(\alpha^{q_j} + \beta^{q_j}), \ldots, 0) \\
&= (0, \ldots, \gamma^{q_i}, 0 \ldots, a^{q_j}\gamma^{q_j}, \ldots, 0).
\end{aligned}$$

It follows that

$$\begin{cases} \alpha^{q_i} + \beta^{q_i} = \gamma^{q_i} \\ \alpha^{q_j} + \beta^{q_j} = \gamma^{q_j} \end{cases}$$

for all $i, j \in \{1, \ldots, n\}$. Hence

$$(\alpha^{q_i} + \beta^{q_i})^{q_j} = (\alpha^{q_j} + \beta^{q_j})^{q_i}.$$

By Theorem 5.1.18, $q_i \equiv q_j p^l (\mod p^m - 1)$ for some $l \in \{0, 1, \ldots, m-1\}$. Therefore for all $\alpha \in GF(p^m)$, $\psi_i(\alpha) = \psi_j(\alpha^{p^l})$, for some $l \in \{0, 1, \ldots, m-1\}$. $\square$

Theorem 5.1.20. *Let $(V, GF(p^m))$ be a near-vector space with scalar multiplication defined for $\alpha \in GF(p^m)$ and $(x_1, \ldots, x_n) \in V$ by*

$$(x_1, \ldots, x_n)\alpha = (x_1\alpha^{q_1}, \ldots, x_n\alpha^{q_n}).$$

Then there exists a near-vector space $(V', GF(p^m))$, with $V' = (GF(p^m))^n$, isomorphic to V such that there is $r \in \{1, \ldots, n\}$ such that

$$L_{GF(p^m)}(V') = \begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & 0 & A_{r-1} & 0 \\ 0 & 0 & \ldots & 0 & A_r \end{pmatrix},$$

where A_i is of the form

$$A_i = \begin{pmatrix} GF(p^m) & \ldots & GF(p^m) \\ \vdots & \ddots & \vdots \\ GF(p^m) & \ldots & GF(p^m) \end{pmatrix}.$$

Proof. Let $\Phi_1, \ldots, \Phi_r$ be the equivalence classes of $\{\psi_1, \ldots, \psi_n\}$ with respect to the equivalence relation $\sim$ defined in Lemma 5.1.17, with $|\Phi_i| = n_i$. Put $V' = (GF(p^m))^n$ and consider the near-vector space $(V', GF(p^m))$ with the scalar multiplication defined by $(x_1, \ldots, x_n)\alpha = (x_1\phi_1(\alpha), \ldots, \phi_n(\alpha))$ such that $\phi_i \in \Phi_{k+1}$ for $n_1 + n_2 + \ldots + n_k + 1 \leq i \leq n_1 + n_2 + \ldots + n_k + n_{k+1}$, where $0 \leqslant k \leqslant r-1$. Then $(V, GF(p^m))$ and $(V', GF(p^m))$ are isomorphic, since they have the same dimension and $\{\psi_1, \ldots, \psi_n\} = \{\phi_1, \ldots, \phi_n\}$. From Theorem 5.1.15 we have

$$L_{GF(p^m)}(V') = \begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & 0 & A_{r-1} & 0 \\ 0 & 0 & \ldots & 0 & A_r \end{pmatrix}$$

where A_i is of the form

$$A_i = \begin{pmatrix} GF(p^m) & \ldots & GF(p^m) \\ \vdots & \ddots & \vdots \\ GF(p^m) & \ldots & GF(p^m) \end{pmatrix}.$$

□

The proof of the next corollary is similar to that of Corollary 3.3.32.

Corollary 5.1.21. *Let $(V, GF(p^m))$ be a near-vector space with scalar multiplication defined for $\alpha \in GF(p^m)$ and $(x_1, \ldots, x_n) \in V$ by*

$$(x_1, \ldots, x_n)\alpha = (x_1\alpha^{q_1}, \ldots, x_n\alpha^{q_n}).$$

Then V is regular if and only if $L_{GF(p^m)}(V) = \mathcal{M}_n(GF(p^m))$.

Proof. The proof follows from Lemma 5.1.19 and Lemma 5.1.17. □

Now we study some properties of the ring $L_F(V)$.

Theorem 5.1.22. *Let F be a finite field or $\mathbb{R}$ and consider the near-vector space (V, F) where $V = F^n$ and scalar multiplication defined for all $\alpha \in F$ and $(x_1, \ldots, x_n) \in V$ by*

$$(x_1, \ldots, x_n)\alpha = (x_1\alpha^{q_1}, \ldots, x_n\alpha^{q_n}).$$

Then the ideals of $L_F(V)$ are of the form

$$I = \begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & 0 & A_{r-1} & 0 \\ 0 & 0 & \ldots & 0 & A_r \end{pmatrix}$$

where A_i is of the form

$$A_i = \begin{pmatrix} F & \dots & F \\ \vdots & \ddots & \vdots \\ F & \dots & F \end{pmatrix} \text{ or } A_i = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}.$$

Proof. We know from Theorems 5.1.10 and 5.1.20 that if I is an ideal of $L_F(V)$, then

$$I = \begin{pmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \dots & 0 & A_{r-1} & 0 \\ 0 & 0 & \dots & 0 & A_r \end{pmatrix}$$

where A_i is of the form

$$A_i = \begin{pmatrix} F & \dots & F \\ \vdots & \ddots & \vdots \\ F & \dots & F \end{pmatrix} \text{ or } A_i = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}.$$

□

Corollary 5.1.23. *Let F be a finite field or $\mathbb{R}$ and consider the near-vector space (V, F) where $V = F^n$ and scalar multiplication defined for all $\alpha \in F$ and $(x_1, \dots, x_n) \in V$ by*

$$(x_1, \dots, x_n)\alpha = (x_1\alpha^{q_1}, \dots, x_n\alpha^{q_n}).$$

The maximal ideals of $L_F(V)$ are

$$I = \begin{pmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \dots & 0 & A_{r-1} & 0 \\ 0 & 0 & \dots & 0 & A_r \end{pmatrix}$$

such that there is a unique j, $1 \leq j \leq r$, with

$$A_j = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \text{ and } A_i = \begin{pmatrix} F & \dots & F \\ \vdots & \ddots & \vdots \\ F & \dots & F \end{pmatrix} \text{ for } i \neq j.$$

Corollary 5.1.24. *Let F be a finite field or $\mathbb{R}$ and consider the near-vector space (V, F) where $V = F^n$ and scalar multiplication defined for all $\alpha \in F$ and $(x_1, \ldots, x_n) \in V$ by*

$$(x_1, \ldots, x_n)\alpha = (x_1\alpha^{q_1}, \ldots, x_n\alpha^{q_n}).$$

The ring $L_F(V)$ is a Noetherian ring.

Proof. Since $L_F(V)$ has a finite number of ideals and we know that each ideal is contained in a maximal ideal, every ascending chain of ideals is stationary. Therefore $L_F(V)$ is Noetherian. □

The following is a well known result in ring theory.

Lemma 5.1.25. *Suppose that there are (not necessarily distinct) maximal ideals $m_1, \ldots, m_t$ of R with $m_1 \cdots m_t = (0)$. Then A is Artinian if and only if A is Noetherian.*

We use it to show that

Proposition 5.1.26. *Let F be a finite field or $\mathbb{R}$ and consider the near-vector space (V, F) where $V = F^n$ and scalar multiplication defined for all $\alpha \in F$ and $(x_1, \ldots, x_n) \in V$ by*

$$(x_1, \ldots, x_n)\alpha = (x_1\alpha^{q_1}, \ldots, x_n\alpha^{q_n}).$$

The ring $L_F(V)$ is an Artinian ring.

Proof. We know from Corollary 5.1.23 what the maximal ideals of $L_F(V)$ are. Let $m_1, \ldots, m_r$ be the maximal ideals such that

$$m_j = \begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & 0 & A_{r-1} & 0 \\ 0 & 0 & \ldots & 0 & A_r \end{pmatrix},$$

with

$$A_j = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix} \text{ and } A_i = \begin{pmatrix} F & \ldots & F \\ \vdots & \ddots & \vdots \\ F & \ldots & F \end{pmatrix} \text{ for } i \neq j.$$

It is not difficult to show that $m_1 \cdots m_r = (0)$. Therefore from Lemma 5.1.25 $L_F(V)$ is Artinian. □

Proposition 5.1.27. *The set of units of $L_F(V)$, which corresponds to the set of all isomorphisms of V, is given by*

$$\begin{pmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \dots & 0 & A_{r-1} & 0 \\ 0 & 0 & \dots & 0 & A_r \end{pmatrix},$$

where the A_i's are invertible square matrices.

Proof. An element of $L_F(V)$ is invertible if and only if its matrix is invertible. So the set of units of $L_F(V)$ corresponds to the set of all invertible matrices in $L_F(V)$. But the set of of all invertible matrices is exactly the subset of $L_F(V)$ such that each A_i is invertible for $1 \leq i \leq r$. □

5.2 Linear mappings from one space to another

We begin with the following definition

Definition 5.2.1. *([7], Definition Definition 5.1) Let (V, F) and (W, F) be near-vector spaces over F. A function $T : V \to W$ is a linear mapping from V to W if*

$$T(v_1 + v_2) = T(v_1) + T(v_2), \text{ for all } v_1, v_2 \in V$$
$$T(v\alpha) = T(v)\alpha, \text{ for all } v \in V, \alpha \in F.$$

We will denote the set of all linear mappings from V to W by $(\mathcal{L}(V, W), F)$.

In [7], Lemma 5.4, it is shown that linear mappings preserve regular subspaces.

Lemma 5.2.2. *([7], Lemma 5.4) Let T be a linear mapping from (V, F) into (W, F). If V_j is a regular subspace of V, then $T(V_j)$ is a regular subspace of W.*

Since V_j is regular, by Theorem 3.3.31 $Q(V_j) = R_u F$ for all $u \in Q(V_j) \setminus \{0\}$. Moreover if there is a $u \in V_j$ such $Q(V_j) = R_u$ then:

Lemma 5.2.3. *Let T be a linear mapping from (V, F) into (W, F). If V_j is a regular subspace of V and there is $u \in V_j$ such that $Q(V_j) = R_u$, then $T(V_j)$ is a regular subspace of W and there is $w \in W$ such that $Q(T(V_j)) = R_w$.*

Proof. Suppose that V_j is a regular subspace of V, such that there is $u \in V_j$ and $Q(V_j) = R_u$. We know from Lemma 5.2.2 that $T(V_j)$ is regular. Let $w \in Q(T(V_j)) \setminus \{0\}$ and $\alpha, \beta \in F$. So there is $v \in Q(V_j) \setminus \{0\}$ such that $w = T(v)$. Since $T(V_j)$ is regular, $w\alpha + w\beta = w(\alpha +_w \beta)$. It follows that $T(v\alpha + v\beta) = T(v(\alpha +_w \beta))$. Also since $Q(V_j) = R_u$, $T(v\alpha + v\beta) = T(v(\alpha +_u \beta))$. Hence $w(\alpha +_w \beta) = w(\alpha +_u \beta)$. Since $w \neq 0$ and F acts fixed point free on W, $(\alpha +_w \beta) = \alpha +_u \beta$. For all $w' \in Q(T(V_j)) \setminus \{0\}$ we have $+_{w'} = +_u = +_w$. Therefore for all $w' \in Q(T(V_j)) \setminus \{0\}$ we have $w' \in R_w \setminus \{0\}$. Thus $Q(T(V_j)) \setminus \{0\} \subseteq R_w \setminus \{0\}$. By Theorem **??** it is clear that $R_w \setminus \{0\} \subseteq Q(T(V_j)) \setminus \{0\}$. Therefore $Q(T(V_j)) = R_w$. □

If we define addition on $\mathcal{L}(V, W)$ as $(T_1 + T_2)(v) = T_1(v) + T_2(v)$ for all $v \in V$ and $T_1, T_2 \in \mathcal{L}(V, W)$ and the scalar multiplication as $(T\alpha)(v) = T(v\alpha)$ for all $T \in \mathcal{L}(V, W)$ and $\alpha \in F$ then it is not difficult to verify that

Proposition 5.2.4. *Let (V, F) and (W, F) be near-vector spaces, with $Q(V) \neq \{0\}, Q(W) \neq \{0\}$. Then $(\mathcal{L}(V, W), F)$ is an F-group.*

Proof.

- We have $(\mathcal{L}(V, W), +)$ is a group and F is a set of endomorphism of V.
- F contains $0, 1, -1$, since for all $v \in V$, $T(-v) = -T(v)$.
- $A \setminus \{0\}$ is a subgroup of $Aut(\mathcal{L}(V, W))$. Let $\alpha \in F \setminus \{0\}$ and suppose for all $v \in V$, $(T\alpha)(v) = T(v\alpha) = 0$. Then $T = 0$, so α is injective. Also α is surjective, since for all $U \in \mathcal{L}(V, W)$ we have

  $$\begin{aligned} T : V &\to W \\ v &\mapsto U(v)\alpha^{-1} \end{aligned}$$

  is an element of $\mathcal{L}(V, W)$ and $T\alpha = U$.
- Let $\alpha, \beta \in F$, $T \in \mathcal{L}(V, W) \setminus \{0\}$ such that $(T\alpha)(v) = (T\beta)(v)$ for all $v \in V$. Then there is $v_1 \in V$ such that $T(v_1) \neq 0$. Since F acts fixed point free on W and $T(v_1) \neq 0$, $T(v_1)\alpha = T(v_1)\beta$ implies that $\alpha = \beta$. Therefore F acts fixed point free on $\mathcal{L}(V, W)$.

□

Proposition 5.2.5. *Let (V, F) and (W, F) be near-vector spaces over F. If $Q(V) = V \neq \{0\}$ or $Q(W) = W \neq \{0\}$, then $(\mathcal{L}(V, W), F)$ is a near-vector space.*

Proof. By Proposition 5.2.4 we have that $(\mathcal{L}(V, W), F)$ is an F-group. In either case $Q(\mathcal{L}(V, W)) = \mathcal{L}(V, W)$. In fact we have for all $T \in \mathcal{L}(V, W)$, $\alpha, \beta \in F$ and $v \in V \setminus \{0\}$, $(T\alpha + T\beta)(v) = T(v\alpha + v\beta) = T(v(\alpha +_v \beta)) = T(\alpha +_v \beta)(v)$. Therefore $T\alpha + T\beta = T(\alpha +_v \beta)$. Therefore $T \in Q(\mathcal{L}(V, W))$. Therefore $(\mathcal{L}(V, W), F)$ is a near-vector space. $\square$

Lemma 5.2.6. *Let (V, F) and (W, F) be near-vector spaces, with $Q(V) \neq \{0\}$, $Q(W) \neq \{0\}$, such that $(\mathcal{L}(V, W), F)$ is a near-vector space. Then for all $u \in Q(V) \setminus \{0\}$, there is $T \in Q(\mathcal{L}(V, W))$ such that $T(u) \neq 0$.*

Proof. Suppose that there is $u \in Q(V) \setminus \{0\}$ such that for all $T \in Q(\mathcal{L}(V, W))$, $T(u) = 0$. Since $Q(\mathcal{L}(V, W))$ generates $\mathcal{L}(V, W)$, for all $T \in \mathcal{L}(V, W)$ we have $T(u) = 0$, which is not true. In fact let $(e_i)_{i \in I}$, with I an indexed set, be a basis of V. Then $u = \sum_{i \in I} e_i \alpha_i$, $\alpha_i \in F$ for all $i \in I$. Since $u \neq 0$, there is $i_0 \in I$ such that $\alpha_{i_0} \neq 0$. Hence we define the following linear map T such that $T(e_{i_0}) \neq 0$ and $T(e_i) = 0$ for all $i \in I \setminus \{i_0\}$. Therefore $T(u) = T(e_{i_0})\alpha_{i_0} \neq 0$. $\square$

Lemma 5.2.7. *Let (V, F) be a near-vector space such that $Q(V) \neq \{0\}$. The relation " $\sim$ " defined on $Q(V) \setminus \{0\}$ by $u \sim v$ if and only if $v \in R_u \setminus \{0\}$ is an equivalence relation.*

Proof.
We have $v \in R_u \setminus \{0\}$ if and only if $+_u = +_v$, which gives that " $\sim$ " is an equivalence relation. $\square$

Theorem 5.2.8. *Let (V, F) and (W, F) be near-vector spaces, with $Q(V) \neq \{0\}$, $Q(W) \neq \{0\}$, such that $(\mathcal{L}(V, W), F)$ is a near-vector space. Then for all $u \in Q(V) \setminus \{0\}$ we have $+_u = +_{u\lambda}$, for all $\lambda \in F \setminus \{0\}$.*

Proof. From Lemma 5.2.6 we have that for all $u \in Q(V) \setminus \{0\}$ there is $T \in Q(\mathcal{L}(V, W))$ such that $T(u) \neq 0$. Since $T \in Q(\mathcal{L}(V, W))$, for all $\alpha, \beta \in F$ there is $\gamma \in F$ such that $T\alpha + T\beta = T\gamma$. Then $T(u\alpha + u\beta) = T(u\gamma)$. But since $u \in Q(V)$, $u\alpha + u\beta = u(\alpha +_u \beta)$. It follows that $T(u\alpha + u\beta) = T(u(\alpha +_u \beta))$. Since F acts fixed point free on W and $T(u) \neq 0$, $\gamma = \alpha +_u \beta$. Also since $u\lambda \in Q(V)$, for $\lambda \in F \setminus \{0\}$, we have $u\lambda\alpha + u\lambda\beta = u\lambda(\alpha +_{u\lambda} \beta)$. Then

$T(u\lambda\alpha + u\lambda\beta) = T(u\lambda(\alpha +_{u\lambda} \beta))$ and $T(u\lambda\alpha + u\lambda\beta) = T(u\lambda\gamma)$. Hence $\alpha +_{u\lambda} \beta = \gamma = \alpha +_u \beta$, for all $\alpha, \beta \in F$. Therefore $+_u = +_{u\lambda}$. □

We know by Theorem 3.3.27 and Theorem 3.3.28 that every near-vector space can be uniquely decomposed into maximal regular subspaces, called the canonical decomposition of the near-vector space. In the remaining results we write $V = \bigoplus_{i \in J} V_j$ to refer to the canonical decomposition of V.

Corollary 5.2.9. *Let (V, F) and (W, F) be near-vector spaces, with $Q(V) \neq \{0\}, Q(W) \neq \{0\}$, such that $V = \bigoplus_{i \in J} V_j$. If $(\mathcal{L}(V, W), F)$ is a near-vector space, then for all $j \in J$, $Q(V_j) = R_{u_j}$, for all $u_j \in Q(V_j) \setminus \{0\}$.*

Proof. We know from Lemma 5.2.7 that if $v \in R_u \setminus \{0\}$, then $R_u = R_v$. Also from Theorem 5.2.8 we have that for all $\lambda \in F \setminus \{0\}$ and for all $u \in Q(V) \neq \{0\}$, $u\lambda \in R_u$. Let $u \in Q(V) \setminus \{0\}$. Then for all $v \in R_u \setminus \{0\}$ and $\lambda \in F \setminus \{0\}$, we have $v\lambda \in R_v = R_u$. Hence $R_u F \setminus \{0\} \subseteq R_u \setminus \{0\}$. It is clear that $R_u \setminus \{0\} \subseteq R_u F \setminus \{0\}$. Therefore $R_u \setminus \{0\} = R_u F \setminus \{0\}$. Now from Lemma **??** we know that for all $j \in J$, $Q(V_j) = R_{u_j} F$ for all nonzero $u_j \in Q(V_j)$, since the V_j are maximal regular subspaces of V. Thus $Q(V_j) \setminus \{0\} = R_{u_j} \setminus \{0\}$ and $Q(V_j) = R_{u_j}$. □

Lemma 5.2.10. *Let (V, F) and (W, F) be near-vector spaces, with $Q(V) \neq \{0\}, Q(W) \neq \{0\}$, such that $V = \bigoplus_{i \in J} V_j$. Suppose that for all $j \in J$ and $u_j \in Q(V_j) \setminus \{0\}$, $Q(V_j) = R_{u_j}$. Then for any $j \in J$, a linear map T, such that $T = 0$ on $V \setminus V_j$, is an element of the quasi kernel $Q(\mathcal{L}(V, W))$.*

Proof. Let $j \in J$ and $T \in \mathcal{L}(V, W)$ such that $T = 0$ on $V \setminus V_j$. Let $\alpha, \beta \in F$. For all $v \in V_j$, we have $v = \sum v_i$, for $v_i \in Q(V_j) = R_{u_j}$, since $Q(V_j)$ generates V_j additively. So

$$\begin{aligned}
(T\alpha + T\beta)(v) &= T(v\alpha + v\beta) \\
&= T(\sum(v_i\alpha + v_i\beta)) \\
&= \sum T(v_i\alpha + v_i\beta) \\
&= \sum T(v_i(\alpha +_{u_j} \beta)) \\
&= T(\sum v_i(\alpha +_{u_j} \beta)) \\
&= T(\alpha +_{u_j} \beta)(v)
\end{aligned}$$

for all $v \in V_j$ and $T = 0$ on $V \setminus V_j$. Hence for any $\alpha, \beta \in F$, there is $\gamma = \alpha +_{u_j} \beta \in F$ such that $T\alpha + T\beta = T\gamma$. Thus $T \in Q(\mathcal{L}(V, W))$. $\square$

We can now give a necessary and sufficient condition for when $(\mathcal{L}(V, W), F)$ is a near-vector space.

Theorem 5.2.11. *Let (V, F) and (W, F) be near-vector spaces, with $Q(V) \neq \{0\}, Q(W) \neq \{0\}$, such that $V = \bigoplus_{i \in J} V_j$. $(\mathcal{L}(V, W), F)$ is a near-vector space if and only if for all $j \in J$, $Q(V_j) = R_{u_j}$, for all $u_j \in Q(V_j) \setminus \{0\}$.*

Proof. We suppose that for all $j \in J$, $Q(V_j) = R_{u_j}$, for all $u_j \in Q(V_j) \setminus \{0\}$. Let $T \in \mathcal{L}(V, W)$ and T_j be a linear map such that $T_j = T$ on V_j and $T_j = 0$ on $V \setminus V_j$. From Lemma 5.2.10 $T_j \in Q(\mathcal{L}(V, W)$ for all $j \in J$. We now show that $T = \sum_{j \in J} T_j$. For any $x \in V$, there exists a unique $x_j \in V_j$ such that $x = \sum_{j \in J} x_j$. Then

$$T(x) = T(\sum_{j \in J} x_j) = \sum_{j \in J} T(x_j) = \sum_{j \in J} T_j(x_j) = \sum_{j \in J} T_j(x).$$

Hence $T = \sum_{j \in J} T_j$. Therefore $Q(\mathcal{L}(V, W)$ generates $\mathcal{L}(V, W)$. From Proposition 5.2.4 we know that $(\mathcal{L}(V, W), F)$ is an F-group. Thus $\mathcal{L}(V, W)$ is a near-vector space.
The converse follows from Corollary 5.2.9. $\square$

Theorem 5.2.12. *Let (V, F) and (W, F) be near-vector spaces, with $Q(V) \neq \{0\}, Q(W) \neq \{0\}$, such that $V = \bigoplus_{J \in J} V_j$. Suppose that $(\mathcal{L}(V, W), F)$ is a near-vector space. Then*

$$Q(\mathcal{L}(V, W)) = \{T \in \mathcal{L}(V, W) | \exists j \in J, T = 0 \text{ on } V \setminus V_j\}.$$

Proof. From Lemma 5.2.10 we have $Q(\mathcal{L}(V, W)) \supseteq \{T \in \mathcal{L}(V, W) | \exists j \in J, T = 0 \text{ on } V \setminus V_j\}$. Let $T \in Q(\mathcal{L}(V, W)) \setminus \{0\}$. Then for all $\alpha, \beta \in F$, there is $\gamma \in F$ such that $T\alpha + T\beta = T\gamma$. Since $T \neq 0$, there is $v \in Q(V) \setminus \{0\}$ such that $T(v) \neq 0$. There is a unique V_j such that $v \in V_j$ by the Decomposition Theorem. We now show that if $u \notin R_v$, then $T(u) = 0$. Suppose that $u \notin R_v$. Then there are $\alpha, \beta \in F$ such that $\alpha +_u \beta \neq \alpha +_v \beta$. But we also have $T(u\alpha + u\beta) = T(u(\alpha +_v \beta))$ and $T(u\alpha + u\beta) = T(u(\alpha +_u \beta))$. Then $T(u)(\alpha +_u \beta) = T(u)(\alpha +_v \beta)$. Since F acts fixed point free on $\mathcal{L}(V, W)$ and $\alpha +_u \beta \neq \alpha +_v \beta$, $T(u) = 0$. But by Theorem 5.2.11 we know that for all $j \in J$, $Q(V_j) = R_{u_j}$, for all $u_j \in Q(V_j) \setminus \{0\}$. Hence $T = 0$ on $V \setminus V_j$. Therefore $Q(\mathcal{L}(V,W)) \subseteq \{T \in \mathcal{L}(V,W) | \exists j \in J, T = 0 \text{ on } V \setminus V_j\}$. Thus

$$Q(\mathcal{L}(V,W)) = \{T \in \mathcal{L}(V,W) | \exists j \in J, T = 0 \text{ on } V \setminus V_j\}.$$

□

Corollary 5.2.13. *Let (V,F) and (W,F) be near-vector spaces, with $Q(V) \neq \{0\}, Q(W) \neq \{0\}$, such that $(\mathcal{L}(V,W),F)$ is a near-vector space. If V is regular, $\mathcal{L}(V,W) = Q(\mathcal{L}(V,W))$.*

Proof. From Theorem 5.2.12, we know that $Q(\mathcal{L}(V,W)) = \{T \in \mathcal{L}(V,W) | \exists j \in J, T = 0 \text{ on } V \setminus V_j\}$, where V_j is a maximal regular subspace of V, for $j \in J$. Since V is regular, it is the only maximal regular subspace, so we have that $Q(\mathcal{L}(V,W)) = \mathcal{L}(V,W)$. □

Example 5.2.14.

- *Let F be a near-field which is not a field and $V = F \oplus F$ a near-vector space with the scalar multiplication $(x,y)\alpha = (x\alpha, y\alpha)$. Since F is a not a field, we have $F_d \subsetneq F$, where F_d denotes the distributive elements of the near-field. We know that $Q(V) = \{(d_1,d_2)F | d_1,d_2 \in F_d\}$. Let $a \in F \setminus F_d$. We show that $(1,1)a \notin R_{(1,1)}$. Suppose that $(1,1)a \in R_{(1,1)}$. Then for all $\alpha, \beta \in F$, we have $(a,a)\alpha + (a,a)\beta = (a,a)(\alpha +_{(1,1)} \beta)$. But $\alpha +_{(1,1)} \beta = \alpha + \beta$. So $a\alpha + a\beta = a(\alpha + \beta)$, hence $a \in F_d$, giving a contradiction. Therefore $(1,1)a \notin R_{(1,1)}$. It is follows that $\mathcal{L}(V,V)$ is not a near-vector space over F.*

- *Let $F = \mathbb{R}$ and $V = F \oplus F$ the near-vector space with the scalar multiplication $(x,y)\alpha = (x\alpha^3, y\alpha^3)$. Let $T \in \mathcal{L}(V,W)$, with W a near-vector space over F. Then since $Q(V) = V$ by Proposition 5.2.5, $\mathcal{L}(V,W)$ is a near-vector space. Moreover, for all $\alpha, \beta \in F$, we have $T\alpha + T\beta = T(\alpha^3 + \beta^3)^{\frac{1}{3}}$. Thus $Q(\mathcal{L}(V,W)) = \mathcal{L}(V,W)$.*

Theorem 5.2.15 (Decomposition Theorem)**.** *Let (V,F) and (W,F) be near-vector spaces, with $Q(V) \neq \{0\}, Q(W) \neq \{0\}$, such that $V = \bigoplus_{i \in J} V_j$. Suppose that $(\mathcal{L}(V,W),F)$ is a near-vector space. Then*

$$\mathcal{L}(V,W) = \bigoplus_{i \in J} \mathcal{L}(V_j,W),$$

where $\mathcal{L}(V_j, W) = \{T \in \mathcal{L}(V, W) | T = 0 \text{ on } V \setminus V_j\}$*. Furthermore* $\mathcal{L}(V_j, W)$ *is a maximal regular subspace of* $\mathcal{L}(V, W)$ *and we have* $Q(\mathcal{L}(V_j, W)) = \mathcal{L}(V_j, W)$*, for all* $j \in J$*.*

Proof. From Theorem 5.2.12 we know that $Q(\mathcal{L}(V, W)) = \{T \in \mathcal{L}(V, W) | \exists j \in J, T = 0 \text{ on } V \setminus V_j\}$. So $Q = \bigcup_{j \in J} Q_j$, with $Q_j = \{T \in \mathcal{L}(V, W) | T = 0 \text{ on } V \setminus V_j\}$. It follows that T_1 and T_2 are compatible if and only if T_1 and T_2 are from the same Q_j. In fact let $T_1 \in Q_i$ and $T_2 \in Q_j$, with $i \neq j$. Then for all $a \in F \backslash \{0\}$, suppose that $T_1 + T_2 a \in Q(\mathcal{L}(V, W))$. So for all $\alpha, \beta \in F$ there is $\gamma \in F$ such that $(T_1 + T_2 a)\alpha + (T_1 + T_2 a)\beta = (T_1 + T_2 a)\gamma$. For $v \in Q(V_i) \setminus \{0\}$ we have $T_2(v) = 0$. So $\gamma = \alpha +_v \beta$. For $u \in Q(V_j) \setminus \{0\}$, $T_1(u) = 0$. So $\gamma = \alpha +_u \beta$. But V_j are V_i are maximal regular subspaces of V and we cannot have $+_u = +_v$ with $u \in V_j, v \in V_i$. Hence $Q_j, j \in J$ are the equivalence classes of the compatibility relation and since V_j is regular for all $j \in J$, by Corollary 5.2.13 we have $Q(\mathcal{L}(V_j, W)) = \mathcal{L}(V_j, W)$, for all $j \in J$. Therefore

$$\mathcal{L}(V, W) = \bigoplus_{i \in J} \mathcal{L}(V_j, W).$$

$\square$

List of References

[1] R. B. Allenby. *Rings, fields and groups: An introduction to abstract algebra*. Hodder Education, 1983.

[2] J. André. Lineare algebra über fastkörpern. *Mathematische Zeitschrift*, 136(4):295–313, 1974.

[3] J. Beidleman. *On near-rings and near-ring modules*. PhD thesis, Pennsylvania State University, 1964.

[4] T. Boykett. Distribution and generalized center in planar nearrings. *arXiv preprint arXiv:1607.01204*, 2016.

[5] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, 4(2):123–134, 1991.

[6] K.-T. Howell. *Contributions to the Theory of Near Vector Spaces*. PhD thesis, University of the Free State, 2008.

[7] K.-T. Howell. On subspaces and mappings of near-vector spaces. *Communications in Algebra*, 43(6):2524–2540, 2015.

[8] K.-T. Howell and J. Meyer. Finite-dimensional near-vector spaces over fields of prime order. *Communications in Algebra*, 38(1):86–93, 2009.

[9] K.-T. Howell and J. Meyer. Near-vector spaces determined by finite fields. *Journal of Algebra*, 398:55–62, 2014.

[10] K.-T. Howell and S. Sanon. Linear mappings of near-vector spaces. *Quaestiones Mathematicae, accepted, to appear*, 2017.

[11] J. Meldrum. Near-rings and their links with groups, pitman publishing company. *Co.(Research Notes Ser. 134), London*, 1985.

[12] G. Pilz. *Near-rings: the theory and its applications*. New York, 1977.

[13] 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.