Int. J. Math. And Appl., 10(3)(2022), 1–17
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of *Mathematics And its Applications*

The Decomposition Theorem for Near Vector Spaces

Jeromy Kalunga[1,*], Kelone Tefoetsile[2], Henry. M. Phiri[3] and Saviour Chibeti[3]

1 Department of Mathematics, Copperbelt University, Kitwe, Zambia.

2 Department of Mathematics and Statistical Sciences, Bostwana International University of Science and Technology, Palapye, Botswana.

3 Economics Department, University of Lusaka, Lusaka, Zambia.

Abstract: In this paper, we study the Decomposition Theorem for near vector space defined by André [1] and we then show how the theorem can be used to determine the cardinality of the quasi-kernel of finite dimensional near vector spaces as in [2].

Keywords: Vector spaces, Near vector spaces, Regularity, Compatibility, Fields, Near-fields, A-group and Quasi-kernel.

1. Introduction

The concept of a vector space is well known, i.e, linear space is generalised by a bit more non-linearity the so called near vector space introduced by André in [1]. A pair (V, A) is called a *near vector space* if it satisfies the condition of an $A-$group and the quasi-kernel $Q(V)$ generates a group $(V, +)$. In recent years, near vector spaces have been used in several applications, including secret sharing schemes in cryptography (see [3]) and to construct interesting examples of families of planar near-rings in [4]. Additionally, they have proved to be of interesting from model theory perspective too. This paper introduces the theory of near vector space. It gives important definitions, examples and some useful theorems. Regularity is the central part in the study of near vector space and the Decomposition Theorem largely depends on the regularity notion. The main objective of this paper is to understand the Decomposition Theorem which states that every near vector space can be written as the direct sum of maximal regular subspaces. This paper is organised in four sections. In section 2 we introduce the concept of a near-field. Near-fields are a source of scalars in the study of near vector space. Near-fields are also used in the construction of near vector space as we shall see in section 4. In this paper we shall make use of right near-fields as in André ([1]). In section 3 the theory of near vector space is presented. We start by introducing the most important definitions: a near vector space, concept of the quasi-kernel and compatibility. We shall then introduce the concept of regularity. Regularity plays a very important role in the theory of near vector space. As André stated in ([1]) that regular near vector space are the building blocks of near vector space. We then build on the notion of regularity to understand the Decomposition Theorem. We shall then give examples by applying the Decomposition Theorem and investigate how near vector spaces are decomposed into maximal regular subspaces. In section 4 we will introduce the concept of cardinality of the quasi-kernel $Q(V)$. Here will shall use the already existing examples to determine the cardinality of near vector spaces.

* *E-mail: jeromy.kalunga@cbu.ac.zm*

2. Preliminary Material

Near-fields will serve as the source of scalars in the theory of near vector spaces. Let us start by defining a near-ring.

Definition 2.1 ([5]). *A near-ring N is a set together with two binary operations $+$ and $\cdot$ which satisfies the following axioms:*

(i). $(N,+)$ *is a group,*

(ii). $(N,\cdot)$ *is a semi group,*

(iii). $(a_1+a_2)\cdot a_3 = a_1\cdot a_3 + a_2\cdot a_3 \ \forall\ a_1,a_2,a_3 \in N$.

This is the definition for a right near-ring, since the right distributive law is satisfied. The set N is said to be a near-field if $N\setminus\{0\}$ is also a group.

Remark 2.2. *We may also define a left nearing where axiom (iii) becomes*

(iii) $a_3\cdot(a_1+a_2) = a_3\cdot a_1 \ + a_3\cdot a_2 \ \forall\ a_1,a_2,a_3 \in N$.

In this paper we will consider right near-rings. 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 near-ring and is denoted by 0. Throughout this paper we shall use $N^* = N\setminus\{0\}$.

Example 2.3 ([5]).

(i). Every ring is near-ring.

(ii). If R is a commutative ring with identity, it can be shown that $(R[x],+,\circ)$ is a near-ring, under pointwise addition and composition, where $R[x]$ is the set of polynomials with coefficient in R.

(iii). Let $(G,+)$ be a group. Define $M(G)$ to be the set of all functions from G to G with pointwise addition $(f+g)(x) := f(x)+g(x)$ for all $f,g \in M(G), x \in G$ and composition of maps $(f\circ g)(x) := f(g(x))$. Then $(M(G),+,\circ)$ is right near-ring

We now give a definition of a Dickson near-field which shall be used in section 4.

Definition 2.4 ([5]). *Let N be a near-field and let $Aut(N,+,\cdot)$ be the set of all automorphisms of N. A map $\phi :\to Aut(N,+,\cdot)$; $n \mapsto \phi_n$ is said to be a coupling map if for all $n,m \in N^*$, we have $\phi_n\circ\phi_m = \phi_{\phi_{n(m).n}}$ and $N^* = N\setminus\{0\}$. If ϕ is a coupling map on N then*

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

If ϕ is a coupling map on N then $(N,+,\circ_\phi)$ is again a near-field.

Definition 2.5 ([5]). *If $(N,+,\cdot)$ is a near-field and ϕ a coupling on N^*. Then $(N,+,\circ_\phi)$ is called $\phi-$ derivation of $(N,+,\cdot)$. Thus a nearfield N is called a Dickson near-field if N is the $\phi-$ derivation of some field F, i.e $F^\phi = N$.*

Definition 2.6 ([6]). *A pair of numbers $(p,m) \in \mathbb{N}^2$ is called a Dickson pair if*

(i). m is some power of a prime p.

(ii). Each prime divisor of m divides $p-1$.

Remark 2.7. *Every finite field is a Dickson near-field. In this paper our examples will be restricted to $\mathbb{Z}_p$, where p is a prime and $\mathbb{R}$, the field of real numbers.*

3. The Theory of Near Vector Spaces

This section introduces the fundamental theory of near vector spaces. We shall give the most important definitions, lemmas and theorems of a near vector spaces.

3.1. Near Vector Space

Let us define right vector space over a division ring A.

Definition 3.1 ([1]). *A right vector space V over a division ring A is set V such that for each $\alpha \in A$ and $v \in V$, there is a unique element $v\alpha \in V$ such that the following conditions hold for all $\alpha, \beta \in A$ and $u, v \in V$;*

(i) $(V, +)$ *is an abelian group,*

(ii) $(v + u)\alpha = v\alpha + u\alpha$,

(iii) $v(\alpha + \beta) = v\alpha + v\beta$,

(iv) $v(\alpha\beta) = (v\alpha)\beta$,

(v) $v1 = v$.

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.

We then define the concept of a near vector space which shall be used mostly in this section.

Definition 3.2 ([2, 7]). *A near vector space is a pair (V, A) which satisfies the following conditions;*

(i) $(V, +)$ *is a group and A is a set of endomorphisms of V.*

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

(iii) $A^* := A \setminus \{0\}$ *is a subgroup of the group of automorphisms of* $(V, +)$.

(iv) If $x\alpha = x\beta$ with $x \in V$ and $\alpha, \beta \in A$, then we have $\alpha = \beta$ or $x = 0$, i.e A acts fixed point free on V.

(v) The quasi-kernel $Q(V)$ of V, generates V as a group. Here,

$$Q(V) = \{x \in V | \forall \alpha, \beta \in A, \exists \gamma \in A \text{ such that } x\alpha + x\beta = x\gamma\}.$$

The concept of the Quasi-kernel $Q(V)$ of V is mostly used in the theory of near vector spaces and has the important properties that shall be used on this section.

Lemma 3.3 ([1, 7]). *The Quasi-kernel has the following properties;*

(i) $0 \in Q$,

(ii) If $u \in Q \setminus \{0\}$, then γ is uniquely determined in Definition 3.2 (v) by α and β,

(iii) For $u \in Q$ and $\lambda \in A$, we have $u\lambda \in Q$, i.e $uA \subset Q$,

(iv) Foru $\in Q$ and $\alpha, \beta \in A$, there exists $\gamma \in A$ such that $u\alpha - u\beta = u\gamma$

(v) If $u \in Q$ and $\lambda_i \in A$, $i = 1, 2, \ldots, n$, then $\sum_{i=1}^{n} u\lambda_i = u\eta \in Q$ for some $\eta \in A$ and for all integers $i \geqslant 1$

Proof.

(i) Let $\alpha, \beta \in A$. Take any $\lambda \in A$, then $0\alpha + 0\beta = 0\lambda$. Thus $0 \in Q$.

(ii) Let $u \in Q \setminus \{0\}$ and $\alpha, \beta \in A$. Suppose there exists $\gamma, \gamma' \in A$ such that $u\alpha + u\beta = u\gamma = u\gamma'$. Then by Definition 3.2 (iv) we have $\gamma = \gamma'$, as $u \neq 0$.

(iii) Suppose $u \in Q$ and $\lambda \in A$. There are two cases to consider

Case 1: $\lambda = 0$. Thus $u\lambda = u0 = 0 \in Q$

Case 2: $\lambda \neq 0$ Let $\alpha, \beta \in A$. Then by Definition 3.2 (iii), $\lambda\alpha \in A$ and $\lambda\beta \in A$. Now since $u \in Q$, there exists a $\gamma \in A$ such that $u(\lambda\alpha) + u(\lambda\beta) = u\lambda = u\lambda\lambda^{-1}\gamma$. So $(u\lambda)\alpha + (u\lambda)\beta = (u\lambda)(\lambda^{-1}\gamma)$ which implies that $u\lambda \in Q$. Thus $uA \subseteq Q$.

(iv) Let $u \in Q \setminus \{0\}$ and $\alpha, \beta \in A$. Then $(-1)\beta \in A$ and by Definition 3.2 (iv), $(-1)\beta = -\beta$ since $u(-\beta) = (-u)\beta = u(-1)\beta$. But $u \in Q$, so there exists a $\gamma \in A$ such that $u\alpha + u(-\beta) = u\gamma$, which implies that $u\alpha - u\beta = u\gamma$.

We shall use induction on n. Let $S = \{n \in \mathbb{N} | \sum_{i=1}^{n} u\lambda_i \in uA\}$ if $u \in Q, \lambda_i \in A, i = 1, 2, \ldots, n\}$. By Lemma 3.3 (c) above, $1 \in S$. Now suppose $m \in S$ i.e, $u\eta = \sum_{i=1}^{m} u\lambda_i \in Q$ if $u \in Q$. Then

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

Hence $m + 1 \in S$ and consequently $S = N$. □

Definition 3.4 ([1, 8]). *A pair (V, A) is said to be a linear $A-$group if $V = 0$ or $Q(V) \neq 0$.*

Definition 3.5 ([1, 8]). *Let (V, A) be a linear $A-$group, and let $u \in Q(V) \setminus \{0\}$. Define the operation $+_u$ on A by $u(\alpha +_u \beta) := u\alpha + u\beta$ for $\alpha, \beta \in A$.*

Theorem 3.6 ([1, 8]). *Let $Q(V)$ be the Quasi-kernel of the near vector space (V, A) such that $V = 0$ or $Q \neq 0$ and suppose that $u, v \in Q \setminus \{0\}$ with $v \notin uA$. Then , for any $\lambda A \setminus \{0\}$, $u + v\lambda \in Q$ if and only if $+_u = +_{v\lambda}$.*

Lemma 3.7 ([1]). *Let V be a near vector space and let $B = \{u_i | i \in I\}$ be a basis of $Q(V)$. Then each $x \in V$ is a unique linear combination of elements of B, i.e there exists $\lambda_i \in A$, with $\lambda_i \neq 0$ for at most a finite number $i \in I$ which are uniquely determined by x and B, such that $x = \sum_{i \in I} u_i\lambda_i$.*

Proof. Let $x \in V$. Then by Definition 3.2 (v), there exist $v_1, v_2, \cdots, v_n \in Q$ such that $x = \sum_{j=1}^{n} v_j$. Since each v_j is a linear combination of elements B, x is also a linear combination of elements of B. To prove uniqueness, let $\sum_{i \in I} u_i\lambda_i = \sum_{i \in I} u_i\lambda_i'$ with at most a finite number of λ_i and λ_i' not zero and $u_i \in B (i \in I)$. Since $B \subseteq Q$ then $u_i \in Q (i \in I)$. Hence, by Lemma 3.3 (iv), then $\eta_i \in A (i \in I)$ such that $u_i\lambda_i - u_i\lambda_i' = u_i\eta_i$ for all $i \in I$. But $\sum_{i \in I}(u_i\lambda_i - u_i\lambda_i') = 0$ showing that $\sum_{i \in I} u_i\eta_i = 0$. Thus, since B is linearly independent $\eta_i = 0$ for each $i \in I$. $u_i\lambda_i - u_i\lambda_i' = 0$ and so $u_i\lambda_i = u_i\lambda_i'$. Therefore for each $i \in I, \lambda_i = \lambda_i'$ since $u_i \neq 0$ for each $i \in I$. □

Definition 3.8 ([1, 8]). *The elements u and v of $Q(V) \setminus \{0\}$ are said to be compatible (denoted by u cp v) if there is a $\lambda \in A \setminus \{0\}$ such that $u + v\lambda \in Q$.*

Lemma 3.9. *The elements u and v of $Q \setminus \{0\}$ are compatible if and only if there is a $\lambda \in A \setminus \{0\}$ such that $+_u = +_{v\lambda}$.*

Proof. If $v \notin uA$, then it clearly follows from Theorem 3.6. Let $v \in uA$ then if $v = u\alpha$ for any $\alpha \in A \setminus \{0\}$. Then the following conditions holds

(i) u *cp* $u\alpha$ and by Lemma 3.3 (d) we have that $u + u\alpha\lambda \in Q$ for each $\lambda \in A$.

(ii) Since $v\lambda = +_{v\lambda}$ we have that $+_u = +_{v\lambda} = u\alpha\alpha^{-1} = u$ if we take $\lambda = \alpha^{-1}$. □

Theorem 3.10 ([1])**.** *The compatibility relation cp is an equivalence relation on $Q \setminus \{0\}$.*

Proof. We show that the compatibility relation *cp* is reflexive, symmetric and transitive.

(i) Reflexivity: Let $u \in Q$, then u *cp* u by Lemma 3.3-(v) and thus u *cp* u.

(ii) Symmetry: Let $u, v \in Q \setminus \{0\}$ and suppose that u *cp* v. Then there exist a $\lambda \in A \setminus \{0\}$ such that $u + v\lambda \in Q$ and by Lemma 3.3-(iii), we have that $(u + v\lambda)\lambda^{-1} = v + u\lambda^{-1} \in Q$. Thus v *cp* u.

(iii) Transitive: Let $u, v, w \in Q \setminus \{0\}$ and supoose that u *cp* v and v *cp* w and so by Lemma 3.9, $+_u = +_{v\lambda}$ and also $+_v = +w\mu$. Then we show that$+_u = +_{w\eta}$ for $w, \eta, \mu \in A \setminus \{0\}$.

$$\begin{aligned} +_u = +_{v\lambda} \implies \alpha +_u \beta &= (\alpha^\lambda +_v \beta^\lambda)^{\lambda^{-1}} \\ &= (\alpha^\lambda +_{w\mu} \beta^\lambda)^{\lambda^{-1}} = \alpha +_{w\eta\lambda} \beta \\ &= \alpha +_{w\eta} \beta \text{ for } \eta = w\mu \in A \setminus \{0\}. \end{aligned}$$

□

Theorem 3.11 ([1])**.** *Let $u, v \in Q \setminus \{0\}$ and if $u + v \in Q \setminus \{0\}$ then*

(i) u cp v, and

(ii) u cp $u + v$.

Definition 3.12 ([1])**.** *A near vector space V is regular if any two vectors of $Q(V) \setminus \{0\}$ are compatible, i.e , for any two vectors u and v of $Q(V) \setminus \{0\}$ there exists a $\lambda \in A \setminus \{0\}$ such that $u + v\lambda \in Q(V)$.*

Theorem 3.13 ([1])**.** *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 of regularity of a near vector space, any two vectors of $Q \setminus \{0\}$ are compatible. Thus every basis of $Q \setminus \{0\}$, also of V consists of mutually pairwise compatible vectors.
Conversely, suppose that V is a near vector space with basis B consisting of mutually pairwise compatible vectors. Let $u \in Q \setminus \{0\}$. Then by Lemma 3.7 u,can be expressed as a linear combination of the basis elements of B, that is u can be written as $u = \sum_{i=1}^{r} u_i\lambda_i$ where $u_i \in B$ and $\lambda_i \neq 0$ for $i \in \{1, 2, \cdots, r\}$. Now

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

Thus $u = u' + u_r\lambda_r \in Q$ and so there exists $\alpha, \beta \in A$ such that for $\gamma \in A$, we have

$$(u' + u_r\lambda_r)\alpha + (u' + u_r\lambda_r)\beta = u\alpha + u\beta = u\gamma = (u' + u_r\lambda_r)\gamma.$$

Hence $u'\alpha + u_r\lambda_r\alpha + u'\beta + u_r\lambda_r\beta = u'\gamma + u_r\lambda_r\gamma$, and therefore $u'\alpha + u'\beta + u_r\lambda_r\alpha + u_r\lambda_r\beta = u'\gamma + u_r\lambda_r\gamma$. But $u_r \notin \{u_1, u_2, \ldots, u_{r-1}\}$ and if $u_r \in \{u_1, u_2, \cdots, u_{r-1}\}$ then u_r is equal to one of the elements in $\{u_1, u_2, \cdots, u_{r-1}\}$. Suppose $u_r = u_2$ then $u_1\alpha_1 + u_2\alpha_2 + \cdots + u_r\alpha_r = 0$ if we take $\alpha_1 = \alpha_2 = \cdots = \alpha_{r-1} = 0$. This contradicts the linear independence of B. Thus by Lemma 3.7, we have that $u_r\lambda_r\alpha + u_r\lambda_r\beta = u_r\lambda_r\gamma$ and therefore $u'\alpha + u'\beta = u'\gamma$ which implies that $u_r\lambda_r, u' \in Q$. Now we show that u and u_r are compatible.

Now we show that if $u' = 0$ then $u = u_r\lambda_r$ and thus by Theorem 3.9 we have that u_r *cp* $u_r\lambda_r$. If $u \neq 0$, then by Theorem 3.11, $u_r\lambda_r$ *cp* u since $u', u_r\lambda_r, u = u' + u_r\lambda_r + u' \in Q$. But, Lemma 3.11 u_r *cp* $u_r\lambda_r$. Thus, by Lemma 3.9, we have u_r *cp* u. By assumption, u_r is compatible with every other vector of B. Thus, it follows from the transitivity of *cp* Theorem 3.11 that u is compatible with every other vector of B. Since $u \in Q \setminus \{0\}$ was arbitrarily chosen. Thus if $v, w \in Q \setminus \{0\}$ then v *cp* u_i and w *cp* u_i with $u_i \in B$ for $i \in \{1, \cdots, r\}$. Thus by transitivity of Theorem 3.11 v *cp* w. Thus every two elements of $Q \setminus \{0\}$ are compatible. Therefore V is regular. □

Definition 3.14 ([9]). *Suppose (V, A) is a near vector space and $\emptyset \neq V' \subseteq V$ is such that V' is a subgroup of $(V, +)$ generated additively by $XA = \{x\alpha | x \in X, \alpha \in A\}$, where X is an independent subset of $Q(V)$, then we say (V', A) is a subspace of (V, A).*

Theorem 3.15 ([7]). *If W is a subspace of V, then $Q(W) = W \cap Q(V)$.*

Proof. Let $u \in Q(W)$. Then for each $\alpha, \beta \in A$ there exists $\gamma \in A$, such that $u\alpha + u\beta = u\gamma$. Since $u \in W$ and W is a subspace of $V, u \in V$. Since $Q(V) \subseteq V$ and by the above equation $u \in Q(V)$. Thus $Q(W) \subseteq W \cap Q(V)$. Suppose $u \in Q(V) \cap W$. Then $u \in Q(V)$. Then for each $\alpha, \beta \in A$ there exists $\gamma \in A$, such that

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

Since $u \in W$ and by the above equation $u \in Q(W)$. Thus $W \cap Q(V) \subseteq Q(W)$. □

Theorem 3.16 ([1]). *A near vector space (V, A), with $V \neq \{0\}$ is regular near vector space if and only if A is a near-field and V is isomorphic to A^I for some non-empty index set I, where $(\eta_i)\lambda = (\eta_i\lambda)$ where $(\eta_i) \in A^I$ and $\lambda \in A$.*

We will need the definition of direct sum of subspace.

Definition 3.17. *[2] The near vector space (V, A) is said to be a direct sum of subspaces $W_1, W_2, \cdots, W_n$ symbolised by $V = W_1 \oplus W_2 \oplus \cdots \oplus W_n$ if and only if*

(i) $V = W_1 + W_2 + \cdots + W_n$, and

(ii) $W_i \cap (W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_n) = 0$ for each i.

The sufficient condition for $V = W_1 \oplus W_2 \oplus \cdots \oplus W_n$ is that every vector $v \in V$ has a unique representation $v = v_1 + v_2 + \cdots + v_n$ with $v_i \in W_i$ for $i = 1, 2, \cdots, n$.

Lemma 3.18. *Let (V, A) be a regular near vector space. Then any subspace W of V is also regular.*

Proof. Suppose that (V, A) is regular and that W is a subspace of V which is not regular. Take $u \in Q(W)$ and $v \in Q(V)$. Then u is not compatible with v, but $Q(W) \subseteq Q(V)$, a contradiction. □

The following theorem characterises a finite near vector spaces.

Theorem 3.19 ([10]). *Let V be a group and let $A := D \cup \backslash\{0\}$, where D is a fixed point free group of automorphism of V. Then (V, A) is a finite-dimensional near vector space if and only if there exists a finite number of nearfields $F_1, F_2, \cdots, F_n$, semigroup $\varphi_i : A \to F_i$ and a group $\phi : V \to F_1 \oplus F_2 \oplus \cdots \oplus F_n$ such that if $\phi(v) = (x_1, x_2, \cdots, x_n), (x_i \in F_i)$ then $\phi(v\alpha) = (x_1\varphi_1(\alpha), x_2\varphi_2(\alpha), \cdots, x_n\varphi_n(\alpha))$, for all $v \in V$ and $\alpha \in A$.*

We shall not give a proof for this theorem but we will explain how it is applied.

According to this theorem, we can specify a finite-dimensional near vector space by taking n near-fields $F_1, F_2, \cdots, F_n$ for which there are semi-group 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 $(F_{i0}, \cdot)$ as the semigroup of endomorphisms by defining $(x_1, x_2, \cdots, x_n)\alpha = (\ x_1\vartheta_{1i_0}(\alpha), x_2\vartheta_{2i_0}(\alpha), \cdots, x_n\vartheta_{ni_0}(\alpha)\ )$ for $x_j \in F_j, j \in \{1, \cdots, n\}$ and all $\alpha \in F_{i0}$. The next theorem is the most important theorem in the study of near vector space.

3.2. The Decomposition Theorem

Theorem 3.20 (The Decomposition Theorem [1]). *Every near vector space V is the direct sum of regular subspaces V_j for $j \in J$ such that $u \in Q \setminus \{0\}$ lies precisely in 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 $V_j \in J$. We start by partitioning $Q \setminus \{0\}$ into sets Q_j of mutually pairwise compatible vectors. This partitioning is possible by Theorem 3.10. Furthermore, let $B \subseteq Q \setminus \{0\}$ 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 subset of B. Furthermore, $B = U_{j\in J}B_j$. Again by Theorem 3.10 $Q \setminus \{0\} = U_{j\in J}Q_j$, so

$$U_{j\in J}B_j = U_{j\in J}(B \cap Q_j) = B \cap (U_{j\in J}Q_j) = B \cap (Q \setminus \{0\}) = B.$$

Now let $B = \{b_i | i \in I\}$ with I an index set. Since $B = U_{j\in J}B_j$ with the $B_{j'}s$ are mutually disjoint for each $i \in I, b_i \in J$. 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 $I = U_{j\in J}I_j$. Let $V_j := \langle B_j \rangle$ be the subspaces of V generated by B_j. By Theorem 3.13, V_j is regular since $B_j \subseteq Q_j$ consists of mutually pairwise compatible vectors. Let $x \in V$. Then by Lemma 3.7, $x = \sum_{i\in I} b_i\eta_i$ with $b_i \in B$ and $\eta_i = 0$ for a mosta finite number of $i \in I$. Hence $x = \sum_{j\in J}\left(\sum_{i\in I_j} b_{ij}\eta_{ij}\right)$ 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

$$x = \sum_{i\in J} x_j. \tag{1}$$

By Lemma 3.7, $x = \sum_{i\in I} b_i\eta_i$ can be written in a unique way. If we apply Lemma 3.7 to the *near vector space* V_j with basis B_j for all $j \in J$ 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 $V = \bigoplus_{j\in J} V_j$.

(ii) Next we show that each $u \in Q \setminus \{0\}$ lies precisely in one summand V_j.

Suppose that there exists elements in $Q \setminus \{0\}$ which are not elements of V_j for any $j \in J$. let u be such an element with atleast possible number of summands in the decomposition given by Equation 1, i.e. Let

$$u = \sum_{j\in J} u_j, \tag{2}$$

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

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

and

$$u\delta = \Big(\sum_{j\in J} u_j\Big)\delta.$$

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

$$\Big(\sum_{j\in J'} u_j\Big)\alpha + \Big(\sum_{j\in J'} u_j\Big)\beta = \Big(\sum_{j\in J'} u_j\Big)\delta \text{ for all } J' \subseteq J. \tag{3}$$

Consequently,

$$u' = \sum_{j\in J'} u_j \in Q \text{ (with } u' \neq 0). \tag{4}$$

Let J_u be the set of all $j \in J$ for which $u_j \neq 0$ in the decomposition of Equation 2. Since J_u is finite and $u \notin V_j$ for any $j \in J$, $|J_u| > 1$. To see this , suppose that $|J_u| = 1$ then $u = u_j \in V_j$, a contradiction. Furthermore, by the definition of u, $|J_{u^*}| \geqslant |J_u|$ for all $u^* \in Q \setminus U_{j\in J}V_j$. Next will show that if $J' \subseteq J$ such that $J_u \cap (J/J') \neq 0$, then $|J_{u'}| = 1$ with u' defined in Equation 4. To see this, suppose that $|J_{u'}| > 1$ (note: $|J_{u'}| \neq 0$ since $u' \neq 0$). Then $u' = u_{j1} + u_{j2} + \cdots + u_{j_n}$ with $n > 1$ and $J_{u'} = \{j_1, j_2, \cdots, j_n\}$. Then $u' \notin V_{ji}$ with $j_i \in J'$, since $u' \in V_{ji}$ implies that $u' - u_{ji} \in V_{ji} \cap \oplus_{j\in J\setminus\{ji\}} V_j = \{0\}$. But then $u' = u_{ji}$ and $u_{ji} \in V_{ji}$, so $u' \in V_{ji}$, a contradiction.

Moreover $u' \in V_{j'}$ with $j^{'} \in J/J'$, since $u' \in V_{j'}$ implies that $u' \in V_{j'} \cap \oplus_{j\in J\setminus\{j'\}} V_j$, a contradiction. Thus $u' \in Q \setminus U_{j\in J}V_j$. Hence $|j_{u'}| \geq |J_u|$. However, this is a contradiction to our assumption that $J' \subseteq J$ is such that $J_u \cap (J/J') \neq \emptyset$. 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 $J_u \cap (J/J') \neq 0$). Then $u - u' = u_{j1} + u_{j2} + \cdots + u_{jm}$. Thus $u - u' \notin V_{ji}$, since $u - u' \in V_{ji}$ implies that $u - u' - u_{ji} \in V_{ji} \oplus_{j\in J\setminus\{ji\}} V_j = \{0\}$. But $u - u' = V_{ji}$ and $u_{ji} \in V_{ji}$, thus $u - u' \in V_{ji}$, a contradiction. Moreover $u - u' \notin V_{ji}$ with $j' \in J/J'$, since$u - u' \in V_{j'}$ implies that $u - u' \in V_{j'} \cap \oplus_{j\in J\setminus\{j'\}} V_j = \{0\}$, that is $u - u' = 0$, a contradiction. Hence $u - u' \in U_{j\in J}V_j$. Furthermore by Equation 3, $u - u' \in Q$. Hence $u - u' \in Q \setminus U_{j\in J}$. Therefore , $|j_{u-u'}| \geq |J_u|$. This contradicts $J_{u'} = \{j'\}$. Hence $J_{u-u'} = \{j''\}$ for some $j'' \in J$, with $j'' \neq j'$. Suppose that $j := j' = j'''$. Then $u' = u_j$ and $u - u' = u_j$. Hence $u = 2u_j \in V_j$, a contradiction. We therefore obtain

$$u = u' + (u - u') \tag{5}$$

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 Equation 5). Thus $j' = j''$, a contradiction. Therefore $Q \subseteq U_{j\in J}V_j$. Hence each $u \in Q \setminus \{0\}$ is contained in atleast one V_j and $V_j \cap V_{j'} = \{0\}$ for $j \neq J'$, each $u \in Q \setminus \{0\}$ is contained atleast 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 exist a $j_0 \in J$ such that $V_{j0} \subsetneq W$ with W a regular subspace of V. Suppose that $Q(V_{j0}) = Q(W)$. Then since V_{jo} is generated by $Q(V_{j0})$ and W is generated by $Q(W)$, $V_{j0} = W$, which is impossible. Thus, there exists a $u \in Q \cap (W/V_{j0})$. Since $u \in Q \setminus \{0\}$, $u \in V_j$ for some $j \in J \setminus \{j_0\}$. But W is regular, so since $Q(V_{j0}) \subsetneq Q(W)$, u is compatible with each $v \in Q(V_{j0}) \setminus \{0\}$. This contradicts the fact that $j \neq j_0$. □

Remark 3.21. *When V is regular it is its own decomposition since it is the maximal regular subspace of itself. As seen in the proof of the above theorem, the decomposition of the near vector spaces V results in a decomposition of $Q(V)$. We can show how the Decomposition Theorem results in the decomposition of the quasi-kernel for near vector spaces constructed under $\mathbb{Z}_p$ where p is prime.*

Lemma 3.22 ([11])**.** *Suppose that V is an n-dimensional near vector space over $\mathbb{Z}_p$ where p is prime, with $Q(V) \neq V$ and that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ is the canonical decomposition of V. Then $Q(V) = Q_1 \oplus Q_2 \oplus \cdots \oplus Q_k$ where $Q_i = V_i$ for each $i \in \{1, 2, \cdots, k\}$.*

Proof. By Theorem 3.10 it is possible to partition the quasi-kernel $Q(V)$, that is, $Q(V) = \cup_{i=1}^{k} Q_i$, where $Q_j = \{(a_1, 0, \cdots, a_i, 0)\}|a_i$ in position i with $i \in A_j$ for $j \in \{1, 2, \cdots, k\}$, furthermore, this partitions $Q(V) \setminus \{0\}$ into sets $Q_1 \setminus \{0\}, Q_2 \setminus \{0\}, \cdots, Q_k \setminus \{0\}$ of mutually pairwise compatible vectors. If we intersect each of these with a basis B of V, and let $B_j = B \cap Q_j$ for $i \in \{1, 2, \cdots, k\}$ and consider $V_j = \langle B_j \rangle$ we obtain $Q_j = V_j$ for each $j \in \{1, 2, \cdots, k\}$. □

We now give a short description of the procedure to decompose a near vector space V into maximal regular near vector spaces:

(i) Start by partition $Q(V) \setminus \{0\}$ into sets Q_j for $j \in J$ of mutually pairwise compatible vectors.

(ii) Let $B \subset Q(V) \setminus \{0\}$ be a basis of V and let $B_j = B \cap Q_j$.

(iii) Let $V_j = \langle B_j \rangle$ be the subspace of V generated by B_j, then each V_j is a maximal regular subspace of V and V is the direct sum of the V_j.

Definition 3.23 ([1])**.** *The uniquely determined direct decomposition of a near vector V into maximal regular subspaces, is called the canonical direct decomposition.*

Theorem 3.24 (The Uniqueness Theorem [1])**.** *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 Theorem 3.20. Now to show the uniqueness, let

$$V = \bigoplus_{j \in J} V_j = \bigoplus_{j' \in J'} V'_{j'} \tag{6}$$

be two direct decompositions of V into maximal regular subspaces $V_j(j \in J)$ and $V'_{j'}(j' \in J')$, respectively. Furthermore let $Q_j = (Q(V)) \setminus \{0\}) \cap V_j(j \in J)$. By Definition 3.2, $V_j = \langle Q_j \rangle$ for each $j \in J$. Now each of two vectors in Q_j are by Definition 3.12 compatible. But Q_j is not properly contained in a set of mutually compatible vectors. This can be show as follows: Suppose that, for some $j \in J$, there exists a $u \in Q(V) \setminus Q_j$ such that u *cp* v for all $v \in Q_j$.
Let $Q(W)\setminus\{0\}$ be an equivalence class(with respect to *cp*), with $Q(W_j\setminus\{0\})$. Then $Q_j \subsetneq Q(W_j)\setminus\{0\}$. Let $W_j = \langle Q(W_j)\rangle\setminus\{0\}$. Then W_j is regular since any two vectors of $Q(W_j) \setminus \{0\}$ are compatible. But $V_j \subsetneq W_j$ 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 symmentry $\{V'_{j'} | j' \in J'\} \subseteq \{V_j | j \in J\}$. Consequently, $\{V'_{j'} | j' \in J'\} = \{V_j | j \in J\}$. □

3.3. Examples of Near Vector Spaces

In this section we give examples of near vector spaces which are not vector spaces. Each example of a near vector spaces will be presented in two parts. Firstly, we shall that the pair (V, A) is a near vector spaces and secondly, we show that V can be decomposed into maximal regular near vector spaces by using the Decomposition Theorem.

Example 3.25. *Suppose we have (V, A) where $V = \mathbb{R}^3$ and $A = \mathbb{R}$ and let each $\alpha \in \mathbb{R}$ act as an endomorphism on V by defining $(x_1, x_2, x_3)\alpha := (x_1\alpha, x_2\alpha^3, x_3\alpha^5)$, for all $(x_1, x_2, x_3) \in V$.*

(1) We show that (V, A) is a near vector space as follows:

(i) $(V, +)$ is a group. Moreover, let $\alpha \in A$ and $(x_1, x_2, x_3), (y_1, y_2, y_3) \in V$. Then we have

$$\begin{aligned}[(x_1, x_2, x_3) + (y_1, y_2, y_3)]\alpha &= (x_1 + y_1, x_2 + y_2, x_3 + y_3)\alpha \\ &= ((x_1 + y_1)\alpha, (x_2 + y_2)\alpha^3, (x_3 + y_3)\alpha^5\ ) \\ &= (\ x_1\alpha + y_1\alpha\ ,\ x_2\alpha^3 + y_2\alpha^3\ ,\ x_3\alpha^5 + y_5\alpha^5\ ) \\ &= (x_1\alpha, x_2\alpha^3, x_3\alpha^5) + (y_1\alpha, y_2\alpha^3, y_3\alpha^5) \\ &= (x_1, x_2, x_3)\alpha + (y_1, y_2, y_3)\alpha.\end{aligned}$$

Thus α is an endomorphism of V.

(ii) Let $(x_1, x_2, x_3) \in V$. Then we have

$$\begin{aligned}(x_1, x_2, x_3)0 &= (x_10, x_20^3, x_30^5) = (0, 0, 0) \\ (x_1, x_2, x_3)1 &= x(_11, x_21^3, x_31^5) = (x_1, x_2, x_3\ ) \\ (x_1, x_2, x_3)(-1) &= x_1(-1), x_2(-1)^3, x_3(-1)^5) = (-x_1, -x_2, -x_3).\end{aligned}$$

(iii) Now we show that $(A^*, \cdot)$ is a subgroup of $Aut(V)$, the automorphism group of $(V, +)$. Let $\alpha \in A^*$, then α is an endomorphism as shown above. Next we show that α is a bijection. Let $(x_1, x_2, x_3), (y_1, y_2, y_3) \in V$ and suppose we have $(x_1, x_2, x_3)\alpha = (y_1, y_2, y_3)\beta$. Then $(x_1\alpha, x_2\alpha^3, x_3\alpha^5) = (y_1\beta, y_2\beta^3, y_3\beta^5\ )$ so that $x_1\alpha = y_1\beta, x_2\alpha^3 = y_2\beta^3$ and $x_3\alpha^5 = y_3\beta^5$. Thus, since $\alpha \neq 0$ and the fact that A is a field, we have $x_1 = y_1, x_2 = y_2$ and $x_3 = y_3$. Thus α is injective. Furthermore, let $(x_1, x_2, x_3) \in V$. Then $(x_1\alpha^{-1}, x_2\alpha^{-3}, x_3\alpha^{-5}) \in V$ and we have $(x_1\alpha^{-1}, x_2\alpha^{-3}, x_3\alpha^{-5})\alpha = (x_1\alpha^{-1}\alpha, x_2\alpha^{-3}\alpha^3, x_3\alpha^{-5}\alpha^5) = (x_1, x_2, x_3)$. hence α is surjective. Since $(A^*, \cdot)$ is a group and $(A, \cdot)$ is a subset of $Aut(V), (A^*, \cdot)$ is a subgroup of $Aut(V)$.

(iv) Let $(x_1, x_2, x_3) \in V$ and $\alpha, \beta \in A$. Suppose that $(x_1\alpha, x_2\alpha^3, x_3\alpha^5\ ) = (y_1\beta, y_2\beta^3, y_3\beta^5\ )$, implying that $x_1\alpha = x_1\beta, x_2\alpha^3 = y_2\beta^3$ and $y_3\alpha^5 = y_3\beta^5$. Hence $\alpha = \beta$ or $x_1 = 0$, $\alpha^3 = \beta^3$ or$x_2 = 0$ and $\alpha^5 = \beta^5$ or$x_3 = 0$. If $\alpha \neq \beta$, then $\alpha^3 \neq \beta^3$ and so $\alpha^5 = \beta^5$. If $\alpha \neq \beta$ then $\alpha^3 \neq \beta^3$ and $\alpha^5 \neq \beta^5$ and thus $x_1 = 0, x_2 = 0$ and $x_3 = 0$. Hence $(x_1, x_2, x_3) = (0, 0, 0)$.

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

(i_1) *Suppose* $(a,0,0) \in V$. *For* $\alpha, \beta \in A$ *we have,*

$$\begin{aligned}(a,0,0)\alpha + (a,0,0)\beta &= (a\alpha, 0, 0) + (a\beta, 0, 0)\\ &= (a\alpha + a\beta, 0, 0)\\ &= (a(\alpha+\beta), 0, 0)\\ &= (a,0,0)(\alpha+\beta), \text{ where } \alpha+\beta \in A\end{aligned}$$

Thus $(a,0,0) \in Q(V)$ *for each* $a \in A$

(i_2) *Consider* $(0,b,0) \in V$, *then*

$$\begin{aligned}(\ 0\ ,\ b,\ 0\ )\alpha + (\ 0\ ,\ b\ ,\ 0\ )\beta &= (\ 0\ ,\ b\alpha^3\ ,\ 0\ ) + (\ 0\ ,\ b\beta^3\ ,\ 0\ )\\ &= (\ 0\ ,\ b\alpha^3\ + b\ \beta^3\ ,\ 0\ )\\ &= (\ 0\ ,\ b\ ,\ 0\ )(\alpha^3+\beta^3)\\ &= (\ 0\ ,\ b\ ,\ 0\ )(\alpha^3+\beta^3)^{\frac{1}{3}}, \text{ and } (\alpha^3+\beta^3)^{\frac{1}{3}} \in A,\end{aligned}$$

Thus $(\ 0\ ,\ b\ ,\ 0\ ) \in Q(V)$ *for each* $b \in A$.

(i_3) *Consider* $(\ 0\ ,\ 0\ ,\ c\ ) \in V$, *then*

$$\begin{aligned}(\ 0\ ,\ 0\ ,\ c\ )\alpha + (\ 0\ ,\ 0\ ,\ c\ )\beta &= (\ 0\ ,\ 0\ ,\ c\alpha^5\ ) + (\ 0\ ,\ 0\ ,\ c\beta^5\ )\\ &= (\ 0\ ,\ 0\ ,\ c(\alpha^5+\beta^5)\ )\\ &= (\ 0\ ,\ 0\ ,\ c\ )(\alpha^5+\beta^5)^{\frac{1}{5}}, \text{ where } (\alpha^5+\beta^5)^{\frac{1}{5}} \in A\end{aligned}$$

Hence $(\ 0\ ,\ 0\ ,\ c\ ) \in Q(V)$ *for each* $c \in A$.

(*vi*) *Finally let us consider* $(\ a\ ,\ b\ ,\ c\ ) \in V$ *for each* $a,b,c \in A \setminus \{0\}$. *Then*

$$\begin{aligned}(\ a\ ,\ b\ ,\ c\ )\alpha + (\ a\ ,\ b\ ,\ c\ )\beta &= (\ a\alpha\ ,\ b\alpha^3\ ,\ c\alpha^5\ ) + (\ a\beta\ ,\ b\beta^3\ ,\ c\beta^5\ )\\ &= (\ a\alpha + a\beta\ ,\ b\alpha^3 + b\beta^3\ ,\ c\alpha^5 + c\beta^5\ )\\ &= (\ a(\ \alpha+\beta)\ ,\ b(\alpha^3+\beta^3)\ ,\ c(\alpha^5+\beta^5)\ )\\ &\neq (\ a\ ,\ b\ ,\ c\ )\gamma,\end{aligned}$$

for any $\alpha \in A$, *since in general,* $(\alpha+\beta)^3 \neq \alpha^3+\beta^3$ *and* $(\alpha^5+\beta^5) \neq \alpha^5+\beta^5$. *Thus* $(\ a\ ,\ b\ ,\ c\ ) \neq Q(V)$ *for each* $a,b,c \in A$. *Hence*

$$Q(V) = \{(\ a\ ,\ 0\ ,\ 0\ )|a \in A\} \cup \{(\ 0\ ,\ b\ ,\ 0\ )|b \in A\} \cup \{(\ 0\ ,\ 0\ ,\ c\ )|c \in A\}.$$

Moreover we check that $Q(V)$ *generates the group* $(V,+)$. *To do this let* $(\ a\ ,\ b\ ,\ c\ ) \in V$, *then we have that*

$$\begin{aligned}(\ a\ ,\ b\ ,\ c\ ) &= (\ a\ ,\ 0\ ,\ 0\ ) + (\ 0\ ,\ b\ ,\ 0\ ) + (\ 0\ ,\ 0\ ,\ c\ )\\ &= (\ 1\ ,\ 0\ ,\ 0\ )a + (\ 0\ ,\ 1\ ,\ 0\ )b + (0,0,1)c\end{aligned}$$

and thus $\{(1,0,0),(0,0,1),(0,0,1)\} \subseteq Q(V)$*, we have that* $Q(V)$ *generates the group* $(V,+)$*. Since all the conditions of a near vector space* (V,A) *is a near vector space. But* (V,A) *is not a vector space. To see this, let* $(\ a\ ,\ b\ ,\ c\ ) \in V$ *and* $\alpha, \beta \in A$ *then we have*

$$(\ a\ ,\ b\ ,\ c\ )(\ \alpha+\beta\ ) = (\ a(\alpha+\beta)\ ,\ (b(\alpha+\beta)^3)\ ,\ (\alpha+\beta)^5\ )$$

and

$$\begin{aligned}(\ a\ ,\ b\ ,\ c\ )\alpha + (\ a\ ,\ b\ ,\ c\ )\beta &= (\ (\ a\alpha+b\beta\ ),\ (b\alpha^3+b\beta^3)\ ,\ (c\alpha^5+c\beta^5)\ ) \\ &= (\ a(\ \alpha+\beta\ ),\ b(\ \alpha+\beta\ )^3, c(\ \alpha+\beta\ )^5\ )\end{aligned}$$

and in general $(\alpha+\beta)^3 \neq \alpha^3+\beta^3$ *nor is* $(\alpha+\beta)^5 \neq \alpha^5+\beta^5$*. Thus the distributive law for scalars does not hold in general,* (V,A) *is not a vector space.*

(2) Let $Q(V)\setminus\{0\} = \{(\ a\ ,\ 0\ ,\ 0\ )|a \in A\} \cup \{(\ 0\ ,\ b\ ,\ 0\ )|b \in A\} \cup \{(\ 0\ ,\ 0\ ,\ c\ )|c \in A\} \setminus \{\ 0\ ,\ 0\ ,\ 0\ \}$*. It is not difficult to check that* $B = \{(\ 1\ ,\ 0\ ,\ 0\ ),(\ 0\ ,\ 1\ ,\ 0\ ),(\ 0\ ,\ 0\ ,\ 1\ )\}$ *is a basis of* $Q(V)$*. Then* V *can be decomposed into maximal regular near vector space in the following way:*

Now, $Q(V) \setminus \{0\} = \{(\ a\ ,\ 0\ ,\ 0\ )|a \in A\} \cup \{(\ 0\ ,\ b\ ,\ 0\ )|b \in A\} \cup \{(\ 0\ ,\ 0\ ,\ c\ )|c \in A\} \setminus \{\ 0\ ,\ 0\ ,\ 0\ \}$*. Put*

$$\begin{aligned}Q_1(V) &= \{(\ a\ ,\ 0\ ,\ 0\ )|a \in A\}, \\ Q_2(V) &= \{(\ 0\ ,\ b\ ,\ 0\ )|b \in A\}, \\ Q_3(V) &= \{(\ 0\ ,\ 0\ ,\ c\ )|c \in A\}.\end{aligned}$$

Then

$$\begin{aligned}B_1 &= B \cap Q_1(V) = \{(\ 1\ ,\ 0\ ,\ 0\ )\} \\ B_2 &= B \cap Q_2(V) = \{(\ 0\ ,\ 1\ ,\ 0\ )\} \\ B_3 &= B \cap Q_3(V) = \{\ 0\ ,\ 0\ ,\ 1\ \}.\end{aligned}$$

Now let

$$\begin{aligned}V_1' &= \langle B_1\rangle = \{(\ 1\ ,\ 0\ ,\ 0\ )\ a|\ a \in A\} = \{(\ a\ ,\ 0\ ,\ 0\ )|\ a \in A\} \\ V_2' &= \langle B_2\rangle = \{(\ 0\ ,\ 1\ ,\ 0\ )\ b|\ b \in A\} = \{(\ 0\ ,\ b\ ,\ 0\ )|\ b \in A\} \\ V_3' &= \langle B_3\rangle = \{(\ 0\ ,\ 0\ ,\ 1\ )\ c|\ c \in A\} = \{(\ 0\ ,\ 0\ ,\ c\ )|\ c \in A\}\end{aligned}$$

The regular near vector space V_1', V_2', V_3' *are generated by* B_1, B_2, B_3 *respectively. Thus by the Decomposition Theorem,* $V = V_1' \oplus V_2' \oplus V_3'$*.*

Example 3.26. *Put* $V = (\mathbb{Z}_2)^2$ *and* $A = \mathbb{Z}_2$*. Let* $\alpha \in A$ *acts as an endomorphism on* V *by defining* $(x_1,x_2)\alpha = (x_1\alpha^3, x_2\alpha)$ *where* $(x_1,x_2) \in V$*.*

(1) We show that the pair (V,A) *is near vector space*

(i) $(V,+)$ *is a group. Moreover, let* $\alpha \in A$ *and let* (x_1,x_2), $(y_1,y_2) \in A$. *Then*

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

Thus α *is an endomorphism of* V.

(ii) Let $(\ x_1\ ,\ x_2\ ) \in V$. *Then*

$$\begin{aligned}(\ x_1\ ,\ x_2\ )0 &= (\ x_1 0^3\ ,\ x_2 0\ ) = (\ 0\ ,\ 0\ ), \\ (\ x_1\ ,\ x_2\ )1 &= (\ x_1 1^3\ ,\ x_2 1\ ) = (\ x_1\ ,\ x_2\ ) \\ (\ x_1\ ,\ x_2\ )(-1) &= (\ x_1\ ,\ x_2\ )1\ (-1=1\ in\ \mathbb{Z}_2) \\ &= (\ x_1 1^3\ ,\ x_2 1\ ) \\ &= (\ x_1 1\ ,\ x_2 1\ ) \\ &= (\ x_1(-1)\ ,\ x_2(-1)\ ) \\ &= (\ -x_1\ ,\ -x_2\ )\end{aligned}$$

(iii) Let $\alpha \in A^*$ *where* $A^*=\{0,1\}$ *and let* $(\ x_1\ ,\ x_2\ ),(\ y_1\ ,\ y_2\ ) \in V$.

(i₁) Suppose that $(\ x_1\ ,\ x_2\ )\alpha = (\ y_1\ ,\ y_2\ )\alpha$. *Then* $(\ x_1\alpha^3\ ,\ x_2\alpha\ ) = (\ y_1\alpha^3\ ,\ y_2\alpha\ )$, *which implies that* $x_1\alpha^3 = y_1\alpha^3$, $x_2\alpha = y_2\alpha$. *Hence* $(x_1-y_1)\alpha=0$, $(x_2-y_2)\alpha=0$. *Therefore, since* $\alpha \neq 0, x_1=y_1, x_2=y_2$. *Hence* $(\ x_1\ ,\ x_2\ ) = (\ y_1\alpha^3\ ,\ y_2\alpha\ )$. *Consequently* α *is injective.*

(i₂) Let $(\ x_1\ ,\ x_2\ ) \in V$ *and let* $\alpha \in A^*$. *Then* $(\ x_1\alpha^{-3}\ ,\ x_2\alpha^{-1}\ ) \in V$ *and* $(\ x_1\alpha^{-3}\ ,\ x_2\alpha^{-1}\ ) = (\ x_1\ ,\ x_2\ )$. *Hence* α *is surjective. Therefore* $(A^*,\cdot)$ *is subset of the group of automorphisms of* $(V,+)$. *Furthermore, since* α *is an endomorphism and* $(A^*,+)$ *and* A *is a field,* A^* *is a subgroup of the automorphism group* $(V,+)$.

(iv) Let $(\ x_1\ ,\ x_2\ ) \in V$ *and let* $\alpha,\beta \in A$. *Suppose that* $(\ x_1\ ,\ x_2\ )\alpha = (\ y_1\ ,\ y_2\ )\beta$. *Then* $(\ x_1\alpha^3\ ,\ x_2\alpha\ ) = (\ x_1\beta^3\ ,\ x_2\beta\ )$, *which implies that* $x_1\alpha^3 = x_1\beta^3$, $x_2\alpha = x_2\beta$. *If* $\alpha \neq \beta$, *then* $\alpha^3=\beta^3$ *and so* $x_1 = x_2 = 0$, *i.e* $(\ x_1\ ,\ x_2\ ) = (\ 0\ ,0\ )$.

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

(i) Consider $(\ a\ ,\ 0\ ) \in V$. *For each* $\alpha,\beta \in A$,

$$\begin{aligned}(\ a\ ,\ 0\ )\alpha+(\ a\ ,\ 0\ )\beta &= (\ a\alpha^3,\ 0\ )+(\ a\beta^3\ ,\ 0\ ) \\ &= (\ (a\alpha^3+\ a\beta^3\ ),\ 0\ ) \\ &= (\ a(\alpha^3+\ \beta^3\ ),\ 0\ ) \\ &= (\ a\ ,\ 0\ )(\alpha^3+\ \beta^3\ )^{\frac{1}{3}}\ where\ (\alpha+\ \beta\ )^{\frac{1}{3}} \in A\end{aligned}$$

Thus $(\ a\ ,\ 0\ ) \in Q(V)$ *for each* $a \in A$.

(ii) Consider $(\ 0\ ,\ b\ ) \in V$. *For each* $\alpha, \beta \in A$,

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

Thus $(\ 0\ ,\ b\ ) \in Q(V)$ *for each* $b \in A$.

(iii) Consider $(\ a\ ,\ b\ ) \in V$. *For each* $\alpha, \beta \in A$,

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

since in general $\alpha^3 + \beta^3 \neq (\alpha + \beta)^3$. *Moreover,* $(\ a,\ b) \neq Q(V)$ *for each* $\alpha, \beta \in A$. *Hence* $Q(V)$ *is*

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

Let $(a, b) \in V$ *and* $a, b \in A$, *then we have that*

$$\begin{aligned}(\ a\ ,\ b\ ) &= (\ a\ ,\ 0\ ) + (\ 0\ ,\ b\ ), \\ &= (\ a\ ,\ 0\ ) + (\ 0\ ,\ b\ ) \\ &= (\ 1\ ,\ 0\ )a + (\ 0\ ,\ 1\ )b.\end{aligned}$$

It is not difficult to check that $\{(\ 1\ ,\ 0\ ), (\ 0\ ,\ 1\ )\}$ *is linearly independent. Moreover,* $\{(\ 1\ ,\ 0\ ), (\ 0\ ,\ 1\ )\} \in Q(V)$. *Thus* $Q(V)$ *generates the group* $(V, +)$. *Thus, since all the five conditions of a near vector space are satisfied,* (V, A) *is a near vector space. But* (V, A) *is not a vector space. To see this, let* $(a, b) \in V$ *and* $\alpha, \beta \in A$ *then we have* $(\ a\ ,\ b\ )(\alpha + \beta) = (\ a\ (\alpha + \beta)^3,\ b\ (\alpha + \beta))$ *and*

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

In general $(\alpha + \beta)^3 \neq \alpha^3 + \beta^3$. *Thus the distributive law for scalars does not hold in general, so* V *is not a vector space over* A.

(2) Then V *can be decomposed into maximal regular near vector space in the following way:*

Let $Q(V) \setminus \{0\} = \{(\ a\ ,\ 0\ ) \mid a \in A\} \cup \{(\ 0\ ,\ b\ ) \mid b \in A\} \setminus \{(\ 0\ ,\ 0\ )\}$. *We already have that* $B = \{(\ 1\ ,\ 0\ )\}, \{(\ 0\ ,\ 1\ )\}$ *is a basis of* $Q(V)$. *Put* $Q_1(V) = \{\ (a, 0) \mid a\ \in A\} \setminus \{(\ 0\ ,\ 0\ )\}$ *and* $Q_2(V) = Q_1(V) = \{\ (0, b) \mid b\ \in A\} \setminus \{(\ 0\ ,\ 0\ )\}$. *Then* $B_1 = B \cap Q_1 = \{(\ 1\ ,\ 0\ )\}$ *and* $B_2 = B \cap Q_2(V) = \{(\ 0\ ,\ 1\ )\}$. *Let* $V_1' = \langle B_1 \rangle = \{(\ 1\ ,\ 0\ )a \mid a \in A\}$ *and* $V_2' = \langle B_2 \rangle = \{(\ 0\ ,\ 1\ )b \mid b \in A\}$. *The regular near vector spaces* V_1' *and* V_2' *are generated by* B_1 *and* B_2, *respectively. Thus* $V = V_1' \oplus V_2'$ *by the Decomposition Theorem.*

4. The Cardinality of Quasi-kernel $Q(V)$ for $V = F^n$ where F is a Dickson nearfield

Our aim in this section is to determine the cardinality of the near vector spaces constructed in section 3.3.

We shall derive a formula to calculate the cardinality of the quasi-kernel for both regular and non regular near vector spaces. We will use the construction of near vector spaces according to Van Der Walt's Theorem 3.19 where F is a finite field nearfield. It is known that all finite near-fields are Dickson near-fields except for the seven exceptional cases. We shall focus on the construction where $F = DF(p^m)$ elements, where (p, m) is a Dickson pair and $V = F^n$ the scalar multiplication is defined as $(x_1, x_2, \cdots, x_n)\alpha = (x_1\theta_1(\alpha), x_2\theta_2(\alpha), \cdots, x_n\theta_n(\alpha))$ for all $(x_1, x_2, \cdots, x_n) \in V$ and $\alpha \in F$ where the $\theta_{i'}s$ are automorphisms of $(F, \cdots)$ and they can be equal. Any finite field is a Dickson near-field, so our formula can be applied to constructions where F is a finite field too.

Let $V = V_1 \oplus V_2, \cdots, V_r$ be the Canonical decomposition of V, i.e, the V_i are maximal regular subspaces of V. Then for $i, j \in \{1, 2, \cdots, r\}$ such that $i \neq j$ we have $V_i \cap V_j = \{0\}$. Thus applying Theorem 3.19, we see that V_i is isomorphic to $F^{\eta i}$ for some $\eta i \in \mathbb{N}$. Thus the problem is reduced to finding the cardinality of an arbitrary regular near vector space of the form $V = F^n$.

Definition 4.1 ([2]). *Let F be a near-field. Define the kernel F_d of F to be the set of all distributive elements of F, i.e. $F_d = \{d \in F | d(a + b) = da + db, \forall a, b \in F\}$. For the construction of $Q(V) = UV_i$, with $V_i = (d_1, d_2, \cdots, d_n)F$, and $d_i \in F_d, i \in \{1, \cdots, n\}$.*

Lemma 4.2 ([2]). *For $j = \{0, 1, \cdots, n-1\}$, let $B_j = \{(d_1, d_2, \cdots,)F^* | d_i \in GF(p), i = 1, 2, \cdots, n\}$, be subsets of $Q(V) \setminus \{0\}$ such that $(d_1, d_2, \cdots, d_n)$ has exactly j zeros, and atleast one of the $d_i = 1$. Then the family $\{B_j, j = 0, \cdots, n-1\}$ forms a partition of $Q(V) \setminus \{0\}$.*

Proof. We have that $B_j \neq \emptyset$ for all $j = 0, 1, \cdots, n-1$. Let $(a_1, a_2, \cdots a_n) \in B_k \cap B_l$ and suppose $l \neq k$. Then $(a_1, a_2, \cdots a_n) \in B_k$ with k zeros. Also $(a_1, a_2, \cdots, a_n) \in B_l$ with exactly l zeros. This is impossible. So $B_k \cap B_l = \emptyset \; \forall \; l \neq k$. Finally since $B_{j'}s$ are subsets of $Q(V)\{0\}, B_0 \cup B_1 \cup \cdots B_{n-1} \subseteq Q(V) \setminus \{0\}$. Also for a non-zero element $(a_1, a_2, \cdots, a_n) \in Q(V)$, let $k = |\{a_i | a_i = 0\}|$. Then $0 \leq k \leq n-1$ and so $(a_1, a_2, \cdots, a_n) \in B_k$. Therefore, $Q(V) \setminus \{0\} = B_0 \cup B_1, \cdots, B_{n-1}$. Since the family $B_j \; \{j = 0, 1, \cdots, n-1\}$ forms a partition of $Q(V) \setminus \{0\}$,

$$|Q(V)| = \sum_{n-1}^{k=0} |B_k| + 1.$$

□

Theorem 4.3 ([2]). *For the regular near vector space (V, F) where $V = F^n$ and $F = DF(p^m)$ of a finite Dickson near-field with scalar multiplication defined by $(x_1, x_2, \cdots, x_n)\alpha = (x_1\alpha, x_2\alpha, \cdots, x_n\alpha)$, for all $(x_1, x_2, \cdots, x_n) \in V, \alpha \in F$, we have that*

$$| \; Q(V) \; | = \frac{p^n - 1}{p - 1}(p^m - 1) + 1.$$

For the general case where V is not necessarily regular we make use of the Decomposition Theorem. Let the canonical decomposition of V into maximal regular subspaces be given by $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ respectively. Let $n_1, \cdots, n_r$ be the dimension of $V_1, \cdots V_r$ respectively. Then we have the following theorem.

Theorem 4.4 ([2]). *For the near vector space (V, F) where $V = F^n$ and $F = DF(p^m)$, the Dickson near-field of p^m elements and scalar multiplication defined by $(x_1, x_2, \cdots, x_n)\alpha = (x_1\theta_1(\alpha), x_2\theta_2(\alpha), \cdots, x_n\theta_n(\alpha))$, for all $(\; x_1, x_2, \cdots, x_n) \in V$ and*

$\alpha \in F$ where the $\theta_{i's}$ are automorphisms of $(F,\cdot)$ and they can be equal, we have that

$$\begin{aligned}|Q(V)| &= |Q(V_1)\setminus\{0\}| + \cdots + |Q(V_r)\setminus\{0\}| + 1\\ &= \frac{p^{n_1}-1}{p-1}(p^m-1) + \cdots + \frac{p^{n_r}-1}{p-1}(p^m-1) + 1\\ &= \frac{p^{n_1}+\cdots+p^{n_r}-r}{p-1}(p^m-1) + 1.\end{aligned}$$

Thus, this formula applies to all finite near vector spaces. Now let us apply this formula to the*near vector space* constructed in the section 3.3.

Example 4.5. *From Example 3.26 the quasi kernel is given by* $Q_1(V_2) = \{\ (a,0) \mid a\ \in A\}\setminus\{(\ 0\ ,\ 0\ )\}$ *and* $Q_2(V_2) = \{\ (0,b) \mid b\ \in A\}\setminus\{(\ 0\ ,\ 0\ )\}$. *From the formula p is the number of distributive elements in the nearfield and so $p=2$ and $n_1=1$ and $n_2=1$ and for finite fields $m=1$. Therefore applying the formula we have*

$$\begin{aligned}|\ Q(V)\ | &= \frac{p^{n_1}+\cdots+p^{n_r}-r}{p-1}(p^m-1)+1\\ &= \frac{p^{n_1}+p^{n_2}-2}{p-1}(p^m-1)+1\\ &= \frac{2^1+2^1-2}{1}+1\\ &= \frac{4-2}{1}+1\\ &= 3.\end{aligned}$$

5. Conclusion

The main objective of this paper was to introduce the theory of near vector spaces and discuss the proof of the Decomposition Theorem as in André [1]. We have seen that regularity is a central notion in the study of near vector spaces and that the regular subspaces are the building blocks of near vector spaces. We have shown that given a near vector space V which is not regular, we can decompose V into maximal regular near vector spaces. In closing we gave an application of the Decomposition Theorem, where it is used to determine the cardinality of the quasi-kernel $Q(V)$ of V for both non-regular and regular near vector spaces.

References

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

[2] S. Dorfling, K.-T. Howell and S. Sanon, *The decomposition of finite-dimensional nearvector spaces*, Communications in Algebra, 46(7)(2018), 3033-3046.

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

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

[5] J. Neuberger, *Gunter pilz, near-rings, the theory and its applications*, Bulletin of the American Mathematical Society, 84(5)(1978), 934-937.

[6] G. Pilz, *Near-rings: the theory and its applications*, Elsevier, (2011).

[7] K.-T. Howell, *Contributions to the theory of near vector spaces*, Ph.D. dissertation, University of the Free State, (2007).

[8] A. De Bruyn, *Near vector spaces*, Ph.D. dissertation, Stellenbosch: Stellenbosch University, (1990).

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

[10] A. P. van der Walt, *Matrix near-rings contained in 2-primitive near-rings with minimal subgroups*, Journal of Algebra, 148(2)(1992), 296-304.

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