Contributions to the Theory of Near Vector Spaces

Karin Therese Howell

Acknowledgement

First and foremost, I would like to extend my sincere thanks to my supervisor, Professor J.H. Meyer for his support and dedication throughout this process.

I have been extremely blessed throughout my academic career. My love for the subject was fueled by superb lecturers who were always available to answer questions. For this reason I am very indebted to the staff of the UFS Mathematics and Applied Mathematics Department. In particular, I would like to extend my sincere thanks to Dr H.W. Bargenda for his commitment and support throughout my postgraduate studies.

No one can set out to realise a dream without a very strong support network. I have an incredible family. Without them, I would not have been able to see this journey through. Thank you.

Financial assistance from the NRF is gratefully acknowledged.

Finally, my thanks to the management and staff of the National Institute for Higher Education (Northern Cape) for their support.

This thesis has been a labour of love and the realisation of a lifelong dream for me.

I am blessed.

K-T Howell

For my Dad

Preface

The main purpose of this thesis is to give an exposition of and expand the theory of near vector spaces, as first introduced by André [1].

The notion of a vector space is well known. For this reason the material in this thesis is presented in such a way that the parallels between near vector spaces and vector spaces are apparent.

In Chapter 1 several elementary definitions and properties are given. In addition, some important examples that will be referred to throughout this paper are cited.

In Chapter 2 the theory of near vector spaces is presented. We start off with some preliminary results in 2.1 and build up to the definition of a regular near vector space in 2.5. In addition, we show how a near vector space can be decomposed into maximal regular subspaces. We conclude this chapter by showing when a near vector space will in fact be a vector space. We follow the format of De Bruyn's thesis; however, both De Bruyn and André make use of left nearfields to define the near vector spaces. In light of the material we want to present in Chapter 4, it is more standard to use the notation as in the papers by van der Walt, [12], [13]. Thus we develop the material using right nearfields with scalar multiplication on the right of vectors.

The third chapter contains some examples of near vector spaces and serves as an illustration of much of the work of Chapter 2. Examples 1, 2 and 3 were used in De Bruyn's thesis. However, on closer inspection, it was revealed that in Example 2, the element $(a, 0, 0, d)$ is omitted as an element of $Q(V)$. This error is corrected. And in keeping with our use of right nearfields, the necessary changes are made to Example 1 and 3. In particular, the definition of $\circ$ in Example 3 is adapted and the necessary adjustments are made. We conclude this chapter by developing a theory that allows us to characterise all finite dimensional near vector spaces over $\mathbb{Z}_p$, for p a prime.

In Chapter 4 we turn our attention to the work done by van der Walt in [12] and [13]. In

Section 4.1 we consider the effects that 'perturbations' in the action of a (right) nearfield F has on the well known structures, the ring of linear transformations of V and the near-ring of homogeneous functions of V into itself. This first section sets the scene for the more generalised situation described in 4.2 and leads to the introduction of the nearring of matrices determined by n multiplicatively isomorphic nearfields and a matrix of isomorphisms. We conclude this chapter by summarising some properties of this nearring in 4.3 and 4.4.

Note that throughout this paper, $\subset$ will be used to convey a proper subset, whereas $\subseteq$ will convey the possibility of equality.

K-T Howell

September 2007

Contents

1 Basic Definitions and Examples **6**

1.1 Nearrings 6

1.2 Nearring Modules 11

1.3 Rings 13

2 The Theory of Near Vector Spaces **16**

2.1 Some Preliminary Results 16

2.2 F-groups 21

2.3 Quasi-kernels 22

2.4 A Dependence Relation between $Q(V)$ and $2^{Q(V)}$ 30

2.5 Near Vector Spaces 33

2.6 The Structure of Regular Near Vector Spaces 49

3 Examples of Near Vector Spaces **54**

3.1 Some examples 54

3.2 Finite dimensional near vector spaces over $\mathbb{Z}_p$ 76

4 Homogeneous and Near Linear Transformations **85**

4.1 Homogeneous Transformations 85

4.2 The Nearring of Near Linear Transformations 101

4.3 Some Left Ideals of S 106

4.4 The Kernel and Image of Elements of S 108

Bibliography **109**

Chapter 1

Basic Definitions and Examples

1.1 Nearrings

We begin by defining some elementary structures. These are standard definitions. They can be found in most elementary algebra books, for example, [7], [8] and [10]. The more complicated structures are then defined in terms of these elementary ones.

DEFINITION 1:

A *semigroup* is a pair $(S, \diamond)$, where S is a nonempty set and $\diamond$ is a binary operation on S, that satisfies the associative law:

$$r \diamond (s \diamond t) = (r \diamond s) \diamond t \text{ for all } r, s, t \in S.$$

■

Different symbols are used to denote binary operations as, for example, in:

DEFINITION 2:

A *group* is a pair $(G, +)$ which satisfies:

i) $(G, +)$ is a semigroup;

ii) there is an *identity* element $0 \in G$ so that for each $x \in G$

$$0 + x = x + 0 = x;$$

iii) for each $x \in G$ there is an *inverse* element $-x \in G$ so that

$$x + (-x) = (-x) + x = 0.$$

■

These definitions also illustrate the format of this thesis. Definitions, examples, propositions and theorems are numbered sequentially in each chapter. Thus the definition of a semigroup will be referred to as Definition 1 in this chapter and Definition 1.1-1 in subsequent chapters. Some definitions and theorems are followed by Notes. In such a case the note has the same number as the definition or theorem to which it refers. Also,

■ indicates the end of a definition, example, proposition or theorem.

To return to semigroups, a semigroup $(S, \diamond)$ is called *abelian* or *commutative* if it satisfies the commutative law:

$$s \diamond t = t \diamond s \text{ for all } s, t \in S.$$

Our main tool for comparing semigroups is:

DEFINITION 3:
Suppose that $(S, \diamond)$ and $(T, \bullet)$ are semigroups. A function α: $S \to T$ is called a *homomorphism* if

$$\alpha(x \diamond y) = \alpha x \bullet \alpha y \text{ for all } x, y \in S.$$

■

Since every group is a semigroup, homomorphisms can be used to compare groups too. A bijective homomorphism is called an *isomorphism.* Also, a homomorphism from a semigroup to itself is called an *endomorphism.* Recall that for any homomorphism α of groups, $\alpha 0 = 0$, since $\alpha 0 = \alpha(0 + 0) = \alpha 0 + \alpha 0$ and in a group 0 is the only element that satisfies $x = x + x$.

Next we define an algebraic structure that will play an important role in this study:

DEFINITION 4:

A *right nearring* is a triple $(N, +, \cdot)$ which satisfies:

i) $(N, +)$ is a group;

ii) $(N, \cdot)$ is a semigroup;

iii) $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in N$.

N is a *nearfield* if $(N\backslash\{0\}, \cdot)$ is also a group. ∎

As with groups, the nearring $(N, +, \cdot)$ is denoted by just N when the operations are clearly understood. If the usual rules for performing operations are understood, then superfluous parentheses are omitted. Also, multiplication is almost always written simply using juxtaposition. If N contains an element 1 so that $a1 = 1a = a$ for all $a \in N$, then 1 is called the *multiplicative identity* of N.

The identity element of the additive group structure of $(N, +, \cdot)$ is called the *zero* of the nearring and is denoted by 0.

The first example of a right nearring given here is a right nearring of mappings.

EXAMPLE 5

Let $(G, +)$ be group. Define $M(G)$ to be the set of all mappings from G to G, with addition defined pointwise:

$$(f + g)(x) := f(x) + g(x) \text{ for all } x \in G.$$

Multiplication is defined as the usual composition of maps:

$$(f \circ g)(x) := f(g(x)) \text{ for all } x \in G.$$

Then $M(G)$ is a right nearring. The verification of this is direct. It is included here for the sake of completeness and for easy reference. Define the mapping ζ by $\zeta(x) := 0$ for all $x \in G$. Then ζ is an element of $M(G)$, and hence, $M(G)$ is not empty. For any $f, g \in M(G)$, $(f \circ g)(x) := f(g(x))$ which belongs to G. Hence, composition is a binary

operation on $M(G)$. Also for any $f, g, h \in M(G)$,

$$\begin{aligned}(f \circ (g \circ h))(x) &= f((g \circ h)(x)) \\ &= f(g(h(x))) \\ &= (f \circ g)(h(x)) \\ &= ((f \circ g) \circ h)(x) \text{ for all } x \in G.\end{aligned}$$

So $(M(G), \circ)$ is a semigroup.

Turning our attention to pointwise addition, for $f, g \in M(G)$, $(f + g)(x) = f(x) + g(x)$ which belongs to G. Hence, pointwise addition is a binary operation on $M(G)$. Also for $f, g, h \in M(G)$,

$$\begin{aligned}(f + (g + h))(x) &= f(x) + (g + h)(x) \\ &= f(x) + (g(x) + h(x)) \\ &= (f(x) + g(x)) + h(x) \\ &= ((f + g) + h)(x) \text{ for all } x \in G.\end{aligned}$$

So $(M(G), +)$ is a semigroup.

In fact, $(M(G), +)$ is a group. Let f be an arbitrary element of $M(G)$. Define $-f\colon G \to G$ by $(-f)(x) := -f(x)$ for all $x \in G$. Then, for all $x \in G$,

$$\begin{aligned}(\zeta + f)(x) &= \zeta(x) + f(x) = 0 + f(x) = f(x), \\ (f + \zeta)(x) &= f(x) + \zeta(x) = f(x) + 0 = f(x), \\ (f + (-f))(x) &= f(x) + (-f)(x) = f(x) - f(x) = 0 = \zeta(x), \\ ((-f) + f)(x) &= (-f)(x) + f(x) = -f(x) + f(x) = 0 = \zeta(x).\end{aligned}$$

Hence, for any $f \in M(G)$, $\zeta + f = f + \zeta = f$ and $f + (-f) = (-f) + f = \zeta$. This means that ζ is an identity for pointwise addition and that each element of $M(G)$ has an additive inverse. Thus, $M(G)$ satisfies all the conditions for a group.

Finally, composition distributes over pointwise addition in one direction in $M(G)$.

For $f, g, h \in M(G)$,

$$\begin{aligned}[(f+g)\circ h](x) &= (f+g)(h(x)) \\ &= f(h(x)) + g(h(x)) \\ &= (f\circ h)(x) + (g\circ h)(x) \\ &= [f\circ h + g\circ h](x) \text{ for all } x \in G.\end{aligned}$$

So $(f+g)\circ h = f\circ h + f\circ g$. Hence, the right distributive law holds.

Therefore, $(M(G), +, \circ)$ is a right nearring. Note that if G contains more than one element, then the *left distributive law* (i.e. $f\circ(g+h) = f\circ g + f\circ h$ for all f, g and h) does not hold in $M(G)$. To see this, suppose that $y, z \in G$, and define h_y and h_z by $h_y(x) := y$ and $h_z(x) := z$ for all $x \in G$. Then, for any $f \in M(G)$,

$$[f\circ(h_y + h_z)](x) = f((h_y + h_z)(x)) = f(h_y(x) + h_z(x)) = f(y+z),$$

while

$$\begin{aligned}[f\circ h_y + f\circ h_z](x) &= (f\circ h_y)(x) + (f\circ h_z)(x) \\ &= f(h_y(x)) + f(h_z(x)) \\ &= f(y) + f(z)\end{aligned}$$

for all $x \in G$. Thus, the left distributive law does not hold unless $f(y+z) = f(y) + f(z)$ for all $y, z \in G$. This means that f must be an endomorphism for the left distributive law to hold. When G contains more than one element, not all the mappings in $M(G)$ are endomorphisms (e.g. h_y for $y \neq 0$). ∎

This brings us to our next definition,

DEFINITION 6:

A *left nearring* is a triple $(N, +, \cdot)$ which satisfies:

i) $(N, +)$ is a group;

ii) $(N, \cdot)$ is a semigroup;

iii) $a\cdot(b+c) = a\cdot b + a\cdot c$ for all $a, b, c \in N$. ∎

Various authors favour different types of nearrings. For example, right nearrings are used in [10], while left nearrings are used in [4] and [8]. Only right nearrings will be used in this

thesis. However, we follow the format of [8] in the definitions. Recall that in a nearring N, $0n = 0$ for all $n \in N$. In general it is not true that $n0 = 0$ for all $n \in N$ and in the case that this is so, we call N a *zero-symmetric nearring.* In this thesis we will restrict our attention to nearrings that are zero-symmetric.

1.2 Nearring Modules

We begin by defining the tool that allows us to compare nearrings:

DEFINITION 1:

Let $(N, +, \cdot)$ and $(S, +, \cdot)$ be nearrings. Then a mapping θ from N to S is called a *nearring homomorphism* if

i) $\theta(n_1 + n_2) = \theta(n_1) + \theta(n_2)$;

ii) $\theta(n_1 n_2) = \theta(n_1)\theta(n_2)$ for all $n_1, n_2 \in N$. ∎

It has been proved (refer to [8] or [10] for a proof) that every nearring can be considered as a subnearring of a nearring of the form $M(G)$ for some group $(G, +)$. This context, namely a nearring and a group on which it acts provides valuable insight into the structure of nearrings. Thus we are led to the notion of modules over nearrings.

DEFINITION 2:

Let $(G,+)$ be a group, $(N, +, \cdot)$ be a nearring. We call G a *(left) N - module* if there is a nearring homomorphism $\theta : (N, +, \cdot) \to (M(G), +, \cdot)$. Such a homomorphism is called a *representation* of N. A representation θ is called *faithful* if Ker $\theta = 0$. ∎

EXAMPLE 3:

Let $(G, +)$ be a group, and let S be a subsemigroup of endomorphisms of G. We define the *centralizer nearring* $M_S(G)$ by

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

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

To verify this, we show that $M_S(G)$ is a subnearring of $M(G)$ under the operations defined

in Example 1.1-5. It is clear that the mapping ζ defined in Example 1.1-5 is an element of $M_S(G)$, so $M_S(G)$ is nonempty. Now let $\alpha, \beta \in M_S(G)$. Then

$$\begin{aligned}(\alpha - \beta)(sg) &= \alpha(sg) - \beta(sg) \\ &= s(\alpha(g)) - s(\beta(g)) \\ &= s(\alpha(g) - \beta(g)) \\ &= s((\alpha - \beta)(g)) \text{ for all } g \in G.\end{aligned}$$

Thus $(M_S(G), +)$ is a subgroup of $(M(G), +)$. Turning our attention to composition, for $\alpha, \beta \in M_S(G)$,

$$\begin{aligned}(\alpha \circ \beta)(sg) &= \alpha(\beta(sg)) \\ &= \alpha(s(\beta(g))) \\ &= s(\alpha(\beta(g))) \\ &= s((\alpha \circ \beta)(g)) \text{ for all } g \in G.\end{aligned}$$

Hence, composition is a binary operation on $M_S(G)$. The associativity follows from the fact that $(M(G), \circ)$ is a semigroup. Thus $(M_S(G), \circ)$ is a subsemigroup of $(M(G), \circ)$. Thus $(M_S(G), +, \circ)$ is a right nearring. The identity homomorphism serves as the representation of $M_S(G)$ and clearly it is faithful. Thus G is a faithful $M_S(G)$ - module. ∎

We will focus our attention on a particular class of nearrings, namely 2-primitive nearrings. In order to define this class we need two more definitions:

DEFINITION 4:

Let N be a nearring and let G be an N-module. We call G *monogenic* if there exists a $g \in G$ such that $Ng = G$. In such a case, g is called a *generator* of G. ∎

DEFINITION 5:

Let N be a nearring, G an N-module.

i) A subgroup H of G such that $nh \in H$ for all $h \in H$, $n \in N$ is called an N-*submodule* of G.

ii) A normal subgroup K of G such that $n(g + k) - ng \in K$ for all $g \in G$, $n \in N$, $k \in K$ is called an N-*ideal* of G. ∎

DEFINITION 6:

Let N be a nearring. An *ideal* of N is a subgroup I of N which satisfies

i) $(I, +)$ is a normal subgroup of $(N, +)$;

ii) $IN \subseteq I$;

iii) $n(n' + i) - nn' \in I$ for all $n, n' \in N, i \in I$.

If I satisfies (i) and (ii) it is called a *right ideal* of N. If I satisfies (i) and (iii) it is called a *left ideal* of N. ∎

DEFINITION 7:

A nearring N is called *simple* if its only ideals are $\{0\}$ and N. ∎

DEFINITION 8:

A nearring N is called *2-primitive on* G if G is a faithful N-module of type 2, i.e. if G is monogenic and has no proper nontrivial N-submodules. ∎

1.3 Rings

For completeness we conclude this chapter by giving a formal definition of a special kind of nearring and some related structures.

DEFINITION 1:

A *ring* is a triple $(R, +, \cdot)$ which satisfies:

i) $(R, +)$ is an abelian group;

ii) $(R, \cdot)$ is a semigroup;

iii) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$;

iv) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in R$. ∎

It is clear that every ring is a nearring. So the notation introduced for nearrings can be used with rings. If a ring has an multiplicative identity, we say that the ring has *unity (or identity)* and we will denote this element by 1. In keeping with our example of a right nearring, we give a well-known example of a ring of functions. A proof of the next

example can be found in [3](Example 1.1.3, p.7).

EXAMPLE 2:

Let $(A, +)$ be an abelian group. We define addition and multiplication of elements of $End(A)$ by:

$$(f + g)(x) := f(x) + g(x)$$

for all $x \in G$. Multiplication is defined as the usual composition of maps:

$$(f \circ g)(x) := f(g(x))$$

for all $x \in G$. Then $(End(A), +, \cdot)$ is a ring. ∎

We next review some well-known classes of rings:

DEFINITION 3:

Let $(R, +, \cdot)$ be a ring.

i) R is called a *commutative ring* if $a \cdot b = b \cdot a$ for all $a, b \in R$;

ii) R is called an *integral domain* if R is commutative, $1 \neq 0$, and $a \cdot b = 0$ implies $a = 0$ or $b = 0$, for any $a, b \in R$;

iii) R is called a *field* if R is an integral domain such that for each nonzero element $r \in R$ there exists an element $r^{-1} \in R$ such that $r \cdot r^{-1} = 1$. ∎

We close this chapter with the noncommutative analogs of integral domains and fields:

DEFINITION 4:

Let $(R, +, \cdot)$ be a ring in which $1 \neq 0$.

i) R is called a *noncommutative domain* if R is a noncommutative ring and $a \cdot b = 0$ implies $a = 0$ or $b = 0$, for any $a, b \in R$;

ii) R is called a *division ring* if every nonzero element of R is invertible, i.e., for each nonzero element $r \in R$ there exists an element $r^{-1} \in R$ such that $r \cdot r^{-1} = r^{-1} \cdot r = 1$. ∎

Throughout this thesis the terms *subsemigroup, subgroup, subnearring* and *subring* will convey the same meaning, i.e. we will be referring to a nonempty subset of the appropriate structure with the added property that under the operation(s) of the larger structure it

inherits the same attributes.

Chapter 2

The Theory of Near Vector Spaces

2.1 Some Preliminary Results

Recall the following definition:

DEFINITION 1:

A set V is said to be a *(right) vector space* over a division ring F, if $(V, +)$ is an abelian group and, if for each $\alpha \in F$ and $v \in V$, there is a unique element $v\alpha \in V$ such that the following conditions hold for all $\alpha, \beta \in F$ and all $u, v \in V$:

i) $(v + u)\alpha = v\alpha + u\alpha$;

ii) $v(\alpha + \beta) = v\alpha + v\beta$;

iii) $v(\alpha\beta) = (v\alpha)\beta$;

iv) $v1 = v$. ∎

The members of V are called *vectors* and the members of the division ring are called *scalars.* The operation that combines a scalar α and a vector v to form the vector $v\alpha$ is called *scalar multiplication.*

NOTE 1:

(a) 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 $x \in V$).

(b) If V is a vector space over a division ring F, then for every $\alpha, \beta \in F$ and for each $x \in V$, there is a $\gamma \in F$ (viz, $\gamma = \alpha + \beta$) such that $x\alpha + x\beta = x\gamma$.

A vector space is a special instance of a more general concept - a near vector space. This concept was introduced and studied by Andrè in [1]. We will follow the format of de Bruyn's thesis [5] in this chapter. However, both Andrè and de Bruyn use left nearfields for their near vector spaces. It is more standard to use the notation as in van der Walt [12], where the nearrings of near linear transformations are right nearrings and scalar multiplication is done on the right of vectors (implying the use of right nearfields). Before we can proceed with the main body of this chapter, we need some basic results.

DEFINITION 2:

Let Q be a set and let 2^Q be the set of all subsets of Q. A relation between Q and 2^Q, denoted by $v \lhd M$, with $v \in Q$ and $M \subseteq Q$, is a *dependence relation* if the following conditions are satisfied (where $u, v, w \in Q$ and $M, N \subseteq Q$):

(D_1) $v \in M$ implies that $v \lhd M$;

(D_2) $w \lhd M$ and $v \lhd N$ for each $v \in M$, implies that $w \lhd N$;

(D_3) $v \lhd M$ and the falsehood of $v \lhd M\backslash\{u\}$ (denoted $v \not\lhd M\backslash\{u\}$), implies that $u \lhd (M\backslash\{u\}) \cup \{v\}$. ∎

Let $\lhd$ be a dependence relation on Q.

THEOREM 3:

Let $M \subseteq N \subseteq Q$. If $w \lhd M$, then $w \lhd N$.

Proof

Suppose $w \lhd M$. If $v \in M$, then $v \in N$ since $M \subseteq N$. Thus by (D_1), $v \lhd N$. But now $w \lhd M$ and $v \lhd N$ for all $v \in M$, so by (D_2), $w \lhd N$. ∎

DEFINITION 4:

(i) A finite subset E of Q is *independent* if there is no $v \in E$ such that $v \lhd E\backslash\{v\}$.

(ii) An infinite subset M of Q is *independent* if every finite subset of M is independent. ∎

THEOREM 5:

Let $N \subseteq M \subseteq Q$. If M is independent, then N is independent.

Proof

Suppose M is independent. Let M be finite and suppose that N is not independent. Then there exists a $v \in N$ such that $v \triangleleft N\backslash\{v\}$. But $N \subseteq M$, so $v \in M$ and by Theorem 3, $v \triangleleft M\backslash\{v\}$, which is a contradiction. Thus N is independent. If M is infinite the result follows from the definition. ∎

THEOREM 6:

Let $B \subseteq Q$ and $x \in Q$. If B is independent and $B \cup \{x\}$ is not independent, then $x \triangleleft B$.

Proof

Suppose B is independent and $B \cup \{x\}$ is not independent. Then there exists a finite subset $B^{'}$ of $B \cup \{x\}$ which is not independent. Thus there exists a $v \in B^{'}$ such that $v \triangleleft B^{'}\backslash\{v\}$. There are two possible cases to consider:

Case 1: $v = x$

Then $B^{'}\backslash\{v\} \subseteq B$ so by Theorem 3, $x \triangleleft B$.

Case 2: $v \neq x$

In this case, if $x \notin B'$, then $B' \subseteq B$, implying (by Theorem 5) that B' is independent, a contradiction. Hence, assume that $B^{'} = B_e \cup \{x\}$ with B_e a finite subset of B, so that $v \in B_e$. But B_e is independent by Theorem 5, so $v \not\triangleleft B_e\backslash\{v\}$. Furthermore, $B^{'}\backslash\{v\} = (B_e \cup \{x\})\backslash\{v\} =: M$. Also, $M\backslash\{x\} = B_e\backslash\{v\}$. So $v \triangleleft M$ and $v \not\triangleleft M\backslash\{x\}$. Hence by (D_3), $x \triangleleft (M\backslash\{x\}) \cup \{v\}$. But $(M\backslash\{x\}) \cup \{v\} = (B_e\backslash\{v\}) \cup \{v\} = B_e$. Hence $x \triangleleft B_e$. So by Theorem 3, $x \triangleleft B$. ∎

DEFINITION 7:

Let M and N be subsets of Q. Then M *depends on* N (M *is generated by* N) if, for each $v \in M$, there exists a finite subset $N^{'}$ of N such that $v \triangleleft N^{'}$. ∎

By making use of this definition in conjunction with Theorem 3, we have the following lemma:

LEMMA 8:

Let M be a subset of Q and N a finite subset of Q. Then M depends on N if and only if $v \triangleleft N$ for each $v \in M$.

Proof

Suppose M depends on N. Then there exists a finite $N' \subseteq N$ such that for all $v \in M$, $v \triangleleft N'$. But $N' \subseteq N \subseteq Q$ and $v \triangleleft N'$, thus by Theorem 3, $v \triangleleft N$ for all $v \in M$.

Conversely, suppose $v \triangleleft N$ for all $v \in M$. We have to show that there exists a finite subset N' of N such that $v \triangleleft N'$ for all $v \in M$. Clearly N will serve as a suitable candidate. ∎

Note that the forward direction holds irrespective of whether or not N is finite.

THEOREM 9:

Let N and N' be subsets of Q. If N is independent and contains n elements, N' contains m elements and N depends on N', then $n \leq m$.

Proof

Let $S := \{s \mid$ there exists an independent set $N_s \subseteq N \cup N'$ such that N_s contains n elements of which s of them are in $N'\}$. Then S is nonempty since $N \subseteq N \cup N'$, N is independent and $|N| = n$ of which q elements with $0 \leq q \leq m$ are in N'. Let $r = \max S$. Then $0 \leq r \leq m$:

Suppose $r < n$. Then there exists $w \in N_r$ such that $w \notin N'$, but $w \in N$. Since N_r is independent, $w \not\triangleleft N_r \backslash \{w\}$. Moreover, by Lemma 8, $w \triangleleft N'$ since N depends on N'. Hence by (D_2), there exists a $v \in N'$ such that $v \not\triangleleft N_r \backslash \{w\}$. Hence by (D_1), $v \notin N_r \backslash \{w\}$.

Next, let $N^* = (N_r \backslash \{w\}) \cup \{v\}$. Then N^* contains n elements with $r + 1$ of them in N'. Thus N^* is not independent. But by Theorem 5, $N_r \backslash \{w\}$ is independent. Hence by Theorem 6, $v \triangleleft N_r \backslash \{w\}$, a contradiction. Thus $n = r \leq m$. ∎

DEFINITION 10:

A subset B of Q is a *basis* of Q if

(i) B is independent and

(ii) Q depends on B. ∎

THEOREM 11:

If L is an independent subset of Q, then there is a basis B of Q with $L \subseteq B$.

Proof

Let $\mathcal{E}$ be the set of all independent subsets of Q. Let $\mathcal{C} := \{L\}$ and let $\mathcal{K}$ be the set of all chains $\mathcal{L}$ of independent subsets of Q such that $L \in \mathcal{L}$. For any chain $\mathcal{L}_1 \subseteq \mathcal{L}_2 \subseteq \cdots$ of these chains, $\cup \mathcal{L}_i$ is a chain containing L and it is an upper bound for the chain $\mathcal{L}_1 \subseteq \mathcal{L}_2 \subseteq \cdots$. By Zorn's Lemma $\mathcal{K}$ contains a maximal element $\mathcal{M}$ with $\mathcal{C} \subseteq \mathcal{M} \subseteq \mathcal{E}$. Let $B := \cup \{M \,|\, M \in \mathcal{M}\}$. Then $L \subseteq B \subseteq Q$. Let B_e be a finite subset of B. Then B_e is contained in a finite union of sets of $\mathcal{M}$. Since $\mathcal{M}$ is a chain, $B_e \subseteq M_e$, where M_e is the largest of these sets. Hence by Theorem 5, B_e is independent. Thus by definition, B is independent.

Suppose that Q does not depend on B. Then there exists an $x \in Q$ such that $x \not\lhd B_l$ for each finite subset B_l of B. Furthermore, by (D_1), $x \notin B$ [otherwise $x \lhd \{x\}$, and $\{x\}$ is a finite subset of B]. It follows that $B_l \cup \{x\}$ is independent for every finite subset B_l of B, otherwise, if $B_l \cup \{x\}$ is not independent for some finite B_l, then $x \lhd B_l$, by Theorem 6, and this is a contradiction. Therefore $B \cup \{x\}$ is independent, by Definition 4. Next, let $\mathcal{M}' = \mathcal{M} \cup \{B \cup \{x\}\}$. Then $\mathcal{M}'$ is a chain in Q and $\mathcal{C} \subseteq \mathcal{M} \subseteq \mathcal{M}' \subseteq \mathcal{E}$. But $\mathcal{M} \neq \mathcal{M}'$ for $B \cup \{x\} \notin \mathcal{M}$ since $x \notin B$. This contradicts the maximality of $\mathcal{M}$. Hence Q depends on B. Thus B is a basis for Q. ∎

THEOREM 12:

Let B be a finite basis of Q with n elements. Then any other basis D of Q also has n elements.

Proof

Let $B = \{x_1, x_2, \ldots, x_n\}$. Then since Q depends on D, there exist finite subsets D_i of D such that $x_i \lhd D_i$ for $i = 1, 2, \ldots, n$. Let $E := \cup \{D_i \,|\, i = 1, 2, \ldots, n\}$. Then $E \subseteq D$. In fact, we will show that $E = D$. Suppose that this is not the case, i.e. suppose that there exists a $y \in D$ with $y \notin E$. Since Q depends on B, by Lemma 8, $y \lhd B$. But by Theorem 3, $x_i \lhd E$ for $i = 1, 2, \ldots, n$. Therefore by (D_2), $y \lhd E$. Moreover, since $y \notin E$,

$(E \cup \{y\})\backslash\{y\} = E$. Hence $y \lhd (E \cup \{y\})\backslash\{y\}$. Therefore the finite subset $E \cup \{y\}$ of D is not independent. This contradicts the independence of D. Hence $D = E$.

Suppose D contains m elements. Let $x \in B \subseteq Q$. Then $x \lhd D$. Therefore by Lemma 8, B depends on D. Hence by Theorem 9, $n \leq m$. Similarly, D depends on B. Hence $m = n$.

■

THEOREM 13:

Let B and D be bases of Q. Then B and D have the same cardinal number.

Proof

The finite case is dealt with in Theorem 12. Thus let B and D be infinite bases with cardinal numbers κ_1 and κ_2 respectively. Let $B := \{x_\alpha \,|\, \alpha \in \Lambda\}$. Then since Q depends on D, there is for each $\alpha \in \Lambda$, a finite subset D_α of D such that $x_\alpha \lhd D_\alpha$.

Let $E := \cup\,\{D_\alpha \,|\, \alpha \in \Lambda\}$. Then $E \subseteq D$. We want to show that $E = D$. Suppose that $E \subset D$. Then there exists a $y \in D$ such that $y \notin E$. Since Q depends on B, there exists a finite subset B_e of B such that $y \lhd B_e$. But $B_e = \{x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_q}\}$ with $\{\alpha_1, \alpha_2, \ldots, \alpha_q\} \subseteq \Lambda$. Let $E_q := \cup\,\{D_{\alpha_i} \,|\, i = 1, 2, \ldots, q\}$. Then by Theorem 3, $x_{\alpha_i} \lhd E_q$ for $i = 1, 2, \ldots, q$. Hence by (D_2), $y \lhd E_q$. Moreover, since $y \notin E_q$, $(E_q \cup \{y\})\backslash\{y\} = E_q$. Hence $y \lhd (E_q \cup \{y\})\backslash\{y\}$. Thus the finite subset $E_q \cup \{y\}$ of D is not independent. This contradicts the independence of D. Thus $D = E$.

Since $D := \cup\,\{D_\alpha \,|\, \alpha \in \Lambda\}$, $\kappa_2 \leq \aleph_0\kappa_1$ with $\aleph_0$ the cardinal number of the set of all natural numbers. Furthermore, since κ_1 is infinite, $\aleph_0\kappa_1 = \kappa_1$. Thus $\kappa_2 \leq \kappa_1$. Similarly $\kappa_1 \leq \kappa_2$. Therefore $\kappa_2 = \kappa_1$. ■

As a consequence of the above two theorems we define the *dimension* of Q, denoted $\dim Q$ as the cardinal number of a basis of Q.

2.2 F-groups

DEFINITION 1:

An *F-group* is a structure (V, F) which satisfies the following conditions:

(F_1) $(V, +)$ is a group and F is a set of endomorphisms of V;

(F_2) The endomorphisms 0, 1 and -1, defined by $x0 = 0$, $x1 = x$ and $x(-1) = -x$ for each $x \in V$, are elements of F;

(F_3) $F^* := F\backslash\{0\}$ is a subgroup of the group of automorphisms of $(V, +)$;

(F_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* (fpf) on V. ∎

NOTE 1:

(a) If $V \neq \{0\}$, then there is a $v \in V$, with $v \neq 0$. Hence $v0 = 0 \neq v1$. Consequently $0 \neq 1$.

(b) $(V, +)$ is abelian, since by (F_2):

$x + y = (-x)(-1) + (-y)(-1) = (-x - y)(-1) = ((-(y + x))(-1) = y + x$.

(c) A vector space over a division ring F is an F-group. Refer to Note 2.1-1(a). More examples will be given in Chapter 3.

(d) If $\alpha \in F$, then $0\alpha = 0$ and $(-x)\alpha = -(x\alpha)$ since α is an endomorphism of V.

2.3 Quasi-kernels

DEFINITION 1:

Let (V, F) be an F-group. The *quasi-kernel* $Q(V)$ (or just Q if there is no danger of confusion) of (V, F) is the set of all $u \in V$ such that, for each pair $\alpha, \beta \in F$, there exists a $\gamma \in F$ for which

$$u\alpha + u\beta = u\gamma. \tag{2.1}$$

∎

LEMMA 2:

The quasi-kernel Q has the following properties:

(a) $0 \in Q$;

(b) For $u \in Q\backslash\{0\}$, γ in (2.1) is uniquely determined by α and β;

(c) If $u \in Q$ and $\lambda \in F$, then $u\lambda \in Q$, i.e. $uF \subseteq Q$;

(d) If $u \in Q$ and $\lambda_i \in F$, $i = 1, 2, \ldots, n$, then $\sum_{i=1}^{n} u\lambda_i = u\eta \in Q$ for some $\eta \in F$ and for all integers $n \geq 1$;

(e) If $u \in Q\backslash\{0\}$ and $\alpha, \beta \in F$, then there exists a $\gamma \in F$ such that $u\alpha - u\beta = u\gamma$.

Proof

(a) Let $\alpha, \beta \in F$. Take any $\gamma \in F$, then $0\alpha + 0\beta = 0\gamma$. Thus $0 \in Q$.

(b) Let $u \in Q\backslash\{0\}$ and $\alpha, \beta \in F$. Now suppose there exist $\gamma, \gamma' \in F$ such that $u\alpha + u\beta = u\gamma = u\gamma'$. Then by (F_4), $\gamma = \gamma'$, as $u \neq 0$.

(c) Suppose $u \in Q$ and $\lambda \in F$. There are two cases to consider:

Case 1: $\lambda = 0$

Then $u\lambda = u0 = 0 \in Q$.

Case 2: $\lambda \neq 0$

Let α, β be elements of F. Then by (F_3), $\lambda\alpha \in F$ and $\lambda\beta \in F$. So since $u \in Q$, there exists a $\gamma \in F$ such that $u(\lambda\alpha) + u(\lambda\beta) = u\gamma = u\lambda\lambda^{-1}\gamma$. So $(u\lambda)\alpha + (u\lambda)\beta = (u\lambda)(\lambda^{-1}\gamma)$ which implies that $u\lambda \in Q$. Thus $uF \subseteq Q$.

(d) We shall use induction on n. Let $S := \{n \in \mathbb{N} \mid \sum_{i=1}^{n} u\lambda_i \in uF \text{ if } u \in Q, \lambda_i \in F, i = 1, 2, \ldots, n\}$. By (c) above, $1 \in S$. Now suppose $k \in S$, i.e. $u\eta := \sum_{i=1}^{k} u\lambda_i \in Q$ if $u \in Q$. Then

$$\begin{aligned} \textstyle\sum_{i=1}^{k+1} u\lambda_i &= \textstyle\sum_{i=1}^{k} u\lambda_i + u\lambda_{k+1} \\ &= u\eta + u\lambda_{k+1} \\ &= u\mu \text{ for some } \mu \in F, \text{ since } u \in Q. \end{aligned}$$

Hence $k + 1 \in S$ and consequently $S = \mathbb{N}$.

(e) Let $u \in Q\backslash\{0\}$ and $\alpha, \beta \in F$. Then $(-1)\beta \in F$ and by (F_4), $(-1)\beta = -\beta$ since $u(-\beta) = (-u)\beta = u(-1)\beta$. But $u \in Q$, so there exists a $\gamma \in F$ such that $u\alpha + u(-\beta) = u\gamma$, which implies that $u\alpha - u\beta = u\gamma$. ∎

DEFINITION 3:

(V, F) is said to be a *linear* F-group if $V = \{0\}$ or $Q(V) \neq \{0\}$. ∎

We shall, in what follows, associate a nearfield with each $u \in Q(V)\backslash\{0\}$ in a linear

F-group.

DEFINITION 4:

Let (V, F) be a linear F-group, and let $u \in Q(V)\backslash\{0\}$. Define the operation $+_u$ on F by

$$u(\alpha +_u \beta) := u\alpha + u\beta \ (\alpha, \beta \in F). \tag{2.2}$$

■

NOTE 4:

(a) On account of Lemma 2, $\alpha +_u \beta$ is uniquely determined by α and β in F.

(b) Since V is abelian, the set of all endomorphisms of V is a ring if we define addition in the following way:

$$x(\alpha + \beta) := x\alpha + x\beta$$

(Refer to Example 1.3-2). In general, $\alpha + \beta$, for α and β in F, does not belong to F, since F is not necessarily the set of all endomorphisms of $(V, +)$. It therefore differs from the sum defined in Definition 4.

THEOREM 5:

Let (V, F) be a linear F-group and let $u \neq 0$ be an element of the quasi-kernel $Q(V)$. Then $(F, +_u, \cdot)$ with addition $+_u$ as defined in Definition 4, is a nearfield.

Proof

Let α, β and γ be elements of F and $u \in Q(V)\backslash\{0\}$.

First we will show that $(F, +_u)$ is an abelian group.

(i)

$$\begin{aligned} u[(\alpha +_u \beta) +_u \gamma] &= u(\alpha +_u \beta) + u\gamma \\ &= (u\alpha + u\beta) + u\gamma \\ &= u\alpha + (u\beta + u\gamma) \\ &= u\alpha + u(\beta +_u \gamma) \\ &= u[\alpha +_u (\beta +_u \gamma)] \end{aligned}$$

Hence by (F_4), since $u \neq 0$, $(\alpha +_u \beta) +_u \gamma = \alpha +_u (\beta +_u \gamma)$. Thus $+_u$ is associative.

(ii)

By (F_2), 0: $V \to V$ defined by $v0 := 0$ for all $v \in V$ is an element of F. But

$$\begin{aligned} u(f +_u 0) &= uf + u0 \\ &= uf + 0 \\ &= uf. \end{aligned}$$

Hence by (F_4), since $u \neq 0$, $f +_u 0 = f$. Similarly, $0 +_u f = f$. Therefore 0: $V \to V$ is the zero element of $(F, +_u)$.

(iii)

Define for each $f \in F$, $-f$: $V \to V$ by $-f := (-1)f$ (Refer to the proof of Lemma 2(e)). Then

$$\begin{aligned} u(-f +_u f) &= u(-f) + uf \\ &= (-u)f + uf \\ &= (-u + u)f \\ &= 0f \\ &= 0 \\ &= u0. \end{aligned}$$

Hence by (F_4), since $u \neq 0$, $-f +_u f = 0$. Similarly, $f +_u -f = 0$. Therefore, for each $f \in F$, the additive inverse $-f$ exists and is an element of $(F, +_u)$.

(iv)

$(F, +_u)$ is abelian:

$$\begin{aligned} u(\beta +_u \gamma) &= u\beta + u\gamma \\ &= u\gamma + u\beta, \text{ since } (V, +) \text{ is abelian} \\ &= u(\gamma +_u \beta) \end{aligned}$$

Hence by (F_4), since $u \neq 0$, $\beta +_u \gamma = \beta +_u \gamma$. Thus $(F, +_u)$ is an abelian group. We also have by (F_3), that $(F^*, \cdot)$ is a group. All that we still need to verify is that the right

distributive law holds:

$$\begin{aligned} u(\alpha +_u \beta)\gamma &= (u\alpha + u\beta)\gamma \\ &= (u\alpha)\gamma + (u\beta)\gamma \\ &= u(\alpha\gamma) + u(\beta\gamma) \\ &= u(\alpha\gamma +_u \beta\gamma) \end{aligned}$$

Hence by (F_4), since $u \neq 0$, $(\alpha +_u \beta)\gamma = (\alpha\gamma +_u \beta\gamma)$. Thus $(F, +_u, \cdot)$ is a nearfield. ∎

COROLLARY 6:

If (V, F) is a linear F-group with $V \neq 0$, then F^* is the multiplicative group of a nearfield.

∎

THEOREM 7:

If $u \in Q(V)\backslash\{0\}$ and $\lambda \in F\backslash\{0\}$, then the nearfields $(F, +_u, \cdot)$ and $(F, +_{u\lambda}, \cdot)$ are isomorphic.

Proof

Define f: $(F, +_{u\lambda}, \cdot) \to (F, +_u, \cdot)$ by $f(\alpha) := \lambda\alpha\lambda^{-1} =: \alpha^\lambda$ for each $\alpha \in F^*$ and $f(0) = 0$. First we check that f is well-defined: Let $\alpha = \beta$. Then $f(\alpha) = \lambda\alpha\lambda^{-1} = \lambda\beta\lambda^{-1} = f(\beta)$. Next we check that f is bijective: Suppose $f(\alpha) = f(\beta)$. Then $\lambda\alpha\lambda^{-1} = \lambda\beta\lambda^{-1}$ so that $\alpha = \lambda^{-1}\lambda\alpha\lambda^{-1}\lambda = \lambda^{-1}\lambda\beta\lambda^{-1}\lambda = \beta$. Thus f is injective. Furthermore, let $\beta \in (F, +_u, \cdot)$. Then $\lambda^{-1}\beta\lambda = \alpha \in F$. Hence $\beta = \lambda\alpha\lambda^{-1}$. Therefore there exists an α in $(F, +_{u\lambda}, \cdot)$ such that $f(\alpha) = \lambda\alpha\lambda^{-1} = \beta$. Hence f is surjective.

Finally, f respects the operations:

$$\begin{aligned} u[f(\alpha +_{u\lambda} \beta)] &= (u\lambda)(\alpha +_{u\lambda} \beta)\lambda^{-1} \\ &= ((u\lambda)\alpha + (u\lambda)\beta)\lambda^{-1} \\ &= u\lambda\alpha\lambda^{-1} + u\lambda\beta\lambda^{-1} \\ &= u[\lambda\alpha\lambda^{-1} +_u \lambda\beta\lambda^{-1}] \\ &= u[f(\alpha) +_u f(\beta)] \end{aligned}$$

Hence by (F_4), since $u \neq 0$,

$$f(\alpha +_{u\lambda} \beta) = f(\alpha) +_u f(\beta). \tag{2.3}$$

Also,

$$\begin{aligned} u[f(\alpha\beta)] &= u(\lambda\alpha\beta\lambda^{-1}) \\ &= u(\lambda\alpha\lambda^{-1}\lambda\beta\lambda^{-1} \\ &= (u\lambda\alpha\lambda^{-1})(\lambda\beta\lambda^{-1}) \\ &= (uf(\alpha))f(\beta) \\ &= u(f(\alpha)f(\beta)) \end{aligned}$$

Hence by (F_4), since $u \neq 0$,

$$f(\alpha\beta) = f(\alpha)f(\beta).$$

Therefore $(F, +_u, \cdot) \cong (F, +_{u\lambda}, \cdot)$. ∎

NOTE 7:

From (2.3), we have $f(\alpha +_{u\lambda} \beta) = f(\alpha) +_u f(\beta)$. Hence

$$\lambda(\alpha +_{u\lambda} \beta)\lambda^{-1} = \lambda\alpha\lambda^{-1} +_u \lambda\beta\lambda^{-1}.$$

This implies that

$$(\alpha +_{u\lambda} \beta)^\lambda = \alpha^\lambda +_u \beta^\lambda.$$

Therefore

$$\alpha +_{u\lambda} \beta = (\alpha^\lambda +_u \beta^\lambda)^{\lambda^{-1}}. \tag{2.4}$$

DEFINITION 8:

Let (V, F) be a linear F-group, and let $u \in Q(V)\backslash\{0\}$. Define the *kernel* $R_u(V) = R_u$ of (V, F) by the set

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

∎

NOTE 8:

(a) $u \in R_u$: Indeed, $u \in V$ and $u(\alpha +_u \beta) = u\alpha + u\beta$ for all $\alpha, \beta \in F$.

(b) $R_u \subseteq Q$: Let $v \in R_u$, then for every $\alpha, \beta \in F$ there exists a $\gamma \in F$, namely $\gamma := \alpha +_u \beta$ such that $v\alpha + v\beta = v\gamma$.

(c) $0 \in R_u$: $0(\alpha +_u \beta) = 0 = 0\alpha + 0\beta$, for all $\alpha, \beta \in F$.

(d) $(R_u, +)$ is a subgroup of $(V, +)$: Let $v, w \in R_u$. Then

$$\begin{aligned}(v-w)(\alpha +_u \beta) &= v(\alpha +_u \beta) + (-w)(\alpha +_u \beta) \\ &= v(\alpha +_u \beta) - w(\alpha +_u \beta) \\ &= v\alpha + v\beta - (w\alpha + w\beta) \\ &= v\alpha - w\alpha + v\beta - w\beta, \text{ since } (V, +) \text{ is abelian} \\ &= (v-w)\alpha + (v-w)\beta.\end{aligned}$$

Hence $v - w \in R_u$.

THEOREM 9:

$Q \supseteq R_uF := \{v\lambda \mid \lambda \in F, v \in R_u\}$.

Proof

Let $v\lambda \in R_uF$, where $\lambda \in F$ and $v \in R_u$. By Note 8(b), $v \in Q$. Hence by Lemma 2(c), $v\lambda \in Q$. ∎

NOTE 9:

$Q = R_uF$ only in special cases. See Section 2.6.

LEMMA 10:

Let u and v be elements of $Q\backslash\{0\}$. If $v \notin uF$ and $u\alpha + v\beta = u\alpha' + v\beta'$ $(\alpha, \beta, \alpha', \beta' \in F)$, then $\alpha = \alpha'$ and $\beta = \beta'$.

Proof

Since u and v are in Q, there exists by Lemma 2(e), $\gamma, \delta \in F$ such that $u\gamma = u\alpha - u\alpha'$ and $v\delta = v\beta' - v\beta$. But $u\alpha - u\alpha' = v\beta' - v\beta$, so $u\gamma = v\delta$. Suppose that $\delta \neq 0$. Then $v = u\gamma\delta^{-1} = u(\gamma\delta^{-1}) \in uF$, a contradiction. Thus $\delta = 0$. Hence $v\beta = v\beta'$. But $v \neq 0$, hence by (F_4), $\beta = \beta'$. But then $u\alpha = u\alpha'$, so $\alpha = \alpha'$, since $u \neq 0$. ∎

LEMMA 11:

If $v \in R_u$, $w, v + w \in Q$ and $w \notin vF$, then $w \in R_u$.

Proof

Since $v + w \in Q$, there exists for every $\alpha, \beta \in F$, a $\gamma \in F$ such that

$$(v + w)\alpha + (v + w)\beta = (v + w)\gamma.$$

Hence

$$\begin{aligned} v\alpha + v\beta + w\alpha + w\beta &= v\alpha + w\alpha + v\beta + w\beta \\ &= v\gamma + w\gamma, \end{aligned}$$

which implies that

$$v(\alpha +_u \beta) + w\alpha + w\beta = v\gamma + w\gamma. \tag{2.5}$$

But $w \in Q$, thus there exists a $\gamma' \in F$ such that $w\alpha + w\beta = w\gamma'$. Hence

$$v(\alpha +_u \beta) + w\gamma' = v\gamma + w\gamma.$$

But $w \notin vF$, so by Lemma 10,

$$\alpha +_u \beta = \gamma = \gamma'.$$

Hence $w\alpha + w\beta = w\gamma' = w\gamma = w(\alpha +_u \beta)$ by (2.5). Thus $w \in R_u$. ∎

NOTE 11:

By Note 8(d), we have that $v + w$, as in the lemma above, is an element of R_u.

THEOREM 12:

Let $Q(V)$ be the quasi-kernel of the F-group V and suppose that $u, v \in Q(V)\backslash\{0\}$ with $v \notin uF$. Then, for any $\lambda \in F\backslash\{0\}$,

$$u + \lambda v \in Q(V) \text{ if and only if } +_u = +_{v\lambda}.$$

Proof

Suppose that $u + v\lambda \in Q$. By Note 8(a), $u \in R_u$ and by Lemma 2(c), $v \in Q$ implies that $v\lambda \in Q$. Furthermore, $v \notin uF$ implies that $v\lambda \notin uF$.

To see this, suppose that $v\lambda \in uF$. Then $v\lambda = u\alpha$ for some $\alpha \in F\backslash\{0\}$. Hence $v =$

$(u\alpha)(\lambda^{-1}) = u(\alpha\lambda^{-1})$, a contradiction.

Hence by Lemma 11, $v\lambda \in R_u$. Therefore for every $\alpha, \beta \in F$,

$$\begin{aligned} v\lambda(\alpha +_u \beta) &= v\lambda\alpha + v\lambda\beta \\ &= v\lambda(\alpha +_{v\lambda} \beta). \end{aligned}$$

Hence by (F_4), since $v\lambda \neq 0$, $\alpha +_u \beta = \alpha +_{v\lambda} \beta$.

Conversely, suppose $+_u = +_{v\lambda}$. Then, for all $\alpha, \beta \in F$,

$$v\lambda(\alpha +_u \beta) = v\lambda(\alpha +_{v\lambda} \beta) = v\lambda\alpha + v\lambda\beta,$$

so $v\lambda \in R_u$. Furthermore, $u \in R_u$. Hence by Note 8(d), $u + v\lambda \in R_u$. Consequently, by Note 8(b), $u + v\lambda \in Q$. ∎

2.4 A Dependence Relation between $Q(V)$ and $2^{Q(V)}$

Let $Q = Q(V)$ be the quasi-kernel of the 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 $\lambda_i \in F (i = 1, 2, \ldots, n)$ such that

$$v = \sum_{i=1}^{n} u_i \lambda_i. \tag{2.6}$$

THEOREM 1:

Let Q be the quasi-kernel of the F-group V. Then the relation defined in (2.6) is a dependence relation between Q and 2^Q.

Proof

Since the empty cases are trivial to handle, we assume that M and N are nonempty subsets of Q. We verify that the necessary conditions hold. Refer to Definition 2.1-2.

(D_1):

Suppose $v \in M$. Then $v = v1$ with $1 \in F$. Thus $v \lhd M$.

(D_2):

Suppose that $w \triangleleft M$ and $v \triangleleft N$ for all $v \in M$. Then $w = \sum_{i=1}^{n} u_i\lambda_i$ with $\lambda_i \in F$ and $u_i \in M$, $i = 1, 2, \ldots, n$. But for every i $(1 \leq i \leq n)$, $u_i = \sum_{j=1}^{m_i} \omega_{ji}\beta_{ji}$ with $\beta_{ji} \in F$ and $\omega_{ji} \in N$ for $j = 1, 2, \ldots, m_i$. Hence

$$w = \sum_{i=1}^{n}(\sum_{j=1}^{m_i} \omega_{ji}\beta_{ji})\lambda_i = \sum_{i=1}^{n}\sum_{j=1}^{m_i} \omega_{ji}\beta_{ji}\lambda_i$$

with $\beta_{ji}\lambda_i \in F$ and $\omega_{ji} \in N$ for every i $(1 \leq i \leq n)$ and every j $(1 \leq i \leq m_i)$. Hence $w \triangleleft N$.

(D_3):

Suppose that $v \triangleleft M$ and $v \not\triangleleft M\backslash\{u\}$. Then $v = \sum_{i=1}^{n} u_i\lambda_i$ with $\lambda_i \in F$ and $u_i \in M$, $i = 1, 2, \ldots, n$. If $u \neq u_j$ for all $j = 1, 2, \ldots, n$, then $v \triangleleft M\backslash\{u\}$, a contradiction. Thus $u = u_j$ for some j $(1 \leq j \leq n)$. Hence

$$v = u_1\lambda_1 + \cdots + u_{j-1}\lambda_{j-1} + u_j\lambda_j + u_{j+1}\lambda_{j+1} + \cdots + u_n\lambda_n,$$

with $\lambda_j \neq 0$. This implies that

$$u = u_j = -u_1\lambda_1\lambda_j^{-1} - \cdots - u_{j-1}\lambda_{j-1}\lambda_j^{-1} - u_{j+1}\lambda_{j+1}\lambda_j^{-1} - \cdots - u_n\lambda_n\lambda_j^{-1} + v\lambda_j^{-1}.$$

But by (F_3), $\lambda_j^{-1} \in F$. Hence $\lambda_i\lambda_j^{-1} \in F$ for every i $(1 \leq i \leq n)$. Therefore $u \triangleleft (M\backslash\{u\}) \cup \{v\}$. ∎

NOTE 1:

By Theorem 1, the concepts and theorems of Section 2.1 are applicable to $Q(V)$.

Next we prove a very useful result that relates the definition of independence given in Section 2.1 to the well-known definition of linear independence in vector spaces.

PROPOSITION 2:

A subset M of Q is independent if and only if $\sum_{i=1}^{n} u_i\lambda_i = 0$, with $u_i \in M$ and $\lambda_i \in F$ $(i = 1, 2, \ldots, n)$, implies that $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

Proof

Suppose that $M \subseteq Q$ is independent and that $\sum_{i=1}^{n} u_i\lambda_i = 0$, with $u_i \in M$ and $\lambda_i \in F$ $(i = 1, 2, \ldots, n)$. Suppose without loss of generality that $\lambda_1 \neq 0$, then $\lambda_1^{-1} \in F$ and

$$u_1 = -u_2\lambda_2\lambda_1^{-1} - u_3\lambda_3\lambda_1^{-1} - \cdots - u_n\lambda_n\lambda_1^{-1},$$

a contradiction.

Conversely, suppose that $\sum_{i=1}^{n} u_i\lambda_i = 0$, with $u_i \in M$ and $\lambda_i \in F$ $(i = 1, 2, \ldots, n)$, implies that $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$. Suppose that M is not independent. Then there exists a finite subset M' of M which is not independent. Thus there exists a $m \in M'$ such that

$$m = u_1\lambda_1 + u_2\lambda_2 + \cdots + u_n\lambda_n,$$

with $u_i \in M'\backslash\{m\}$ and $\lambda_i \in F$ $(i = 1, 2, \ldots, n)$. This implies that

$$m1 - u_1\lambda_1 - u_2\lambda_2 - \cdots - u_n\lambda_n = 0,$$

which by hypothesis implies that $1 = 0$, a contradiction. ∎

COROLLARY 3:

For $x \in Q$, $x \neq 0, \{x\}$ is independent. ∎

NOTE 3:

(a) A subset E of Q is called a *generating system* of Q if Q depends on E, i.e. if for every $v \in Q$, there exist $\lambda_i \in F$ and $u_i \in E$, $(i = 1, 2, \ldots, n)$ such that $v = \sum_{i=1}^{n} u_i\lambda_i$.

(b) As stated at the end of Section 2.1, the dimension of Q, denoted $\dim Q$, is the cardinal number of a basis of Q.

LEMMA 4:

If $\{u_i \,|\, i \in I\}$ is a basis of Q and $\lambda_i \in F\backslash\{0\}$ for each $i \in I$, then $\{u_i\lambda_i \,|\, i \in I\}$ is a basis of Q.

Proof

Let $v \in Q$. Then since $\{u_i \,|\, i \in I\}$ is a basis of Q,

$$\begin{aligned} v &= \sum_{r=1}^{n} u_r\alpha_r \\ &= \sum_{r=1}^{n} (u_r\lambda_r)(\lambda_r^{-1}\alpha_r), \end{aligned}$$

with $\alpha_r \in F$ and $u_r \in \{u_i \mid i \in I\}$, $(1 \leq r \leq n)$. Hence Q depends on $\{u_i\lambda_i \mid i \in I\}$.
Next we show that $\{u_i\lambda_i \mid i \in I\}$ is independent. Suppose that $\sum_{j=1}^{m}(u_j\lambda_j)\alpha_j = 0$ with $\alpha_j \in F$, $u_j \in \{u_i \mid i \in I\}$ $(1 \leq j \leq m)$, then $\sum_{j=1}^{m} u_j(\lambda_j\alpha_j) = 0$. Hence by Proposition 2, $\lambda_1\alpha_1 = \lambda_2\alpha_2 = \cdots = \lambda_m\alpha_m = 0$. Therefore, since $\lambda_j \neq 0$ $(1 \leq j \leq m)$, $\alpha_j = 0$ $(1 \leq j \leq m)$. Hence again by Proposition 2, $\{u_j\lambda_j \mid j \in I\}$ is independent. ∎

2.5 Near Vector Spaces

DEFINITION 1:

An F-group (V, F) is called a *near vector space over* F if the following condition holds:

(Q_1) The quasi-kernel $Q = Q(V)$ of V generates the group $(V, +)$. ∎

NOTE 1:

(a) Every near vector space over F is a linear F-group.

(b) In a near vector space V with quasi-kernel Q, a basis of Q is called a basis of V, and we define $\dim V := \dim Q$.

(c) Every vector space is a near vector space.

(d) A nearfield F over itself is a near vector space, but in general not a vector space, of dimension one. This can be verified as follows:

Firstly, (F, F) satisfies the conditions of an F-group. Furthermore, since F is a nearfield, it has an identity e. Moreover, $e \in Q(F)$, since $e\alpha + e\beta = e(\alpha + \beta)$. Now let $x \in F$. Then $ex \in Q(F)$ by Lemma 2.3-2(c). Hence $F \subseteq Q(F)$. But $Q(F) \subseteq F$. Hence $Q(F) = F$. Therefore $Q(F)$ generates F. Clearly $\{x\}$ is a basis for (F, F), for any $x \in F$, $x \neq 0$, so $\dim F = 1$.

DEFINITION 2:

Two near vector spaces, (V, F) and (W, F) are *isomorphic* if there is a bijection $\psi : V \to W$ satisfying:

(i) $\psi(v_1 + v_2) = \psi(v_1) + \psi(v_2)$ for all $v_1, v_2 \in V$,

(ii) $\psi(v\alpha) = \psi(v)\alpha$ for all $v \in V$, $\alpha \in F$. ∎

The next theorem gives us an important example of a near vector space.

THEOREM 3:

Let $F = (F, +, \cdot)$ be a (right) nearfield and let I be a nonempty index set. Then the set

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

is a near vector space over F, if we define addition and multiplication component wise as follows:

$$(\xi_i) + (\eta_i) := (\xi_i + \eta_i)$$

and

$$(\xi_i)\lambda := (\xi_i\lambda), \tag{2.7}$$

where ξ_i, η_i and λ are elements of F and (ξ_i) is used as an abbreviation for $(\xi_i)_{i\in I}$.

Proof

First we will show that $(F^{(I)}, F)$ is an F-group:

(F_1):

(i)

$$\begin{aligned}[(\xi_i) + (\eta_i)] + (\alpha_i) &= (\xi_i + \eta_i) + (\alpha_i) \\ &= ((\xi_i + \eta_i) + \alpha_i) \\ &= (\xi_i + (\eta_i + \alpha_i)) \\ &= (\xi_i) + [(\eta_i) + (\alpha_i)].\end{aligned}$$

Thus $+$ is associative.

(ii) (0) is an element of $(F^{(I)}, +)$ and moreover, it is the identity of $(F^{(I)}, +)$ since

$$(\xi_i) + (0) = (\xi_i + 0) = (\xi_i)$$

and

$$(0) + (\xi_i) = (0 + \xi_i) = (\xi_i).$$

(iii) For each $(\xi_i) \in F^{(I)}$, $(-\xi_i) \in F^{(I)}$ and

$$(\xi_i) + (-\xi_i) = (\xi_i - \xi_i) = (0)$$

and

$$(-\xi_i) + (\xi_i) = (-\xi_i + \xi_i) = (0).$$

So $-(\xi_i) = (-\xi_i) \in F^{(I)}$.

Furthermore, F is a set of endomorphisms of $F^{(I)}$, since,

$$\begin{aligned}
[(\xi_i) + (\eta_i)]\lambda &= (\xi_i + \eta_i)\lambda \\
&= ((\xi_i + \eta_i)\lambda) \\
&= (\xi_i\lambda + \eta_i\lambda), \quad \text{since } F \text{ is a right nearfield} \\
&= (\xi_i\lambda) + (\eta_i\lambda) \\
&= (\xi_i)\lambda + (\eta_i)\lambda.
\end{aligned}$$

(F_2):

The endomorphisms $0, 1, -1$ defined by

$$(\xi_i)0 = (\xi_i 0) = (0),$$

$$(\xi_i)1 = (\xi_i 1) = (\xi_i),$$

$$(\xi_i)(-1) = (\xi_i(-1)) = (-\xi_i),$$

are elements of F.

(F_3):

F^* is a subgroup of the automorphism group of $(F^{(I)}, +)$. To see this, let $\lambda \in F^*$. Then λ is a bijection:

Let $(\xi_i)\lambda = (\eta_i)\lambda$, then $(\xi_i\lambda) = (\eta_i\lambda)$ which implies that $\xi_i\lambda = \eta_i\lambda$ for each $i \in I$ and so $(\xi_i - \eta_i)\lambda = 0$. Thus for each $i \in I$, since $\lambda \neq 0$, $\xi_i = \eta_i$, which implies that $(\xi_i) = (\eta_i)$. Thus λ is an injection.

Now let (ξ_i) be an element of $F^{(I)}$. Then since $\lambda \neq 0$, λ^{-1} exists and is an element of F. Hence $\xi_i\lambda^{-1} \in F$ for each $i \in I$. Therefore $(\xi_i\lambda^{-1}) \in F^{(I)}$. But $(\xi_i\lambda^{-1})\lambda = (\xi_i\lambda^{-1}\lambda) = (\xi_i)$. Hence λ is surjective.

Consequently F^* is a subset of the automorphism group of $(F^{(I)}, +)$. But F is a nearfield. Hence F^* is a subgroup of the automorphism group of $(F^{(I)}, +)$.

(F_4):

Let $(\xi_i)\lambda = (\xi_i)\mu$. Then $(\xi_i\lambda) = (\xi_i\mu)$, which implies that for each $i \in I$, $\xi_i\lambda = \xi_i\mu$. Suppose that $\lambda \neq \mu$. Then if there exists a $j \in I$ such that $\xi_j \neq 0$, $\xi_j^{-1} \in F$. Hence $\xi_j^{-1}\xi_j\lambda = \xi_j^{-1}\xi_j\mu$. Therefore, $\lambda = \mu$, a contradiction. Hence $\xi_i = 0$ for each $i \in I$.

Finally, we show that $Q(F^{(I)})$ generates $(F^{(I)}, +)$. Let $e_j := (\delta_{ji})_{i\in I} = (\delta_{ji})$, where δ_{ji} is the Kronecker symbol. Then, for every $\alpha, \beta \in F$,

$$\begin{aligned} e_j\alpha + e_j\beta &= (\delta_{ji}\alpha) + (\delta_{ji}\beta) \\ &= (\delta_{ji}\alpha + \delta_{ji}\beta) \\ &= (\delta_{ji}(\alpha + \beta)) \\ &= (\delta_{ji})(\alpha + \beta) \\ &= e_j(\alpha + \beta). \end{aligned}$$

Thus $\{e_j \mid j \in I\} \subseteq Q(F^{(I)})$ and since every element of $F^{(I)}$ is of the form $\sum_{j\in K} e_j\lambda_j$, with $\lambda_j \in F$ and K a finite subset of I, $Q(F^{(I)})$ generates $(F^{(I)}, +)$. ∎

DEFINITION 4:

Let F be a nearfield. Define the *kernel* of F to be the set of all distributive elements of F, i.e.

$$F_d := \{\kappa \in F \mid \kappa(\xi + \eta) = \kappa\xi + \kappa\eta \text{ for every } \xi, \eta \in F\}.$$

∎

THEOREM 5:

Let F be a nearfield. Then

(a) F_d, with the operations of F, is a division ring, and

(b) F is a left vector space over F_d.

Proof

(a) $\emptyset \neq F_d \subseteq F$ since $1 \in F_d : 1(\xi + \eta) = \xi + \eta = 1\xi + 1\eta$ for every $\xi, \eta \in F$.

Now let κ_1, κ_2 be elements of F_d and ξ, η elements of F. Then

$$\begin{aligned}(\kappa_1 - \kappa_2)(\xi + \eta) &= \kappa_1(\xi + \eta) - \kappa_2(\xi + \eta) \\ &= \kappa_1\xi + \kappa_1\eta - \kappa_2\xi - \kappa_2\eta \\ &= \kappa_1\xi - \kappa_2\xi + \kappa_1\eta - \kappa_2\eta \\ &= (\kappa_1 - \kappa_2)\xi + (\kappa_1 - \kappa_2)\eta.\end{aligned}$$

Hence $\kappa_1 - \kappa_2 \in F_d$. Therefore F_d is a subgroup of $(F, +)$. But $(F, +)$ is an abelian group so $(F_d, +)$ is an abelian group.

Furthermore, $(F_d^*, \cdot)$ is a subgroup of $(F^*, \cdot)$:

Let $\kappa \in F_d$, $\kappa \neq 0$ and consider κ^{-1}. Now

$$\begin{aligned}\kappa[\kappa^{-1}(\xi + \eta)] &= \xi + \eta \\ &= \kappa(\kappa^{-1}\xi) + \kappa(\kappa^{-1}\eta) \\ &= \kappa(\kappa^{-1}\xi + \kappa^{-1}\eta)\end{aligned}$$

which implies that

$$\kappa([\kappa^{-1}(\xi + \eta)] - [\kappa^{-1}\xi + \kappa^{-1}\eta]) = 0.$$

But $\kappa \neq 0$ thus

$$\kappa^{-1}(\xi + \eta) = \kappa^{-1}\xi + \kappa^{-1}\eta$$

so $\kappa^{-1} \in F_d$.

Moreover,

$$\begin{aligned}\kappa_1\kappa_2(\xi + \eta) &= \kappa_1(\kappa_2\xi + \kappa_2\eta) \\ &= \kappa_1(\kappa_2\xi) + \kappa_1(\kappa_2\eta) \\ &= (\kappa_1\kappa_2)\xi + (\kappa_1\kappa_2)\eta.\end{aligned}$$

Hence $\kappa_1\kappa_2 \in F_d$. Thus $(F_d^*, \cdot)$ is a subgroup of $(F^*, \cdot)$.

Finally, $(\eta + \kappa)\xi = \eta\xi + \kappa\xi$ and by definition $\kappa(\eta + \xi) = \kappa\eta + \kappa\xi$ for every $\eta, \xi, \kappa \in F_d$. Hence F_d is a division ring.

(b) Let $\xi, \eta \in F$ and $\kappa_1, \kappa_2 \in F_d$. Then

(i) $(F, +)$ is an abelian group,

(ii) $\kappa_1\xi \in F$,

(iii) $\kappa_1(\xi + \eta) = \kappa_1\xi + \kappa_1\eta$,

(iv) $(\kappa_1 + \kappa_2)\xi = \kappa_1\xi + \kappa_2\xi$,

(v) $(\kappa_1\kappa_2)\xi = \kappa_1(\kappa_2\xi)$,

(vi) $1\xi = \xi$.

Thus F is a left vector space over F_d. ∎

COROLLARY 6:

Let F be a right nearfield. Then $F = F_d$ if and only if F is a division ring.

Proof

Suppose $F = F_d$. Then F is a division ring, since by the previous theorem, F_d is a division ring.

Conversely, suppose F is a division ring. Then all elements of F are left distributive and the result follows trivially. ∎

THEOREM 7:

Consider the F-group $(F^{(I)}, F)$. Then

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

Proof

Let $\alpha, \beta \in F$ and $\kappa_i \in F_d$ for all $i \in I$. Then

$$\begin{aligned}(\kappa_i)\alpha + (\kappa_i)\beta &= (\kappa_i\alpha) + (\kappa_i\beta)\\ &= (\kappa_i\alpha + \kappa_i\beta)\\ &= (\kappa_i[\alpha + \beta])\\ &= (\kappa_i)[\alpha + \beta].\end{aligned}$$

Thus $(\kappa_i) \in Q(F^I)$. Therefore, by Lemma 2.3-2(c), $(\kappa_i)\lambda \in Q(F^{(I)})$ for any $\lambda \in F$.

Conversely, let $(\xi_i) \in Q(F^{(I)})$. If $(\xi_i) = (0)$, then $(\xi_i) = (\kappa_i)\lambda$ with $\lambda = 0$ and $\kappa_i \in F_d$ for all $i \in I$. Hence, suppose $(\xi_i) \neq (0)$, i.e. there exists an $i_0 \in I$ such that $\xi_{i_0} \neq 0$. Let $\kappa_i := \xi_i\xi_{i_0}^{-1}$ for each $i \in I$. Then $(\xi_i) = (\kappa_i)\xi_{i_0}$ and since $(\kappa_i) = (\xi_i\xi_{i_0}^{-1}) = (\xi_i)\xi_{i_0}^{-1}$ and $\xi_{i_0}^{-1} \in F$ and $(\xi_i) \in Q(F^I)$, by Lemma 2.3-2(c), $(\kappa_i) \in Q(F^{(I)})$. Thus there exists a $\gamma \in F$

such that for each $i \in I$,

$$\kappa_i\alpha + \kappa_i\beta = \kappa_i\gamma \text{ (for each } \alpha, \beta \in F). \tag{2.8}$$

But $\kappa_{i_0} = \xi_{i_0}\xi_{i_0}^{-1} = 1$. Hence, since (2.8) holds for each $i \in I$, $1\alpha + 1\beta = 1\gamma$, which implies that $\alpha + \beta = \gamma$. Thus $\kappa_i\alpha + \kappa_i\beta = \kappa_i(\alpha + \beta)$ for each $i \in I$ and all $\alpha, \beta \in F$. Consequently, $\kappa_i \in F_d$ for each $i \in I$. ∎

In the next theorem we shall show how the space $F^{(I)}$ can be characterised as an F-group. First, we need to prove the following lemma.

LEMMA 8:

Let V be a near vector space and let $B = \{u_i \mid i \in I\}$ be a basis of Q. Then each $x \in V$ is a unique linear combination of elements of B, i.e. there exists $\xi_i \in F$, with $\xi_i \neq 0$ for at most a finite number of $i \in I$, which are uniquely determined by x and B, such that

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

Proof

Let $x \in V$. By (Q_1), there exists $v_1, v_2, \ldots, v_n \in Q$ such that

$$x = \sum_{j=1}^{n} v_j.$$

Since each v_j is a linear combination of elements of B, x is also a linear combination of elements of B.

To prove the uniqueness, let

$$\sum_{i \in I} u_i\xi_i = \sum_{i \in I} u_i\xi_i'$$

with at most a finite number of the ξ_i and ξ_i' not zero and $u_i \in B$ $(i \in I)$. Since $B \subseteq Q$, $u_i \in Q$ $(i \in I)$. Hence, by Lemma 2.3-2(e), there are $\eta_i \in F$ $(i \in I)$ such that $u_i\xi_i - u_i\xi_i' = u_i\eta_i$ for all $i \in I$. But

$$\sum_{i \in I}(u_i\xi_i - u_i\xi_i') = 0,$$

showing that $\sum_{i\in I} u_i\eta_i = 0$. Thus, since B is independent, $\eta_i = 0$ for all $i \in I$. Hence for each $i \in I$,

$$u_i\xi_i - u_i\xi_i^{'} = 0$$

and so $u_i\xi_i = u_i\xi_i^{'}$. Therefore for each $i \in I$, $\xi_i = \xi_i^{'}$ since $u_i \neq 0$ for each $i \in I$. ∎

THEOREM 9:

Let F be a nearfield and V an F-near vector space. Then there exists an index set I and a bijection f: $V \to F^{(I)}$ which is homogeneous, i.e.

$$f(x\alpha) = f(x)\alpha \ \ (\alpha \in F, x \in V),$$

where $f(x)\alpha$ is defined as in (2.7).

Proof

Take any basis B of V as index set and define f by

$$f(x) = f(\sum_{u\in B} u\xi_u) := (\xi_u)_{u\in B}.$$

Then f is well defined:

Let x and y be elements of V. Then there are ξ_u $(u \in B)$ and η_u $(u \in B)$ such that $x = \sum_{u\in B} u\xi_u$ and $y = \sum_{u\in B} u\eta_u$. Suppose that $x = y$, i.e. $\sum_{u\in B} u\xi_u = \sum_{u\in B} u\eta_u$. Then by Lemma 8, $\xi_u = \eta_u$ for all $u \in B$. Hence $(\xi_u)_{u\in B} = (\eta_u)_{u\in B}$. Therefore $f(x) = f(y)$.

Next we show that f is a bijection:

Let $f(x) = f(y)$, then $f(\sum_{u\in B} u\xi_u) = f(\sum_{u\in B} u\eta_u)$, which implies that $(\xi_u)_{u\in B} = (\eta_u)_{u\in B}$. Hence $\xi_u = \eta_u$ for all $u \in B$. Therefore $x = \sum_{u\in B} u\xi_u = \sum_{u\in B} u\eta_u = y$. Hence f is injective. To show that f is surjective, let $(\xi_u)_{u\in B}$ be an element of $F^{(B)}$. Then $\xi_u \in F$ for all $u \in B$. Let $x = \sum_{u\in B} u\xi_u$. Then since V is a near vector space, $x \in V$ and $f(x) = f(\sum_{u\in B} u\xi_u) = (\xi_u)_{u\in B}$.

Finally, we show that f is homogeneous:

Let $x \in V$, then there are ξ_u $(u \in B)$ such that $x = \sum_{u \in B} u\xi_u$. Hence

$$\begin{aligned} f(x\alpha) &= f((\textstyle\sum_{u \in B} u\xi_u)\alpha) \\ &= f(\textstyle\sum_{u \in B} u(\xi_u\alpha)) \\ &= (\xi_u\alpha) \\ &= (\xi_u)\alpha \\ &= f(x)\alpha. \end{aligned}$$

■

NOTE 9:

Let $\{u_i \,|\, i \in I\}$ be a basis of Q and let f be as defined in Theorem 9. Then $f(u_i) = (\delta_{ij})_{j \in I} := e_j$ where δ_{ij} is the Kronecker symbol.

For further investigation of the structure of near vector spaces, we need the following relation.

DEFINITION 10:

The elements u and v of $Q\backslash\{0\}$ are called *compatible* (u cp v), if there is a $\lambda \in F\backslash\{0\}$ such that $u + v\lambda \in Q$. ■

LEMMA 11:

The elements u and v of $Q\backslash\{0\}$ are compatible if and only if there exists a $\lambda \in F\backslash\{0\}$ such that $+_u = +_{v\lambda}$.

Proof

If $v \notin uF$, the result follows immediately from Theorem 2.3-12. Suppose now that $v \in uF$, i.e. $v = u\alpha$ for an $\alpha \in F\backslash\{0\}$. Then the following two statements hold simultaneously:

(i)

$$u \text{ cp } u\alpha \tag{2.9}$$

since by Lemma 2.3-2(d), $u1 + u\alpha\lambda \in Q$ for each $\lambda \in F$.

(ii) $+_u = +_{v\lambda}$, since $v\lambda = u\alpha\alpha^{-1} = u$ if we take $\lambda = \alpha^{-1}$. ■

THEOREM 12:

The compatibility relation cp is an equivalence relation on $Q\backslash\{0\}$.

Proof

(i) Reflexivity:

u cp u since by Lemma 2.3-2(d), $u + u\lambda \in Q$ for any $u \in Q$.

(ii) Symmetry:

Let $u, v \in Q\backslash\{0\}$ and suppose u cp v. Then there exists a $\lambda \in F\backslash\{0\}$ such that $u+v\lambda \in Q$. Hence by Lemma 2.3-2(c), $(u + v\lambda)\lambda^{-1} = u\lambda^{-1} + v = v + u\lambda^{-1} \in Q$. Hence v cp u.

(iii) Transitivity:

Let $u, v, w \in Q$ and suppose u cp v and v cp w. Then by Lemma 10, $+_u = +_{v\lambda}$ and $+_v = +_{w\mu}$ for certain $\lambda, \mu \in F\backslash\{0\}$. It suffices to show that $+_u = +_{w\eta}$ for some $\eta \in F\backslash\{0\}$. Now

$$\begin{aligned} \alpha +_u \beta &= \alpha +_{v\lambda} \beta \\ &= (\alpha^\lambda +_v \beta^\lambda)^{\lambda^{-1}} \text{ (by (2.4))} \\ &= (\alpha^\lambda +_{w\mu} \beta^\lambda)^{\lambda^{-1}} \\ &= \alpha +_{w\mu\lambda} \beta \\ &= \alpha +_{w\eta} \beta, \text{ where } \eta = \mu\lambda \in F\backslash\{0\}. \end{aligned}$$

Hence by Lemma 10, u cp w. ∎

THEOREM 13:

Let u, v and $u + v$ be elements of $Q\backslash\{0\}$. Then

(a) u cp v, and

(b) u cp $u + v$.

Proof

(a) Since $u + v$ is an element of Q, u cp v follows from Definition 10 by putting $\lambda = 1$.

(b) If $v = u\alpha$ with $\alpha \in F\backslash\{0\}$, then u cp $u + v$ since $u + (u + v)1 = u + (u + u\alpha)1 \in Q$ by Lemma 2.3-2(d).

If $v \notin uF$, then by Lemma 2.3-15, $u+v \in R_u$. Hence by Note 2.3-8, $u+(u+v) \in R_u \subseteq Q$. Therefore u cp $u + v$. ∎

DEFINITION 14:

A near vector space V is called a *regular near vector space* if the following condition holds:

(Q_2) Any two vectors of $Q\backslash\{0\}$ are compatible. ∎

THEOREM 15:

A near vector space V is regular if and only if there exists a basis which consists of mutually pairwise compatible vectors.

Proof

Suppose V is regular. Then, by definition, any two vectors of $Q\backslash\{0\}$ are compatible. Therefore, every basis of Q (by Note 1(b) also of V) consists of mutually pairwise compatible vectors.

Conversely, let V be a near vector space with a basis B consisting of mutually pairwise compatible vectors. Let $u \in Q\backslash\{0\}$. Then by Lemma 8, u can be written as a linear combination of basis elements. Therefore, without loss of generality, suppose $u = \sum_{i=1}^{r} u_i\lambda_i$ with $u_i \in B$ and $\lambda_i \neq 0$ for all $i \in \{1, 2, \ldots, r\}$. Let

$$u' = \begin{cases} \sum_{i=1}^{r-1} u_i\lambda_i & \text{if } r > 1 \\ 0 & \text{if } r = 1. \end{cases}$$

Then $u = u' + u_r\lambda_r \in Q$. Hence, for every $\alpha, \beta \in F$, there exists a $\xi \in F$ such that

$$\begin{aligned} (u' + u_r\lambda_r)\alpha + (u' + u_r\lambda_r)\beta &= u\alpha + u\beta \\ &= u\xi \\ &= (u' + u_r\lambda_r)\xi. \end{aligned}$$

Hence $u'\alpha + u_r\lambda_r\alpha + u'\beta + u_r\lambda_r\beta = u'\xi + u_r\lambda_r\xi$, and therefore $u'\alpha + u'\beta + u_r\lambda_r\alpha + u_r\lambda_r\beta = u'\xi + u_r\lambda_r\xi$. But $u_r \notin \{u_1, u_2, \ldots, u_{r-1}\}$. Hence, by uniqueness (Lemma 8), $u_r\lambda_r\alpha + u_r\lambda_r\beta = u_r\lambda_r\xi$. Therefore $u'\alpha + u'\beta = u'\xi$ which implies that $u' \in Q$.

Now we will show that u and u_r are compatible:

If $u' = 0$ then $u = u_r\lambda_r$ and hence by (2.9), u_r cp $u_r\lambda_r$.

If $u' \neq 0$, then by Theorem 13, $u_r\lambda_r$ cp u since u', $u_r\lambda_r$ and $u = u' + u_r\lambda_r = u_r\lambda_r + u'$ are elements of Q. But, by (2.9), u_r cp $u_r\lambda_r$. Consequently, by Theorem 12, u_r cp u.

But, by assumption, u_r is compatible with every other vector of B. Therefore, it follows from the transitivity of cp (Theorem 12), that u is compatible with every other vector of

B. But $u \in Q\backslash\{0\}$ was arbitrarily chosen. Thus if $v, w \in Q\backslash\{0\}$ then v cp u_i and w cp u_i with $u_i \in B$. Hence again, by Theorem 12, v cp w. Thus every two elements of $Q\backslash\{0\}$ are compatible. Consequently, V is regular. ∎

LEMMA 16:

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

Proof

Suppose that $w \in Q(W)$. Then for each $\alpha, \beta \in F$, there exists a $\gamma \in F$, such that

$$w\alpha + w\beta = w\gamma.$$

But W is a subspace of V, so $w \in V$ and by the above equation, $w \in Q(V)$. Thus $Q(W) \subseteq W \cap Q(V)$.

Now suppose $w \in W \cap Q(V)$. Then, since $w \in Q(V)$, for each $\alpha, \beta \in F$, there exists a $\gamma \in F$, such that

$$w\alpha + w\beta = w\gamma,$$

but $w \in W$, so by the above equation, $w \in Q(W)$. Thus $W \cap Q(V) \subseteq Q(W)$. ∎

THEOREM 17: (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 $u \in Q\backslash\{0\}$ lies in precisely one direct summand V_j. The subspaces V_j are maximal regular near vector spaces.

Proof

(i) First we will show that V is the direct sum of regular near vector spaces V_j $(j \in J)$.

We start by partitioning $Q\backslash\{0\}$ into sets Q_j $(j \in J)$ of mutually pairwise compatible vectors. This is possible by Theorem 12. Furthermore, let $B \subseteq Q\backslash\{0\}$ be a basis of V and let $B_j := B \cap Q_j$. By our partitioning, the B_j's are disjoint and clearly each B_j is an independent set of B. Furthermore, $B = \cup_{j\in J} B_j$:

We know that $Q\backslash\{0\} = \cup_{j\in J} Q_j$, so

$$\cup_{j\in j} B_j = \cup_{j\in j}(B \cap Q_j) = B \cap (\cup_{j\in j} Q_j) = B \cap (Q\backslash\{0\}) = B.$$

Now let $B = \{b_i \,|\, i \in I\}$ with I an index set. Since $B = \cup_{j\in J} B_j$ with the B_j's mutually disjoint, for each $i \in I$, $b_i \in B_j$ for some $j \in J$. Let $I_j = \{i \in I \,|\, b_i \in B_j\}$. Then for each $j \in J$, $B_j = \{b_{ij} := b_i \,|\, i \in I_j\}$, and $I = \cup_{j\in J} I_j$. Let $V_j := \langle B_j \rangle$ be the subspace of V generated by B_j. By Theorem 15, V_j is regular since B_j ($\subseteq Q_j$) consists of mutually pairwise compatible vectors. Let $x \in V$. Then by Lemma 8, $x = \sum_{i\in I} b_i\eta_i$ with $b_i \in B$ and $\eta_i \neq 0$ for at most a finite number of $i \in I$. Hence $x = \sum_{j\in J}(\sum_{i\in I_j} b_{ij}\eta_{ij})$ with $b_{ij} \in B_j$ and $\eta_{ij} = \eta_i$ if $b_i \in B_j$. Moreover, since $V_j = \langle B_j \rangle$, there is an $x_j \in V_j$ such that $x_j = \sum_{i\in I_j} b_{ij}\eta_{ij}$. Hence

$$x = \sum_{j\in J} x_j. \tag{2.10}$$

By Lemma 8, $x = \sum_{i\in I} b_i\eta_i$ can be written in a unique way. If we apply the same lemma to the near vector space V_j with basis B_j for all $j \in J$, then for each $j \in J$ there exists a unique $x_j \in V_j$ which corresponds to $\sum_{i\in I_j} b_{ij}\eta_{ij}$. Hence $x = \sum_{j\in J} x_j$ is uniquely determined. Thus $V = \oplus_{j\in J} V_j$.

(ii) Next we will show that each $u \in Q\backslash\{0\}$ lies in precisely one direct summand V_j. Suppose that there exist elements in $Q\backslash\{0\}$ which are not elements of V_j for any $j \in J$. Let u be such an element with the least possible number of summands in the decomposition given by (2.10), i.e. let

$$u = \sum_{j\in J} u_j, \tag{2.11}$$

with $u_j \in V_j$ ($j \in J$) and with the number of $u_j \neq 0$ ($j \in J$) as small as possible. Since $u \in Q$, for every $\alpha, \beta \in F$ there exists a $\delta \in F$ such that $u\alpha + u\beta = u\delta$. But

$$\begin{aligned} u\alpha + u\beta &= (\textstyle\sum_{j\in J} u_j)\alpha + (\sum_{j\in J} u_j)\beta \\ &= \textstyle\sum_{j\in J} u_j\alpha + \sum_{j\in J} u_j\beta \\ &= \textstyle\sum_{j\in J}(u_j\alpha + u_j\beta) \end{aligned}$$

and

$$\begin{aligned} u\delta &= (\textstyle\sum_{j\in J} u_j)\delta \\ &= \textstyle\sum_{j\in J} u_j\delta. \end{aligned}$$

Hence $\sum_{j\in J}(u_j\alpha + u_j\beta) = \sum_{j\in J} u_j\delta$. But since $\oplus_{j\in J} V_j$ is a direct sum, $V_i \cap V_j = \{0\}$ for $i \neq j$. Hence $u_j\alpha + u_j\beta = u_j\delta$ for all $j \in J$. This implies that $\sum_{j\in J'}(u_j\alpha + u_j\beta) =$

$\sum_{j\in J'} u_j\delta$ for all $J' \subseteq J$. Hence

$$(\sum_{j\in J'} u_j)\alpha + (\sum_{j\in J'} u_j)\beta = (\sum_{j\in J'} u_j)\delta \text{ for all } J' \subseteq J. \tag{2.12}$$

Consequently,

$$u' := \sum_{j\in J'} u_j \in Q \ (u' \neq 0). \tag{2.13}$$

Let J_u be the set of all $j \in J$ for which $u_j \neq 0$ in the decomposition (2.11). Since J_u is finite and $u \notin V_j$ for some $j \in J$, $|J_u| > 1$. Furthermore, by the definition of u, $|J_{u^*}| \geq |J_u|$ for all $u^* \in Q\backslash \cup_{j\in J} V_j$. Next we will show that if $J' \subseteq J$ such that $J_u \cap (J\backslash J') \neq \emptyset$, then $|J_{u'}| = 1$ with u' as defined in (2.13). To see this, suppose that $|J_{u'}| > 1$ (Note: $|J_{u'}| \neq 0$ since $u' \neq 0$). Then $u' = u_{j_1} + u_{j_2} + \cdots + u_{j_n}$ with $n > 1$ and $J_{u'} = \{j_1, j_2, \ldots, j_n\}$. Then $u' \notin V_{j_i}$ with $j_i \in J'$ since $u' \in V_{j_i}$ implies that $u' - u_{j_i} \in V_{j_i} \cap \oplus_{j\in J\backslash\{j_i\}} V_j = \{0\}$. But then $u' = u_{j_i}$ and $u_{j_i} \in V_{j_i}$, so $u' \in V_{j_i}$, a contradiction. Moreover, $u' \notin V_{j'}$ with $j' \in J\backslash J'$, since $u' \in V_{j'}$ implies that $u' \in V_{j'} \cap \oplus_{j\in J\backslash\{j'\}} V_j = \{0\}$, a contradiction. Hence $u' \notin \cup_{j\in J} V_j$. Thus $u' \in Q\backslash \cup_{j\in J} V_j$. Hence $|J_{u'}| \geq |J_u|$. However, this is contradictory to our assumption that J' $(\subseteq J)$ is such that $J_u \cap (J\backslash J') \neq \emptyset$. Hence $J_{u'} = \{j'\}$ for some $j' \in J$. Also $|J_{u-u'}| = 1$. To see this, suppose $|J_{u-u'}| = m$ with $m > 1$ (Note: $|J_{u-u'}| \neq 0$ since $J_u \cap (J\backslash J') \neq \emptyset$). Then $u - u' = u_{j_1} + u_{j_2} + \cdots + u_{j_m}$. As shown in the above paragraph, $u - u' \notin \cup_{j\in J} V_j$. Furthermore, by (2.12), $u - u' \in Q$. Hence $u - u' \in Q\backslash \cup_{j\in J} V_j$. Therefore, $|J_{u-u'}| \geq |J_u|$. This contradicts $J_{u'} = \{j'\}$. Hence $J_{u-u'} = \{j''\}$ for some $j'' \in J$, with $j'' \neq j'$. [If $j := j' = j''$, then $u' = u_j$ and $u - u' = u_j$. Hence $u = 2u_j \in V_j$, a contradiction.] We therefore obtain the following:

$$u = u' + (u - u') \tag{2.14}$$

with $u' \in V_{j'}$ and $u - u' \in V_{j''}$. But $u' \in Q$ and $u - u' \in Q$. Hence $u' \in Q \cap V_{j'} =: Q_{j'}$ and $u - u' \in Q \cap V_{j''} =: Q_{j''}$. But u' cp $u - u'$ (see (2.14)). Thus $j' = j''$, a contradiction. Therefore $Q \subseteq \cup_{j\in J} V_j$. Hence each $u \in Q\backslash\{0\}$ is contained in at least one V_j and since $V_j \cap V_{j'} = \{0\}$ for $j \neq j'$, each u is contained in precisely one V_j.

(iii) Finally we show that the subspaces V_j $(j \in J)$ are maximal regular near vector spaces.

Suppose to the contrary that there exists a $j_0 \in J$ such that $V_{j_0} \subset W$ with W a regular subspace of V. Suppose that $Q(V_{j_0}) = Q(W)$. Then since V_{j_0} is generated by $Q(V_{j_0})$ and W is generated by $Q(W)$, $V_{j_0} = W$, which is contrary to our assumption. Hence, there exists a $u \in Q \cap (W \backslash V_{j_0})$ (Lemma 16). Since $u \in Q \backslash \{0\}$, $u \in V_j$ for some $j \in J \backslash \{j_0\}$. But W is regular, so since $V_{j_0} \subset W$, u is compatible with each $v \in Q(V_{j_0}) \backslash \{0\}$. This contradicts the fact that $j \neq j_0$. ∎

THEOREM 18: (The Uniqueness Theorem)

There exists only one direct decomposition of a near vector space into maximal regular near subspaces.

Proof

The existence of such a decomposition was shown in the previous theorem. Now to show the uniqueness, let

$$V = \oplus_{j \in J} V_j = \oplus_{j' \in J'} V'_{j'} \tag{2.15}$$

be two direct decompositions of V in maximal regular subspaces V_j $(j \in J)$ and $V'_{j'}$ $(j' \in J')$ respectively. Furthermore let $Q_j := (Q(V) \backslash \{0\}) \cap V_j$ $(j \in J)$. By (Q_1), $V_j = \langle Q_j \rangle$ for each $j \in J$. Now each two vectors in Q_j, are, by (Q_2), compatible. But Q_j is not properly contained in a set of mutually compatible vectors. This can be shown as follows: Suppose that, for some $j \in J$, there exists a $u \in Q(V) \backslash Q_j$ such that u cp v for all $v \in Q_j$. Let $Q(W_j) \backslash \{0\}$ be the equivalence class (with respect to cp), with $u \in Q(W_j) \backslash \{0\}$. Then $Q_j \subset Q(W_j) \backslash \{0\}$. Let $W_j := \langle Q(W_j) \backslash \{0\} \rangle$. Then W_j is regular since any two elements of $Q(W_j) \backslash \{0\}$ are compatible. But $V_j \subset W_j$, which contradicts the maximality of V_j. Moreover, every $V'_{j'}$ $(j' \in J')$ is maximal regular and so $Q'_{j'}$ is not properly contained in a set of mutually compatible vectors, and therefore corresponds to a Q_j $(j \in J)$. Hence $Q_j \subseteq V'_{j'}$ and therefore $V_j \subseteq V'_{j'}$. But V_j is maximal regular and so $V_j = V'_{j'}$. Therefore $\{V_j \,|\, j \in J\} \subseteq \{V'_{j'} \,|\, j' \in J'\}$. By symmetry, $\{V'_{j'} \,|\, j' \in J'\} \subseteq \{V_j \,|\, j \in J\}$. Consequently, $\{V'_{j'} \,|\, j' \in J'\} = \{V_j \,|\, j \in J\}$. ∎

DEFINITION 19:

The uniquely determined direct decomposition of a near vector space V into maximal

regular subspaces, is called the *canonical* direct decomposition of V. ∎

THEOREM 20:

A direct decomposition

$$V = \oplus_{j\in J} V_j \tag{2.16}$$

of a near vector space V into regular subspaces V_j $(j \in J)$ is canonical if and only if

$$Q \subseteq \cup_{j\in J} V_j. \tag{2.17}$$

Proof

Suppose that a direct decomposition $V = \oplus_{j\in J} V_j$ of a near vector space V into regular subspaces V_j $(j \in J)$ is canonical. By Theorem 18 such a decomposition is unique and in the proof of Theorem 17 it is shown that $Q \subseteq \cup_{j\in J} V_j$.

Conversely, suppose that $Q \subseteq \cup_{j\in J} V_j$. Furthermore, assume that there exists a V_{j_0} in (2.16) which is not maximal regular, i.e. $V_{j_0} \subset W$, where by Zorn's Lemma, we can assume, without loss of generality, that W is maximal regular in V. Then there exists an $x \in Q(V) \cap (W \backslash V_{j_0})$ (see the proof of Theorem 17). By (2.17) there exists a $j_1 \in J$ such that $x \in V_{j_1}$ and $j_1 \neq j_0$. Also, $V_{j_1} + W$ is regular:

To see this let $u \in V_{j_1} \cap W$ and $u \in Q(V)\backslash\{0\}$. Then for any $v \in V_{j_1} \cap (Q(V)\backslash\{0\})$, u and v are compatible since V_{j_1} is regular. Similarly, u and w are compatible for any $w \in W \cap (Q(V)\backslash\{0\})$. By Theorem 12, v and w are compatible. Hence any two vectors of $((Q(V)\backslash\{0\} \cap V_{j_1}) \cup ((Q(V)\backslash\{0\}) \cap W))$ are compatible. But $((Q(V)\backslash\{0\} \cap V_{j_1}) \cup ((Q(V)\backslash\{0\}) \cap W))$ generates $V_{j_1} + W$. Hence $V_{j_1} + W$ contains a basis B such that $B \subseteq ((Q(V)\backslash\{0\} \cap V_{j_1}) \cup ((Q(V)\backslash\{0\}) \cap W))$. Therefore by Theorem 15, $V_{j_1} + W$ is regular.

Since W is maximal regular, $V_{j_1} + W = W$. Hence $V_{j_1} \subseteq W$ and $V_{j_0} + V_{j_1} \subseteq W$. For $u_k \in V_{j_k} \cap (Q(V)\backslash\{0\}$ $(k = 0, 1)$, there exists a $\lambda \in F\backslash\{0\}$ such that $u_0 + u_1\lambda \in Q(V)\backslash\{0\}$ since $u_0, u_1 \in W \cap (Q(V)\backslash\{0\})$. By (2.17), there exists a $j_2 \in J$ such that

$$u_0 + u_1\lambda \in V_{j_2}\backslash\{0\}. \tag{2.18}$$

Since $u_0 + u_1\lambda \notin V_{j_0}$ and $u_0 + u_1\lambda \notin V_{j_1}$, $V_{j_2} \neq V_{j_0}$ and $V_{j_2} \neq V_{j_1}$. Hence by the direct sum decomposition (2.16), $(V_{j_0} + V_{j_1}) \cap V_{j_2} = \{0\}$. This, however, contradicts (2.18). Consequently, every V_j in (2.16) is maximal. ∎

THEOREM 21:

Let V be a near vector space with quasi-kernel Q. If $u \in Q\backslash\{0\}$, $x \in V\backslash uF$ and

$$u\alpha + x\beta = u\alpha^{'} + x\beta^{'} \ (\alpha, \beta, \alpha^{'}, \beta^{'} \in F), \tag{2.19}$$

then $\alpha = \alpha^{'}$ and $\beta = \beta^{'}$.

Proof

Let $u =: u_0$. Extend {u} to a basis B of Q (See Theorem 2.1-11). By Lemma 8 there exists a linear combination $x = \sum_{i=0}^{r} u_i\eta_i$, $\eta_i \in F$, $u_i \in B$ $(0 \leq i \leq r)$. Since $x \notin uF$, we can take $\eta_1 \neq 0$ without loss of generality [If $\eta_i = 0$ for $1 \leq i \leq r$, then $x = u_0\eta_0 \in uF$]. By (2.19):

$$u_0\alpha + (\sum_{i=0}^{r} u_i\eta_i)\beta = u_0\alpha^{'} + (\sum_{i=0}^{r} u_i\eta_i)\beta^{'}.$$

This implies that

$$u_0(\alpha +_{u_0} \eta_0\beta) + \sum_{i=1}^{r} u_i\eta_i\beta = u_0(\alpha^{'} +_{u_0} \eta_0\beta^{'}) + \sum_{i=1}^{r} u_i\eta_i\beta^{'}.$$

Hence, as a result of the uniqueness of this representation (Lemma 8), $\alpha +_{u_0} \eta_0\beta = \alpha^{'} +_{u_0} \eta_0\beta^{'}$ and $\eta_1\beta = \eta_1\beta^{'}$. Since $\eta_1 \neq 0$, by (F_4), $\beta = \beta^{'}$. Therefore since $\alpha +_{u_0} \eta_0\beta = \alpha^{'} +_{u_0} \eta_0\beta^{'}$, we also have $\alpha = \alpha^{'}$. ∎

2.6 The Structure of Regular Near Vector Spaces

THEOREM 1:

A near vector space V is regular if and only if

$$Q = \{v\lambda \,|\, \lambda \in F, v \in R_u\} =: R_uF, \tag{2.20}$$

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

Proof

Let V be a regular near vector space and let $u, v \in Q\backslash\{0\}$. There are two cases to consider:

Case 1:

Suppose that $v \in uF$, i.e. $v = u\lambda$ for a $\lambda \in F$. Then $v \in R_uF$ since $u \in R_u$.

Case 2:

Suppose that $v \notin uF$. Then since V is regular and $u, v \in Q\backslash\{0\}$, u cp v. Hence there exits a $\lambda \in F\backslash\{0\}$ such that $u + v\lambda \in Q$. Then since $u \in R_u$, $v\lambda \in Q$, $v\lambda \notin uF$ and $u + v\lambda \in Q$, by Lemma 2.3-11 , $v\lambda \in R_u$. Hence $v \in R_uF$ ($v\lambda\lambda^{-1} \in R_uF$).

Therefore in both cases, $Q \subseteq R_uF$, but by Theorem 2.3-9, $R_uF \subseteq Q$, so $Q = R_uF$.

Conversely, suppose that (2.20) holds for a $u \in Q\backslash\{0\}$. Then for each $v \in Q\backslash\{0\}$, there exists a $v_0 \in R_u$ and $\alpha \in F\backslash\{0\}$ such that $v = v_0\alpha$. Since $u, v_0 \in R_u$ it follows by Note 2.3-8(b) that $u + v_0 = u + v\alpha^{-1} \in R_u \subseteq Q$. Hence u cp v. But v was arbitrarily chosen so $Q\backslash\{0\}$ has only one equivalence class with respect to cp. Hence V is regular. ∎

THEOREM 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 nearfield and V is isomorphic to $F^{(I)}$, for some index set I, as defined in Theorem 2.5-3.

Proof

Suppose F is a nearfield and let I be a nonempty index set. By Theorem 2.5-3,

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

is a near vector space with addition and multiplication defined by $(\xi_i) + (\eta_i) := (\xi_i + \eta_i)$ and $(\xi_i)\lambda := (\xi_i\lambda)\,(\lambda, \xi_i, \eta_i \in F)$. Now suppose V and $F^{(I)}$ are isomorphic. Then, without loss of generality, we can take V to be equal to $F^{(I)}$. By Definition 2.5-4,

$F_d := \{\kappa \in F \,|\, \kappa(\xi + \eta) = \kappa\xi + \kappa\eta \text{ for every } \xi, \eta \in F\}$ is the kernel of F. Moreover, by Theorem 2.5-7, $Q(F^{(I)}) = \{(\kappa_i)_{i\in I}\lambda \,|\, \lambda \in F, \kappa_i \in F_d\}$. Hence $Q(F^{(I)}) = RF$ where $R := \{(\kappa_i) \,|\, \kappa_i \in F_d\}$. Now $R_{e_j} = \{(\xi_i) \in F^{(I)} \,|\, (\xi_i)(\alpha +_{e_j} \beta) = (\xi_i)\alpha + (\xi_i)\beta \text{ for every } \alpha, \beta \in F\}$

is the kernel of the linear F-group $(F^{(I)}, F)$ with respect to $e_j := (\delta_{ji})_{i\in I}$, where δ_{ji} is the Kronecker symbol.

We will show that $R_{e_j} = R$.

Let $(\kappa_i) \in R$. For R to be a subset of R_{e_j}, it suffices to show that $(\kappa_i)(\alpha +_{e_j} \beta) = (\kappa_i)\alpha + (\kappa_i)\beta$ for every $\alpha, \beta \in F$.

First we show that $+_{e_j} = +$.

Let α, β be any two elements of F. Then

$$e_j\alpha + e_j\beta = e_j(\alpha + \beta).$$

Furthermore, by Definition 2.3-4,

$$e_j\alpha + e_j\beta = e_j(\alpha +_{e_j} \beta).$$

Hence $\alpha + \beta = \alpha +_{e_j} \beta$. Finally,

$$\begin{aligned}(\kappa_i)\alpha + (\kappa_i)\beta &= (\kappa_i\alpha) + (\kappa_i\beta)\\ &= (\kappa_i\alpha + \kappa_i\beta)\\ &= (\kappa_i(\alpha + \beta))\\ &= (\kappa_i)(\alpha + \beta)\\ &= (\kappa_i)(\alpha +_{e_j} \beta).\end{aligned}$$

Thus $(\kappa_i) \in R_{e_j}$, implying that $R \subseteq R_{e_j}$.

Now let $(\xi_i) \in R_{e_j}$. Then for every $\alpha, \beta \in F$,

$$(\xi_i)(\alpha +_{e_j} \beta) = (\xi_i)\alpha + (\xi_i)\beta,$$

which implies that

$$(\xi_i)(\alpha + \beta) = (\xi_i)\alpha + (\xi_i)\beta.$$

Therefore $(\xi_i(\alpha + \beta)) = (\xi_i\alpha) + (\xi_i\beta) = (\xi_i\alpha + \xi_i\beta)$. Hence, for each $i \in I$,

$$\xi_i(\alpha + \beta) = \xi_i\alpha + \xi_i\beta.$$

This implies that $\xi_i \in F_d$ for each $i \in I$. Thus $(\xi_i) \in R$. Therefore $R_{e_j} \subseteq R$.

Consequently, $R_{e_j} = R$. Hence $Q = RF = R_{e_j}F$. Therefore, by Theorem 1, V is regular.

Conversely, let V be a regular near vector space. Then by Note 2.5-1(a), V is a linear F-group. Now let $B = \{u_i \,|\, i \in I\}$ be a basis of Q. Then by Theorem 1, there exist $\lambda_i \in F\backslash\{0\}$ $(i \in I)$ such that $v_i := u_i\lambda_i \in R_{u_o}$ for a $u_o \in B$. Hence, by Lemma 2.4-4, $B' := \{v_i \,|\, i \in I\} \subseteq R_{u_o}$ is a basis of V. Moreover, by Theorem 2.3-5, $(F, +_{u_o}, \cdot)$ is a nearfield. Define $f : V \to F^{(I)}$ by $f(x) := (\xi_i)_{i\in I}$. Then f is well defined:
Let $x = \sum_{i\in I} v_i\xi_i$ and $y = \sum_{i\in I} v_i\eta_i$ be elements of V. Suppose $x = y$. Then $\sum_{i\in I} v_i\xi_i = \sum_{i\in I} v_i\eta_i$. As a result of the uniqueness of the representation (Lemma 2.5-8), $\xi_i = \eta_i$ for each $i \in I$. Hence $(\xi_i) = (\eta_i)$ and thus $f(x) = f(y)$.
Secondly, f respects operations, i.e.

$$\begin{aligned}(i) f(x+y) &= f(\textstyle\sum_{i\in I} v_i\xi_i + \sum_{i\in I} v_i\eta_i)\\ &= f(\textstyle\sum_{i\in I} v_i(\xi_i +_{u_o} \eta_i))\\ &= (\xi_i +_{u_o} \eta_i)\\ &= (\xi_i) +_{u_o} (\eta_i)\\ &= f(x) +_{u_o} f(y).\end{aligned}$$

$$\begin{aligned}(ii) f(x)\lambda &= (f(\textstyle\sum_{i\in I} v_i\xi_i))\lambda\\ &= (\xi_i)\lambda\\ &= (\xi_i\lambda)\\ &= f(\textstyle\sum_{i\in I} v_i(\xi_i\lambda))\\ &= f((\textstyle\sum_{i\in I} v_i\xi_i)\lambda)\\ &= f(x\lambda).\end{aligned}$$

Finally we show that f is a bijection:
Let $f(x) = f(y)$. Then $f(\sum_{i\in I} v_i\xi_i) = f(\sum_{i\in I} v_i\eta_i)$ which implies that $(\xi_i) = (\eta_i)$. Hence $\xi_i = \eta_i$ for each $i \in I$. Therefore $\sum_{i\in I} v_i\xi_i = \sum_{i\in I} v_i\eta_i$, so $x = y$ and f is injective. Finally, to show that f is surjective, let $(\xi_i)_{i\in I}$ be an element of $F^{(I)}$. Put $x = \sum_{i\in I} v_i\xi_i$. Then $x \in V$ since $\xi_i \neq 0$ for at most a finite number of $i \in I$ and B' is a basis of V. Moreover, $f(x) = f(\sum_{i\in I} v_i\xi_i) = (\xi_i)_{i\in I}$. ∎

THEOREM 3:

Let (V, F) be a near vector space with $\dim V > 1$. Then F is a division ring and V a

vector space over F, if and only if $V = Q$.

Proof

Suppose F is a division ring and V a vector space over F. We have that $Q \subseteq V$. Let $v \in V$ and $\alpha, \beta \in F$, then $v\alpha + v\beta = v(\alpha + \beta)$. Hence $v \in Q$, so $Q = V$.

Conversely, suppose that $V = Q$ and that $\dim V > 1$, i.e. $\dim Q > 1$. Then there exists a $u \in Q\backslash\{0\}$. We will show that $Q = R_u$. If $v \in Q\backslash uF$, then by Lemma 2.3-11, $v \in R_u$. Therefore, suppose that $v \in uF\backslash\{0\}$. Then, since $\dim V > 1$, there exists a $w \in Q\backslash uF$. Hence by Lemma 2.3-11, $w \in R_u$. But since $v \notin wF$ ($v = w\lambda$ implies that $w = v\lambda^{-1} \in uF$) it follows, by Lemma 2.3-11, that $v \in R_u$. Hence

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

Therefore $v(\alpha +_u \beta) = v\alpha + v\beta$ for all $v \in V$. Hence $\alpha +_u \beta = \alpha + \beta$. This implies that for all $\alpha, \beta \in F$ and each $v \in V$,

$$v(\alpha + \beta) = v\alpha + v\beta. \tag{2.21}$$

Therefore, for each $x \in V$, $x\gamma(\alpha + \beta) = x\gamma\alpha + x\gamma\beta = x(\gamma\alpha + \gamma\beta)$. Hence, by (F_4),

$$\gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta. \tag{2.22}$$

Now since $Q = R_u$, by Theorem 1, V is regular. If we now apply Theorem 2, we have that F is a nearfield. This together with (2.22) shows that F is a division ring. Finally, by (2.21), V is a vector space over F. ∎

NOTE 3:

(a) Theorem 3 does not hold when $\dim V = 1$. This can be shown as follows:

Let (V, F) be any near vector space of dimension one, i.e. Q is of dimension one. Let $\{v_0\}$ be a basis of Q and let $v \in V$. Then $v = v_0\lambda$ for some $\lambda \in F$. Hence, by Lemma 2.3-2(c), $v \in Q$. Hence $Q = V$. Therefore, if Theorem 3 holds for $\dim V = 1$, the fact that $Q = V$ would imply that every near vector space of dimension one is a vector space. This contradicts Note 2.5-1(d).

(b) In Theorem 3 it is sufficient to require that (V, F) is an F-group. Indeed, if $V = Q$, then Q generates V and hence, by definition, (V, F) is a near vector space.

Chapter 3

Examples of Near Vector Spaces

A vector space and a nearfield over itself are examples of near vector spaces which have already been given (see Note 2.5-1). In this chapter we shall give further examples of near vector spaces which are not vector spaces.

Each example (V, F) is divided into five parts. First, we shall show that (V, F) is an F-group. Its quasi-kernel $Q(V)$ will then be investigated. Furthermore, we shall define $+_u$ on F for each $u \in Q(V)\backslash\{0\}$, after which the kernel R_u of (V, F) will be determined for some $u \in Q(V)\backslash\{0\}$. Finally, we shall show that (V, F) is a near vector space and it is shown how V is decomposed into maximal regular near vector spaces.

3.1 Some examples

EXAMPLE 1:

Put $V := \mathbb{R}^2$, $F := \mathbb{R}$ and let each $\alpha \in F$ act as an endomorphism on V by defining $(x_1, x_2)\alpha := (x_1\alpha, x_2\alpha^3)$.

(I) We show that (V, F) is an F-group:

(F_1): $(V, +)$ is a group. Moreover, let $\alpha \in F$ and let $(x_1, x_2), (y_1, y_2) \in V$. Then

$$\begin{aligned}
[(x_1, x_2) + (y_1, y_2)]\alpha &= (x_1 + y_1, x_2 + y_2)\alpha \\
&= ((x_1 + y_1)\alpha, (x_2 + y_2)\alpha^3) \\
&= (x_1\alpha + y_1\alpha, x_2\alpha^3 + y_2\alpha^3) \\
&= (x_1\alpha, x_2\alpha^3) + (y_1\alpha, y_2\alpha^3) \\
&= (x_1, x_2)\alpha + (y_1, y_2)\alpha.
\end{aligned}$$

Hence α is an endomorphism of V.

(F_2): Let $(x_1, x_2) \in V$. Then

$$\begin{aligned}
(x_1, x_2)0 &= (x_1 0, x_2 0^3) &&= (0, 0), \\
(x_1, x_2)1 &= (x_1 1, x_2 1^3) &&= (x_1, x_2), \text{ and} \\
(x_1, x_2)(-1) &= (x_1(-1), x_2(-1)^3) &&= (-x_1, -x_2).
\end{aligned}$$

(F_3): Let $(A, \cdot)$ be the automorphism group of $(V, +)$. We shall now show that $F^* \subseteq A$. Let $\alpha \in F^*$. Then α is an endomorphism. It suffices to show that α is a bijection. Let $(x_1, x_2), (y_1, y_2) \in V$ and suppose that $(x_1, x_2)\alpha = (y_1, y_2)\alpha$. Then $(x_1\alpha, x_2\alpha^3) = (y_1\alpha, y_2\alpha^3)$, which implies that $x_1\alpha = y_1\alpha$ and $x_2\alpha^3 = y_2\alpha^3$. Hence, since $\alpha \neq 0$ and F is a field, $x_1 = y_1$ and $x_2 = y_2$. Therefore α is injective. Furthermore, let $(x_1, x_2) \in V$. Then $(x_1\alpha^{-1}, x_2\alpha^{-3}) \in V$ and $(x_1\alpha^{-1}, x_2\alpha^{-3})\alpha = (x_1\alpha^{-1}\alpha, x_2\alpha^{-3}\alpha^3) = (x_1, x_2)$. Hence α is surjective. Finally, since F is a field, $(F^*, \cdot)$ is a subgroup of $(A, \cdot)$.

(F_4): Let $(x_1, x_2) \in V$ and $\alpha, \beta \in F$. Suppose that $(x_1, x_2)\alpha = (x_1, x_2)\beta$. Then $(x_1\alpha, x_2\alpha^3) = (x_1\beta, x_2\beta^3)$, which implies that $x_1\alpha = x_1\beta$ and $x_2\alpha^3 = x_2\beta^3$. Hence $\alpha = \beta$ or $x_1 = 0$ and $\alpha^3 = \beta^3$ or $x_2 = 0$. If $\alpha \neq \beta$, then $\alpha^3 \neq \beta^3$ and so $x_1 = 0$ and $x_2 = 0$. Hence $(x_1, x_2) = (0, 0)$.

(II) The quasi-kernel $Q(V)$ of V consists of all those elements u of V such that for every $\alpha, \beta \in F$ there exists a $\gamma \in F$ for which $u\alpha + u\beta = u\gamma$.

(i) Consider $(a,0) \in V$. For $\alpha, \beta \in F$,

$$\begin{aligned}(a,0)\alpha + (a,0)\beta &= (a\alpha, 0) + (a\beta, 0)\\ &= (a\alpha + a\beta, 0)\\ &= (a[\alpha+\beta], 0)\\ &= (a,0)[\alpha+\beta].\end{aligned}$$

Hence $(a,0) \in Q(V)$ for each $a \in F$.

(ii) Consider $(0,b) \in V$. For $\alpha, \beta \in F$,

$$\begin{aligned}(0,b)\alpha + (0,b)\beta &= (0, b\alpha^3) + (0, b\beta^3)\\ &= (0, b\alpha^3 + b\beta^3)\\ &= (0, b[\alpha^3+\beta^3])\\ &= (0,b)[\alpha^3+\beta^3]^{\frac{1}{3}}.\end{aligned}$$

Hence $(0,b) \in Q(V)$ for each $b \in F$.

Furthermore, consider $(a,b) \in V$ with $a \in F^*$ and $b \in F^*$. Then

$$\begin{aligned}(a,b)\alpha + (a,b)\beta &= (a\alpha, b\alpha^3) + (a\beta, b\beta^3)\\ &= (a\alpha + a\beta, b\alpha^3 + b\beta^3)\\ &= (a[\alpha+\beta], b[\alpha^3+\beta^3])\\ &\neq (a,b)\gamma,\end{aligned}$$

for any $\gamma \in F$ if $(\alpha+\beta)^3 \neq \alpha^3 + \beta^3$. Hence $(a,b) \notin Q(V)$. So

$$Q(V) = \{(a,0) \mid a \in F\} \cup \{(0,b) \mid b \in F\}.$$

Therefore, since $Q(V) \neq \{(0,0)\}$, $(V,\ F)$ is a linear F-group.

(III) For each $u \in Q(V)\backslash\{0\}$, define $+_u$ on F by $u(\alpha +_u \beta) := u\alpha + u\beta$.

(i) Let $u = (a,0)$ with $a \in F^*$. Then

$$\begin{aligned}(a,0)(\alpha +_u \beta) &= (a,0)\alpha + (a,0)\beta\\ &= (a\alpha, 0) + (a\beta, 0)\\ &= (a\alpha + a\beta, 0)\\ &= (a[\alpha+\beta], 0)\\ &= (a,0)(\alpha+\beta).\end{aligned}$$

Thus $\alpha +_u \beta = \alpha + \beta$.

(ii) Let $u = (0, b)$ with $b \in F^*$. Then

$$\begin{aligned}(0,b)(\alpha +_u \beta) &= (0,b)\alpha + (0,b)\beta \\ &= (0, b\alpha^3) + (0, b\beta^3) \\ &= (0, b\alpha^3 + b\beta^3) \\ &= (0, b[\alpha^3 + \beta^3]) \\ &= (0,b)(\alpha^3 + \beta^3)^{\frac{1}{3}}.\end{aligned}$$

Thus $\alpha +_u \beta = (\alpha^3 + \beta^3)^{\frac{1}{3}}$.

We will now show that, with addition as defined in (ii), $(F, +_u, \cdot)$ is a field (Theorem 2.3-5). First we shall show that $(F, +_u)$ is an abelian group:

(a) Let α, β and γ be elements of F. Then

$$\begin{aligned}(\alpha +_u \beta) +_u \gamma &= (\alpha^3 + \beta^3)^{\frac{1}{3}} +_u \gamma \\ &= [((\alpha^3 + \beta^3)^{\frac{1}{3}})^3 + \gamma^3]^{\frac{1}{3}} \\ &= [(\alpha^3 + \beta^3) + \gamma^3]^{\frac{1}{3}} \\ &= [\alpha^3 + (\beta^3 + \gamma^3)]^{\frac{1}{3}} \\ &= [\alpha^3 + ((\beta^3 + \gamma^3)^{\frac{1}{3}})^3]^{\frac{1}{3}} \\ &= \alpha +_u (\beta^3 + \gamma^3)^{\frac{1}{3}} \\ &= \alpha +_u (\beta +_u \gamma).\end{aligned}$$

Hence $+_u$ is associative.

(b) The zero element of $(F, +_u)$ is 0 since,

$$\begin{aligned}0 +_u \alpha &= (0^3 + \alpha^3)^{\frac{1}{3}} = (\alpha^3)^{\frac{1}{3}} = \alpha, \text{ and} \\ \alpha +_u 0 &= (\alpha^3 + 0^3)^{\frac{1}{3}} = (\alpha^3)^{\frac{1}{3}} = \alpha.\end{aligned}$$

(c) For each $\alpha \in F$,

$$\begin{aligned}(-\alpha) +_u \alpha &= ((-\alpha)^3 + \alpha^3)^{\frac{1}{3}} \\ &= (-\alpha^3 + \alpha^3)^{\frac{1}{3}} \\ &= 0.\end{aligned}$$

Similarly, $\alpha +_u (-\alpha) = 0$. Hence each $\alpha \in F$ has an inverse $-\alpha$.

(d) Let $\alpha, \beta \in F$. Then

$$\begin{aligned} \alpha +_u \beta &= (\alpha^3 + \beta^3)^{\frac{1}{3}} \\ &= (\beta^3 + \alpha^3)^{\frac{1}{3}} \\ &= \beta +_u \alpha. \end{aligned}$$

Hence $(F, +_u)$ is an abelian group.

Secondly, let α, β and γ be elements of F. Then

$$\begin{aligned} \alpha(\beta +_u \gamma) &= \alpha(\beta^3 + \gamma^3)^{\frac{1}{3}} \\ &= (\alpha^3)^{\frac{1}{3}}(\beta^3 + \gamma^3)^{\frac{1}{3}} \\ &= [\alpha^3(\beta^3 + \gamma^3)]^{\frac{1}{3}} \\ &= (\alpha^3\beta^3 + \alpha^3\gamma^3)^{\frac{1}{3}} \\ &= [(\alpha\beta)^3 + (\alpha\gamma)^3]^{\frac{1}{3}} \\ &= \alpha\beta +_u \alpha\gamma. \end{aligned}$$

Similarly, $(\alpha +_u \beta)\gamma = \alpha\gamma +_u \beta\gamma$.

Finally, we know that $(F^*, \cdot)$ is an abelian group. Consequently $(F, +_u, \cdot)$ is a field.

By Theorem 2.3-7, we have that $(F, +_u) \cong (F, +_{u\lambda})$. In this case, however, we shall show that $(F, +_u, \cdot) \cong (F, +_v, \cdot)$, where $\alpha +_u \beta = (\alpha^3 + \beta^3)^{\frac{1}{3}}$ and $\alpha +_v \beta = \alpha + \beta$. It suffices to show that $(F, +_u) \cong (F, +_v)$. Define $f : F \to F$ by $f(x) = x^{\frac{1}{3}}$. Then, since $x = y$ if and only if $x^{\frac{1}{3}} = y^{\frac{1}{3}}$, f is well defined and injective. Let $y \in F$. Then $x = y^3 \in F$ and $f(x) = f(y^3) = (y^3)^{\frac{1}{3}} = y$ and it follows that f is bijective.

Finally, f respects the operation:

$$\begin{aligned} f(\alpha +_v \beta) &= (\alpha + \beta)^{\frac{1}{3}} \\ &= ((\alpha^{\frac{1}{3}})^3 + (\beta^{\frac{1}{3}})^3)^{\frac{1}{3}} \\ &= f(\alpha) +_u f(\beta). \end{aligned}$$

(IV) The kernel $R_u(V)$ of V, with $u \in Q(V)\backslash\{0\}$, is defined by

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

Consider the following two cases:

(i) $(1,0) \in Q(V)\backslash\{0\}$. Then $\alpha +_{(1,0)} \beta := \alpha + \beta$ and, for every $\alpha, \beta \in F$ and for each $a \in F$,

$$(a,0)\alpha + (a,0)\beta = (a,0)(\alpha + \beta).$$

Hence $\{(a,0) \mid a \in F\} \subseteq R_{(1,0)}$. Now let $(a,b) \in R_{(1,0)}$. Recall that $R_{(1,0)} \subseteq Q(V)$ (Note 2.3-8), so $v = (a,0)$ for some $a \in F$ or $v = (0,b)$ for some $b \in F$. But $v(\alpha +_{(1,0)} \beta) = v(\alpha + \beta)$, so $v = (a,0)$ for some $a \in F$. Consequently $R_{(1,0)} = \{(a,0) \mid a \in F\}$.

(ii) $(0,1) \in Q(V)\backslash\{0\}$. Then $\alpha +_{(0,1)} \beta := (\alpha^3 + \beta^3)^{\frac{1}{3}}$ and, for every $\alpha, \beta \in F$ and for each $b \in F$,

$$\begin{aligned}(0,b)\alpha + (0,b)\beta &= (0,b)(\alpha^3 + \beta^3)^{\frac{1}{3}} \\ &= (0,b)(\alpha +_{(0,1)} \beta).\end{aligned}$$

Hence $\{(0,b) \mid b \in F\} \subseteq R_{(0,1)}$. Now let $(a,b) \in R_{(0,1)}$. Then $v = (a,0)$ for some $a \in F$ or $v = (0,b)$ for some $b \in F$ ($R_{(0,1)} \subseteq Q(V)$). But $v(\alpha +_{(0,1)} \beta) = v(\alpha^3 + \beta^3)^{\frac{1}{3}}$, so $v = (0,b)$ for some $b \in F$. Consequently $R_{(0,1)} = \{(0,b) \mid b \in F\}$.

(V) (V, F) is a near vector space, since (Q_1) holds:

Let $(a,b) \in V$, then $(a,b) = (1,0)a + (0,1)b^{\frac{1}{3}}$, where $(1,0)$ and $(0,1) \in Q(V)$ and $a, b^{\frac{1}{3}} \in F^*$. Furthermore, $B = \{(1,0),(0,1)\}$ is a basis of V:

Suppose that $(1,0)\lambda_1 + (0,1)\lambda_2 = (0,0)$. Then $(\lambda_1, 0) + (0, \lambda_2^3) = (0,0)$ which implies that $(\lambda_1, \lambda_2^3) = (0,0)$. Thus $\lambda_1 = 0$ and $\lambda_2^3 = 0$ which implies that $\lambda_2 = 0$. Thus B is independent (Proposition 2.4-2). Now let $v \in Q(V)$. Then there are two possibilities:

Case 1: $v = (a,0)$ for some $a \in F$, then

$$(a,0) = (1,0)a + (0,1)0 \text{ with } a, 0 \in F,$$

or Case 2: $v = (0,b)$ for some $b \in F$, then

$$(0,b) = (1,0)0 + (0,1)b^{\frac{1}{3}} \text{ with } 0, b^{\frac{1}{3}} \in F.$$

Thus B is a generating set for $Q(V)$.

Hence V is a near vector space of dimension two. However, since (Q_2) does not hold in

general $[(a,0)+(0,b)\lambda = (a,b\lambda^3) \notin Q(V)]$, V is not regular and therefore not a vector space (Theorem 2.6-3).

We shall now show how V can be decomposed into maximal regular near vector spaces (Theorem 2.5-17).

Let $Q^* := Q(V)\backslash\{0\}$. Then

$$Q^* = \{(a,0) \,|\, a \in F^*\} \cup \{(0,b) \,|\, b \in F^*\}.$$

Put

$$Q_1 := \{(a,0) \,|\, a \in F^*\} \text{ and } Q_2 := \{(0,b) \,|\, b \in F^*\}.$$

Then

$$B_1 := B \cap Q_1 = \{(1,0)\} \text{ and } B_2 := B \cap Q_2 = \{(0,1)\}.$$

Let

$$V_1 := \langle B_1 \rangle = \{(1,0)a \,|\, a \in F\} = \{(a,0) \,|\, a \in F\},$$

the near vector space generated by B_1 and similarly let

$$V_2 := \langle B_2 \rangle = \{(0,1)c \,|\, c \in F\} = \{(0,c^3) \,|\, c \in F\} = \{(0,b) \,|\, b \in F\}.$$

It can be shown as follows that V_1 is a maximal regular near vector space:

Let $(a_1,0)$ and $(a_2,0)$ be elements of $Q(V_1)\backslash\{0\}$. Then

$$(a_1,0)+(a_2,0) = (a_1+a_2,0) \in Q(V_1).$$

Hence V_1 is regular. Moreover, suppose that there exists a regular near vector space $W \supset V_1$ generated by $Q(W)$. Then there exists an $x \in Q(W)\backslash Q(V_1)$. Hence $x = (a,b)$ with $b \neq 0$. But (a,b) cp $(c,0)$ with $c \in F^*$. Therefore $(a,b)+(c,0)\lambda = (a+c\lambda,b) \in Q(V)$, which is a contradiction. Consequently, V_1 is maximal regular. Similarly, V_2 is maximal regular. Furthermore, since $V_1 \cap V_2 = \{(0,0)\}$ and, for each $(a,b) \in V$, $(a,b) = (a,0)+(0,b)$, $V = V_1 \oplus V_2$.

Let $I_j := B_j$, $j = 1, 2$. Then

$$\begin{aligned} F^{(I_j)} &:= \{(\xi_i)_{i\in I_j} \,|\, \xi_i \in F\} \\ &= \{\xi \,|\, \xi \in F\} \\ &= F. \end{aligned}$$

Finally, it can be shown as follows that $V_j \cong F^{(I_j)}$ (Theorem 2.6-2). Define $g : V_2 \to F_2$, with $F_2 = (F, +_u, \cdot)$ and where $\alpha +_u \beta = (\alpha^3 + \beta^3)^{\frac{1}{3}}$, by $g(0, b) = b^{\frac{1}{3}}$. Then g is well defined. Let $(0, b) = (0, c)$. Then $b = c$. Hence

$$g(0, b) = b^{\frac{1}{3}} = c^{\frac{1}{3}} = g(0, c).$$

Secondly, g is a bijection. Let $g(0, b) = g(0, c)$. Then $b^{\frac{1}{3}} = c^{\frac{1}{3}}$. Hence

$$b = (b^{\frac{1}{3}})^3 = (c^{\frac{1}{3}})^3 = c.$$

Therefore $(0, b) = (0, c)$ and so g is injective. Moreover, let $b \in F_2$. Then $(0, b^3) \in V_2$ and $g(0, b^3) = (b^3)^{\frac{1}{3}} = b$. Hence g is surjective.

Finally, we will show that g respects operations. Let $(0, b)$ and $(0, c)$ be elements of V_2 and $\lambda \in F$. Then

$$\begin{aligned} g[(0, b) + (0, c)] &= g(0, b + c) \\ &= (b + c)^{\frac{1}{3}} \\ &= ((b^{\frac{1}{3}})^3 + (c^{\frac{1}{3}})^3)^{\frac{1}{3}} \\ &= b^{\frac{1}{3}} +_u c^{\frac{1}{3}} \\ &= g(0, b) +_u g(0, c) \end{aligned}$$

and

$$\begin{aligned} g[(0, b)\lambda] &= g(0, b\lambda^3) \\ &= b^{\frac{1}{3}}\lambda \\ &= g(0, b)\lambda. \end{aligned}$$

Similarly, $f : V_1 \to F^{(I_1)}$, defined by $f(a, 0) = a$, is an isomorphism. ∎

EXAMPLE 2:

Put $V := (\mathbb{Z}_5)^4$ and $F = \mathbb{Z}_5$. Let α in F act as an endomorphism on V by defining $(x_1, x_2, x_3, x_4)\alpha := (x_1\alpha, x_2\alpha^3, x_3\alpha^3, x_4\alpha)$.

(I) We show that $(V,\ F)$ is an F-group:

(F_1): $(V,\ +)$ is a group. Moreover, let $\alpha \in F$ and let $(x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4) \in V$. Then

$$\begin{aligned}
[(x_1, x_2, x_3, x_4) + (y_1, y_2, y_3, y_4)]\alpha &= (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4)\alpha \\
&= ((x_1 + y_1)\alpha, (x_2 + y_2)\alpha^3, (x_3 + y_3)\alpha^3, (x_4 + y_4)\alpha) \\
&= (x_1\alpha + y_1\alpha, x_2\alpha^3 + y_2\alpha^3, x_3\alpha^3 + y_3\alpha^3, x_4\alpha + y_4\alpha) \\
&= (x_1\alpha, x_2\alpha^3, x_3\alpha^3, x_4\alpha) + (y_1\alpha, y_2\alpha^3, y_3\alpha^3, y_4\alpha) \\
&= (x_1, x_2, x_3, x_4)\alpha + (y_1, y_2, y_3, y_4)\alpha.
\end{aligned}$$

Hence α is an endomorphism of V.

(F_2): Let $(x_1, x_2, x_3, x_4) \in V$. Then

$$\begin{aligned}
(x_1, x_2, x_3, x_4)0 &= (x_1 0, x_2 0^3, x_3 0^3, x_4 0) = (0, 0, 0, 0), \\
(x_1, x_2, x_3, x_4)1 &= (x_1 1, x_2 1^3, x_3 1^3, x_4 1) = (x_1, x_2, x_3, x_4), \text{ and}
\end{aligned}$$

$$\begin{aligned}
(x_1, x_2, x_3, x_4)(-1) &= (x_1, x_2, x_3, x_4)4 \quad (-1 = 4 \text{ in } \mathbb{Z}_5) \\
&= (x_1 4, x_2 4^3, x_3 4^3, x_4 4) \\
&= (x_1 4, x_2 4, x_3 4, x_4 4) \\
&= (x_1(-1), x_2(-1), x_3(-1), x_4(-1)) \\
&= (-x_1, -x_2, -x_3, -x_4).
\end{aligned}$$

(F_3): Let $\alpha \in F^*$ where $F^* = \{1, 2, 3, 4\}$ and let (x_1, x_2, x_3, x_4), $(y_1, y_2, y_3, y_4) \in V$.

First we will show that α is a bijection.

(i) Suppose that $(x_1, x_2, x_3, x_4)\alpha = (y_1, y_2, y_3, y_4)\alpha$. Then

$$(x_1\alpha, x_2\alpha^3, x_3\alpha^3, x_4\alpha) = (y_1\alpha, y_2\alpha^3, y_3\alpha^3, y_4\alpha),$$

which implies that

$$x_1\alpha = y_1\alpha,\ x_2\alpha^3 = y_2\alpha^3,\ x_3\alpha^3 = y_3\alpha^3,\ x_4\alpha = y_4\alpha.$$

Hence $(x_1 - y_1)\alpha = 0, (x_2 - y_2)\alpha^3 = 0, (x_3 - y_3)\alpha^3 = 0, (x_4 - y_4)\alpha = 0$. Therefore, since $\alpha \neq 0$, $x_1 = y_1$, $x_2 = y_2$, $x_3 = y_3$, $x_4 = y_4$. Hence $(x_1, x_2, x_3, x_4) = (y_1, y_2, y_3, y_4)$.

Consequently, α is injective.

(ii) Let $(x_1, x_2, x_3, x_4) \in V$ and let $\alpha \in F^*$. Then $(x_1\alpha^{-1}, x_2\alpha^{-3}, x_3\alpha^{-3}, x_4\alpha^{-1}) \in V$ and $(x_1\alpha^{-1}, x_2\alpha^{-3}, x_3\alpha^{-3}, x_4\alpha^{-1})\alpha = (x_1, x_2, x_3, x_4)$. Hence α is surjective.

Thus F is a subset of the group of automorphisms of $(V, +)$. Furthermore, since α is an endomorphism and F is a field, F^* is a subgroup of the automorphism group of $(V, +)$.

(F_4): Let $(x_1, x_2, x_3, x_4) \in V$ and let $\alpha, \beta \in F$. Suppose that

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

Then

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

which implies that $x_1\alpha = x_1\beta$, $x_2\alpha^3 = x_2\beta^3$, $x_3\alpha^3 = x_3\beta^3$, $x_4\alpha = x_4\beta$. If $\alpha \neq \beta$, then $\alpha^3 \neq \beta^3$ and so $x_1 = x_2 = x_3 = x_4 = 0$, i.e. $(x_1, x_2, x_3, x_4) = (0, 0, 0, 0)$.

(II) The quasi-kernel $Q(V)$ of V consists of all those elements u of V such that for every $\alpha, \beta \in F$ there exists a $\gamma \in F$ for which $u\alpha + u\beta = u\gamma$.

(i) Consider $(a, 0, 0, d) \in V$. For $\alpha, \beta \in F$,

$$\begin{aligned}(a,0,0,d)\alpha + (a,0,0,d)\beta &= (a\alpha, 0, 0, d\alpha) + (a\beta, 0, 0, d\beta)\\ &= (a\alpha + a\beta, 0, 0, d\alpha + d\beta)\\ &= (a[\alpha+\beta], 0, 0, d[\alpha+\beta])\\ &= (a,0,0,d)[\alpha+\beta].\end{aligned}$$

Hence $(a, 0, 0, d) \in Q(V)$ for each $a, d \in F$.

(ii) Consider $(0, b, c, 0) \in V$. For $\alpha, \beta \in F$,

$$\begin{aligned}(0,b,c,0)\alpha + (0,b,c,0)\beta &= (0, b\alpha^3, c\alpha^3, 0) + (0, b\beta^3, c\beta^3, 0)\\ &= (0, b\alpha^3 + b\beta^3, c\alpha^3 + c\beta^3, 0)\\ &= (0, b[\alpha^3+\beta^3], c[\alpha^3+\beta^3], 0)\\ &= (0,b,c,0)[\alpha^3+\beta^3]^{\frac{1}{3}}.\end{aligned}$$

Hence $(0, b, c, 0) \in Q(V)$ for each $b, c \in F$.

Note that $[\alpha^3+\beta^3]^{\frac{1}{3}}$ exists in F for any $\alpha, \beta \in F$: $0^{\frac{1}{3}} = 0$, $1^{\frac{1}{3}} = 1$, $2^{\frac{1}{3}} = 3$, $3^{\frac{1}{3}} = 2$, $4^{\frac{1}{3}} = 4$.

It can easily be verified that elements of the form $(a,b,c,d), (a,b,c,0), (a,b,0,0), (a,0,c,0), (0,b,0,d), (0,0,c,d), (a,b,0,d), (0,b,c,d), (a,0,c,d)$, with $a,b,c,d \in F^*$ are not elements of $Q(V)$. For example, $(a,b,0,0) \notin Q(V)$:

$$\begin{aligned}(a,b,0,0)\alpha + (a,b,0,0)\beta &= (a\alpha, b\alpha^3, 0, 0) + (a\beta, b\beta^3, 0, 0)\\ &= (a\alpha + a\beta, b\alpha^3 + b\beta^3, 0, 0)\\ &= (a[\alpha+\beta], b[\alpha^3+\beta^3], 0, 0)\\ &\neq (a,b,0,0)\gamma\end{aligned}$$

for any $\gamma \in F$, if $\alpha^3 + \beta^3 \neq (\alpha+\beta)^3$ (which is easy to verify). Hence

$$Q(V) = \{(a,0,0,d) \mid a,d \in F\} \cup \{(0,b,c,0) \mid b,c \in F\}.$$

Therefore, since $Q(V) \neq \{(0,0,0,0)\}$, $(V,\ F)$ is a linear F-group.

(III) For each $u \in Q(V)\backslash\{0\}$, define $+_u$ on F by $u(\alpha +_u \beta) := u\alpha + u\beta$.
(i) Let $u = (a,0,0,d)$ with $a,d \in F$, not both zero. Then

$$\begin{aligned}(a,0,0,d)(\alpha +_u \beta) &= (a,0,0,d)\alpha + (a,0,0,d)\beta\\ &= (a\alpha, 0, 0, d\alpha) + (a\beta, 0, 0, d\beta)\\ &= (a\alpha + a\beta, 0, 0, d\alpha + d\beta)\\ &= (a[\alpha+\beta], 0, 0, d[\alpha+\beta])\\ &= (a,0,0,d)(\alpha+\beta)\end{aligned}$$

Hence $\alpha +_u \beta = \alpha + \beta$.
(ii) Let $u = (0,b,c,0)$ with $b,c \in F$, not both zero. Then

$$\begin{aligned}(0,b,c,0)(\alpha +_u \beta) &= (0,b,c,0)\alpha + (0,b,d,0)\beta\\ &= (0, b\alpha^3, c\alpha^3, 0) + (0, b\beta^3, c\beta^3, 0)\\ &= (0, b\alpha^3 + b\beta^3, c\alpha^3 + c\beta^3, 0)\\ &= (0, b[\alpha^3+\beta^3], c[\alpha^3+\beta^3], 0)\\ &= (0,b,c,0)(\alpha^3+\beta^3)^{\frac{1}{3}}.\end{aligned}$$

Thus $\alpha +_u \beta = (\alpha^3+\beta^3)^{\frac{1}{3}}$.

(IV) The kernel $R_u(V)$ of V, with $u \in Q(V)\backslash\{0\}$, is defined by

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

Consider the following two cases:

(i) $(1,0,0,1) \in Q(V)\backslash\{0\}$. Then $\alpha +_{(1,0,0,1)} \beta := \alpha + \beta$ and, for every $\alpha, \beta \in F$ and for each $a, d \in F$,

$$(a,0,0,d)\alpha + (a,0,0,d)\beta = (a,0,0,d)(\alpha + \beta).$$

Hence $\{(a,0,0,d) \mid a,d \in F\} \subseteq R_{(1,0,0,1)}$. Now let $v \in R_{(1,0,0,1)}$. Recall that $R_{(1,0,0,1)} \subseteq Q(V)$ (Note 2.3-8), so $v = (a,0,0,d)$ for some $a, d \in F$ or $v = (0,b,c,0)$ for some $b, c \in F$. But $v(\alpha +_{(1,0,0,1)} \beta) = v(\alpha + \beta)$, so $v = (a,0,0,d)$ for some $a, d \in F$. Consequently $R_{(1,0,0,1)} = \{(a,0,0,d) \mid a,d \in F\}$.

(ii) Similarly, $R_{(0,1,1,0)} = \{(0,b,c,0) \mid b,c \in F\}$.

(V) (V, F) is a near vector space, since (Q_1) holds:

Let $(a,b,c,d) \in V$, then

$$(a,b,c,d) = (1,0,0,0)a + (0,1,0,0)b^{\frac{1}{3}} + (0,0,1,0)c^{\frac{1}{3}} + (0,0,0,1)d,$$

where $(1,0,0,0), (0,1,0,0), (0,0,1,0)$ and $(0,0,0,1) \in Q(V)$ and $a, b^{\frac{1}{3}}, c^{\frac{1}{3}}, d \in F$.

Furthermore, $B = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\}$ is a basis of V:

Suppose that

$$(1,0,0,0)\lambda_1 + (0,1,0,0)\lambda_2 + (0,0,1,0)\lambda_3 + (0,0,0,1)\lambda_4 = (0,0,0,0).$$

Then

$$(\lambda_1,0,0,0) + (0,\lambda_2^3,0,0) + (0,0,\lambda_3^3,0) + (0,0,0,\lambda_4) = (0,0,0,0)$$

which implies that $(\lambda_1, \lambda_2^3, \lambda_3^3, \lambda_4) = (0,0,0,0)$. Thus $\lambda_1 = 0$, $\lambda_2^3 = 0$, $\lambda_3^3 = 0$ and $\lambda_4 = 0$. This implies that $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 0$. Thus B is independent (Proposition 2.4-2). Now let $v \in Q(V)$. Then there are two possibilities:

Case 1: $v = (a,0,0,d)$ for some $a, d \in F$, then

$$(a,0,0,d) = (1,0,0,0)a + (0,1,0,0)0 + (0,0,1,0)0 + (0,0,0,1)d \text{ with } a,0,d \in F$$

or Case 2: $v = (0, b, c, 0)$ for some $b, c \in F$, then

$$(0, b, c, 0) = (1, 0, 0, 0)0 + (0, 1, 0, 0)b^{\frac{1}{3}} + (0, 0, 1, 0)c^{\frac{1}{3}} + (0, 0, 0, 1)0 \text{ with } 0, b^{\frac{1}{3}}, c^{\frac{1}{3}} \in F.$$

Thus B is a generating set for $Q(V)$.

Hence V is a near vector space of dimension four. However, since (Q_2) does not hold in general $((a, 0, 0, 0) + (0, b, 0, 0)\lambda = (a, b\lambda^3, 0, 0) \notin Q(V))$, V is not regular and therefore not a vector space (Theorem 2.6-3).

We shall now show how V can be decomposed into maximal regular near vector spaces (Theorem 2.5-17).

Let $Q^* := Q(V)\backslash\{0\}$. Then

$$Q^* = (\{(a, 0, 0, d) \,|\, a, d \in F\} \cup \{(0, b, c, 0) \,|\, b, c \in F\})\backslash\{(0, 0, 0, 0)\}.$$

Put

$$Q_1 = \{(a, 0, 0, d) \,|\, a, d \in F\}\backslash\{(0, 0, 0, 0)\},$$

and

$$Q_2 = \{(0, b, c, 0) \,|\, b, c \in F\}\backslash\{(0, 0, 0, 0)\}.$$

Then

$$B_1 := B \cap Q_1 = \{(1, 0, 0, 0), (0, 0, 0, 1)\},$$

and

$$B_2 := B \cap Q_2 = \{(0, 1, 0, 0), (0, 0, 1, 0)\}.$$

Let

$$V_1 := \langle B_1 \rangle = \{(1, 0, 0, 0)a + (0, 0, 0, 1)d \,|\, a, d \in F\} = \{(a, 0, 0, d) \,|\, a, d \in F\},$$

the near vector space generated by B_1 and similarly let

$$V_2 := \langle B_2 \rangle = \{(0, 1, 0, 0)b + (0, 0, 1, 0)c \,|\, b, c \in F\} = \{(0, b, c, 0) \,|\, b, c \in F\}.$$

It can be shown as follows that V_2 is a maximal regular near vector space:

Every two elements of Q_2 are compatible. But $Q_2 = (Q\backslash\{0\}) \cap V_2$. Hence V_2 is regular.

Moreover, suppose that there exists a regular near vector space $W \supset V_2$ generated by $Q(W)$. Then there exists a $(a,b,c,d) \in Q(W) \setminus Q_2$ such that at least one of a and d is not zero. But W is regular and so (a,b,c,d) cp $(0,x_1,x_2,0)$ with $x_1, x_2 \in F^*$. Therefore $(a,b,c,d) + (0,x_1,x_2,0)\lambda = (a, b+x_1\lambda^3, c+x_2\lambda^3, d) \in Q(V)$, a contradiction. Consequently, V_2 is maximal regular. Similarly, V_1 is maximal regular. Furthermore, since $V_1 \cap V_2 = \{(0,0,0,0)\}$ and, for each $(a,b,c,d) \in V$, $(a,b,c,d) = (a,0,0,d) + (0,b,c,0)$, $V = V_1 \oplus V_2$.

Let $I_j := B_j$ with $j = 1, 2$. Then

$$\begin{aligned} F^{(I_1)} &:= \{(\xi_i)_{i\in I_1} \,|\, \xi_i \in F\} \\ &= \{(\xi_1, \xi_2) \,|\, \xi_1, \xi_2 \in F\} \\ &= F^2, \end{aligned}$$

and

$$\begin{aligned} F^{(I_2)} &:= \{(\xi_i)_{i\in I_2} \,|\, \xi_i \in F\} \\ &= \{(\xi_1, \xi_2) \,|\, \xi_1, \xi_2 \in F\} \\ &= F^2. \end{aligned}$$

Finally, it can be shown as follows that $V_j \cong F^{(I_j)}$(Theorem 2.6-2). Define $f_1 : V_1 \to F^{(I_1)}$ by $f_1(a,0,0,d) = (a,d)$ and $f_2 : V_2 \to F^{(I_2)}$ by $f_2(0,b,c,0) = (b,c)$. Then f_1 and f_2 are isomorphisms. ∎

EXAMPLE 3:

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 $x^2 + 1 \in \mathbb{Z}_3[x]$.

Addition on $GF(3^2)$ is defined by

$$(a+b\gamma) + (c+d\gamma) = (a+c) \bmod 3 \; + ((b+d) \bmod 3)\gamma,$$

and multiplication by

$\cdot$	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

In [10], p.257, it is observed 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

Define $\theta : GF(3^2) \to GF(3^2)$ by

$$\begin{aligned}
0 &\mapsto 0\\
1 &\mapsto 1\\
2 &\mapsto 2\\
\gamma &\mapsto 2\gamma\\
2\gamma &\mapsto \gamma\\
1+\gamma &\mapsto 1+\gamma\\
2+2\gamma &\mapsto 2+2\gamma\\
2+\gamma &\mapsto 1+2\gamma\\
1+2\gamma &\mapsto 2+\gamma.
\end{aligned}$$

Then θ is an automorphism with respect to $\circ$, but $\theta(\alpha+\beta) \neq \theta(\alpha)+\theta(\beta)$, in general. If there is no danger of confusion, $x \circ y$, with $x, y \in GF(3^2)$, is written xy.

Let F denote the nearfield $(GF(3^2), +, \circ)$ and put $V = F^2$. Let $\alpha \in F$ act as an endomorphism of V by defining $(a,b)\alpha := (a\alpha, b\theta(\alpha))$. Furthermore, let

$$A := \{1, 2, 1+\gamma, 2+2\gamma\}$$

and

$$B := \{\gamma, 2\gamma, 2+\gamma, 1+2\gamma\}.$$

(i.e. A consists of all those nonzero elements that are mapped to themselves, whereas B consists of the nonzero elements that are mapped to their additive inverses by θ.)

(I) We show that (V, F) is an F-group:

(F_1): $(V, +)$ is a group since $(F, +)$ is a group;

Moreover, let $\alpha \in F$ and let $(a,b),(c,d) \in V$. Then

$$\begin{aligned}
[(a,b)+(c,d)]\alpha &= (a+c,b+d)\alpha \\
&= ((a+c)\alpha,(b+d)\theta(\alpha)) \\
&= \begin{cases} ((a+c)\alpha,(b+d)\alpha) & \text{if } \alpha \in A \\ ((a+c)\alpha,(b+d)(-\alpha)) & \text{if } \alpha \in B \end{cases} \\
&= \begin{cases} (a\alpha+c\alpha,b\alpha+d\alpha) & \text{if } \alpha \in A \\ (a\alpha+c\alpha,-b\alpha-d\alpha) & \text{if } \alpha \in B \end{cases} \\
&= \begin{cases} (a\alpha,b\alpha)+(c\alpha,d\alpha) & \text{if } \alpha \in A \\ (a\alpha,-b\alpha)+(c\alpha,-d\alpha) & \text{if } \alpha \in B \end{cases} \\
&= (a\alpha,b\theta(\alpha))+(c\alpha,d\theta(\alpha)) \\
&= (a,b)\alpha+(c,d)\alpha.
\end{aligned}$$

Hence α is an endomorphism of V.

(F_2): Let $(a,b) \in V$. Then

$$\begin{aligned}
(a,b)0 &= (a0,b\theta(0)) = (a0,b0) = (0,0), \\
(a,b)1 &= (a1,b\theta(1)) = (a1,b1) = (a,b), \text{ and} \\
(a,b)(-1) = (a,b)2 &= (a2,b\theta(2)) = (a2,b2) = (-a,-b).
\end{aligned}$$

(F_3): Let $\alpha \in F^*$. Since α is an endomorphism and F a nearfield, it suffices to show that α is a bijection:

(i) Let $(a,b)\alpha = (c,d)\alpha$ with (a,b) and $(c,d) \in V$. Then

$$(a\alpha,b\theta(\alpha)) = (c\alpha,d\theta(\alpha)),$$

which implies that

$$(a\alpha,b\alpha) = (c\alpha,d\alpha) \text{ if } \alpha \in A$$

and

$$(a\alpha,-b\alpha) = (c\alpha,-d\alpha) \text{ if } \alpha \in B.$$

Hence if $\alpha \in A$,

$$a\alpha = c\alpha \text{ and } b\alpha = d\alpha$$

and if $\alpha \in B$,

$$a\alpha = c\alpha \text{ and } -b\alpha = -d\alpha.$$

Therefore, since $\alpha \neq 0$ and F does not contain any zero divisors,

$$a = c \text{ and } b = d.$$

Hence $(a, b) = (c, d)$ and consequently α is injective.
(ii) Let $(c, d) \in V$. Then, if $\alpha \in A$, $(c\alpha^{-1}, d\alpha^{-1}) \in V$ and $(c\alpha^{-1}, d\alpha^{-1})\alpha = (c, d)$. If $\alpha \in B$, then $(c\alpha^{-1}, -d\alpha^{-1}) \in V$ and $(c\alpha^{-1}, -d\alpha^{-1})\alpha = (c, d)$. Hence α is surjective.
(F_4): Let $\alpha, \beta \in F$ and $(a, b) \in V$. Suppose that

$$(a, b)\alpha = (a, b)\beta.$$

Then

$$(a\alpha, b\theta(\alpha)) = (a\beta, b\theta(\beta)),$$

which implies that

$$a\alpha = a\beta \text{ and } b\theta(\alpha) = b\theta(\beta).$$

Let $\alpha \neq \beta$ and suppose that $a \neq 0$. Then there exists an $a^{-1} \in F$ such that $a^{-1}a\alpha = a^{-1}a\beta$, which implies that $\alpha = \beta$. This is a contradiction. Hence $a = 0$. Since θ is a bijection, $\alpha \neq \beta$, implies that $\theta(\alpha) \neq \theta(\beta)$. Now suppose that $b \neq 0$. Then there exists a $b^{-1} \in F$ such that $b^{-1}b\theta(\alpha) = b^{-1}b\theta(\beta)$, which implies that $\theta(\alpha) = \theta(\beta)$. This is a contradiction. Hence $b = 0$. Therefore $(a, b) = (0, 0)$.

(II) The quasi-kernel $Q(V)$ of V consists of all those elements u of V such that for every $\alpha, \beta \in F$ there exists a $\gamma \in F$ for which $u\alpha + u\beta = u\gamma$.
(i) Consider $(1, 0) \in V$. For $\alpha, \beta \in F$,

$$\begin{aligned} (1,0)\alpha + (1,0)\beta &= (\alpha, 0) + (\beta, 0) \\ &= (\alpha + \beta, 0) \\ &= (1,0)[\alpha + \beta]. \end{aligned}$$

Hence $(1, 0) \in Q(V)$.

Now consider $(c, 0) \in V$ with $c \in F^*$. Then, since $(1, 0) \in Q(V)$, $(1, 0)F \subseteq Q(V)$ (Lemma

2.3-2(c)). Thus $(c,0) \in Q(V)$, for all $c \in F$.

(ii) Consider $(0,1) \in V$. For $\alpha, \beta \in F$,

$$\begin{aligned}(0,1)\alpha + (0,1)\beta &= (0,\theta(\alpha)) + (0,\theta(\beta)) \\ &= (0,\theta(\alpha)+\theta(\beta)) \\ &= (0,1)\theta^{-1}(\theta(\alpha)+\theta(\beta)).\end{aligned}$$

Since $\theta : F \to F$ is a bijection, $\theta^{-1} : F \to F$ exists. Hence $\theta^{-1}(\theta(\alpha)+\theta(\beta)) \in F$ and therefore $(0,1) \in Q(V)$.

Now consider $(0,c) \in V$ with $c \in F^*$. Then, since $(0,1) \in Q(V)$, $(0,1)F \subseteq Q(V)$ (Lemma 2.3-2(c)). Consequently, $(0,\theta(\alpha)) \in Q(V)$, for all $\alpha \in F$. Thus $(0,c) \in Q(V)$, for all $c \in F$.

Furthermore, consider $(a,b) \in V$ with $a, b \in F^*$. Then for $\alpha, \beta \in F$,

$$\begin{aligned}(a,b)\alpha + (a,b)\beta &= (a\alpha, b\theta(\alpha)) + (a\beta, b\theta(\beta)) \\ &= (a\alpha + a\beta, b\theta(\alpha) + b\theta(\beta)) \\ &\neq (a,b)\gamma\end{aligned}$$

for any $\gamma \in F$ if $a^{-1}(a\alpha + a\beta) \neq \theta^{-1}(b^{-1}(b\theta(\alpha) + b\theta(\beta)))$. [Take for example, $a = 1$, $b = 1$, $\alpha = \gamma$, $\beta = 1 + \gamma$.] Hence $(a,b) \notin Q(V)$ if $a, b \in F^*$. Therefore

$$Q(V) = \{(c,0) \mid c \in F\} \cup \{(0,c) \mid c \in F\}.$$

Hence, since $Q(V) \neq \{(0,0)\}$, (V, F) is a linear F-group.

(III) For each $u \in Q(V)\backslash\{0\}$, define $+_u$ on F by $u(\alpha +_u \beta) := u\alpha + u\beta$.

(i) Let $u = (c,0)$ with $c \in F^*$. Then

$$\begin{aligned}(c,0)(\alpha +_u \beta) &= (c,0)\alpha + (c,0)\beta \\ &= (c\alpha, 0) + (c\beta, 0) \\ &= (c\alpha + c\beta, 0) \\ &= (c,0)c^{-1}(c\alpha + c\beta).\end{aligned}$$

Thus $\alpha +_u \beta = c^{-1}(c\alpha + c\beta)$.

(ii) Let $u = (0, c)$ with $c \in F^*$. Then

$$\begin{aligned}(0,c)(\alpha +_u \beta) &= (0,c)\alpha + (0,c)\beta \\ &= (0, c\theta(\alpha)) + (0, c\theta(\beta)) \\ &= (0, c\theta(\alpha) + c\theta(\beta)) \\ &= (0,c)\theta^{-1}(c^{-1}(c\theta(\alpha) + c\theta(\beta))).\end{aligned}$$

Thus $\alpha +_u \beta = \theta^{-1}(c^{-1}(c\theta(\alpha) + c\theta(\beta)))$.

By Theorem 2.3-5, $(F, +_u, \circ)$ is a nearfield for $u \in Q(V)\backslash\{0\}$. However, $(F, +_u, \circ)$, in general, is not a field:

For example, consider $(F, +_{(\gamma,0)}, \circ)$. Let $\alpha = 1 + \gamma$, $\beta = 2\gamma$ and $\xi = 1$. Then

$$\begin{aligned}\alpha \circ (\beta +_u \xi) &= (1+\gamma) \circ (2\gamma +_u 1) \\ &= (1+\gamma) \circ (2\gamma \circ (\gamma \circ 2\gamma + \gamma \circ 1)) \\ &= (1+\gamma) \circ (2\gamma \circ (1+\gamma)) \\ &= (1+\gamma) \circ (2+\gamma) \\ &= 2\gamma,\end{aligned}$$

and

$$\begin{aligned}\alpha \circ \beta +_u \alpha \circ \xi &= (1+\gamma) \circ 2\gamma +_u (1+\gamma) \circ 1 \\ &= (1+2\gamma) +_u (1+\gamma) \\ &= 2\gamma \circ (\gamma \circ (1+2\gamma) + \gamma \circ (1+\gamma)) \\ &= 2\gamma \circ (2 + 2\gamma + 1 + 2\gamma) \\ &= 2\gamma \circ \gamma \\ &= 1.\end{aligned}$$

But $2\gamma \neq 1$. Hence $\alpha \circ (\beta +_u \xi) \neq \alpha \circ \beta +_u \alpha \circ \xi$.

(IV) The kernel $R_u(V)$ of V, with $u \in Q(V)\backslash\{0\}$, is defined by

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

Consider the following two cases:

(i) $(1,0) \in Q(V)\backslash\{0\}$. Then

$$\begin{aligned}R_{(1,0)} &= \{v \in V \mid v(\alpha +_u \beta) = v\alpha + v\beta \text{ for every } \alpha, \beta \in F\} \\ &= \{(0,0), (1,0), (2,0)\}.\end{aligned}$$

(ii) $(0,1) \in Q(V)\backslash\{0\}$. Then

$$\begin{aligned} R_{(0,1)} &= \{v \in V \mid v(\theta^{-1}(\theta(\alpha)+\theta(\beta))) = v\alpha + v\beta \text{ for every } \alpha, \beta \in F\} \\ &= \{(0,0),(0,1),(0,2)\}. \end{aligned}$$

(V)$(V,\ F)$ is a near vector space, since (Q_1) holds:
Let $(a,b) \in V$, then $(a,b) = (1,0)a + (0,1)\theta^{-1}(b)$, where $(1,0)$ and $(0,1) \in Q(V)$. However, since (Q_2) does not hold $((0,1) + (1,0)\lambda = (\lambda,1) \notin Q(V))$, V is not a regular near vector space. Therefore V is a near vector space, but not a vector space over F (Theorem 2.6-3). We shall now show how V can be decomposed into maximal regular near vector spaces (Theorem 2.5-17).
Let $Q^* := Q(V)\backslash\{0\}$. Then

$$Q^* = \{(a,0) \mid a \in F^*\} \cup \{(0,a) \mid a \in F^*\}.$$

Put

$$Q_1 := \{(a,0) \mid a \in F^*\} \text{ and } Q_2 := \{(0,a) \mid a \in F^*\}.$$

But $B = \{(1,0),(0,1)\}$ is a basis of V:
Suppose that $(1,0)\lambda_1 + (0,1)\lambda_2 = (0,0)$. Then $(\lambda_1,0) + (0,\theta(\lambda_2))) = (0,0)$ which implies that $(\lambda_1,\theta(\lambda_2)) = (0,0)$. Thus $\lambda_1 = 0$ and $\theta(\lambda_2) = 0$ which implies that $\lambda_2 = 0$. Thus B is independent (Proposition 2.4-2). Now let $v \in Q(V)$. Then there are two possibilities:
Case 1: $v = (a,0)$ for some $a \in F$, then

$$(a,0) = (1,0)a + (0,1)0 \text{ with } a, 0 \in F,$$

or Case 2: $v = (0,b)$ for some $b \in F$, then

$$(0,b) = (1,0)0 + (0,1)\theta^{-1}(b) \text{ with } 0, \theta^{-1}(b) \in F.$$

Thus B is a generating set for $Q(V)$.
Hence

$$B_1 := B \cap Q_1 = \{(1,0)\} \text{ and } B_2 := B \cap Q_2 = \{(0,1)\}.$$

Let $V_j := \langle B_j \rangle$, then

$$V_1 = \{(a,0) \mid a \in F\} \text{ and } V_2 = \{(0,a) \mid a \in F\}.$$

Since $V_1 \cap V_2 = \{(0,0)\}$ and, for each $(a,b) \in V$, $(a,b) = (a,0) + (0,b)$, $V = V_1 \oplus V_2$. Moreover, it can be shown as follows that V_j $(j = 1,2)$ is maximal regular:

Consider V_1. Then since $Q_1 = (Q(V)\backslash\{0\}) \cap V_1$ and every two elements in Q_1 are compatible, V_1 is regular. Furthermore, suppose that there exists a regular near vector space $W \supset V_1$ generated by $Q(W)$. Then there exists an $(a,b) \in Q(W)\backslash Q_1$ such that $b \neq 0$. But since W is regular, (a,b) cp $(c,0)$ with $c \in F^*$. Therefore $(a,b) + (c,0)\lambda = (a + c\lambda, b) \in Q(V)$, which is a contradiction. Consequently, V_1 is maximal regular. Similarly, V_2 is maximal regular.

We have that $(V_2,\ F_2)$, with $F_2 := (F,\ +_{(1,0)},\ \circ)$ is a regular near vector space. Hence, by Theorem 2.6-2, $V_2 \cong F_2^{(I_2)}$ for some index set I_2. Let $I_2 := B_2$. Then $g : V_2 \to F_2^{(I_2)}$, defined by $g(0,b) = \theta^{-1}(b)$ is an isomorphism. This can be shown as follows:

Suppose that $(0,b) = (0,c)$. Then $b = c$. Hence since θ is a bijection, $\theta^{-1}(b) = \theta^{-1}(c)$. This implies that $g(0,b) = g(0,c)$. Therefore g is well defined. Secondly, g is a bijection. Let $g(0,b) = g(0,c)$. Then $\theta^{-1}(b) = \theta^{-1}(c)$. But θ^{-1} is injective. Hence $b = c$. This implies that $(0,b) = (0,c)$ and so g is injective. Moreover, let $b \in F_2$. Then $(0,\theta(b)) \in V_2$ and $g(0,\theta(b)) = \theta^{-1}(\theta(b)) = b$. Hence g is surjective.

Finally, we will show that g respects operations. Let $(0,b)$ and $(0,c)$ be elements of V_2. Then

$$\begin{aligned} g[(0,b) + (0,c)] &= g(0, b+c) \\ &= \theta^{-1}(b+c) \\ &= \theta^{-1}(\theta(\theta^{-1}(b) + \theta(\theta^{-1}(c)))) \\ &= \theta^{-1}(b) +_{(0,1)} \theta^{-1}(c) \\ &= g(0,b) +_{(0,1)} g(0,c) \end{aligned}$$

and

$$\begin{aligned} g[(0,b)\lambda] &= g(0, b\theta(\lambda)) \\ &= \theta^{-1}(b\theta(\lambda)) \\ &= \theta^{-1}(b)\lambda \\ &= g(0,b)\lambda. \end{aligned}$$

Similarly, $g' : V_1 \to F_1^{(I_1)}$, defined by $g'(a,0) = a$, is an isomorphism. Thus $V_1 \cong F_1^{(I_1)}$. ∎

3.2 Finite dimensional near vector spaces over $\mathbb{Z}_p$

Now we develop a theory that will characterise all finite dimensional near vector spaces over $\mathbb{Z}_p$ for p a prime number. In what follows, p will be an odd prime, since for the case $p = 2$ the results will follow trivially.

LEMMA 4:

Let q be a positive integer. Each element of $\mathbb{Z}_p$ has a q-th root in $\mathbb{Z}_p$ if and only if $\gcd(q, p-1) = 1$.

Proof

Suppose that every $x \in \mathbb{Z}_p$ has a q-th root in $\mathbb{Z}_p$. Then

$$1 \equiv x_1^q,\ 2 \equiv x_2^q, \ldots, p-1 \equiv x_{p-1}^q, \tag{3.1}$$

where $x_1, x_2, \ldots, x_{p-1}$ are the nonzero elements of $\mathbb{Z}_p$, in some order.

Now suppose that $d|(p-1)$, were $d > 1$. By [2], Corollary, p.153, the congruence

$$x^d \equiv 1 \pmod{p}$$

has exactly d incongruent solutions. Hence, there exist distinct $y_1, y_2, \ldots, y_d \in \mathbb{Z}_p$ such that $y_i^d \equiv 1 \pmod{p}$ $(1 \leq i \leq d)$. If $d|q$, then $y_i^q \equiv 1 \pmod{p} (1 \leq i \leq d)$, contrary to the fact that there is only one $x \in \mathbb{Z}_p$ with $x^q \equiv 1 \pmod{p}$ (See (3.1)). So if $d|(p-1)$ and $d > 1$, then $d \nmid q$. Consequently $\gcd(q, p-1) = 1$.

Conversely, suppose that $\gcd(q, p-1) = 1$. Then $aq + b(p-1) = 1$ for some $a, b \in \mathbb{Z}$. Let

$x \in \mathbb{Z}_p$, $x \neq 0$ [$x = 0$ has a q-th root, namely itself]. Since $\gcd(x, p) = 1$,

$$x^{p-1} \equiv 1 \pmod{p} \text{ ([2] Theorem 5.1, p.88).}$$

Thus

$$x^{b(p-1)} \equiv 1^b \equiv 1 \pmod{p} \text{ ([2] Theorem 4.2, p.65),}$$

which implies that

$$x \equiv x^1 \equiv x^{aq+b(p-1)} \equiv (x^a)^q \pmod{p} .$$

Thus x has a q-th root in $\mathbb{Z}_p$, namely x^a. ∎

LEMMA 5:

Let p be prime, q_1, q_2 positive integers and $\gcd(q_i, p-1) = 1$ for $i = 1, 2$. Then $q_1 \equiv q_2 \pmod{p-1}$ if and only if

$$(a^{q_1} + b^{q_1})^{\frac{1}{q_1}} = (a^{q_2} + b^{q_2})^{\frac{1}{q_2}}$$

for all $a, b \in \mathbb{Z}_p$.

Proof

Assume that $q_1 \equiv q_2 \pmod{p-1}$, then $q_2 = q_1 + k(p-1)$, for some $k \in \mathbb{Z}$. So for nonzero $a, b \in \mathbb{Z}_p$,

$$\begin{aligned} (a^{q_1} + b^{q_1})^{q_2} &= (a^{q_2-k(p-1)} + b^{q_2-k(p-1)})^{q_1+k(p-1)} \\ &= (a^{q_2} + b^{q_2})^{q_1}. \end{aligned}$$

(Note: $x^{p-1} \equiv 1 \pmod{p}$ for nonzero $x \in \mathbb{Z}_p$. Also, if $a^{q_1} + b^{q_1} = 0$, then $a^{q_1} = -b^{q_1} = (-b)^{q_1}$ (since q_1 is odd). This implies that $a = -b$ (each element in $\mathbb{Z}_p$ has a unique q-th root, by Lemma 4.) So we have that $a^{q_2} = (-b)^{q_2} = -b^{q_2}$ (q_2 is odd). This implies that $a^{q_2} + b^{q_2} = 0$, so $(a^{q_1} + b^{q_1})^{q_2} = (a^{q_2} + b^{q_2})^{q_1}$ in this case as well).

If at least one of a and b is zero, then it follows trivially that

$$(a^{q_1} + b^{q_1})^{q_2} = (a^{q_2} + b^{q_2})^{q_1}.$$

We deduce that, for all $a, b \in \mathbb{Z}_p$,

$$(a^{q_1} + b^{q_1})^{\frac{1}{q_1}} = (a^{q_2} + b^{q_2})^{\frac{1}{q_2}}.$$

Conversely, assume that

$$(a^{q_1} + b^{q_1})^{\frac{1}{q_1}} = (a^{q_2} + b^{q_2})^{\frac{1}{q_2}} \text{ for all } a, b \in \mathbb{Z}_p.$$

Then

$$(a^{q_1} + b^{q_1})^{q_2} = (a^{q_2} + b^{q_2})^{q_1} \text{ for all } a, b \in \mathbb{Z}_p.$$

We want to show that $q_1 \equiv q_2 \pmod{p-1}$, a result that is trivially true for $p = 2$. Henceforth, assume that $p \geq 3$. We know that

$$q_1 = k_1(p-1) + r_1,\ 0 \leq r_1 < p-1,$$

$$q_2 = k_2(p-1) + r_2,\ 0 \leq r_2 < p-1,$$

for certain $k_1, k_2 \in \mathbb{Z}$. But since $\gcd(q_i, p-1) = 1$, we must have $0 < r_i < p-1$, $i = 1, 2$. Now suppose that $q_1 \not\equiv q_2 \pmod{p-1}$. Then we may assume that $0 < r_1 < r_2 < p-1$. Consider the polynomial $f(x) = g_1(x) - g_2(x)$, where $g_1(x) = (1 + x^{r_1})^{r_2}$ and $g_2(x) = (1 + x^{r_2})^{r_1}$. Then

$$g_1(x) = \sum_{k=0}^{r_2} \binom{r_2}{k} x^{kr_1}$$

and

$$g_2(x) = \sum_{k=0}^{r_1} \binom{r_1}{k} x^{kr_2}.$$

Furthermore, $kr_1 \equiv t_k \pmod{(p-1)}$ $(0 \leq k \leq r_2)$ and $kr_2 \equiv s_k \pmod{(p-1)}$ $(0 \leq k \leq r_1)$, where $s_k, t_k \in \{0, 1, \ldots, p-2\}$. All the t_k are distinct, for if $t_{k_i} = t_{k_j}$, then $(p-1)|(k_i - k_j)r_1$. But since $\gcd(p-1, r_1) = 1$, $(p-1)|k_i - k_j$, an impossibility. [Note: $\gcd(p-1, r_1) = \gcd(p-1, r_1 + k_1(p-1)) = \gcd(p-1, q_1) = 1$.] Similarly, all the s_k are distinct. We note that $f(0) = 0 \pmod{p}$. So assume that $x \not\equiv 0 \pmod{p}$ from now on. Then, using $x^{p-1} \equiv 1 \pmod{p}$ if $x \not\equiv 0 \pmod{p}$, we see that

$$\begin{aligned} f(x) = g_1(x) - g_2(x) &= h_1(x) - h_2(x) \\ &= \textstyle\sum_{k=0}^{r_2} \binom{r_2}{k} x^{t_k} - \sum_{k=0}^{r_1} \binom{r_1}{k} x^{s_k} \pmod{\text{p}}. \end{aligned}$$

But $h_1(x) = \sum_{k=0}^{r_2} \binom{r_2}{k} x^{t_k}$ contains more terms than $h_2(x) = \sum_{k=0}^{r_1} \binom{r_1}{k} x^{s_k}$, so the terms of $h_2(x)$ cannot cancel all the terms of $h_1(x)$. Moreover, $p \not| \binom{r_2}{k}$ for all $k = 0, 1, \ldots, r_2$ since $1 \leq r_2 \leq p-2$. This implies that $f(x)$ is a nonzero polynomial (modulo p) of degree at most $p-2$.

But under the assumption

$$(a^{q_1} + b^{q_1})^{q_2} = (a^{q_2} + b^{q_2})^{q_1} \text{ for all } a, b \in \mathbb{Z}_p,$$

if we let $a = 1$ and $b = 1, 2, \ldots, p-1$, we find that $f(x) = 0 \pmod{p}$ for all $x = 1, 2, \ldots, p-1$. This contradicts Theorem 8.5 [[2], p.152]. Consequently, $q_1 \equiv q_2 \pmod{p-1}$. ∎

PROPOSITION 6:

Let φ be an automorphism of the group with zero $(\mathbb{Z}_p, \cdot)$. Then there exists a $q \in \mathbb{Z}$, with $1 \leq q \leq p-2$ and $\gcd(q, p-1) = 1$, such that $\varphi(x) = x^q$ for all $x \in \mathbb{Z}_p$.

Proof

Since $(\mathbb{Z}_p, +, \cdot)$ is a finite field, $(\mathbb{Z}_p^*, \cdot)$ is a cyclic group [[7], Theorem 5.4, p.279], say $\mathbb{Z}_p^* = \langle \alpha \rangle = \{\alpha, \alpha^2, \ldots, \alpha^{p-1}\}$. Let $\varphi(\alpha) = \alpha^k$, for some k, $1 \leq k \leq p-2$. (We cannot have $k = p-1$, since $\alpha^{p-1} = 1$ for all $\alpha \in \mathbb{Z}_p^*$.) Then $\varphi(\alpha^i) = \alpha^{ik}$, $1 \leq i \leq p-1$. But $\{\alpha^i \mid 1 \leq i \leq p-1\} = \mathbb{Z}_p^*$, so $\{\alpha^{ik} \mid 1 \leq i \leq p-1\} = \mathbb{Z}_p^*$, since φ is a bijection on $\mathbb{Z}_p^*$. This means that every element of $\mathbb{Z}_p$ has a k-th root. Hence by Lemma 4, $\gcd(k, p-1) = 1$. So we can take $q = k$. ∎

By [13] [Theorem 3.4(2), p.301], all n-dimensional near vector spaces over $\mathbb{Z}_p$ can be obtained as follows:

Take $V = \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (n copies) and let $\vartheta_i : (\mathbb{Z}_p, \cdot) \to (\mathbb{Z}_p, \cdot)$ $(1 \leq i \leq n)$ be semigroup isomorphisms. Define scalar multiplication by

$$(x_1, x_2, \ldots, x_n)\alpha = (x_1\vartheta_1(\alpha), x_2\vartheta_2(\alpha), \ldots, x_n\vartheta_n(\alpha)).$$

By Proposition 6, every ϑ_i is a q-th power function for some q, $1 \leq q \leq p-2$ and $\gcd(q, p-1) = 1$. The number of q's satisfying this is $\phi(p-1)$ (where ϕ denotes Euler's

totient function). This implies that there are $\phi(p-1)$ distinct semigroup isomorphisms $\vartheta_i : (\mathbb{Z}_p, \cdot) \to (\mathbb{Z}_p, \cdot)$.

This leads to:

THEOREM 7:

If $V_{\mathbb{Z}_p}$ is an n-dimensional near vector space, then it cannot contain more than $\phi(p-1)$ maximal regular subspaces.

Proof

The scalar multiplication of this space is given by

$$(x_1, x_2, \ldots, x_n)\alpha = (x_1\alpha^{q_1}, x_2\alpha^{q_2}, \ldots, x_n\alpha^{q_n}),$$

where each q_i satisfies $1 \leq q_i \leq p-2$ and $\gcd(q_i, p-1) = 1$. All those q_i that coincide lead to a maximal regular subspace, as in Example 2. Since there are not more than $\phi(p-1)$ distinct q_i, the result follows. ∎

If $q_1, q_2, \ldots, q_n$ is a sequence of q_i satisfying $1 \leq q_i \leq p-2$, $\gcd(q_i, p-1) = 1$, that leads to the near vector space $V_{\mathbb{Z}_p}$ with scalar multiplication

$$(x_1, x_2, \ldots, x_n)\alpha = (x_1\alpha^{q_1}, x_2\alpha^{q_2}, \ldots, x_n\alpha^{q_n})$$

and τ is any permutation of $1, 2, \ldots, n$, then the sequence $q_{\tau(1)}, q_{\tau(2)}, \ldots, q_{\tau(n)}$ leads to a near vector space $V'_{\mathbb{Z}_p}$ with scalar multiplication

$$(x_1, x_2, \ldots, x_n)\alpha = (x_1\alpha^{q_{\tau(1)}}, x_2\alpha^{q_{\tau(2)}}, \ldots, x_n\alpha^{q_{\tau(n)}})$$

that is isomorphic to the first one. This can easily be verified by considering the bijection $\zeta : V \to V$;

$$\zeta(x_1, x_2, \ldots, x_n) = (x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}).$$

We may therefore always assume that $q_1 \leq q_2 \leq \cdots \leq q_n$.

If $q'_1 \leq q'_2 \leq \cdots \leq q'_n$ is another sequence satisfying $1 \leq q'_i \leq p-2$, $\gcd(q'_i, p-1) = 1$, but $q'_k \neq q_k$, for some k, then the corresponding near vector spaces are not isomorphic:

Suppose there exists an isomorphism $\psi : V_{\mathbb{Z}_p} \to V'_{\mathbb{Z}_p}$, where we use scalar multiplications

according to $q_1 \leq q_2 \leq \cdots \leq q_n$ in $V_{\mathbb{Z}_p}$ and according to $q_1^{'} \leq q_2^{'} \leq \cdots \leq q_n^{'}$ in $V_{\mathbb{Z}_p}^{'}$. Consider for any $k \in \{1, 2, \ldots, n\}$ any subsequence $q_k = q_{k+1} = \cdots = q_{k+l}$ where either $k = 1$ or $q_{k-1} < q_k$, and $l \geq 0$ as large as possible.

Let $e_i = (0, \ldots, 1, \ldots, 0)$, with 1 in position i, and zeros elsewhere $(1 \leq i \leq n)$. Then

$$\begin{array}{rcl} \psi(e_k) & = & (\omega_{k,1}, \ldots, \omega_{k,n}) \\ \vdots & = & \vdots \\ \psi(e_{k+l}) & = & (\omega_{k+l,1}, \ldots, \omega_{k+l,n}), \end{array}$$

for certain $\omega_{i,j} \in \mathbb{Z}_p$. Also, for $\alpha \in \mathbb{Z}_p$,

$$\begin{array}{rcccl} \psi(e_k\alpha) & = & \psi(0, \ldots, \alpha^{q_k}, \ldots, 0) & = & (\omega_{k,1}\alpha^{q_1^{'}}, \ldots, \omega_{k,n}\alpha^{q_n^{'}}) \\ \vdots & = & \vdots & = & \vdots \\ \psi(e_{k+l}\alpha) & = & \psi(0, \ldots, 0, \alpha^{q_{k+l}}, \ldots, 0) & = & (\omega_{k+l,1}\alpha^{q_1^{'}}, \ldots, \omega_{k+l,n}\alpha^{q_n^{'}}) \end{array}$$

where α^{q_j} in position j for $j = k, \ldots, k+l$. Hence,

$$\begin{array}{rcl} \psi(e_k\alpha^{\frac{1}{q_k}}) & = & \psi(0, \ldots, \alpha, \ldots, 0), \text{ with } \alpha \text{ in position } k, \\ & = & (\omega_{k,1}\alpha^{\frac{q_1^{'}}{q_k}}, \ldots, \omega_{k,n}\alpha^{\frac{q_n^{'}}{q_k}}). \end{array}$$

Hence for $\alpha, \beta \in \mathbb{Z}_p$,

$$\begin{array}{rcl} \psi(e_k\alpha^{\frac{1}{q_k}} + e_k\beta^{\frac{1}{q_k}}) & = & \psi(e_k\alpha^{\frac{1}{q_k}}) + \psi(e_k\beta^{\frac{1}{q_k}}) \\ & = & (\omega_{k,1}\alpha^{\frac{q_1^{'}}{q_k}}, \ldots, \omega_{k,n}\alpha^{\frac{q_n^{'}}{q_k}}) + (\omega_{k,1}\beta^{\frac{q_1^{'}}{q_k}}, \ldots, \omega_{k,n}\beta^{\frac{q_n^{'}}{q_k}}) \\ & = & (\omega_{k,1}(\alpha^{\frac{q_1^{'}}{q_k}} + \beta^{\frac{q_1^{'}}{q_k}}), \ldots, \omega_{k,n}(\alpha^{\frac{q_n^{'}}{q_k}} + \beta^{\frac{q_n^{'}}{q_k}})) \end{array}$$

which equals

$$\psi(e_k(\alpha+\beta)^{\frac{1}{q_k}}) = (\omega_{k,1}(\alpha+\beta)^{\frac{q_1^{'}}{q_k}}, \ldots, \omega_{k,n}(\alpha+\beta)^{\frac{q_n^{'}}{q_k}}).$$

As e_k is nonzero, at least one of $\omega_{k,1}, \ldots, \omega_{k,n}$ is nonzero, say $\omega_{k,t} \neq 0$. Then

$$\omega_{k,t}(\alpha^{\frac{q_t^{'}}{q_k}} + \beta^{\frac{q_t^{'}}{q_k}}) = \omega_{k,t}(\alpha+\beta)^{\frac{q_t^{'}}{q_k}},$$

for all $\alpha, \beta \in \mathbb{Z}_p$. Put $\alpha = \gamma^{q_k}$ and $\beta = \delta^{q_k}$. Then it follows that

$$(\gamma^{q_{t'}} + \delta^{q_{t'}})^{\frac{1}{q_{t'}}} = (\gamma^{q_k} + \delta^{q_k})^{\frac{1}{q_k}},$$

for all $\gamma, \delta \in \mathbb{Z}_p$. This can only happen if $q_t^{'} = q_k$, by Lemma 5, which then also implies that $\omega_{k,j} = 0$ if $q_j^{'} \neq q_k$.

Now assume that $q_k = q_t^{'} = q_{t+1}^{'} = \cdots = q_{t+s}^{'}$, where either $t = 1$ or $q_{t-1}^{'} < q_t^{'}$ and s as large as possible. Then

$$\begin{aligned}
\psi(e_k) &= (0, \ldots, 0, \omega_{k,t}, \ldots, \omega_{k,t+s}, 0, \ldots, 0) \\
\psi(e_{k+1}) &= (0, \ldots, 0, \omega_{k+1,t}, \ldots, \omega_{k+1,t+s}, 0, \ldots, 0) \\
\vdots &= \vdots \\
\psi(e_{k+l}) &= (0, \ldots, 0, \omega_{k+l,t}, \ldots, \omega_{k+l,t+s}, 0, \ldots, 0).
\end{aligned}$$

Now, if $s < l$, then the $l+1$ vectors $\psi(e_k), \ldots, \psi(e_{k+l})$ are linearly dependent in $V_{\mathbb{Z}_p}^{\prime}$. So there exist scalars $\xi_0, \ldots, \xi_l \in \mathbb{Z}_p$, not all zero, such that

$$\begin{aligned}
\textstyle\sum_{i=0}^{l} \psi(e_{k+i})\xi_i &= \textstyle\sum_{i=0}^{l} \psi(e_{k+i}\xi_i) \\
&= \psi(\textstyle\sum_{i=0}^{l} e_{k+i}\xi_i) \\
&= 0.
\end{aligned}$$

So $\sum_{i=0}^{l} e_{k+i}\xi_i = 0$, a contradiction, as $\{e_k, e_{k+1}, \ldots, e_{k+l}\}$ is linearly independent. So $s \geq l$. By considering the inverse isomorphism $\psi^{-1} : V_{\mathbb{Z}_p}^{\prime} \to V_{\mathbb{Z}_p}$, it follows similarly that $s \leq l$, implying that $s = l$.

Consequently, if there are exactly $l+1$ copies of q_k in the sequence $q_1 \leq q_2 \leq \cdots \leq q_n$, then there must be exactly $l+1$ copies of q_k $(= q_t^{'})$ in the sequence $q_1^{'} \leq q_2^{'} \leq \cdots \leq q_n^{'}$ as well. This means that the two sequences $q_1 \leq q_2 \leq \cdots \leq q_n$ and $q_1^{'} \leq q_2^{'} \leq \cdots \leq q_n^{'}$ are identical. ∎

THEOREM 8:

Let ϕ denote Euler's totient function. There are exactly $\binom{n + \phi(p-1) - 1}{n}$ n-dimensional near vector spaces over $\mathbb{Z}_p$, up to isomorphism. Each of these is completely determined by a choice of integers $1 \leq q_1 \leq \cdots \leq q_n \leq p-2$, $\gcd(q_i, p-1) = 1$ $(1 \leq i \leq n)$ that defines the scalar multiplication

$$(x_1, x_2, \ldots, x_n)\alpha = (x_1\alpha^{q_1}, x_2\alpha^{q_2}, \ldots, x_n\alpha^{q_n}).$$

Proof

There are $\phi(p-1)$ integers q_i such that $1 \leq q_i \leq p-2$ and $\gcd(q_i, p-1) = 1$. We need to choose n of these, and count the number of ways in which we obtain different sequences $q_1 \leq q_2 \leq \cdots \leq q_n$. This is the same as the number of selections of n objects chosen from $\phi(p-1)$ types, which is given by $\binom{n+\phi(p-1)-1}{n}$[[11], Theorem 2, p.197]. ∎

EXAMPLE 9:

For $n = 4$ and $p = 5$, we have $\binom{4+\phi(4)-1}{4} = \binom{5}{4} = 5$ distinct 4-dimensional near vector spaces over $\mathbb{Z}_5$, up to isomorphism. They are determined by the sequences

$$(q_1, q_2, q_3, q_4) \in \{(1,1,1,1), (1,1,1,3), (1,1,3,3), (1,3,3,3), (3,3,3,3)\}.$$

∎

THEOREM 10:

$V_{\mathbb{Z}_p}$ is a vector space if and only if $q_1 = q_2 = \cdots = q_n = 1$.

Proof

We know that the choice $q_1 = q_2 = \cdots = q_n = 1$ gives a vector space, since, in this case, the scalar multiplication is given by

$$(x_1, x_2, \ldots, x_n)\alpha = (x_1\alpha, x_2\alpha, \ldots, x_n\alpha),$$

for all $(x_1, x_2, \ldots, x_n) \in {\mathbb{Z}_p}^n$ and $\alpha \in \mathbb{Z}_p$. For any other choice of the q_i's, we have seen that non-isomorphic near vector spaces are created, so no one of them can be a vector space. (Vector spaces with a given dimension and over a given field are unique up to isomorphism). ∎

COROLLARY 11:

There is only one n-dimensional near vector space over $F = \mathbb{Z}_p$, $p \in \{2, 3\}$, namely (F^n, F), with scalar multiplication

$$(x_1, x_2, \ldots, x_n)\alpha = (x_1\alpha, x_2\alpha, \ldots, x_n\alpha),$$

and this is a vector space. ∎

It should now be clear why the case $p = 2$ follows trivially, as pointed out before Lemma 4.

Chapter 4

Homogeneous and Near Linear Transformations

4.1 Homogeneous Transformations

DEFINITION 1:

Let $(V,\ F)$ be a near vector space. A function $g : V \to V$ is called a *homogeneous transformation* of V if for each $x \in V$ and for each $\alpha \in F$,

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

■

The nearring $M_F(V)$ of homogeneous functions of V into itself (refer to Example 1.2-3),

$$M_F(V) := \{f : V \to V \mid f(x\alpha) = f(x)\alpha, \text{ for all } x \in V, \alpha \in F\}.$$

has the following subset

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

i.e. the set of all *linear mappings* from V to itself.

We start this chapter by proving that $L_F(V)$ is a ring. We use a slightly different approach.

PROPOSITION 2:

$L_F(V)$ is a subnearring of $M_F(V)$.

Proof

Since $0 \in L_F(V)$, $L_F(V)$ is nonempty. Now suppose that $s, s' \in L_F(V)$. Then since $s \in M_F(V)$, $-s \in M_F(V)$ and

$$\begin{aligned} -s(v_1) + (-s(v_2)) &= (-1)s(v_1) + (-1)s(v_2) \\ &= (-1)(s(v_1) + s(v_2)) \\ &= (-1)(s(v_1 + v_2)) \\ &= -s(v_1 + v_2). \end{aligned}$$

Thus $-s \in L_F(V)$.

Since $s, s' \in M_F(V)$, $s + s' \in M_F(V)$ and

$$\begin{aligned} (s + s')(v_1 + v_2) &= s(v_1 + v_2) + s'(v_1 + v_2) \\ &= s(v_1) + s(v_2) + s'(v_1) + s'(v_2) \\ &= s(v_1) + s'(v_1) + s(v_2) + s'(v_2) \\ &= (s + s')v_1 + (s + s')v_2. \end{aligned}$$

Thus $s + s' \in L_F(V)$.

Finally, since $s, s' \in M_F(V)$, $ss' \in M_F(V)$ and

$$\begin{aligned} (ss')(v_1 + v_2) &= s(s'(v_1 + v_2)) \\ &= s(s'(v_1) + s'(v_2)) \\ &= s(s'(v_1)) + s(s'(v_2)) \\ &= ss'(v_1) + ss'(v_2). \end{aligned}$$

Thus $ss' \in L_F(V)$. Thus $L_F(V)$ is a subnearring of $M_F(V)$. ∎

From Example 1.2-3, we have that V is a faithful $M_F(V)$-module. We also have that $L_F(V)$ is a subnearring of $M_F(V)$. Thus by restricting the identity representation of $M_F(V)$ on V to $L_F(V)$, we have that V is a faithful $L_F(V)$-module. In addition, since $(V, +)$ is abelian, $(L_F(V), +)$ is an abelian group. This allows us to use the next lemma ([8](Lemma 3.7, p.51)).

LEMMA 3:

Let V be an R-module with the properties:

(i) V is faithful as an R-module;

(ii) $(R, +)$ is an abelian group;

(iii) for all $r \in R$, the map $\rho_r : V \to V$ given by $\rho_r(v) := rv$ is an endomorphism of V;

Then R is a ring. ∎

THEOREM 4:

$L_F(V)$ is a ring.

Proof

Let $s \in L_F(V)$ and consider the map $\rho_s : V \to V$ defined by $\rho_s(v) := sv$.

Let $v_1, v_2 \in V$, then

$$\begin{aligned} \rho_s(v_1 + v_2) &= s(v_1 + v_2) \\ &= s(v_1) + s(v_2) \\ &= \rho_s(v_1) + \rho_s(v_2). \end{aligned}$$

Thus ρ_s is an endomorphism of V, so by Lemma 3, $L_F(V)$ is a ring. ∎

We start our next discussion with an example:

EXAMPLE 5:

Consider the near vector space (V, F) as defined in Example 3.1, i.e. $V := \mathbb{R}^2, F := \mathbb{R}$ and

$$\begin{pmatrix} x \\ y \end{pmatrix} \alpha := \begin{pmatrix} x\alpha \\ y\alpha^3 \end{pmatrix}$$

with $\alpha \in \mathbb{R}$ and $\begin{pmatrix} x \\ y \end{pmatrix} \in V$.

Furthermore, let

$$N := \{f : V \to V \mid f \text{ is a homogeneous transformation of } V\}.$$

Then N is 2-primitive on V:

Firstly, we know that N is a (right) nearring (refer to Example 1.2-3). Moreover, for

$u \neq 0$, and for each $x \in V$, there exists a $f_{u,x} \in N$ defined by

$$f_{u,x}(y) = \begin{cases} x\alpha & \text{if } y \neq 0 \text{ and } y = u\alpha \text{ for some } \alpha \in F, \\ 0 & \text{otherwise.} \end{cases}$$

(a) $f_{u,x}$ is well defined:

Case 1: Let $y \neq 0$ and $y = u\alpha$. Suppose that $u\alpha = u\alpha'$. Then $u(\alpha - \alpha') = 0$. Therefore, since $u \neq 0$, $\alpha = \alpha'$. Then $f_{u,x}(y) = x\alpha$.

Case 2: Let $y \neq 0$ and $y \neq u\alpha$ for each $\alpha \in F$. Then $f_{u,x}(y) = 0$.

Case 3: Let $y = 0$. Then $f_{u,x}(y) = 0$.

(b) $f_{u,x} \in N$:

It suffices to show that, for each $\beta \in F$,

$$f_{u,x}(y\beta) = (f_{u,x}(y))\beta.$$

Case 1: Let $y = 0$. Then for each $\beta \in F$, $y\beta = 0$. Hence $f_{u,x}(y\beta) = 0$, but $f_{u,x}(y) = 0$. Therefore $(f_{u,x}(y))\beta = 0$.

Case 2: Let $y \neq 0$ and $\beta = 0$. Then $f_{u,x}(y\beta) = f_{u,x}(0) = 0$ and $(f_{u,x}(y))\beta = (f_{u,x}(y))0 = 0$.

Case 3: Let $y \neq 0$, $\beta \neq 0$ and $y\beta = u\alpha$ for some $\alpha \in F$. Then $y = u\alpha\beta^{-1}$. Hence $f_{u,x}(y\beta) = x\alpha$ and $f_{u,x}(y) = x\alpha\beta^{-1}$. Therefore $f_{u,x}(y\beta) = (f_{u,x}(y))\beta$.

Case 4: Let $y \neq 0$, $\beta \neq 0$ and $y\beta \neq u\alpha$ for each $\alpha \in F$. Then $y \neq u\alpha$ for each $\alpha \in F$. Hence $f_{u,x}(y) = 0 = f_{u,x}(y\beta)$.

Clearly V is an N-module and V is monogenic, i.e. there exists a $u \neq 0 \in V$ such that $Nu = V$. We have that $Nu \subseteq V$ for every $u \neq 0 \in V$. Now take any $u \neq 0$ and any $x \in V$, then since $u = u1$, $f_{u,x}(u) = x$. Thus $V = Nu$ and so V is monogenic. In addition, since $V = Nu$ for every $u \neq 0 \in V$, V is of type 2.

Finally, V is faithful, since the zero mapping is an element of N and it is the only element of N that maps every element of V to zero.

Let $\mathbf{M_2}(F)$ be the 2 x 2 matrix ring over F. For each $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathbf{M_2}(F)$, we

define the mapping $A_\phi : V \to V$ by

$$A_\phi \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2^{\frac{1}{3}} \\ a_{21}x_1^3 + a_{22}x_2 \end{pmatrix}.$$

The mapping A_ϕ is an element of N:

Let $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in V$ and $\alpha \in F$. Then

$$\begin{aligned} A_\phi \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \alpha \right) &= A_\phi \begin{pmatrix} x_1\alpha \\ x_2\alpha^3 \end{pmatrix} \\ &= \begin{pmatrix} a_{11}x_1\alpha + a_{12}x_2^{\frac{1}{3}}\alpha \\ a_{21}x_1^3\alpha^3 + a_{22}x_2\alpha^3 \end{pmatrix} \\ &= \begin{pmatrix} (a_{11}x_1 + a_{12}x_2^{\frac{1}{3}})\alpha \\ (a_{21}x_1^3 + a_{22}x_2)\alpha^3 \end{pmatrix} \\ &= \begin{pmatrix} a_{11}x_1 + a_{12}x_2^{\frac{1}{3}} \\ a_{21}x_1^3 + a_{22}x_2 \end{pmatrix} \alpha \\ &= \left(A_\phi \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right) \alpha. \end{aligned}$$

However,

$$\begin{aligned} A_\phi \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) &= A_\phi \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix} \\ &= \begin{pmatrix} a_{11}(x_1 + y_1) + a_{12}(x_2 + y_2)^{\frac{1}{3}} \\ a_{21}(x_1 + y_1)^3 + a_{22}(x_2 + y_2) \end{pmatrix} \end{aligned}$$

and

$$A_\phi \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + A_\phi \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2^{\frac{1}{3}} \\ a_{21}x_1^3 + a_{22}x_2 \end{pmatrix} + \begin{pmatrix} a_{11}y_1 + a_{12}y_2^{\frac{1}{3}} \\ a_{21}y_1^3 + a_{22}y_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}(x_1 + y_1) + a_{12}(x_2^{\frac{1}{3}} + y_2^{\frac{1}{3}}) \\ a_{21}(x_1^3 + y_1^3) + a_{22}(x_2 + y_2) \end{pmatrix}.$$

Hence, in general,

$$A_\phi \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) \neq A_\phi \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + A_\phi \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Therefore $A_\phi : V \to V$ is in general not a linear transformation.

Let $X := \{A_\phi \mid A \in \mathbf{M_2}(F)\}$. Then $X \subseteq N$. Furthermore, let T be the subnearring of N generated by X, i.e. the intersection of all subnearrings of N which contain X.

Then T is 2-primitive on V:

First, we know that T is a subnearring of N. Hence, since V is an N-module, V is a T-module. But T is a set of functions on V, hence V is a faithful T-module.

Secondly, V is monogenic:

Let $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in V$. Then $\begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}_\phi \in T$ for any $x_3, x_4 \in \mathbb{R}$ and

$$\begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}_\phi \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 + 0 \\ x_2 + 0 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Hence $T \begin{pmatrix} 1 \\ 0 \end{pmatrix} = V$.

Finally, V is of type 2:

Let H be a T-submodule of V and let $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in H$ with $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

If $x_1 \neq 0$, then since $TH \subseteq H$,

$$\begin{pmatrix} x_1^{-1} & 0 \\ 0 & 0 \end{pmatrix}_\phi \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in H.$$

Hence $TH = V$. Therefore $H = V$.

If $x_1 = 0$, then

$$\begin{pmatrix} 0 & x_2^{-\frac{1}{3}} \\ 0 & 0 \end{pmatrix}_{\phi} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in H,$$

and so as before $H = V$.

Consequently, V does not contain any proper non-trivial T-submodules.

We now show that T is a proper subnearring of N:

Consider the orbit $B := \begin{pmatrix} 1 \\ 1 \end{pmatrix} F = \left\{ \begin{pmatrix} \alpha \\ \alpha^3 \end{pmatrix} \mid \alpha \in F \right\}$.

Define $e : V \to V$ by

$$e \begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} \begin{pmatrix} x \\ y \end{pmatrix} & \text{if } \begin{pmatrix} x \\ y \end{pmatrix} \in B \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} & \text{if } \begin{pmatrix} x \\ y \end{pmatrix} \notin B. \end{cases}$$

Then

$$e\left(\begin{pmatrix} x \\ y \end{pmatrix} \alpha\right) = e \begin{pmatrix} x\alpha \\ y\alpha^3 \end{pmatrix} = \begin{pmatrix} x\alpha \\ y\alpha^3 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \alpha = \left(e \begin{pmatrix} x \\ y \end{pmatrix}\right) \alpha,$$

if $\begin{pmatrix} x \\ y \end{pmatrix} \in B$, and

$$e\left(\begin{pmatrix} x \\ y \end{pmatrix} \alpha\right) = e \begin{pmatrix} x\alpha \\ y\alpha^3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \left(e \begin{pmatrix} x \\ y \end{pmatrix}\right) \alpha,$$

if $\begin{pmatrix} x \\ y \end{pmatrix} \notin B$. Hence $e \in N$.

Now elements of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}_{\phi}$ and products and sums of finitely many such elements are the only elements of T. We proceed to show that e is not in T, showing that T is a proper subnearring of N.

LEMMA 6:

Let $f(x,y) = f_1(x) + f_2(y)$, with $f_1 : \mathbb{R} \to \mathbb{R}$ and $f_2 : \mathbb{R} \to \mathbb{R}$ continuous on $\mathbb{R}$. Then $f : \mathbb{R}^2 \to \mathbb{R}$ is continuous on $\mathbb{R}^2$.

Proof

Let $(x_0, y_0) \in \mathbb{R}^2$. Then f_1 is continuous at x_0 and f_2 is continuous at y_0. Let $\epsilon > 0$. Then there exists $\delta_1 > 0$ and $\delta_2 > 0$ such that,

$$|f_1(x) - f_1(x_0)| < \frac{\epsilon}{2} \text{ if } |x - x_0| < \delta_1$$

and

$$|f_2(y) - f_2(y_0)| < \frac{\epsilon}{2} \text{ if } |y - y_0| < \delta_2.$$

Let $\delta = \min\{\delta_1, \delta_2\}$. If

$$\sqrt{(x - x_0)^2 + (y - y_0)^2} < \delta,$$

then

$$|x - x_0| < \delta \leq \delta_1 \text{ and } |y - y_0| < \delta \leq \delta_2.$$

Therefore

$$\begin{aligned} |f(x,y) - f(x_0,y_0)| &= |f_1(x) + f_2(y) - (f_1(x_0) + f_2(y_0))| \\ &= |f_1(x) - f_1(x_0) + f_2(y) - f_2(y_0)| \\ &\leq |f_1(x) - f_1(x_0)| + |f_2(y) - f_2(y_0)| \\ &\leq \tfrac{\epsilon}{2} + \tfrac{\epsilon}{2} \\ &= \epsilon. \end{aligned}$$

■

Continuing with the example, let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}_\phi : V \to V$ be a mapping defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}_\phi \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by^{\frac{1}{3}} \\ cx^3 + dy \end{pmatrix}$$

and let $g(x,y) = ax + by^{\frac{1}{3}}$ and $h(x,y) = cx^3 + dy$. But the functions k_1, k_2, k_3 and k_4, defined by $k_1(x) = ax$, $k_2(y) = by^{\frac{1}{3}}$, $k_3(x) = cx^3$ and $k_4(y) = dy$, are continuous on $\mathbb{R}$.

Hence, by Lemma 6, g and h are continuous on $\mathbb{R}^2$ $(= V)$.

Next, define $\theta : V \to V$ by

$$\theta(x, y) = (g(x, y), h(x, y)).$$

Let $\epsilon > 0$. Then there exist $\delta_1 > 0$ and $\delta_2 > 0$ such that

$$|g(x, y) - g(x_0, y_0)| < \frac{\epsilon}{\sqrt{2}} \quad \text{if} \quad \| (x, y) - (x_0, y_0) \| < \delta_1,$$

and

$$|h(x, y) - h(x_0, y_0)| < \frac{\epsilon}{\sqrt{2}} \quad \text{if} \quad \| (x, y) - (x_0, y_0) \| < \delta_2.$$

Let $\delta = \min\{\delta_1, \delta_2\}$. If

$$\| (x, y) - (x_0, y_0) \| = \sqrt{(x - x_0)^2 + (y - y_0)^2} < \delta,$$

then

$$\| (x, y) - (x_0, y_0) \| < \delta_1 \text{ and } \| (x, y) - (x_0, y_0) \| < \delta_2.$$

Therefore

$$\begin{aligned}
\| \theta(x, y) - \theta(x_0, y_0) \| &= \| (g(x, y), h(x, y)) - (g(x_0, y_0), h(x_0, y_0)) \| \\
&= \| (g(x, y) - g(x_0, y_0), h(x, y) - h(x_0, y_0)) \| \\
&= \sqrt{(g(x, y) - g(x_0, y_0))^2 + (h(x, y) - h(x_0, y_0))^2} \\
&< \sqrt{\tfrac{\epsilon^2}{2} + \tfrac{\epsilon^2}{2}} \\
&= \sqrt{\tfrac{2\epsilon^2}{2}} \\
&= \epsilon.
\end{aligned}$$

Consequently, $\theta \left(= \begin{pmatrix} a & b \\ c & d \end{pmatrix}_{\phi} \right)$ is continuous on V.

Furthermore, since the sum and the product of finitely many continuous functions are continuous, each element of T is continuous on V.

However,

$$\lim_{y \to 1} e(1, y)' = (0, 0)' \neq (1, 1)' = e(1, 1)'.$$

Therefore e is discontinuous at $(1, 1)'$. Consequently $e \notin T$. ∎

The next note is a summary of the properties of T that we have proved:

NOTE 5:

(a) T is a nearring with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{\phi}$.

(b) T is 2-primitive on the T-module V.

(c) T is not a ring.

(d) $T \subset N$.

The following theorem is a well-known result by Betsch. A proof can be found in [8](Theorem 3.35, p.65). Recall that

$$M_D(G) = \{\alpha \in M(G) \mid \alpha(gd) = (\alpha g)d \text{ for all } d \in D, g \in G\} \text{ (Example 1.2-3),}$$

where D is a semigroup of endomorphisms of G. We need a definition first.

DEFINITION 7:

Let M be a subnearring of the nearring N with a natural faithful representation on the N-module V. Then M is said to be *dense* in N if given any finite subset $\{v_1, v_2, \ldots, v_k\}$, $k \geq 1$, of V and any element n of N, there exists an $m \in M$ such that $mv_i = nv_i$ for $1 \leq i \leq k$. ∎

THEOREM 8:

Let R be a nearring with identity which is 2-primitive on the R-module G. Let $C := End_R G$, $D := Aut_R G$. Then $R \subseteq M_D G$, $C = D^0$, D is fix point free and either R is a primitive ring on the faithful simple R-module G or R is not a ring and is a dense subnearring of $M_D G$. ∎

Therefore by Note 5,

COROLLARY 9:

T is a proper dense subnearring of N. ∎

Example 5 sets the scene for a more general situation, discussed in [12] and [13].

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

ring of linear transformations of V, also known as the ring of F-endomorphisms of V, which can be identified with the ring $\mathcal{M}_n(F)$, the ring of $n \times n$ matrices over F (See [3](Proposition 3.1.12, p.145)). This ring is contained in the second structure, namely the nearring $M_F(V)$ of homogeneous functions of V into itself. The object is to consider "perturbations" in the action of F on V and to investigate the effects thereof on $\mathcal{M}_n(F)$. To be more specific, we wish to change the action of the group $(F^*, \cdot)$ on V in such a way that it remains a group of *fix point free automorphisms of* V, i.e. if $\lambda \in F^*$, $v \neq 0 \in V$ and $v\lambda = v$, then $\lambda = 1$.

DEFINITION 10:

A *perturbation* in the action of F on V is an n-vector $\Psi := (\psi_i)$ of automorphisms of the group with zero $(F, \cdot)$. The action of F on V under the perturbation Ψ is defined by

$$(x_i) \circ_\Psi \lambda := (x_i \psi_i(\lambda)) \text{ for all } (x_i) \in V, \lambda \in F,$$

and the corresponding nearring of (F, V)-functions,

$$\{f : V \to V \mid f((x_i) \circ_\Psi \lambda) = f((x_i)) \circ_\Psi \lambda \text{ for all } (x_i) \in V, \lambda \in F\},$$

is denoted by $M_{(F,\Psi)}(V)$. ∎

Let $I = \{1, 2, \ldots, n\}$ from now on.

PROPOSITION 11:

(V, F), under the perturbed action defined above, is a near vector space.

Proof

First we will show that (V, F) is an F-group:

(F_1): $(V, +)$ is a group:

(i)

$$\begin{aligned} [(\xi_i) + (\eta_i)] + (\alpha_i) &= (\xi_i + \eta_i) + (\alpha_i) \\ &= ((\xi_i + \eta_i) + \alpha_i) \\ &= (\xi_i + (\eta_i + \alpha_i)) \\ &= (\xi_i) + [(\eta_i) + (\alpha_i)]. \end{aligned}$$

Thus $(V, +)$ is associative.

(ii) (0) is an element of $(V, +)$ and moreover, it is the identity of $(V, +)$ since

$$(\xi_i) + (0) = (\xi_i + 0) = (\xi_i)$$

and

$$(0) + (\xi_i) = (0 + \xi_i) = (\xi_i).$$

(iii) For each $(\xi_i) \in V$, $(-\xi_i) \in V$ and

$$(\xi_i) + (-\xi_i) = (\xi_i - \xi_i) = (0)$$

and

$$(-\xi_i) + (\xi_i) = (-\xi_i + \xi_i) = (0).$$

So $-(\xi_i) = (-\xi_i) \in V$.

Furthermore, F is a set of endomorphisms of V, since,

$$\begin{aligned}
[(\xi_i) + (\eta_i)]\lambda &= (\xi_i + \eta_i)\lambda \\
&= ((\xi_i + \eta_i)\psi_i(\lambda)) \\
&= (\xi_i\psi_i(\lambda) + \eta_i\psi_i(\lambda)) \text{ since } F \text{ is right distributive,} \\
&= (\xi_i\psi_i(\lambda)) + (\eta_i\psi_i(\lambda)) \\
&= (\xi_i)\lambda + (\eta_i)\lambda.
\end{aligned}$$

(F_2):

The endomorphisms $0, 1, -1$ defined by

$$(\xi_i)0 = (\xi_i\psi_i(0)) = (0),$$

$$(\xi_i)1 = (\xi_i\psi_i(1)) = (\xi_i),$$

$$(\xi_i)(-1) = (\xi_i\psi_i(-1)) = (\xi_i(-1)) = (-\xi_i),$$

with $(\xi_i) \in V$, are elements of F.

(F_3):

Let $\lambda \in F^*$. Then λ is a bijection:

Let $(\xi_i)\lambda = (\eta_i)\lambda$, then $(\xi_i\psi_i(\lambda)) = (\eta_i\psi_i(\lambda))$ which implies that $\xi_i\psi_i(\lambda) = \eta_i\psi_i(\lambda)$ for each $i \in I$ and so $(\xi_i - \eta_i)\psi_i(\lambda) = 0$. Thus for each $i \in I$, since $\lambda \neq 0$, $\xi_i = \eta_i$, which implies that $(\xi_i) = (\eta_i)$. Thus λ is an injection.

Now let (ξ_i) be an element of V. Then since ψ_i is an automorphism for each $i \in I$, ψ_i^{-1} exists for each $i \in I$ and $\psi_i^{-1}(\lambda) \in F$. But $(\xi_i\psi_i^{-1}(\lambda))\lambda = (\xi_i\psi_i^{-1}(\lambda)\psi_i(\lambda)) = (\xi_i)$. Hence λ is surjective.

Consequently F^* is a subset of the automorphism group of $(V, +)$. But F is a field. Hence F^* is a subgroup of the automorphism group of $(V, +)$.

(F_4):

Let $(\xi_i)\lambda = (\xi_i)\mu$. Then $(\xi_i\psi_i(\lambda)) = (\xi_i\psi_i(\mu))$, which implies that for each $i \in I$, $\xi_i\psi_i(\lambda) = \xi_i\psi_i(\mu)$. Suppose that $\lambda \neq \mu$, then $\psi_i(\lambda) \neq \psi_i(\mu)$ for each $i \in I$ (ψ_i is an automorphism for each $i \in I$). If there exists a $j \in I$ such that $\xi_j \neq 0$, $\xi_j^{-1} \in F$ and $\xi_j^{-1}\xi_j\psi_i(\lambda) = \xi_j^{-1}\xi_j\psi_i(\mu)$. Therefore, $\psi_i(\lambda) = \psi_i(\mu)$, a contradiction. Hence $\xi_i = 0$ for each $i \in I$.

Finally, we show that $Q(V)$ generates $(V, +)$:

Let $e_j := (\delta_{ji})_{i\in I}$, where δ_{ji} is the Kronecker symbol. Then, for every $\alpha, \beta \in F$,

$$\begin{aligned} e_j\alpha + e_j\beta &= (\delta_{ji}\psi_i(\alpha)) + (\delta_{ji}\psi_i(\beta)) \\ &= (\delta_{ji}\psi_i(\alpha) + \delta_{ji}\psi_i(\beta)) \\ &= (\delta_{ji}(\psi_i(\alpha) + \psi_i(\beta))) \\ &= e_j\psi_j^{-1}(\psi_j\alpha + \psi_j\beta). \end{aligned}$$

Thus $\{e_j \mid j \in I\} \subseteq Q(V)$ and since every element of V is of the form $\sum_{j\in K} e_j\lambda_j$, with $\lambda_j \in F$ and K a finite subset of I, $Q(V)$ generates V. ∎

NOTE 11:

(i) V under this perturbed action is not generally a vector space. As a counter example consider Example 3.1. Put $\psi_1(\alpha) := \alpha$ and $\psi_2(\alpha) := \alpha^3$ for each $\alpha \in F$. Then $(x_1, x_2)\alpha = (x_1\alpha, x_2\alpha^3)$. Since (Q_2) does not hold in general, V is not regular and therefore not a vector space.

(ii) $M_F(V) = M_{(F,\mathbf{1})}(V)$ where $\mathbf{1}$ is an n-vector of identity automorphisms, the *identity perturbation.*

Next we ask what substructure of $M_{(F,\Psi)}(V)$ should be regarded as the counterpart of $\mathcal{M}_n(F)$ in $M_{(F,\mathbf{1})}(V)$. The answer is derived from the following result:

LEMMA 12:

$\mathcal{M}_n(F)$ is the smallest 2-primitive subnearring of $M_{(F,\mathbf{1})}(V)$ that contains all the distributive elements of $M_{(F,\mathbf{1})}(V)$.

Proof

For each $(x_i) \in V$, define $h_{(x_i)}$ by $h_{(x_i)}(e_1\lambda) := (x_i\lambda)$ for all $\lambda \in F$, 0 otherwise. Then $h_{(x_i)}$ is in $M_{(F,\mathbf{1})}(V)$:

Let $\lambda \in F$, $(y_i) \in V$. Then

$$\begin{aligned} h_{(x_i)}((y_i)\lambda) &= \begin{cases} (x_i y_1 \lambda) & \text{if } y_i = 0 \text{ for all } i \geq 2 \\ 0 & \text{otherwise} \end{cases} \\ &= (h_{(x_i)}(y_i))\lambda. \end{aligned}$$

For a function f to be distributive in $M_{(F,\mathbf{1})}(V)$ it implies that

$$f \circ (h_{(x_i)} + h_{(y_i)}) = f \circ h_{(x_i)} + f \circ h_{(y_i)}.$$

This in turn implies that

$$f((x_i) + (y_i)) = f(x_i) + f(y_i),$$

so f is an endomorphism, i.e. $f \in End_F(V)$. So the distributive elements in $M_{(F,\mathbf{1})}(V)$ are exactly the F-endomorphisms of V.

Next we show that $\mathcal{M}_n(F)$ is 2-primitive on V. Let $(y_i) \in V$ with (y_i) nonzero. Let $(z_i) \in V$. If $y_r \neq 0$, then $(d_{ij})(y_i) = (z_i)$ with $d_{ij} = 0$ if $j \neq r$ and $d_{ir} = z_i y_r^{-1}$.

Finally since $\mathcal{M}_n(F)(\cong End_F(V))$ consists exactly of all the distributive elements of $M_F(V)$, it must be the smallest 2-primitive subnearring of $M_F(V)$ that contains all the distributive elements of $M_F(V)$. ∎

So our aim is to find the smallest 2-primitive subnearring of $M_{(F,\Psi)}(V)$ that contains all the distributive elements of $M_{(F,\Psi)}(V)$.

DEFINITION 13:

The subnearring of $M_{(F,\Psi)}(V)$ generated by the set of all square matrices, $C := (c_{ij})$, where $c_{ij} \in F$, with the action on V defined by

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

where $\vartheta_{ij} = \psi_i\psi_j^{-1}$, is called the *nearring of near linear transformations of the near vector space* $(V,\ F_\Psi)$, where F_Ψ indicates the action of F under the perturbation Ψ. It will be denoted by $\mathcal{M}_n(F, \Theta)$, where $\Theta = (\vartheta_{ij})$ denotes the matrix of automorphisms of $(F,\ \cdot)$ used here. ∎

This nearring is the desired candidate:

THEOREM 14:

$\mathcal{M}_n(F, \Theta)$ is the smallest 2-primitive subnearring of $M_{(F,\Psi)}(V)$ which contains every distributive element of $M_{(F,\Psi)}(V)$. ∎

THEOREM 15:

$\mathcal{M}_n(F, \Theta)$ is a simple nearring. ∎

Proofs of the above two theorems can be found in [12] (Theorem 2, p.191 and Theorem 4, p.192 respectively).

For our next result we need to branch into matrix nearrings. We will only define the basic structures needed for the proof. We refer the reader to [9] for more information.

Let n be any natural number and let $(N,\ +,\ \cdot)$ be a nearring with identity. Denote by N^n the direct sum of n copies of the group $(N,\ +)$. Note that $(N,\ +)$ is not necessarily abelian.

To each element r of N there corresponds a function $f^r : N \to N$ defined by $f^r(s) = rs$

for all $s \in N$. We define $n \times n$ matrices as functions from N^n to N^n. As building blocks for these matrices, we introduce the functions $f_{ij}^r : N^n \to N^n$, where $f_{ij}^r := \iota_i f^r \pi_j$ for $1 \leq i, j \leq n$ and $r \in N$, where the symbols ι_j and π_j will respectively denote the familiar j-th coordinate injection and projection functions. In the ring case, f_{ij}^r corresponds to an $n \times n$ matrix with r in the (i, j)-th position and 0 elsewhere.

DEFINITION 16:

The nearring of $n \times n$ matrices over N, denoted by $\mathbb{M}_n(N)$, is the subnearring of $M(N^n)$ generated by the set $\{f_{ij}^r \,|\, r \in N, 1 \leq i, j \leq n\}$. The elements of $\mathbb{M}_n(N)$ will be referred to as $n \times n$ matrices over N. ∎

The following proposition is taken from [9](Proposition 1.3, p.2).

PROPOSITION 17:

If R is a ring with identity, then $\mathbb{M}_n(R)$ is isomorphic to the usual full ring of $n \times n$ matrices over R. ∎

THEOREM 18:

For any specific pair (i, j): $f_{ij}^r \in \mathcal{M}_n(F, \Theta)$ for all $r \in F$ if and only if $\psi_i = \psi_j$.

Proof

Suppose $f_{ij}^r \in \mathcal{M}_n(F, \theta)$ for all $r \in F$ and a specific pair (i, j). Let $(x_i) \in V$ and $b \in F$ be arbitrary.

Then

$$\begin{aligned} f_{ij}^r((x_i) \circ_\Psi b) &= f_{ij}^r((x_i\psi_i(b)) \\ &= \iota_i f^r \pi_j((x_i\psi_i(b))) \\ &= (0, 0, \ldots, 0, rx_j\psi_j(b), 0, 0, \ldots, 0), \text{ with } rx_j\psi_j(b) \text{ in the } i\text{-th position,} \end{aligned}$$

while

$$\begin{aligned} f_{ij}^r((x_i)) \circ_\Psi b &= \iota_i f^r \pi_j((x_i)) \circ_\Psi b \\ &= (0, 0, \ldots, 0, rx_j, 0, \ldots, 0) \circ_\Psi b, \text{ with } rx_j \text{ in the } i\text{-th position} \\ &= (0, 0, \ldots, 0, rx_j\psi_i(b), 0, 0, \ldots, 0), \text{ with } rx_j\psi_i(b) \text{ in the } i\text{-th position.} \end{aligned}$$

But $f_{ij}^r((x_i) \circ_\Psi b) = f_{ij}^r((x_i)) \circ_\Psi b$, thus $\psi_j(b) = \psi_i(b)$ for all $b \in F$, so $\psi_j = \psi_i$.

Conversely, suppose that $\psi_i = \psi_j$. Let $r \in F$ and consider the matrix

$$C = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & r & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

with r in position (i, j) and zeros elsewhere. Then, by Definition 13, for arbitrary $(x_i) \in V$,

$$\begin{aligned} C((x_i)) &= \iota_i(r\vartheta_{ij}(x_j)) \\ &= \iota_i(r\psi_i\psi_j^{-1}(x_j)) \\ &= \iota_i(rx_j), \text{ since } \psi_i = \psi_j \\ &= \iota_i f^r \pi_j((x_i)) \\ &= f_{ij}^r((x_i)). \end{aligned}$$

So $f_{ij}^r = C \in \mathcal{M}_n(F, \Theta)$. ∎

COROLLARY 19:

$\mathbb{M}_n(F)$ is a subnearring of $\mathcal{M}_n(F, \Theta)$ if and only if $\psi_1 = \psi_2 = \cdots = \psi_n$.

Proof

Assume that $\psi_1 = \psi_2 = \cdots = \psi_n$. By definition, $\mathbb{M}_n(F)$ is the subnearring of $M(V)$ generated by $\{f_{ij}^r \,|\, r \in F, 1 \leq i, j \leq n\}$. So it is sufficient to prove that each $f_{ij}^r \in \mathcal{M}_n(F, \Theta)$. But as $\psi_1 = \psi_2 = \cdots = \psi_n$, the result follows directly from Theorem 18.

The converse follows trivially. ∎

4.2 The Nearring of Near Linear Transformations

We now present a summary of the results found in [13]. Throughout this section N will denote a zero-symmetric right nearring with identity 1 and all N-modules will be required to be *unitary,* i.e. if G is an N-module, then $1g = g$ for all $g \in G$.

DEFINITION 1:

If the nearring N 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

(i) $e_1 + e_2 + \cdots + e_n = 1$;

(ii) $e_i e_j = 0$ if $i \neq j$;

(iii) each e_i is of rank **1** (see [8](Definition 4.3, p.70) for the definition of rank) and

(iv) each e_i is a distributive element of N;

then N is called a *CDI-nearring.* ∎

Recall that if V is a group and A is group of automorphisms of V, then the centralizer nearring $M_A(V)$ (see Example 1.2-3) is defined by:

$$M_A(V) := \{\alpha \in M(V) \mid \alpha(va) = (\alpha v)a \text{ for all } a \in A, v \in V\}.$$

In his article [12](Theorem 3.4, p.301) van der Walt derives two characterizations of finite dimensional near vector spaces:

THEOREM 2:

Let V be a group and let $A := D \cup \{0\}$, where D is a fix point free group of automorphisms of V. Then

(i) (V, A) is a finite dimensional near vector space if and only if $M_A(V)$ is a CDI-nearring;

(ii) (V, A) is a finite dimensional near vector space if and only if there exists a finite number of nearfields, $F_1, F_2, \ldots, F_n$, semigroup isomorphisms $\psi_i : A \to F_i$ and a group isomorphism $\Phi : V \to F_1 \oplus F_2 \oplus \cdots \oplus F_n$ such that if

$$\Phi(v) = x_1 + x_2 + \cdots + x_n, \quad (x_i \in F_i)$$

then

$$\Phi(v\alpha) = x_1\psi_1(\alpha) + x_2\psi_2(\alpha) + \cdots + x_n\psi_n(\alpha),$$

for all $v \in V$ and $\alpha \in A$. ∎

According to this theorem we can specify a finite dimensional near vector space by taking n nearfields $F_1, F_2, \ldots, F_n$ 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 $(F_{i_o}, \cdot)$ as the semigroup of endomorphisms by defining

$$(x_1, x_2, \ldots, x_n)\alpha := x_1\vartheta_{1i_o}(\alpha) + x_2\vartheta_{2i_o}(\alpha) + \cdots + x_n\vartheta_{ni_o}(\alpha),$$

for all $x_j \in F_j$ and all $\alpha \in F_{i_o}$.

Our object is to study the nearring

$$N := M_{F_{i_o}}(V).$$

More specifically, we follow our line of thought in Section 4.1, i.e. we would like to determine the smallest subnearring S of N which contains the complete set of distributive idempotents $\{e_1, e_2, \ldots, e_n\}$ where e_j is defined by $e_j(x_1+x_2+\cdots+x_n) := x_j$, and which is 2-primitive on V. Since S is supposed to be 2-primitive, given any $(b_{1j}, b_{2j}, \ldots, b_{nj})' \in V$, (we are adopting vector notation, letting transposes be indicated by primes), S must contain an element s_j such that $s_j(0, 0, \ldots, 0, 1, 0, \ldots, 0)' = (b_{1j}, b_{2j}, \ldots, b_{nj})'$, where the 1 is in position j. Now, if $(x_1, x_2, \ldots, x_n)' \in V$, then

$$\begin{aligned} s_j e_j(x_1, x_2, \ldots, x_n)' &= s_j(0, 0, \ldots, 0, x_j, 0, \ldots, 0)' \\ &= s_j(0, \ldots, 0, 1, 0, \ldots, 0)'\vartheta_{ji_o}^{-1}(x_j) \\ &= (b_{1j}, b_{2j}, \ldots, b_{nj})'\vartheta_{ji_o}^{-1}(x_j) \\ &= (b_{1j}\vartheta_{1j}(x_j), b_{2j}\vartheta_{2j}(x_j), \ldots, b_{nj}\vartheta_{nj}(x_j))'. \end{aligned}$$

It follows that $\sum_{j=1}^{n} s_j e_j$ is in S; and the above calculation shows that it can adequately be denoted by the matrix (b_{ij}). In fact, every square matrix $C := (c_{ij})$, where $c_{ij} \in F_i$, represents an element of S, with the action on V defined by

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} c_{11}\vartheta_{11}(x_1) + \cdots + c_{1n}\vartheta_{1n}(x_n) \\ \vdots \\ c_{n1}\vartheta_{n1}(x_1) + \cdots + c_{nn}\vartheta_{nn}(x_n) \end{pmatrix}. \tag{4.1}$$

DEFINITION 3:

The subnearring of $M_{F_{i_o}}(V)$ generated by the set of all square matrices with their action

on V as defined in (4.1) is called the *nearring of matrices determined by the nearfields* $F_1, F_2, \ldots, F_n$ *and the matrix of isomorphisms* (ϑ_{ij}), and is denoted by $\mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$.

■

NOTE 3:

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

THEOREM 4:

$\mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$ is 2-primitive on V.

Proof

Let $(y_1, y_2, \ldots, y_n)' \in V$ be nonzero and let $(z_1, z_2, \ldots, z_n)' \in V$. If $y_r \neq 0$, then $(d_{ij})(y_1, y_2, \ldots, y_n)' = (z_1, z_2, \ldots, z_n)'$, where $d_{ij} = 0$ if $j \neq r$ and $d_{ir} = z_i(\vartheta_{ir}(y_r^{-1}))$. ■

Thus by the discussion preceding Definition 3, $\mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$ must equal S.

We formulate the preceding observations in:

THEOREM 5:

Suppose (V, A) is an n-dimensional near vector space. Then $M_A(V)$ contains a subnearring S isomorphic to a nearring of matrices determined by n nearfields with isomorphic multiplicative semigroups. If S is not a ring, then S is dense in $M_A(V)$. ■

COROLLARY 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 nearfields with isomorphic multiplicative semigroups. ■

Proofs of the above theorem and corollary can be found in [13](Theorem 3.5, p.302 and Corollary 3.6, p.303). The proof of the next theorem is identical to the proof of Theorem 4.1-14 in [12].

THEOREM 7:

$\mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$ is a simple nearring. ■

Let us look at an example:

EXAMPLE 8:

Let $F_1 = F_2 := \mathbb{R}$, the field of real numbers. Let ϑ_{11} and ϑ_{22} be the identity function, and let ϑ_{12} be defined by $\vartheta_{12}(x) := x^{\frac{1}{3}}$ and $\vartheta_{21}(x) := x^3$. Put $V := F_1 \oplus F_2 = \mathbb{R}^2$. Then the situation reduces to what we had in Example 4.1-5, where of course $\mathcal{M}_2(\{F_i\}, (\vartheta_{ij}))$ is just T. ∎

It seems natural now to ask, in the case where the F_i are infinite, is there a constructive way to show that $\mathcal{M}_n(\{F_i\}, (\vartheta_{ij})) = S \subset M_{F_{i_o}}(V)$, for example, can we show that the map that is the identity on one orbit of F_{i_o} on V, and zero elsewhere, is not in S? (See Example 4.1-5).

We have not been able to answer this specific question, but we can still show that S is a proper subnearring of $M_{F_{i_o}}(V)$ by using cardinality arguments.

THEOREM 9:

Let F_{i_o} be infinite, say $|F_{i_o}| = \kappa \geq \mathcal{X}_o$. Then $|S| < |M_{F_{i_o}}(V)|$.

Proof

A full set of orbit representatives of F_{i_o} on $V \cong F_{i_o}^n$ is given by

$$W = \{(1, a_2, \ldots, a_n)\} \cup \{(0, 1, a_3, \ldots, a_n)\} \cup \cdots \cup \{(0, 0, \ldots, 0, 1)\}.$$

Thus $|W| = |V| = \kappa$.

An element of $M_{F_{i_o}}(V)$ is known once its values are known at each $\alpha \in W$. So $|M_{F_{i_o}}(V)|$ equals the number of functions from W to V, which is $|V|^{|W|} = \kappa^\kappa$. But

$$\begin{aligned}
\kappa^\kappa &\geq 2^\kappa \text{ ([7] Exercise 10(c))} \\
&= |\mathcal{P}(F_{i_o})| \text{ ([7] Exercise 10(f))} \\
&> |F_{i_o}| = \kappa \text{ ([7] Theorem 8.5)} \\
&= |fin(F_{i_o})| \text{ ([7] Corollary 8.13)} \\
&= |S|, \text{ since each element of } S \text{ is expressed using only finitely many elements of } F_{i_o}.
\end{aligned}$$

∎

COROLLARY 10:

$\mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$ is a proper subnearring of $M_{F_{i_o}}(V)$ in the case where F_{i_o} is infinite. ∎

In the last two sections of this thesis, we take a closer look at $S = \mathcal{M}_n(\{F_i\}, (\vartheta_{ij}))$.

4.3 Some Left Ideals of S

Since S (as defined in Section 4.2) is 2-primitive on V (Theorem 4.2-4),

$$S\alpha = V, \text{ where } \alpha \text{ is any nonzero element of } V. \tag{4.2}$$

The map $\phi : S \to V$, with $\phi(U) = U\alpha$, for all $U \in S$ is an S-homomorphism between the S-modules ${}_SS$ and ${}_SV$. By (4.2), ϕ is in fact an S-epimorphism. Now,

$$\ker \phi = \{U \in S \,|\, U\alpha = \mathbf{0}\} = L,$$

say. So $S/L \cong V$ as S-modules and since V is a simple S-module, S/L is also simple as an S-module. This implies that L is a maximal left ideal of the nearring S. That L is a left ideal follows from [10](Corollary 1.43(a), p.21).

EXAMPLE 1:

If $\beta = (1, 0, \ldots, 0)'$, then

$$L = \{U \in S \,|\, U\beta = (0, 0, \ldots, 0)'\}$$

is a maximal left ideal of S. ∎

THEOREM 2:

The L of Example 1 contains the left ideal of S generated by

$$X = \left\{ \begin{pmatrix} 0 & c_{12} & \cdots & c_{1n} \\ 0 & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{2n} & \cdots & c_{nn} \end{pmatrix} \,|\, c_{ij} \in F_i \right\}.$$

Proof

Clearly, since every element of X is in L, $\mathrm{li}\langle X\rangle \subseteq L$. ∎

Next we turn our attention to

$$L_k = \mathrm{Ann}_S(F_1 \oplus \cdots \oplus F_{k-1} \oplus \{0\} \oplus F_{k+1} \oplus \cdots \oplus F_n).$$

It is known that in the case of a vector space, L_k is a minimal left ideal. In the case of a near vector space, the general question remains open; however, we do have the following:

THEOREM 3:

If one of $F_1, \ldots, F_{k-1}, F_{k+1}, \ldots, F_n$ is not a field, then L_k is not minimal.

Proof

Say F_1 is not a field (where $1 < k \leq n$). Then there exists $a, b, c \in F_1$ such that $a(b+c) \neq ab + ac$.

Consider

$$U = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \left[\begin{pmatrix} b & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} + \begin{pmatrix} 0 & \cdots & c & \cdots & 0 \\ 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \right] +$$

$$\begin{pmatrix} 0 & \cdots & -ac & \cdots & 0 \\ 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} + \begin{pmatrix} -ab & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

with c and $-ac$ in the k-th column.

Then $U \in L_k \cap L_1$.

Also, $U \neq 0$, since

$$U(1, 1, \ldots, 1)' \neq (0, 0, \ldots, 0)' \quad (a(b+c) - ab - ac \neq 0, \text{ by hypothesis}).$$

Furthermore, $L_k \cap L_1 \subset L_k$,

For example,

$$\begin{pmatrix} 0 & \cdots & 1 & \cdots & 0 \\ 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \in L_k \backslash L_1.$$

So $0 \neq U \in L_k \cap L_1 \subset L_k$. This implies that L_k is not minimal. ∎

4.4 The Kernel and Image of Elements of S

In this section we turn our attention to the kernel and image of elements of S. The question arises whether or not for any $U \in S$, $\ker U$ and $\operatorname{im} U$ are subspaces of V.

THEOREM 1:

For any $U \in S$, $\ker U$ and $\operatorname{im} U$ are not generally subspaces of S.

Proof

As a counterexample, we refer to Example 4.1-5. Put $A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$. Consider the following two elements of V, $\begin{pmatrix} 2 \\ 2^3 \end{pmatrix}$ and $\begin{pmatrix} 3 \\ 3^3 \end{pmatrix}$. Both these elements are in $\ker A_\phi$:

$$A_\phi \begin{pmatrix} 2 \\ 2^3 \end{pmatrix} = \begin{pmatrix} 2 + (-1)(2) \\ -2^3 + 2^3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

and

$$A_\phi \begin{pmatrix} 3 \\ 3^3 \end{pmatrix} = \begin{pmatrix} 3 + (-1)(3) \\ -3^3 + 3^3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

But $\begin{pmatrix} 2 \\ 2^3 \end{pmatrix} + \begin{pmatrix} 3 \\ 3^3 \end{pmatrix} = \begin{pmatrix} 5 \\ 35 \end{pmatrix} \notin \ker A_\phi$:

$$A_\phi \begin{pmatrix} 5 \\ 35 \end{pmatrix} = \begin{pmatrix} 5 - 35^{\frac{1}{3}} \\ -5^3 + 35 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Thus $\ker A_\phi$ is not a subspace of V.

Now consider $\begin{pmatrix} 2 \\ -2 \end{pmatrix}$. Then $\begin{pmatrix} 2 \\ -2 \end{pmatrix} \in \operatorname{im} A_\phi$:

$$A_\phi \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ -2 \end{pmatrix}.$$

But $\begin{pmatrix} 2 \\ -2 \end{pmatrix} + \begin{pmatrix} 2 \\ -2 \end{pmatrix} = \begin{pmatrix} 4 \\ -4 \end{pmatrix} \notin \operatorname{im} A_\phi$:

Suppose $\begin{pmatrix} 4 \\ -4 \end{pmatrix} \in \operatorname{im} A_\phi$, then

$$A_\phi \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 \\ -4 \end{pmatrix},$$

i.e.

$$\begin{pmatrix} x - y^{\frac{1}{3}} \\ -x^3 + y \end{pmatrix} = \begin{pmatrix} 4 \\ -4 \end{pmatrix},$$

which implies that

$$x - y^{\frac{1}{3}} = 4 \tag{4.3}$$

and

$$-x^3 + y = -4. \tag{4.4}$$

From (4.3), $y^{\frac{1}{3}} = x - 4$, thus $y = (x-4)^3$. From (4.4), $y = -4 + x^3$. Thus

$$\begin{aligned} -4 + x^3 &= (x-4)^3 \\ &= (x-4)(x^2 - 8x + 16) \\ &= x^3 - 8x^2 + 16x - 4x^2 + 32x - 64. \end{aligned}$$

Thus $-12x^2 + 48x - 60 = 0$ with no real solutions, as $48^2 - 4(-12)(-60) < 0$, and thus there are no real solutions for y as well. Thus $\operatorname{im} A_\phi$ is not a subspace of V. ∎

Bibliography

[1] J. André, *Lineare Algebra über Fastkörpern,* Math. Z. **136** (1974), 295-313.

[2] D.M. Burton, *Elementary Number Theory,* Mc Graw-Hill, Sixth Edition, 2007.

[3] J.A. Beachy, *Introductory Lectures on Rings and Modules,* London Mathematical Society **47**, 1999.

[4] J. Clay, *Nearrings - Geneses and Applications*, Oxford Science Publications, 1992.

[5] A. de Bruyn, *Near Vector Spaces,* MSc Dissertation, University of Stellenbosch, 1990.

[6] J.A. Gallian, *Contemporary Abstract Algebra,* Houghton Mifflin Company, Fourth Edition, 1998.

[7] T. Hungerford, *Algebra,* Graduate Texts in Mathematics, Springer Science Media, 1974.

[8] J.D.P Meldrum, *Near-rings and Their Links with Groups,* Advanced Publishing Program **134**, Pitman, New York 1985.

[9] J.H. Meyer, *Matrix Near-Rings,* PhD. Thesis, University of Stellenbosch, 1986.

[10] G. Pilz, *Near-rings: The Theory and its Applications,* Revised Edition, Mathematics studies **23**, North Holland, New York 1983.

[11] A. Tucker, *Applied Combinatorics,* Third Edition, John Wiley and Sons Incorporated, 1995.

[12] A.P.J. van der Walt, *Near-Linear Transformations of Near-Vector Spaces,* Proceedings of a Conference held at Oberwolfach, 5-11 Nov. 1989 (ed. G. Betsch, G. Pilz, H. Wefelscheid), Univ. of Duisburg (1995), 189-193.

[13] A.P.J. van der Walt, *Matrix Near-Rings Contained in 2-Primitive Near-Rings with Minimal Subgroups,* J. Algebra, **148**, (1992), 296-304.