# Finite dimensional near vector space constructions using copies of $\mathbb{Z}_p$ for $p$ a prime

Makuochukwu Felix Oguagbaka (makuo@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by: Dr Karin-Therese Howell (Stellenbosch University, South Africa)
Co-Supervised by: Dr Janko Böhm (Kaiserslautern University, Germany)
Dr Magdaleen Marais (University of Pretoria, South Africa)

23 May 2019

*Submitted in partial fulfillment of a structured masters degree at AIMS South Africa*

# Abstract

In this essay, we study how finite-dimensional near vector spaces over $\mathbb{Z}_p$, for $p$ a prime, can be constructed, decomposed into maximal regular near vector spaces and compared for isomorphism. The notion of a near vector space used here is as defined by André. The decomposition of finite-dimensional near vector spaces over $\mathbb{Z}_p$ into maximal regular subspaces was also programmed using *SAGE*. The algorithms are attached.

## Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.

Makuochukwu Felix Oguagbaka, 23 May 2019

# Contents

# 1. Introduction

Over time there have been various attempts at defining near vector spaces, starting with the notion given by Beidleman (1964) where nearring modules are used in the construction. Subsequently, we have another version by Karzel (1984) using a nearfield over itself and one by André (1974).

The near vector spaces discussed in this essay are those of André (1974). He defined a structure which is less linear than a vector space. Subsequently van der Walt (1992) characterised finite-dimensional near vector spaces. In 2009, Howell and Meyer classified, up to isomorphism, near vector spaces over $\mathbb{Z}_p$ for $p$ a prime (Howell and Meyer, 2009). They later extended their results to finite fields (Howell and Meyer, 2014).

The main focus of this essay is the construction and decomposition of near vector spaces constructed over $\mathbb{Z}_p$ for $p$ a prime as first studied by Howell and Meyer (2009). For the construction of such near vector spaces, the notion of suitable sequences is important. Central to the definition of a near vector space is its quasi-kernel which also plays a significant role in its properties and decomposition. The idea of the decomposition of near vector spaces was part of André (1974)'s original work. He proved the important Decomposition Theorem which shows that every near vector space can be expressed as the direct sum of maximal regular near vector spaces. Furthermore, Rodtes and Chomjun (2017) proved a theorem which checks when two finite-dimensional near vector spaces constructed over finite fields are isomorphic.

In this essay, Chapter 2 consists of basic definitions, lemmas and results. In Chapter 3 we discuss van der Walt's Theorem, the generation of suitable sequences with respect to $\mathbb{Z}_p$ for $p$ a prime and the isomorphism of two finite-dimensional near vector spaces constructed using copies of $\mathbb{Z}_p$, for $p$ a prime.

We wrote some algorithms for the construction and decomposition of a near vector space of finite dimension constructed using copies of $\mathbb{Z}_p$ for $p$ a prime. First, an approach to obtaining a suitable sequence with respect to $\mathbb{Z}_p$, for $p$ a prime, is illustrated in Algorithm 9. The action of an endomorphism on $\mathbb{Z}_p^n$, $p$ a prime, $n \in \mathbb{N}, n \geq 1$, is defined by Algorithm 1. Algorithm 3, illustrates how the quasi-kernel can be obtained and Algorithm 6 shows how to partition a non-zero quasi-kernel into equivalence classes. The set of mutually independent compatible vectors of the non-zero quasi-kernel can be generated using Algorithm 7. Finally, Algorithm 8 describes how to obtain the maximal regular subspaces in the Decomposition Theorem.

# 2. Preliminary Material

## 2.1 Definitions and Lemmas

In this section we give the preliminary material we will need for this project.

**2.1.1 Definition.** ((Howell and Sanon, 2018), Definition 2.1) A triple $(H, +, \cdot)$ is said to be a (right) near field if:

$(a)$ $(H, +)$ is a group;

$(b)$ $(H\backslash\{0\}, \cdot)$ is a group;

$(c)$ For all $x, y, z \in H$, $(x + y) \cdot z = x \cdot z + y \cdot z$.

**2.1.2 Remark.** Similar to Definition 2.1.1, is that of a (left) near field which satisfies only the left distributive law.

**2.1.3 Definition.** ((André, 1974), Definition 4.1) Given two sets $V$ and $G$, the pair $(V, G)$ is said to be a *near vector space* if:

$(a)$ $(V, +)$ is a group;

$(b)$ $G$ is a set of endomorphisms of $V$ with the endomorphisms $0, 1, -1 \in G$;

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

$(d)$ $G$ acts fixed point freely (fpf) on $V$, i.e., for $v \in V$ and $\alpha, \beta \in G$, $v\alpha = v\beta$ implies that $v = 0$ or $\alpha = \beta$;

$(e)$ The quasi-kernel of $V$, denoted by $Q(V)$ or simply by $Q$ if there is no ambiguity, defined as $Q(V) = \{v \in V : \forall\ \alpha, \beta \in G,\ \exists\ \gamma \in G$ such that $v\alpha + v\beta = v\gamma\}$ generates $V$ as a group, i.e. $\forall\ v \in V,\ \exists\ v_i \in Q$ for $i \in \{1, \ldots, n\}$, such that $v = \sum_{i=1}^{n} v_i$.

We note that, as in André's original work, the elements of $G$ are the scalars and written on the right of the elements of $V$, called the vectors. If there is no room for confusion we write the near vector space $(V, G)$ as $V$.

**2.1.4 Definition.** ((André, 1974), Definition 4.1) Let $(V, G)$ be a near vector space and let $Q$ be the quasi-kernel of $V$. A subset, $B$ of $Q$ is said to be a *basis* of $Q$ if it is a linearly independent generating set for $Q$, i.e. every element of $Q$ can be written as a linear combination of elements of $B$. The dimension of $Q$ is the cardinality of $B$.

The following can be deduced from Definition 2.1.3:

**2.1.5 Remark.**

$(a)$ $(V, +)$ is abelian since $-1 \in G$.

To see this let $x, y \in V$.

$$\begin{aligned} x + y &= (-x)(-1) + (-y)(-1) && (\text{since } -1 \in G \text{ and } -x, -y \in V) \\ &= (-x + (-y))(-1) && (\text{since } -1 \in G) \\ &= (-x - y)(-1) \\ &= (-(y + x))(-1) \\ &= y + x. && (\text{since } -1 \in G) \end{aligned}$$

$(b)$ For $\alpha \in G, v \in V$, $0\alpha = 0$ and $(-v)\alpha = -(v\alpha)$.

$(c)$ One can easily see that every vector space is a near vector space with the quasi-kernel equal to the whole space.

Next we list some important properties of the quasi-kernel.

**2.1.6 Lemma.** ((André, 1974), Lemma 2.2) The following are properties of the quasi-kernel $Q(V)$ of a near vector space $(V, G)$:

$(a)$ $0 \in Q(V)$;

$(b)$ Given $v \in Q(V)\backslash\{0\}$ and $\alpha, \beta \in G$, there exists a unique $\gamma \in G$ such that $v\alpha + v\beta = v\gamma$;

$(c)$ If $v \in Q(V)$ then $vG \subseteq Q(V)$;

$(d)$ If $v \in Q(V)$ and $\lambda_i \in G, i = 1, 2, \ldots, n$, then $\forall\ n \in \mathbb{N},\ n \geq 1$, $\exists$ a $\tau \in G$ such that $\sum_{i=1}^{n} v\lambda_i = v\tau \in Q(V)$;

$(e)$ If $v \in Q(V)\backslash\{0\}$ and $\eta, \tau \in G$, then $\exists$ a $\lambda \in G$ such that $v\eta - v\tau = v\lambda$.

*Proof.*

$(a)$ Let $\eta, \tau \in G$. Given any $\gamma \in G$, we have $0\eta + 0\tau = 0\gamma$. Thus, $0 \in Q(V)$.

$(b)$ Let $v \in Q(V)\backslash\{0\}$ and $\eta, \tau \in G$. By Definition 2.1.3$(e)$, $\exists$ a $\gamma \in G$ such that $v\eta + v\tau = v\gamma$. Suppose $\exists$ a $\gamma_1 \in G$ such that $v\eta + v\tau = v\gamma_1$. Then, we have $v\gamma = v\gamma_1$. By Definition 2.1.3$(d)$, since $v \neq 0$ we have $\gamma = \gamma_1$.

$(c)$ Let $v \in Q(V)$ and $\lambda \in G$. If $\lambda = 0$, then $v\lambda = v0 = 0 \in Q(V)$. Suppose $\lambda \neq 0$, then $\lambda^{-1} \in G$. Let $\alpha, \beta \in G$. By Definition 2.1.3$(c)$, $\lambda\alpha, \lambda\beta \in G$. By Definition 2.1.3$(e)$, $\exists$ a $\gamma \in G$ such that

$$\begin{aligned} v(\lambda\alpha) + v(\lambda\beta) &= v\gamma \\ (v\lambda)\alpha + (v\lambda)\beta &= v\lambda\lambda^{-1}\gamma = (v\lambda)(\lambda^{-1}\gamma). \end{aligned}$$

So, $v\lambda \in Q(V)$. Thus, $vG \subseteq Q(V)$.

$(d)$ Let $v \in Q(V)$ and $\lambda_i \in G,\ i = 1, 2, \ldots, n$. We show by induction on $n$ that $\forall\ n \in \mathbb{N},\ n \geq 1$, $\exists$ a $\tau \in G$ such that $\sum_{i=1}^{n} v\lambda_i = v\tau \in Q(V)$.

For $n = 1$, we have $v\lambda_1 \in Q(V)$ as seen in $(c)$ above.

Suppose the statement holds for $n = k \in \mathbb{N}$ for some $k > 1$, i.e., $\sum_{i=1}^{k} v\lambda_i = v\eta \in Q(V)$ for some $\eta \in G$.

We show that $\sum_{i=1}^{k+1} v\lambda_i \in Q(V)$.

$$\begin{aligned}\sum_{i=1}^{k+1} v\lambda_i &= \sum_{i=1}^{k} v\lambda_i + v\lambda_{k+1} \\ &= v\eta + v\lambda_{k+1} \\ &= v\tau \in Q(V), \qquad \text{(since } v \in Q(V) \text{ and by Definition 2.1.3}(e)\text{)}\end{aligned}$$

for some $\tau \in G$.

Thus, by induction on $n$ we have that $\forall\ n \in \mathbb{N},\ n \geq 1$, $\exists$ a $\tau \in G$ such that $\sum_{i=1}^{n} v\lambda_i = v\tau \in Q(V)$.

$(e)$ Let $v \in Q(V)\backslash\{0\}$ and $\alpha, \beta \in G$. By Definition 2.1.3$(c)$, we have $(-1)\beta \in G$. This gives us that $v(-\beta) = (-v)\beta = v(-1)\beta$. So, by Definition 2.1.3$(d)$, since $v \neq 0$ we have $-\beta = (-1)\beta$. Thus by Definition 2.1.3$(e)$, $\exists$ a $\gamma \in G$ such that

$$\begin{aligned} v\alpha + v(-\beta) &= v\gamma \\ v\alpha + v(-1)\beta &= v\gamma \\ v\alpha - v\beta &= v\gamma. \end{aligned}$$

□

**2.1.7 Lemma.** ((André, 1974), Lemma 4.5) Let $(V, G)$ be a near vector space and let $J$ be an index set. Let $B = \{b_j \mid j \in J\}$ be a basis of $Q(V)$. Then each $v \in V$ can be written as a unique linear combination of elements of $B$, i.e. $\exists$ uniquely determined $\alpha_j \in G$, with $\alpha_j = 0$ for all but a finite number of $j \in J$, such that $v = \sum_{j\in J} b_j\alpha_j$.

*Proof.* Let $v \in V$. By Definition 2.1.3$(e)$, there exists $v_1, v_2, \ldots, v_n \in Q(V)$ such that

$$v = \sum_{i=1}^{n} v_i. \tag{2.1.1}$$

Given that $B$ is a basis of $Q(V)$, each $v_i \in Q(V)$ can be written as a linear combination of elements of $B$. So, we have

$$v_i = \sum_{j\in J} b_j\alpha_{ij}, \tag{2.1.2}$$

where $\alpha_{ij} \in G$ for $i \in \{1, 2, \ldots, n\}$ and $b_j \in B$ for $j \in J$. Now substituting Equation 2.1.2 into Equation 2.1.1, we have

$$\begin{aligned} v &= \sum_{i=1}^{n} \sum_{j\in J} b_j\alpha_{ij} \\ &= \sum_{j\in J} b_j\Big(\sum_{i=1}^{n} \alpha_{ij}\Big) \\ &= \sum_{j\in J} b_j\beta_j, \end{aligned}$$

with $\beta_j = \sum_{i=1}^{n} \alpha_{ij}$ for $j \in J$. Thus we have that every $v \in V$ can be written as a linear combination of elements of $B$.

Next we show the uniqueness of such linear combinations.

Suppose that $v = \sum_{j\in J} b_j\eta_j$ and $v = \sum_{j\in J} b_j\tau_j$, for $\eta_j, \tau_j \in G$ $(j \in J)$, with $\eta_j = 0, \tau_j = 0$ for all but a finite number of $j \in J$ and $b_j \in B$ $(j \in J)$. We show that $\eta_j = \tau_j$ for each $j \in J$. Now, we have $\sum_{j\in J} b_j\eta_j = \sum_{j\in J} b_j\tau_j$. This gives $\sum_{j\in J} b_j\eta_j - \sum_{j\in J} b_j\tau_j = 0$. This implies that $\sum_{j\in J}(b_j\eta_j - b_j\tau_j) = 0$. Given that $B \subseteq Q(V)$, we have $b_j \in Q(V)$ $(j \in J)$. By Lemma 2.1.6$(e)$, $\exists$ a $\gamma_j \in G$ such that $b_j\eta_j - b_j\tau_j = b_j\gamma_j$ for each $j \in J$. Thus, we have $\sum_{j\in J}(b_j\eta_j - b_j\tau_j) = 0$ implies that $\sum_{j\in J} b_j\gamma_j = 0$. Seeing that $B$ is linearly independent, $\gamma_j = 0\ \forall\ j \in J$. Thus, $b_j\eta_j - b_j\tau_j = b_j\gamma_j = b_j0 = 0$. So, we have $b_j\eta_j = b_j\tau_j$. Since $b_j \neq 0$ and $G$ acts fixed point freely on $V$, $\eta_j = \tau_j$ for each $j \in J$. □

Let us consider an operation, introduced by André (1974), on $G$.

**2.1.8 Definition.** ((André, 1974), Definition 2.3-(2.2)) Let $(V, G)$ be a near vector space with $V = \{0\}$ or $Q(V) \neq \{0\}$ and let $v \in Q(V)\backslash\{0\}$. Let $\alpha, \beta \in G$. We define the operation, $+_v$ on $G$ by

$$v(\alpha +_v \beta) := v\alpha + v\beta.$$

**2.1.9 Remark.** We note that if $(V, G)$ is a vector space, $\alpha +_v \beta = \alpha + \beta,\ \forall\ v \in Q(V)\backslash\{0\}$.

**2.1.10 Definition.** ((André, 1974), Theorem 2.5-(2.4)) Let $(V, G)$ be a near vector space with $V = \{0\}$ or $Q(V) \neq \{0\}$ and let $v \in Q(V)\backslash\{0\}$. Let $\alpha, \beta, \lambda \in G^*$. We define the operation, $+_{v\lambda}$ on $G$ by

$$\alpha +_{v\lambda} \beta := (\alpha^\lambda +_v \beta^\lambda)^{\lambda^{-1}},$$

where $\alpha^\lambda := \lambda\alpha\lambda^{-1}$. A similar definition holds for $\beta^\lambda$.

**2.1.11 Definition.** ((André, 1974), Definition 2.6) Let $(V, G)$ be a near vector space, and let $u \in Q(V)\backslash\{0\}$. The *kernel* of $V$ with respect to $u$, denoted by $R_u(V)$, is defined as

$$R_u(V) := \{v \in V \mid v(\eta +_u \tau) = v\eta + v\tau \text{ for every } \eta, \tau \in G\}.$$

**2.1.12 Remark.** If $(V, G)$ is a vector space then for each $u \in Q(V)\backslash\{0\}$, we have $R_u(V) = V$.

**2.1.13 Lemma.** ((André, 1974), Lemma 2.9) The following are properties of the kernel $R_u(V)$ of a near vector space $(V, G)$:

$(a)$ $u \in R_u(V)$;

$(b)$ $R_u(V) \subseteq Q(V)$;

$(c)$ $0 \in R_u(V)$;

$(d)$ $(R_u(V), +)$ is a subgroup of $(V, +)$.

*Proof.*

$(a)$ Given that $u \in V$, by Definition 2.1.8, $\forall\ \eta, \tau \in G$ we have $u(\eta +_u \tau) = u\eta + u\tau$. Thus $u \in R_u(V)$.

$(b)$ Let $v \in R_u(V)$, and let $\eta, \tau \in G$. Then there exists a $\lambda = \eta +_u \tau \in G$ such that $v\eta + v\tau = v\lambda$. Thus $v \in Q(V)$. Therefore $R_u(V) \subseteq Q(V)$.

$(c)$ Let $\eta, \tau \in G$. We have $0(\eta +_u \tau) = 0 = 0\eta + 0\tau$. Thus $0 \in R_u(V)$.

$(d)$ Let $x, y \in R_u(V)$ and let $\eta, \tau \in G$. Since $R_u(V) \neq \emptyset$ by $(c)$ above, it suffices to show that $x - y \in R_u(V)$.

$$\begin{aligned}(x-y)(\eta +_u \tau) &= x(\eta +_u \tau) + (-y)(\eta +_u \tau)\\ &= x(\eta +_u \tau) - y(\eta +_u \tau)\\ &= x\eta + x\tau - (y\eta + y\tau)\\ &= x\eta - y\eta + x\tau - y\tau\\ &= (x-y)\eta + (x-y)\tau.\end{aligned}$$

Hence, $x - y \in R_u(V)$.

□

**2.1.14 Lemma.** ((André, 1974), Lemma 2.9) If $x \in R_u(V), y, x + y \in Q(V)$ and $y \notin xG$, then $y \in R_u(V)$.

The notion of compatibility is central to the study of near vector spaces.

**2.1.15 Definition.** ((André, 1974), Definition 4.7) Two elements $v$ and $w$ of $Q\backslash\{0\}$ are said to be *compatible*, denoted by $v\ cp\ w$, if $\exists$ a $\lambda \in G^*$ such that $v + w\lambda \in Q$.

**2.1.16 Remark.** Let $v \in Q\backslash\{0\}$ and let $\lambda \in G^*$, then $v\lambda\ cp\ v$.

To see this, we have that since $1 \in G^*$ then by Lemma 2.1.6$(d)$, $v\lambda + v \cdot 1 \in Q$. Therefore, $v\lambda\ cp\ v$.

Compatibility can be related to the operation defined on $G^*$ in Definition 2.1.8 and Definition 2.1.10 as given in the lemma below.

**2.1.17 Lemma.** ((André, 1974), Lemma 4.8) Let $v, w \in Q\backslash\{0\}$, then $v\ cp\ w$ *if and only if* $\exists$ a $\lambda \in G^*$ such that $+_v = +_{w\lambda}$.

We use this lemma to prove:

**2.1.18 Theorem.** *((André, 1974), Theorem 4.9) The compatibility relation $cp$ is an equivalence relation on $Q\backslash\{0\}$.*

*Proof.* Let $x, y, z \in Q\backslash\{0\}$.

Reflexivity

By Lemma 2.1.6$(d)$, for some $\lambda \in G^*$, we have $y + y\lambda \in Q$. Thus, $y\ cp\ y$.

Symmetry

Suppose $y\ cp\ z$. Then, $\exists$ a $\lambda \in G^*$ such that $y + z\lambda \in Q$.

By Lemma 2.1.6$(c)$, $(y + z\lambda)\lambda^{-1} = y\lambda^{-1} + z\lambda\lambda^{-1} = y\lambda^{-1} + z \in Q$.

Thus, $z\ cp\ y$.

Transitivity

Suppose $x\ cp\ y$ and $y\ cp\ z$. By Lemma 2.1.17, we have that $+_x = +_{y\mu}$ and $+_y = +_{z\tau}$, for some

$\mu, \tau \in G^*$. So, it suffices to show that $+_x = +_{z\lambda}$ for some $\lambda \in G^*$. Let $\gamma, \xi \in G^*$.

$$\begin{aligned}\gamma +_x \xi &= \gamma +_{y\mu} \xi \\ &= (\gamma^\mu +_y \xi^\mu)^{\mu^{-1}} \\ &= (\gamma^\mu +_{z\tau} \xi^\mu)^{\mu^{-1}} \\ &= \gamma +_{z\tau\mu} \xi \\ &= \gamma +_{z\lambda} \xi,\end{aligned}$$

where $\lambda = \tau\mu \in G^*$. This implies that $+_x = +_{z\lambda}$ for some $\lambda \in G^*$. Thus, by Lemma 2.1.17, $x \ cp \ z$.

Thus compatibility partitions the non-zero quasi-kernel of a near vector space. □

The following result will also be useful.

**2.1.19 Theorem.** *((André, 1974), Theorem 2.5-13) Let $x, y$ and $x+y$ be elements of $Q(V)\backslash\{0\}$. Then*

$(a)$ *$x \ cp \ y$, and*

$(b)$ *$x \ cp \ x + y$.*

*Proof.*

$(a)$ Let $\lambda = 1 \in G^*$. Then by Definition 2.1.15, $x + y = x + y \cdot 1 \in Q(V)$. Hence, $x \ cp \ y$.

$(b)$ By Lemma 2.1.6$(c)$, we consider two cases.

Suppose $y \in xG$. Let $y = x\lambda$ with $\lambda \in G^*$. Then by Lemma 2.1.6$(d)$, we have $x + (x + y) \cdot 1 = x \cdot 1 + x \cdot 1 + x\lambda \in Q(V)$. Hence, $x \ cp \ x + y$.

Suppose that $y \notin xG$. By Lemma 2.1.13$(a)$, $x \in R_x(V)$. By Lemma 2.1.14, $y \in R_x(V)$. We have that $x + y \in R_x(V)$ by Lemma 2.1.13$(d)$. Thus, by Lemma 2.1.13$(a)$ and 2.1.13$(d)$, $x + (x + y) \in R_x(V) \subseteq Q(V)$. Hence, $x \ cp \ x + y$.

□

Next we need the notion of subspaces.

**2.1.20 Definition.** ((Howell, 2015), Definition 2.3) Given a near vector space $(V, G)$, a non-empty subset $\bar{V}$ of $V$ generated by $XG = \{xg \mid x \in X, g \in G\}$, where $X$ is a maximal independent subset of $Q(V)$, is said to be a *subspace* of $(V, G)$ if $\bar{V}$ is the subgroup of $(V, +)$.

**2.1.21 Remark.**

$(a)$ Let $\bar{V}$ be a subspace of $V$. For $g, g_i \in G$ and $x_i \in X, i \in \{1, 2, \ldots, n\}$, we have

$$\begin{aligned}(x_1g_1 + \cdots + x_ng_n)g &= (x_1g_1)g + \cdots + (x_ng_n)g \\ &= x_1g_1g + \cdots + x_ng_ng \\ &= x_1h_1 + \cdots + x_nh_n,\end{aligned}$$

where $h_i = g_ig \in G$ for $i \in \{1, 2, \ldots, n\}$. Thus, we can say that each element of $\bar{V}$ is a linear combination of elements of $X$. So, $X$ is a basis for $\bar{V}$. Thus, the dimension of $\bar{V}$ is the cardinality of $X$.

$(b)$ Since $V$ is generated by $XG$, where $X$ is a basis of $Q(V)$, then $V$ is its own subspace.

$(c)$ The trivial subspace, $\{0\}$ is generated by the empty subset of $Q(V)$.

The following lemma shows how to obtain the quasi-kernel of a subspace from the quasi-kernel of the corresponding near vector space.

**2.1.22 Lemma.** ((Howell, 2007), Lemma 2.5-16) If $W$ is a subspace of $V$ then $Q(W) = W \cap Q(V)$.

*Proof.* It suffices to show that $Q(W) \subseteq W \cap Q(V)$ and $W \cap Q(V) \subseteq Q(W)$.

" $\Rightarrow$ " Let $y \in Q(W)$. Then $y \in W$. Since $y \in Q(W)$ by Definition 2.1.3$(e)$, for $\alpha, \beta \in G$, $\exists$ a $\lambda \in G$ such that

$$y\alpha + y\beta = y\lambda. \tag{2.1.3}$$

Since $W$ is a subspace of $V$, $y \in V$ and by Equation 2.1.3, we have $y \in Q(V)$. Thus $y \in W \cap Q(V)$. Hence, $Q(W) \subseteq W \cap Q(V)$.

" $\Leftarrow$ " Let $x \in W \cap Q(V)$. This implies that $x \in W$ and $x \in Q(V)$. Given that $x \in Q(V)$, by Definition 2.1.3, for each $\alpha, \beta \in G$, $\exists$ a $\gamma \in G$ such that

$$x\alpha + x\beta = x\gamma. \tag{2.1.4}$$

Since $x \in W$ and Equation 2.1.4 holds, we have $x \in Q(W)$. Thus $W \cap Q(V) \subseteq Q(W)$.

Hence, $Q(W) = W \cap Q(V)$. □

As with vector spaces we have the lemma below:

**2.1.23 Lemma.** ((Howell et al., 2019), Lemma 2.3) Given a near vector space $(V, G)$, a non-empty subset $\bar{V}$ of $V$ is a subspace of $V$ if and only if $\bar{V}$ is closed under addition and scalar multiplication.

**2.1.24 Definition.** ((André, 1974), Definition 4.11) A near vector space $(V, G)$ is said to be *regular* if any two elements, $v$ and $w$ of $Q(V)\backslash\{0\}$ are compatible.

**2.1.25 Remark.**

$(a)$ If $V = Q(V)$ then $V$ is regular.

$(b)$ It is clear by Definition 2.1.24 that any vector space is regular.

**2.1.26 Theorem.** *((André, 1974), Theorem 4.12) A near vector space $(V, G)$ is regular if and only if there exists a basis which consists of mutually pairwise compatible vectors.*

*Proof.* Let $(V, G)$ be a near vector space.

" $\Rightarrow$ " We suppose that $V$ is regular. Definition 2.1.24 gives us that any two non-zero vectors of $Q(V)$ are compatible. Thus any basis, say $B \subseteq Q(V)$ of $V$ comprises of mutually pairwise compatible vectors.

" $\Leftarrow$ " Let $B \subseteq Q(V)$ be a basis of $V$ comprising of mutually pairwise compatible vectors. Let $v \in Q(V)\backslash\{0\}$. By Lemma 2.1.7, $v = \sum_{i=1}^{n} v_i\lambda_i$ where $v_i \in B$ and $\lambda_i \in G$, with $\lambda_i \neq 0$ for all $i \in \{1, 2, \ldots, n\}$. Let

$$v' = \begin{cases} \sum_{i=1}^{n-1} v_i\lambda_i & \text{if } n > 1, \\ 0 & \text{if } n = 1. \end{cases}$$

Then $v = v' + v_n\lambda_n \in Q$. By Definition 2.1.3$(e)$, $\forall\ \alpha, \beta \in G$, $\exists$ a $\gamma \in G$ such that $(v' + v_n\lambda_n)\alpha + (v' + v_n\lambda_n)\beta = (v' + v_n\lambda_n)\gamma \implies v'\alpha + v'\beta + v_n\lambda_n\alpha + v_n\lambda_n\beta = v'\gamma + v_n\lambda_n\gamma$. Given that $v_n \notin \{v_1, v_2, \ldots, v_{n-1}\}$ and $v_n\lambda_n \in Q$, by uniqueness (Lemma 2.1.7), we have $v_n\lambda_n\alpha + v_n\lambda_n\beta = v_n\lambda_n\gamma$. Thus $v'\alpha + v'\beta = v'\gamma \implies v' \in Q$. We investigate two possibilities for $v'$.

If $v' = 0$ then $v = v_n\lambda_n$. Thus by Remark 2.1.16, $v\ cp\ v_n$.

If $v' \neq 0$ then by Theorem 2.1.19, $v_n\lambda_n\ cp\ v$. Since $v_n\ cp\ v_n\lambda_n$ (by Remark 2.1.16) then by transitivity of $cp$ (Theorem 2.1.18), $v\ cp\ v_n$.

We have that each element of $B$ is compatible with $v_n$. Thus by transitivity of $cp$ (Theorem 2.1.18), each element of $B$ is compatible with $v$. Given that $v \in Q(V)\backslash\{0\}$ was chosen arbitrarily, if $x, y \in Q(V)\backslash\{0\}$ then $x\ cp\ v_i$ and $v_i\ cp\ y$ with $v_i \in B$. By transitivity of $cp$ (Theorem 2.1.18), $x\ cp\ y$. Thus $Q(V)\backslash\{0\}$ comprises of mutually pairwise compatible vectors. Hence, $V$ is regular. □

We will also need:

**2.1.27 Definition.** ((Howell et al., 2019), Definition 2.8) Two near vector spaces $(W_1, G_1)$ and $(W_2, G_2)$ are said to be *isomorphic*, $(W_1, G_1) \cong (W_2, G_2)$, if there are group isomorphisms $\phi : (W_1, +) \longrightarrow (W_2, +)$ and $\psi : (G_1^*, \cdot) \longrightarrow (G_2^*, \cdot)$ such that $\phi(w\alpha) = \phi(w)\psi(\alpha)$, $\forall\ w \in W_1, \alpha \in G_1^*$.

## 2.2 An example of a Near Vector Space over $\mathbb{Z}_p$ for $p$ a prime

Let $G = \mathbb{Z}_p$ for $p$ a prime and let $V$ be n-copies of $G$ for $n \in \mathbb{N},\ n \geq 1$. Let $\alpha \in G$ be an endomorphism on $V$. The action of $\alpha$ on $V$ is given as

$$(v_1, \ldots, v_n)\alpha := (v_1\phi_1(\alpha), \ldots, v_n\phi_n(\alpha)),$$

where $(v_1, \ldots, v_n) \in V$ and $\phi_i$ $(i \in \{1, \ldots, n\})$ is a semigroup automorphism of $G\backslash\{0\}$. By Lemma 3.1.3, $\exists$ a $q_i \in \mathbb{Z}$ with $1 \leq q_i < p - 1$ and $\gcd(q_i, p - 1) = 1$ such that $\phi_i(\alpha) = \alpha^{q_i}$ for $i \in \{1, \ldots, n\}$. By Theorem 3.1.1, the pair $(V, G)$ is a near vector space.

For example, let $(V, G) = ((\mathbb{Z}_{11})^3, \mathbb{Z}_{11})$ and let $\alpha \in G$ be an endomorphism on $V$ defined as

$$(x_1, x_2, x_3)\alpha := (x_1\alpha, x_2\alpha^3, x_3\alpha^7)$$

for all $(x_1, x_2, x_3) \in V$.

(I) We verify that $(V, G)$ satisfies the conditions of Definition 2.1.3.
Let $(x_1, x_2, x_3), (y_1, y_2, y_3), (z_1, z_2, z_3) \in V$.

$(a)$ We know that $(V, +) = ((\mathbb{Z}_{11})^3, +)$ is a group.

$(b)$ We show that $G$ is a set of endomorphisms of $V$.

Let $\alpha \in G$. Then,

$$\begin{aligned}[(x_1, x_2, x_3) + (y_1, y_2, y_3)]\alpha &= (x_1 + y_1, x_2 + y_2, x_3 + y_3)\alpha \\ &= ((x_1 + y_1)\alpha, (x_2 + y_2)\alpha^3, (x_3 + y_3)\alpha^7) \\ &= (x_1\alpha + y_1\alpha, x_2\alpha^3 + y_2\alpha^3, x_3\alpha^7 + y_3\alpha^7) \\ &= (x_1\alpha, x_2\alpha^3, x_3\alpha^7) + (y_1\alpha, y_2\alpha^3, y_3\alpha^7) \\ &= (x_1, x_2, x_3)\alpha + (y_1, y_2, y_3)\alpha.\end{aligned}$$

Hence, $\alpha$ is an endomorphism of V.

We show that $0, 1, -1 \in G$.

$$(x_1, x_2, x_3)0 = (x_1 0, x_2 0^3, x_3 0^7) = (0, 0, 0).$$

$$(x_1, x_2, x_3)1 = (x_1 1, x_2 1^3, x_3 1^7) = (x_1, x_2, x_3).$$

$$\begin{aligned}(x_1, x_2, x_3)(-1) &\equiv (x_1, x_2, x_3)10 \\ &= (x_1 10, x_2 10^3, x_3 10^7) \\ &\equiv (x_1 10, x_2 10, x_3 10) \\ &\equiv (x_1(-1), x_2(-1), x_3(-1)) \\ &= (-x_1, -x_2, -x_3).\end{aligned}$$

$(c)$ We show that $G\backslash\{0\}$ is a subgroup of the automorphism group of $(V, +)$.

Let $\beta \in G\backslash\{0\}$. Then $\beta$ is an endomorphism. It remains to show that $\beta$ is a bijection since $G$ is a field.

**Injectivity**

Suppose $(x_1, x_2, x_3)\beta = (y_1, y_2, y_3)\beta$. Then, we have $(x_1\beta, x_2\beta^3, x_3\beta^7) = (y_1\beta, y_2\beta^3, y_3\beta^7)$ imples that $x_1\beta = y_1\beta,\ x_2\beta^3 = y_2\beta^3$ and $x_3\beta^7 = y_3\beta^7$. So, we have $(x_1 - y_1)\beta = 0,\ (x_2 - y_2)\beta^3 = 0$ and $(x_3 - y_3)\beta^7 = 0$. Since $\beta \neq 0$ and $G$ is a field, then $x_1 = y_1,\ x_2 = y_2$ and $x_3 = y_3$. Thus, $\beta$ is injective.

**Surjectivity**

We have $(x_1\beta^{-1}, x_2\beta^{-3}, x_3\beta^{-7}) \in V$. Then, $(x_1\beta^{-1}, x_2\beta^{-3}, x_3\beta^{-7})\beta = (x_1\beta^{-1}\beta, x_2\beta^{-3}\beta^3, x_3\beta^{-7}\beta^7) = (x_1, x_2, x_3)$. Thus, $\beta$ is surjective.

Hence, $G$ is a subgroup of automorphism group of $(V, +)$.

$(d)$ We show that $G$ acts fixed point free on $V$.

Let $\alpha, \beta \in G$.

Suppose $(x_1, x_2, x_3)\alpha = (x_1, x_2, x_3)\beta$. Then, we have $(x_1\alpha, x_2\alpha^3, x_3\alpha^7) = (x_1\beta, x_2\beta^3, x_3\beta^7) \implies x_1\alpha = x_1\beta,\ x_2\alpha^3 = x_2\beta^3$ and $x_3\alpha^7 = x_3\beta^7 \implies x_1(\alpha - \beta) = 0,\ x_2(\alpha^3 - \beta^3) = 0$ and $x_3(\alpha^7 - \beta^7) = 0$.

Suppose $\alpha \neq \beta$, then $\alpha^3 \neq \beta^3$ and $\alpha^7 \neq \beta^7$. Since $G$ is a field, then $x_1 = x_2 = x_3 = 0$.

Suppose $(x_1, x_2, x_3) \neq (0, 0, 0)$. Since $G$ is a field, we have $\alpha - \beta = 0,\ \alpha^3 - \beta^3 = 0,\ \alpha^7 - \beta^7 = 0$ which implies that $\alpha = \beta,\ \alpha^3 = \beta^3,\ \alpha^7 = \beta^7$.

$(e)$ We obtain the quasi-kernel, $Q(V)$ of $V$.

Case 1: For $(u,0,0) \in V$ and $\eta, \tau \in G$,

$$\begin{aligned}(u,0,0)\eta + (u,0,0)\tau &= (u\eta,0,0) + (u\tau,0,0)\\ &= (u\eta + u\tau, 0, 0)\\ &= (u(\eta+\tau),0,0)\\ &= (u,0,0)(\eta+\tau).\end{aligned}$$

Hence, $(u,0,0) \in Q(V)$ for each $u \in G$.

Case 2: For $(0,v,0) \in V$ and $\eta, \tau \in G$,

$$\begin{aligned}(0,v,0)\eta + (0,v,0)\tau &= (0,v\eta^3,0) + (0,v\tau^3,0)\\ &= (0,v\eta^3 + v\tau^3,0)\\ &= (0,v(\eta^3+\tau^3),0,0)\\ &= (0,v,0)(\eta^3+\tau^3)^{\frac{1}{3}}.\end{aligned}$$

Hence, $(0,v,0) \in Q(V)$ for each $v \in G$.

Case 3: For $(0,0,w) \in V$ and $\eta, \tau \in G$,

$$\begin{aligned}(0,0,w)\eta + (0,0,w)\tau &= (0,0,w\eta^7) + (0,0,w\tau^7)\\ &= (0,0,w\eta^7 + w\tau^7)\\ &= (0,0,w(\eta^7+\tau^7))\\ &= (0,0,w)(\eta^7+\tau^7)^{\frac{1}{7}}.\end{aligned}$$

Hence, $(0,0,w) \in Q(V)$ for each $w \in G$.

One can easily check to see that the following elements of $V$, $(u,v,w), (u,v,0), (0,v,w), (u,0,w)$ are not elements of $Q(V)$ for $u,v,w \in G^*$.

Thus, $Q(V) = \{(u,0,0) \mid u \in G\} \cup \{(0,v,0) \mid v \in G\} \cup \{(0,0,w) \mid w \in G\}$.

$(f)$ We show that $Q(V)$ generates $V$ as a group.

Let $(u,v,w) \in V$. We have that, $(u,v,w) = (1,0,0)u + (0,1,0)v^{\frac{1}{3}} + (0,0,1)w^{\frac{1}{7}}$ where $(1,0,0),(0,1,0),(0,0,1) \in Q(V)$ and $u, v^{\frac{1}{3}}, w^{\frac{1}{7}} \in G$.

**Claim**

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

*Proof.* It suffices to show that $B$ is a basis of $Q(V)$.

Let $\lambda_1, \lambda_2, \lambda_3 \in G$. Suppose that $(1,0,0)\lambda_1 + (0,1,0)\lambda_2 + (0,0,1)\lambda_3 = (0,0,0)$. Then, we have $(\lambda_1,0,0) + (0,\lambda_2^3,0) + (0,0,\lambda_3^7) = (0,0,0) \implies (\lambda_1,\lambda_2^3,\lambda_3^7) = (0,0,0) \implies \lambda_1 = 0,\ \lambda_2^3 = 0,\ \lambda_3^7 = 0 \implies \lambda = \lambda_2 = \lambda_3 = 0$. Thus, $B$ is independent.

Let $x \in Q(V)$. We consider three cases

If $x = (u,0,0)$ for some $u \in G$ then $x = (1,0,0)u + (0,1,0)0 + (0,0,1)0$, where $u, 0 \in G$.
If $x = (0,v,0)$ for some $v \in G$ then $x = (1,0,0)0 + (0,1,0)v^{\frac{1}{3}} + (0,0,1)0$, where $v^{\frac{1}{3}}, 0 \in G$.
If $x = (0,0,w)$ for some $w \in G$ then $x = (1,0,0)0 + (0,1,0)0 + (0,0,1)w^{\frac{1}{7}}$, where $w^{\frac{1}{7}}, 0 \in G$.
Thus, $B$ is a basis of $Q(V)$. Therefore, the near vector space $(V,G)$ is of dimension 3.

(II) We move to decompose $V$ into regular near vector spaces that are maximal.

Let $Q^* := Q(V)\backslash\{0\}$ and let $G^* := G\backslash\{0\}$. Then, $Q^* = \{(u,0,0) \mid u \in G^*\} \cup \{(0,v,0) \mid v \in G^*\} \cup \{(0,0,w) \mid w \in G^*\}$. We partition $Q^*$ into sets comprising of mutually pairwise compatible vectors. We begin by defining the following sets:

$$\begin{aligned} Q_1 &:= \{(u,0,0) \mid u \in G^*\} \\ Q_2 &:= \{(0,v,0) \mid v \in G^*\} \\ Q_3 &:= \{(0,0,w) \mid w \in G^*\}. \end{aligned}$$

Then, we set

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

We define subspaces $V_i$ of $V$ generated by $B_i$ respectively for $i = 1,2,3$.

$$\begin{aligned} V_1 &:= \langle B_1\rangle = \{(1,0,0)u \mid u \in G\} = \{(u,0,0) \mid u \in G\}. \\ V_2 &:= \langle B_2\rangle = \{(0,1,0)v \mid v \in G\} = \{(0,v^3,0) \mid v \in G\} = \{(0,v',0) \mid v' = v^3 \in G\}. \\ V_3 &:= \langle B_3\rangle = \{(0,0,1)w \mid w \in G\} = \{(0,0,w^7) \mid w \in G\} = \{(0,0,w') \mid w' = w^7 \in G\}. \end{aligned}$$

We now show that each of the subspaces $V_i$ for $i = 1,2,3$ is a maximal regular near vector space.

Let $(u_1,0,0),(u_2,0,0) \in Q(V_1)\backslash\{0\}$. Then, for $\gamma \in G^*$ we have $(u_1,0,0) + (u_2,0,0)\gamma = (u_1 + u_2\gamma, 0, 0) \in Q(V_1)$. By Definition 2.1.24, $V_1$ is regular.

Now, we suppose that there is a regular near vector space $X$ generated by $Q(X)$ such that $V_1 \subset X$, which implies that $Q(V_1) \subset Q(X)$. Let $x = (u,v,w) \neq (u,0,0)$ and $x \in Q(X)\backslash Q(V_1)$.

Since $X$ is regular and $Q(V_1) \subset Q(X)$, $(u,v,w)$ $cp$ $(y,0,0)$ for $y \in G^*$. Thus, $(u,v,w) + (y,0,0)\lambda = (u+y\lambda, v, w) \in Q(X) \subset Q(V) \implies (u+y\lambda, v, w) \in Q(V)$, which is a contradiction. Thus, $V_1$ is a maximal regular near vector space.

Similarly, $V_2$ and $V_3$ are maximal regular near vector spaces.

Since $\bigcap_{i=1}^{3} V_i = \{(0,0,0)\}$, by Definition 2.3.3, $V = V_1 \oplus V_2 \oplus V_3$.

(III) Let $\eta, \tau \in G$. For each $x \in Q(V)\backslash\{0\}$, we define $+_x$ on $G$ as given in Definition 2.1.8.

Let us consider the following three possibilities for $x \in Q(V)\backslash\{0\}$:

$(a)$ Let $x = (u,0,0)$ with $u \in G\backslash\{0\}$. Then

$$\begin{aligned} (u,0,0)(\eta +_x \tau) &= (u,0,0)\eta + (u,0,0)\tau \\ &= (u\eta,0,0) + (u\tau,0,0) \\ &= (u\eta + u\tau, 0, 0) \\ &= (u(\eta+\tau),0,0) \\ &= (u,0,0)(\eta+\tau). \end{aligned}$$

By Definition 2.1.3$(d)$, $\eta +_x \tau = \eta + \tau$ for $(u,0,0) \in Q(V)\backslash\{0\}$.

$(b)$ Let $x = (0, v, 0)$ with $v \in G\backslash\{0\}$. Then

$$\begin{aligned}(0,v,0)(\eta +_x \tau) &= (0,v,0)\eta + (0,v,0)\tau \\ &= (0, v\eta^3, 0) + (0, v\tau^3, 0) \\ &= (0, v\eta^3 + v\tau^3, 0) \\ &= (0, v(\eta^3 + \tau^3), 0) \\ &= (0,v,0)(\eta^3 + \tau^3)^{\frac{1}{3}}.\end{aligned}$$

By Definition 2.1.3$(d)$, $\eta +_x \tau = (\eta^3 + \tau^3)^{\frac{1}{3}}$ for $(0, v, 0) \in Q(V)\backslash\{0\}$.

$(c)$ Let $x = (0, 0, w)$ with $w \in G\backslash\{0\}$. Then

$$\begin{aligned}(0,0,w)(\eta +_x \tau) &= (0,0,w)\eta + (0,0,w)\tau \\ &= (0, 0, w\eta^7) + (0, 0, w\tau^7) \\ &= (0, 0, w\eta^7 + w\tau^7) \\ &= (0, 0, w(\eta^7 + \tau^7)) \\ &= (0,0,w)(\eta^7 + \tau^7)^{\frac{1}{7}}.\end{aligned}$$

By Definition 2.1.3$(d)$, $\eta +_x \tau = (\eta^7 + \tau^7)^{\frac{1}{7}}$ for $(0, 0, w) \in Q(V)\backslash\{0\}$.

(IV) Let $\eta, \tau \in G$. For each $x \in Q(V)\backslash\{0\}$, we define $R_x(V)$ as given in Definition 2.1.11.

Let us consider the following three cases:

$(a)$ Let $x = (u, 0, 0) \in Q(V)\backslash\{0\}$. Then by $(III)$ above, $\eta +_{(u,0,0)} \tau := \eta + \tau$. For each $u' \in G$,

$$\begin{aligned}(u',0,0)\eta + (u',0,0)\tau &= (u',0,0)(\eta + \tau) \\ &= (u',0,0)(\eta +_{(u,0,0)} \tau).\end{aligned}$$

Thus by Definition 2.1.11, $\{(u', 0, 0) \mid u' \in G\} \subseteq R_{(u,0,0)}(V)$.

Now let $z \in R_{(u,0,0)}(V)$. By Lemma 2.1.13$(b)$, $z \in Q(V)$. Since $z(\eta +_{(u,0,0)} \tau) = z(\eta + \tau)$ then by $(III)$ above, $z = (u', 0, 0)$ for some $u' \in G$. Thus $R_{(u,0,0)}(V) \subseteq \{(u', 0, 0) \mid u' \in G\}$. Hence, $R_{(u,0,0)}(V) = \{(u', 0, 0) \mid u' \in G\}$.

$(b)$ Let $x = (0, v, 0) \in Q(V)\backslash\{0\}$. Then by $(III)$ above, $\eta +_{(0,v,0)} \tau := (\eta^3 + \tau^3)^{\frac{1}{3}}$. For each $v' \in G$,

$$\begin{aligned}(0,v',0)\eta + (0,v',0)\tau &= (0,v',0)(\eta^3 + \tau^3)^{\frac{1}{3}} \\ &= (0,v',0)(\eta +_{(0,v,0)} \tau).\end{aligned}$$

Thus by Definition 2.1.11, $\{(0, v', 0) \mid v' \in G\} \subseteq R_{(0,v,0)}(V)$.

Now let $z \in R_{(0,v,0)}(V)$. By Lemma 2.1.13$(b)$, $z \in Q(V)$. Since $z(\eta +_{(0,v,0)} \tau) = z(\eta^3 + \tau^3)^{\frac{1}{3}}$ then by $(III)$ above, $z = (0, v', 0)$ for some $v' \in G$. Thus $R_{(0,v,0)}(V) \subseteq \{(0, v', 0) \mid v' \in G\}$. Hence, $R_{(0,v,0)}(V) = \{(0, v', 0) \mid v' \in G\}$.

$(c)$ Let $x = (0, 0, w) \in Q(V)\backslash\{0\}$. Then by $(III)$ above, $\eta +_{(0,0,w)} \tau := (\eta^7 + \tau^7)^{\frac{1}{7}}$. For each $w' \in G$,

$$\begin{aligned}(0,0,w')\eta + (0,0,w')\tau &= (0,0,w')(\eta^7 + \tau^7)^{\frac{1}{7}} \\ &= (0,0,w')(\eta +_{(0,0,w')} \tau).\end{aligned}$$

Thus by Definition 2.1.11, $\{(0,0,w') \mid w' \in G\} \subseteq R_{(0,0,w)}(V)$.

Now let $z \in R_{(0,0,w)}(V)$. By Lemma 2.1.13$(b)$, $z \in Q(V)$. Since $z(\eta +_{(0,0,w)} \tau) = z(\eta^7 + \tau^7)^{\frac{1}{7}}$ then by $(III)$ above, $z = (0,0,w')$ for some $w' \in G$. Thus $R_{(0,0,w)}(V) \subseteq \{(0,0,w') \mid w' \in G\}$. Hence, $R_{(0,0,w)}(V) = \{(0,0,w') \mid w' \in G\}$.

## 2.3 The Decomposition Theorem

We start by briefly discussing the notion of direct sum of subspaces of a near vector space.

**2.3.1 Definition.** ((Dorfling et al., 2018), Definition 2.5) A near vector space $(V,G)$ is said to be the direct sum of the subspaces $V_1, V_2, \ldots, V_n$, denoted by $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$ *if and only if* $V = V_1 + V_2 + \cdots + V_n$ and $V_i \cap (V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_n) = \{0\}$, for each $i \in \{1, \ldots, n\}$.

**2.3.2 Remark.** It can be shown that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$ if and only if every vector $v \in V$ has a unique representation $v_1 + v_2 + \cdots + v_n$, with $v_i \in V_i$ $(i = 1, 2, \ldots, n)$.

Now we state and prove the decomposition theorem.

**2.3.3 Theorem.** ***(The Decomposition Theorem)*** *((André, 1974), Theorem 4.13) Every near vector space $(V,G)$ is the direct sum of regular near vector spaces $V_i$ $(i \in I)$ such that each $v \in Q(V)\backslash\{0\}$ lies in precisely one direct summand $V_i$. The subspaces $V_i$ are maximal regular near vector spaces.*

We give the prove of Theorem 2.3.3 in three parts.

*Proof.*

Part 1: Let $(V,G)$ be a near vector space and let $I$ and $J$ be index sets. Applying Theorem 2.1.18, we partition $Q(V)\backslash\{0\}$ into sets, $Q_j$ $(j \in J)$ comprising of mutually pairwise compatible vectors. Let $B = \{b_i \mid i \in I\} \subseteq Q(V)\backslash\{0\}$ be a basis of $V$. We define $B_j := B \cap Q_j$ an independent subset of $Q(V)$ for $j \in J$. Since the $Q_j's$ are disjoint and $B$ is a basis, the $B_j's$ are mutually disjoint independent sets. We have that $\bigcup\limits_{j\in J} B_j = \bigcup\limits_{j\in J} (B \cap Q_j) = B \cap (\bigcup\limits_{j\in J} Q_j) = B \cap (Q\backslash\{0\}) = B$. Thus, for each $i \in I, b_i \in B_j$ for some $j \in J$. Let $I_j = \{i \in I \mid b_i \in B_j\}$. Then, $I = \bigcup\limits_{j\in J} I_j$ and for each $j \in J$, $B_j = \{b_{ij} := b_i \mid i \in I_j\}$. Let $V_j := \langle B_j \rangle$ be the subspace of $V$ generated by $B_j$ for $j \in J$. Since each of the $B_j's$ consists of mutually pairwise compatible vectors, by Theorem 2.1.26, each $V_j$ is regular for $j \in J$.

Let $v \in V$. We show that $V$ can be written as the direct sum of the $V_j's$ for $j \in J$. By Lemma 2.1.7, there exists uniquely $\lambda_i \in G$, with $\lambda_i = 0$ for all but a finite number of $i \in I$ such that

$$\begin{aligned} v &= \sum_{i\in I} b_i \lambda_i \\ &= \sum_{j\in J} \Big( \sum_{i\in I_j} b_{ij} \lambda_{ij} \Big) \\ &= \sum_{j\in J} v_j, \end{aligned}$$

where $v_j = \sum\limits_{i\in I_j} b_{ij}\lambda_{ij}$ for some $v_j \in V_j$, with $b_{ij} = b_i \in B_j$, $\lambda_{ij} = \lambda_i \in G$ and $i \in I_j$.

By Lemma 2.1.7, $v_j \in V_j$ is uniquely determined for $j \in J$. So, $v = \sum_{j\in J} v_j$ is uniquely determined. Hence, $V = \oplus_{j\in J} V_j$.

Part 2: Let $v \in Q(V)\backslash\{0\}$. We show that exactly one of the $V_j$, for $j \in J$ contains $v$.

Suppose we have some $v \in Q(V)\backslash\{0\}$ such that for any $j \in J$, $v \notin V_j$. We take

$$v := \sum_{j\in J} v_j \in Q(V)\backslash\{0\} \tag{2.3.1}$$

to be such an element with the least number of non-zero elements $v_j \in V_j$ $(j \in J)$.
Given that $v \in Q(V)\backslash\{0\}$ by Definition 2.1.3$(e)$, for every $\alpha, \beta \in G$, $\exists$ a $\gamma \in G$ such that $v\alpha + v\beta = v\gamma$. So $\sum_{j\in J} v_j\alpha + \sum_{j\in J} v_j\beta = \sum_{j\in J} v_j\gamma \implies \sum_{j\in J}(v_j\alpha + v_j\beta) = \sum_{j\in J} v_j\gamma$. Since $\oplus_{j\in J} V_j$ is a direct sum, i.e. $V_i \cap V_j = \{0\}$ for $i \neq j$, $v_j\alpha + v_j\beta = v_j\gamma$ for all $j \in J$. Thus for all $J' \subseteq J$, $\big(\sum_{j\in J'} v_j\big)\alpha + \big(\sum_{j\in J'} v_j\big)\beta = \big(\sum_{j\in J'} v_j\big)\gamma$. Thus $\sum_{j\in J'} v_j \in Q(V)$.
Let

$$v' := \sum_{j\in J'} v_j \in Q(V) \tag{2.3.2}$$

such that $v' \neq 0$. Let $J_v = \{j \in J \mid v_j \neq 0 \text{ in Equation 2.3.1}\}$ and $J_{v'} = \{j \in J' \mid v_j \neq 0 \text{ in Equation 2.3.2}\}$. By the definition of $v'$, we have $J_{v'} \subseteq J_v$. Since $v \notin V_j$ for some $j \in J$, $|J_v| > 1$. By definition of $v$, $|J_u| \geq |J_v|$ for all $u \in Q(V)\backslash \bigcup_{j\in J} V_j$.

Let $J' \subseteq J$ such that $J_v \cap (J\backslash J') \neq \emptyset$. We show that $|J_{v'}| = 1$ and $|J_{v-v'}| = 1$ with $v'$ as defined in Equation 2.3.2.

$(a)$ We show that $|J_{v'}| = 1$.
Given that $v' \neq 0$, $|J_{v'}| \neq 0$. Suppose that $|J_{v'}| > 1$. Let $v' = v_{j_1} + v_{j_2} + \cdots + v_{j_m}$ with $m > 1$ and $J_{v'} = \{j_1, j_2, \ldots, j_m\}$. If $v' \in V_{j_i}$ with $j_i \in J'$ then $v' - v_{j_i} \in V_{j_i}$ and $v' - v_{j_i} \in \oplus_{j\in J\backslash\{j_i\}} V_j$. Thus $v' - v_{j_i} \in V_{j_i} \cap \oplus_{j\in J\backslash\{j_i\}} V_j = \{0\} \implies v' = v_{j_i}$. This contradicts our assumption that $m > 1$ in the expression of $v'$. Thus $v' \notin V_{j_i}$ with $j_i \in J'$.

If $v' \in V_{j'}$ with $j' \in J\backslash J'$ then $v' \in V_{j'} \cap \oplus_{j\in J\backslash\{j'\}} V_j = \{0\}$, which implies that $v' = 0$, a contradiction. Thus $v' \notin V_{j'}$ with $j' \in J\backslash J'$. Hence, $v' \notin \bigcup_{j\in J} V_j$. Given that $v' \in Q(V)$, $v' \in Q(V)\backslash \bigcup_{j\in J} V_j$. Thus $|J_{v'}| \geq |J_v|$. Given that $J_{v'} \subseteq J_v$ and $|J_{v'}| \geq |J_v|$, we have $J_{v'} = J_v$. Thus $J_v \cap (J\backslash J') = J_{v'} \cap (J\backslash J') \subseteq J_{v'} \cap (J\backslash J_{v'}) = \emptyset$, which contradicts our assumption. Hence, $J_{v'} = \{j^*\}$ for some $j^* \in J$.

$(b)$ Given that $J_v \cap (J\backslash J') \neq \emptyset$, $|J_{v-v'}| \neq 0$. Suppose $|J_{v-v'}| > 1$. Let $v - v' = v_{j_1} + v_{j_2} + \cdots + v_{j_n}$ with $n > 1$ and $J_{v'} = \{j_1, j_2, \ldots, j_n\}$. If $v - v' \in V_{j_i}$ with $j_i \in J'$ then $v - v' - v_{j_i} \in V_{j_i}$ and $v - v' - v_{j_i} \in \oplus_{j\in J\backslash\{j_i\}} V_j$. Thus $v - v' - v_{j_i} \in V_{j_i} \cap \oplus_{j\in J\backslash\{j_i\}} V_j = \{0\} \implies v - v' = v_{j_i}$. This contradicts our assumption that $n > 1$ in the expression of $v - v'$. Thus $v - v' \notin V_{j_i}$ with $j_i \in J'$.

If $v - v' \in V_{j'}$ with $j' \in J\backslash J'$ then $v - v' \in V_{j'} \cap \oplus_{j\in J\backslash\{j'\}} V_j = \{0\}$, which implies that $v = v'$, which contradicts our assumption that $J_v \cap (J\backslash J') \neq \emptyset$. Thus $v - v' \notin V_{j'}$ with $j' \in J\backslash J'$. Hence, $v - v' \notin \bigcup_{j\in J} V_j$.
Let $\alpha, \beta \in G$. By the definition of $v$ and $v'$, $(v - v')\alpha + (v - v')\beta = v\alpha + v\beta - (v'\alpha + v'\beta) =$

$v\gamma - v'\gamma = (v - v')\gamma$. Thus $v - v' \in Q(V)\backslash \bigcup_{j\in J} V_j$. Hence, $|J_{v-v'}| \geq |J_v|$. Given that $J_{v-v'} \subseteq J_v$ and $|J_{v-v'}| \geq |J_v|$, we have that $J_{v-v'} = J_v$. This implies that $J_{v'} = 0$, a contradiction. Hence, $J_{v-v'} = \{j^{**}\}$ for some $j^{**} \in J$.

Now, let $v' \in V_{j^*}$ and $v - v' \in V_{j^{**}}$. We have $v' \in V_{j^*} \cap Q(V) =: Q_{j^*}$ and $v - v' \in V_{j^{**}} \cap Q(V) =: Q_{j^{**}}$. Since $v - v' + v' = v \in Q(V)$, $v'$ $cp$ $v - v'$. Thus $j^* = j^{**}$. Let $j = j^* = j^{**}$. Then $v' = v_j$ and $v - v' = v_j$, which implies that $v = v' + v - v' = 2v_j \in V_j$, a contradiction.
Thus $Q(V) \subseteq \bigcup_{j\in J} V_j$. Given that $V_j \cap V_k = \{0\}$ for $j \neq k$, we have that $v \in Q(V)\backslash\{0\}$ is contained in exactly one $V_j$.

Part 3: We show that each regular subspace, $V_j$ of $V$ is maximal.

Suppose that there exists a $j_0 \in J$ such that $V_{j_0}$ is not maximal. Let $X$ be a regular subspace of $V$ such that $V_{j_0} \subset X$. We have that $Q(V_{j_0}) \subset Q(X)$. Thus there exist $x \in Q(X)$ such that $x \notin Q(V_{j_0})$. By Lemma 2.1.22, we have that $Q(V_{j_0}) = V_{j_0} \cap Q(X)$. Thus $x \notin V_{j_0}$, which implies that $x \in Q(V) \cap (X\backslash V_{j_0})$. So $x \in V_j$ for some $j \in J\backslash\{j_0\}$, since $x \in Q(V)\backslash\{0\}$. Since $X$ is regular, $x$ $cp$ $w$ for each $w \in Q(V_{j_0})\backslash\{0\}$. This implies that $x \in V_{j_0}$, a contradiction since $j \neq j_0$ and $V_j \cap V_{j_0} = \{0\}$.
Hence, each regular subspace, $V_j$ of $V$ is maximal.

□

The proof of Theorem 2.3.3 can be summarised by the 3 steps below:

Step 1: We partition the non-zero quasi-kernel, $Q(V)\backslash\{0\}$ of $V$ into sets $Q_j$ $(j \in J)$ of mutually pairwise compatible vectors.

Step 2: We obtain a basis, $B \subseteq Q(V)\backslash\{0\}$ of $V$ and let $B_j := B \cap Q_j$.

Step 3: We determine the subspace, $V_j := \langle B_j \rangle$ of $V$ generated by the independent subset, $B_j$ of $Q(V)$. Then each $V_j$ is a maximal regular subspace of $V$ and $V$ is the direct sum of the $V_j's$.

The above three steps can be achieved by the algorithms below.

Given a suitable sequence $(S)$ as described in Definition 3.1.4, Algorithm 1 demonstrates the action of an endomorphism, say $\alpha \in \mathbb{Z}_p$, on an element of $\mathbb{Z}_p^n$ for $n \in \mathbb{N},\ n \geq 1$.

By an abuse of notation we also denote the tuple associated with the suitable sequence $(S)$ by $(S)$ and refer to the entries of the tuple as elements of $(S)$.

**Algorithm 1** $U(t, s, \alpha)$ : Action of $G$ on $V$ for a given near vector space $(V, G)$ of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$ where the endomorphisms $G$ are determined by a suitable sequence $s \in \mathbb{Z}^n$.

**Input:** $\alpha \in \mathbb{Z}_p$ representing an endomorphism of $V$ associated with the suitable sequence $(S) = (s_1, \ldots, s_n) \in \mathbb{Z}^n$ and $t = (t_1, \ldots, t_n) \in \mathbb{Z}_p^n$, where $p$ is a prime and $n \in \mathbb{N},\ n \geq 1$.
**Output:** $t\alpha = w = (w_1, \ldots, w_n)$.
1: **for** $i = 1, \ldots, n$ **do**
2: $\quad w_i = t_i \cdot \alpha^{s_i}$
3: **end for**
4: **return** $w = (w_1, \ldots, w_n)$

Given a near vector space over $\mathbb{Z}_p$, in order to obtain its quasi-kernel, Algorithm 2 shows how to generate possible $\alpha, \beta, \gamma$ mentioned in Definition 2.1.3$(e)$.
Given a suitable sequence $(S)$ with $u \in (S)$ and $f \in \mathbb{Z}_p$, the notation $f^u = \text{mod}(f^u, p) \in \mathbb{Z}_p$.

**Algorithm 2** $G(F, u)$: Set of endomorphisms, associated with an element $u$ of a suitable sequence, of the quasi-kernel of a near vector space of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$.

**Input:** $F = \mathbb{Z}_p$, $p$ a prime, $u \in (S)$, where $(S)$ is the suitable sequence that determines the action of endomorphisms $\mathbb{Z}_p$ on $\mathbb{Z}_p^n$.
**Output:** $\{(\alpha, \beta, \gamma) \in \mathbb{Z}_p^3 \mid v\alpha^u + v\beta^u = v\gamma^u \text{ for some } v \in \mathbb{Z}_p\}$.

$D = \emptyset$
$L = \mathbb{Z}_p^3$
**while** $L \neq \emptyset$ **do**
  **for** $h = (h_1, h_2, h_3) \in L$ **do**
    **if** $h_1^u + h_2^u = h_3^u$ **then**
      $D = D \cup \{h\}$
    **end if**
  **end for**
  $L = L \backslash \{h\}$
**end while**
**return** $D$

Now, Algorithm 3 illustrates how to obtain the quasi-kernel.

**Algorithm 3** $Q(p, n, s)$ : The quasi-kernel of a near vector space of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$.

**Input:** $s = (s_1, \ldots, s_n) \in \mathbb{Z}^n$ the suitable sequence that determines the action of endomorphisms $\mathbb{Z}_p$ on $\mathbb{Z}_p^n$ for $p$ a prime and $n \in \mathbb{N}$, $n \geq 1$.
**Output:** $\{v \in \mathbb{Z}_p^n \mid v\alpha + v\beta = v\gamma \text{ for some } (\alpha, \beta, \gamma) \in \mathbb{Z}_p^3\}$.

$H = \mathbb{Z}_p$
$Q^* = \emptyset$
$L = \mathbb{Z}_p^n$
**for** $t = 1, \ldots, n$ **do**
  **while** $L \neq \emptyset$ **do**
    **for** $k \in L$ **do**
      **if** $\forall\ (i, j, h) \in G(H, s_t),\ U(k, s, i) + U(k, s, j) = U(k, s, h)$ **then**
        $Q^* = Q^* \cup \{k\}$
      **end if**
    **end for**
    $L = L \backslash \{k\}$
  **end while**
**end for**
**return** $Q^*$

Algorithm 4 illustrates how to check when two non-zero elements of the quasi-kernel are compatible as given in Definition 2.1.15.

**Algorithm 4** Compatible$(Q, x, y, E)$: Checks for compatibility of two non-zero elements of the quasi-kernel of a near vector space of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$.

**Input:** $Q$ represents the quasi-kernel of a vector space of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$ with $x, y \in Q\backslash\{0\}$ and $E = \mathbb{Z}_p^* = \mathbb{Z}_p\backslash\{0\}$ for $p$ a prime.
**Output:** True if $x$ and $y$ are compatible and False if otherwise.

$L = \mathbb{Z}_p^*$
**while** $L \neq \emptyset$ **do**
  **for** $\lambda \in L$ **do**
    **if** $x + y\lambda \in Q$ **then**
      **return** true
    **end if**
  **end for**
  **return** false
  $L = L\backslash\{\lambda\}$
**end while**

Given the quasi-kernel, Algorithm 5 demonstrates how to generate all pairs of compatible vectors. Furthermore, Algorithm 6 illustrates how to partition the compatible vectors into equivalence classes.

**Algorithm 5** Compact-pairs$(Q, p, n)$: Pairs of compatible vectors of non-zero elements of the quasi-kernel of a near vector space of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$.

**Input:** The quasi-kernel $Q$ of a near vector space of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$ for $p$ a prime and $n \in \mathbb{N},\ n \geq 1$.
**Output:** $\{(u, v) \in (Q\backslash\{0\})^2 \mid u + v\lambda \in Q \text{ for some } \lambda \in \mathbb{Z}_p\backslash\{0\}\}$ .

$Q^* = Q\backslash\{0\}$
$F = \mathbb{Z}_p^* = \mathbb{Z}_p\backslash\{0\}$
$C = \emptyset$
$J = \{(a, b) \mid a, b \in Q^* \text{ and } (a, b) \in J \implies (b, a) \notin J\}$
**while** $J \neq \emptyset$ **do**
  **for** $u = (u_1, u_2) \in J$ **do**
    **while** $F \neq \emptyset$ **do**
      **for** $\lambda \in F$ **do**
        **if** $u_1 + u_2\lambda \in Q$ **then**
          $C = C \cup \{u\}$
        **end if**
      **end for**
      $F = F\backslash\{\lambda\}$
    **end while**
  **end for**
  $J = J\backslash\{u\}$
**end while**
**return** $C$

**Algorithm 6** $R(C)$: Partition of the non-zero quasi-kernel $Q\backslash\{0\}$, of a near vector space of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$, into equivalence classes.

**Input:** The set $C=\{(u,v) \in (Q\backslash\{0\})^2 \mid u + v\lambda \in Q$ for some $\lambda \in \mathbb{Z}_p\backslash\{0\}\}$ of compatible pairs of vectors.
**Output:** $\{[w] \subseteq Q\backslash\{0\} \mid \forall\ u, v \in [w], u + v\lambda \in Q$ for some $\lambda \in \mathbb{Z}_p\backslash\{0\}\}$.

$T = \emptyset$
**while** $C \neq \emptyset$ **do**
    **for** $p = (p_1, p_2) \in C$ **do**
        exist = false
        **while** $T \neq \emptyset$ **do**
            **for** $E \in T$ **do**
                **if** $p_1 \in E$ or $p_2 \in E$ **then**
                    $E = E \cup \{p_1, p_2\}$
                    exist = true
                    break
                **end if**
            **end for**
            $T = T\backslash\{E\}$
        **end while**
        **if** exist=false **then**
            $T = T \cup \{\{p_1, p_2\}\}$
        **end if**
    **end for**
    $C = C\backslash\{p\}$
**end while**
**return** $T$

Next, given a basis $B \subseteq Q(V)$ of the near vector space, Algorithm 7 highlights how to obtain the set of independent compatible vectors $B_j$.

**Algorithm 7** $D(A, n)$: Partition of a basis, which is a subset of the quasi-kernel $Q$, of a near vector space of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$ into mutually independent compatible vectors.

**Input:** A=$\{[w] \subseteq Q\backslash\{0\} \mid \forall u, v \in [w], u + v\lambda \in Q\}$ of equivalent classes of $Q\backslash\{0\}$ and $n \in \mathbb{N},\ n \geq 1$.
**Output:** $\{X \cap L \mid L \in A$ and $X$ a basis of the near vector space$\}$.

$B = \{e_i \mid 1 \leq i \leq n\}$ ▷ Standard ordered basis
$i = 0$
**while** $A \neq \emptyset$ **do**
    $i = i + 1$
    $F_i = \emptyset$
    **for** $L \in A$ **do**
        $F_i = B \cap L$
    **end for**
    $A = A\backslash\{L\}$
**end while**
**return** $F_1, \ldots, F_i$

Finally, one way of generating the maximal regular subspaces of the near vector space of finite dimension over $\mathbb{Z}_p$ is illustrated in Algorithm 8.

**Algorithm 8** $V(F, H)$: Maximal regular subspaces of a near vector space of the form $(\mathbb{Z}_p^n, \mathbb{Z}_p)$ generated by sets of mutually independent compatible vectors.

**Input:** $H = \mathbb{Z}_p$ for $p$ a prime and $F = \{C \mid C$ is a set of mutually independent compatible vectors$\}$.
**Output:** A set of sets of maximal regular subspaces.

1: $j = 0$
2: **while** $F \neq \emptyset$ **do**
3: $\quad j = j + 1$
4: $\quad M_j = \emptyset$
5: $\quad$ **for** $C \in F$ **do**
6: $\quad\quad M_j = \left\{ \sum_{i=1}^{|C|} u_i\alpha_i \mid u_i \in C \text{ and } \alpha_i \in H \right\}$
7: $\quad$ **end for**
8: $\quad F = F \backslash \{C\}$
9: **end while**
10: **return** $M_1, \ldots, M_j$

**2.3.4 Remark.** If $V$ is regular then it is its own decomposition.

Given a near vector space of finite dimension over $\mathbb{Z}_p$, we state an important consequence of the decomposition theorem.

**2.3.5 Theorem.** *((André, 1974), Theorem 4.14) The direct decomposition of a near vector space, $V$ into maximal regular near subspaces is unique.*

**2.3.6 Definition.** ((André, 1974), Definition 4.15) The uniquely determined direct decomposition of a near vector space $V$ into maximal regular subspaces is referred to as the canonical decomposition of $V$.

It is now clear why André referred to regular subspaces as the building blocks of near vector space theory.

# 3. Constructing finite dimensional near vector spaces using $\mathbb{Z}_p$, for $p$ a prime

## 3.1 van der Walt's Theorem

We begin with a result that will be central in our study.

**3.1.1 Theorem.** ***(van der Walt's Theorem)*** *((van der Walt, 1992), Theorem 3.4-2) Let $(V,+)$ be a group and let $G = C \cup \{0\}$, where $C$ is a fixed point free (fpf) group of automorphism of $V$. Then $(V,G)$ is a near vector space of finite dimension if and only if there exist a finite number of near fields $H_1,\ldots,H_n$, semigroup isomorphisms $\phi_i : (G,\circ) \to (H_i,\cdot)$ and an additive group isomorphism $\psi : V \to H_1 \oplus \cdots \oplus H_n$ such that if $\psi(v) = (v_1, v_2, \ldots, v_n)$, then $\psi(v\lambda) = (v_1\phi_1(\lambda), \ldots, v_n\phi_n(\lambda))$ for all $v \in V, \lambda \in G$.*

Since every field is a near field, suppose we take $H_i = \mathbb{Z}_p$, $i \in \{1,2,\ldots,n\}$, $p$ a prime and put $(V,G) = ((\mathbb{Z}_p)^n, \mathbb{Z}_p)$ for some $n \in \mathbb{N}$, $n \geq 1$. Now, we let $\phi_i : (\mathbb{Z}_p,\cdot) \to (\mathbb{Z}_p,\cdot)$, $i \in \{1,2,\ldots,n\}$ be semigroup automorphisms and define scalar multiplication on $V$ by

$$(v_1, v_2, \ldots, v_n)\lambda = (v_1\phi_1(\lambda), v_2\phi_2(\lambda), \ldots, v_n\phi_n(\lambda))$$

for $(v_1, v_2, \ldots, v_n) \in V$, $\lambda \in \mathbb{Z}_p$. Then by Theorem 3.1.1, $(V,G) = ((\mathbb{Z}_p)^n, \mathbb{Z}_p)$ is a near vector space of dimension $n$.

Thus to construct such near vector spaces using $\mathbb{Z}_p$, we need to find the multiplicative semigroup automorphisms of $(\mathbb{Z}_p,\cdot)$.
We will first state some definitions and results. We write $\mathbb{Z}_p^*$ for $\mathbb{Z}_p \backslash \{0\}$.

The following is a well-known result in number theory.

**3.1.2 Lemma.** 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* $\gcd(q, p-1) = 1$ (for $p$ a prime).

**3.1.3 Lemma.** ((Howell et al., 2019), Lemma 5.2) The mapping $\phi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ is an automorphism group of $(\mathbb{Z}_p^*,\cdot)$ *if and only if* $\forall\ a \in \mathbb{Z}_p^*$, $\exists$ a $q \in \mathbb{Z}$, with $1 \leq q < p-1$ and $\gcd(q, p-1) = 1$, such that $\phi(a) = a^q$.

*Proof.* Let $\phi$ be a mapping from the cyclic group $(\mathbb{Z}_p^*,\cdot)$ to itself. Let $\lambda \in \mathbb{Z}_p^*$ be a generator. Then $\mathbb{Z}_p^* = \langle\lambda\rangle = \{\lambda^i \mid 1 \leq i \leq p-1\}$ and $\lambda^l$ is also a generator for $1 \leq l < p-1$ and $\gcd(l, p-1) = 1$.

" $\Rightarrow$ " Suppose that $\phi$ is an automorphism. Then for all $a \in \mathbb{Z}_p^*$ we seek a $q \in \mathbb{Z}$, with $1 \leq q < p-1$ and $\gcd(q, p-1) = 1$, such that $\phi(a) = a^q$ .

Let $\phi(\lambda) = \lambda^k$, for some $k$, $1 \leq k < p-1$. Then $\phi(\lambda^l) = \lambda^{lk}, 1 \leq l \leq p-1$. Given that $\phi$ is a bijection on $\mathbb{Z}_p^*$, we have $\{\lambda^l \mid 1 \leq l \leq p-1\} = \mathbb{Z}_p^* = \{\lambda^{lk} \mid 1 \leq l \leq p-1, 1 \leq k < p-1\}$. Thus every member of $\mathbb{Z}_p^*$ has a $k$th root. Therefore, by Lemma 3.1.2, $\gcd(k, p-1) = 1$. Hence, we take $q = k$.

" $\Leftarrow$ " Suppose that for all $a \in \mathbb{Z}_p^*$ there exists $q \in \mathbb{Z}$, with $1 \leq q < p-1$ and $\gcd(q, p-1) = 1$, such that $\phi(a) = a^q$ . We show that $\phi$ is an automorphism.

**Well-definedness**
Let $a, b \in \mathbb{Z}_p^*$ with $a = b$. Then $\phi(a) = a^q = b^q = \phi(b)$.

**Injectivity**
Let $a, b \in \mathbb{Z}_p^*$, such that $\phi(a) = \phi(b)$. Then $a = \lambda^{k_1}, b = \lambda^{k_2}$ for some $1 \leq k_1, k_2 \leq p-1$. Therefore, $\phi(a) = \phi(b)$ implies that $\lambda^{qk_1} = a^q = b^q = \lambda^{qk_2}$. Suppose $k_1 \neq k_2$, wlog let $k_2 > k_1$. Then $\lambda^{qk_1} = \lambda^{qk_2} \implies \lambda^{q(k_2-k_1)} = 1 \implies p-1 \mid q(k_2-k_1)$. But with $1 \leq q < p-1$, we have $p-1 \mid (k_2-k_1)$, which is a contradiction since $k_1, k_2 \leq p-1$ and $k_2 > k_1$. Thus $k_1 = k_2$, which implies that $a = b$.

**Surjectivity**
Let $b \in \mathbb{Z}_p^*$. Then there exists $1 \leq l_1 \leq p-1$ such that $b = (\lambda^q)^{l_1}$. Take $a = \lambda^{l_1} \in \mathbb{Z}_p^*$. Then $\phi(a) = \phi(\lambda^{l_1}) = \lambda^{ql_1} = b$.

**Homomorphism**
Let $a, b \in \mathbb{Z}_p^*$. We have $\phi(ab) = (ab)^q = a^q b^q = \phi(a)\phi(b)$.

Thus we have the form of automorphisms of $(\mathbb{Z}_p^*, \cdot)$. □

We can now use suitable sequences as a tool to construct finite dimensional near vector spaces over $\mathbb{Z}_p$.

**3.1.4 Definition.** ((Howell and Meyer, 2014), Definition 2.3) A finite non-decreasing sequence of $n$ integers $x_1, x_2, \ldots, x_n$ is said to be suitable with respect to $\mathbb{Z}_p$, $p$ a prime, written as $(S) = (x_1, x_2, \ldots, x_n)$ if $1 \leq x_i \leq p-1$ and $\gcd(x_i, p-1) = 1$ for all $i = 1, 2, \ldots, n$.

We now describe the procedure for generating a suitable sequence of length $n$ with respect to $\mathbb{Z}_p$. We begin by generating the multiplicative group $U(p-1) = \{k \in \mathbb{Z} \mid 1 \leq k \leq p-1$ and $\gcd(k, p-1) = 1\}$.

Next we obtain the subgroup of $U(p-1)$ generated by $\langle p \rangle$.

Then we obtain the cosets determined by the subgroup $\langle p \rangle$.

Make a list of the least members of each of the cosets.

Finally, we choose $n$ elements in non-decreasing order from the list possibly with repetition.

Algorithm 9 below illustrates the approach to obtaining a suitable sequence described in Definition 3.1.4.

**Algorithm 9** $S(p, n)$ : Suitable sequences with respect to $\mathbb{Z}_p$.

**Input:** $p$ a prime and $n \in \mathbb{N},\ n \geq 1$.
**Output:** $\{(v_1, \ldots, v_n) \in (\mathbb{Z}^+)^n \mid v_i \leq v_{i+1}$ for $i = 1, \ldots, n-1\}$.

```
U = Φ(p − 1)                                   ▷ Euler totient function
Q = {mod (p^m, p − 1) | m ∈ [0, p − 1]}
C = ∅
for j = 1, ..., |U| do
    while Q ≠ ∅ do
        for i ∈ Q do
            C = C ∪ {U[j] · i}
        end for
        Q = Q\{i}
    end while
end for
L = {(c_k)_{k=1}^n ∈ C^n | c_t ≤ c_{t+1} for t = 1, ..., n − 1}
return L
```

**3.1.5 Example.** Let us consider the finite field $\mathbb{Z}_{11}$. We obtain the multiplicative group, $U(10) = \{k \in \mathbb{Z} \mid 1 \leq k \leq 10 \text{ and } \gcd(k, 10) = 1\} = \{1, 3, 7, 9\}$.

We obtain the subgroup, $\langle 11 \rangle$ of $U(10)$. Thus $\langle 11 \rangle = \{11^i \pmod{10} \mid 1 \leq i \leq 10\} = \{1\}$.

Generating all cosets determined by $\langle 11 \rangle$, we have $1\langle 11 \rangle = \{1\},\ 3\langle 11 \rangle = \{3\},\ 7\langle 11 \rangle = \{7\},\ 9\langle 11 \rangle = \{9\}$.

Collecting the smallest element of each coset, we obtain the set $\{1, 3, 7, 9\}$.

We choose a suitable sequence of five integers, say $(S) = (3, 3, 7, 7, 7)$.

## 3.2 Regularity and decomposition

**3.2.1 Theorem.** *((Howell and Meyer, 2014), Theorem 2.2) Let $G = \mathbb{Z}_p$, $l_1, l_2 \in \{1, 2, \ldots, p-1\}$ with $\gcd(l_i, p-1) = 1$ $(i = 1, 2)$ and $l_1 < l_2$. Then $(x^{l_1} + y^{l_1})^{l_2} = (x^{l_2} + y^{l_2})^{l_1}$ for all $x, y \in \mathbb{Z}_p$ if and only if $l_1 \equiv l_2$ $(mod\ p-1)$.*

This result will aid us in the proof of the lemma below. It allows to determine when the near vector spaces we have constructed are regular.

**3.2.2 Lemma.** ((Howell et al., 2019), Lemma 5.8) Let $(V, G) = (\mathbb{Z}_p^n, \mathbb{Z}_p)$ be a near vector space with scalar multiplication defined as

$$(v_1, v_2, \ldots, v_n)\alpha := (v_1\phi_1(\alpha), v_2\phi_2(\alpha), \ldots, v_n\phi_n(\alpha)),$$

where $n \in \mathbb{N},\ n \geq 1,\ p$ a prime, $(v_1, \ldots, v_n) \in V$ and the $\phi_j$ $(j \in J = \{1, 2, \ldots, n\})$ are cyclic automorphism group of $(\mathbb{Z}_p^*, \cdot)$. Then $V$ is regular *if and only if* for all $i, j \in J$ and $\lambda \in G$, $\phi_i(\lambda) = \phi_j(\lambda)$.

*Proof.* " $\Leftarrow$ " Suppose that $\forall\ i, j \in J$ and $\alpha \in \mathbb{Z}$, $\phi_i(\alpha) = \phi_j(\alpha)$.
To show that $V$ is regular, by Theorem 2.1.26, it suffices to find a basis comprising of mutually pairwise compatible vectors.
Let us consider the standard basis, $B = \{e_j \mid \forall\, j \in \{1, 2, \ldots, n\}, e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in the $j$th position$\}$
We show that $B \subseteq Q(V)$. Let $e_j \in B$ and let $\alpha, \beta \in \mathbb{Z}_p$.

$$\begin{aligned} e_j\alpha + e_j\beta &= (0, \ldots, 0, 1, 0, \ldots, 0)\alpha + (0, \ldots, 0, 1, 0, \ldots, 0)\beta \\ &= (0, \ldots, 0, \phi_j(\alpha), 0, \ldots, 0) + (0, \ldots, 0, \phi_j(\beta), 0, \ldots, 0) \\ &= (0, \ldots, 0, \phi_j(\alpha) + \phi_j(\beta), 0, \ldots, 0) \\ &= (0, \ldots, 0, 1, 0, \ldots, 0)\phi_j^{-1}(\phi_j(\alpha) + \phi_j(\beta)) \\ &= (0, \ldots, 0, 1, 0, \ldots, 0)\gamma, \end{aligned}$$

with $\gamma = \phi_j^{-1}(\phi_j(\alpha) + \phi_j(\beta)) \in \mathbb{Z}_p$. Thus $B \subseteq Q(V)$. To show that $B \subseteq Q(V)$ comprises of mutually pairwise compatible vectors, by Theorem 2.1.19, it suffices to show that $e_i + e_j \in Q \backslash \{0\}$ for each

$e_i, e_j \in B$. Let $\alpha, \beta \in \mathbb{Z}_p$.

$$\begin{aligned}(e_i+e_j)\alpha+(e_i+e_j)\beta &= (0,\dots,1,0,\dots,1,0,\dots,0)\alpha+(0,\dots,1,0,\dots,1,0,\dots,0)\beta\\ &= (0,\dots,\phi_i(\alpha),0,\dots,\phi_j(\alpha),0,\dots,0)+(0,\dots,\phi_i(\beta),0,\dots,\phi_j(\beta),0,\dots,0)\\ &= (0,\dots,\phi_i(\alpha)+\phi_i(\beta),0,\dots,\phi_j(\alpha)+\phi_j(\beta),0,\dots,0)\\ &= (0,\dots,\phi_i(\alpha)+\phi_i(\beta),0,\dots,\phi_i(\alpha)+\phi_i(\beta),0,\dots,0)\\ &= (0,\dots,1,0,\dots,1,0,\dots,0)\phi_i^{-1}(\phi_i(\alpha)+\phi_i(\beta))\\ &= (e_i+e_j)\gamma,\end{aligned}$$

with $\gamma = \phi_i^{-1}(\phi_i(\alpha)+\phi_i(\beta)) \in \mathbb{Z}_p$. Thus $e_i+e_j \in Q\backslash\{0\}$. Hence, $B \subseteq Q(V)$ comprises of mutually pairwise compatible vectors. Since $B$ is a basis of $V$, $V$ is regular.

" $\Rightarrow$ " Now we suppose that $V$ is regular. Let $i, j \in J$ and $\alpha \in \mathbb{Z}_p$. We show that $\phi_i(\alpha) = \phi_j(\alpha)$. Given that each $\phi_j$ $(j \in J = \{1,2,\dots,n\})$ is an automorphism of the cyclic group $(\mathbb{Z}_p^*, \cdot)$ by Lemma 3.1.3, for all $a \in \mathbb{Z}_p$, $\phi_i(a) = a^{l_i}$ with $1 \leq l_i < p-1$ and $\gcd(l_i, p-1) = 1$. Then the scalar multiplication becomes

$$(a_1, a_2, \dots, a_n)\alpha = (a_1\alpha^{l_1}, a_2\alpha^{l_2}, \dots, a_n\alpha^{l_n}).$$

Given that $B \subseteq Q(V)$ comprises of mutually pairwise compatible vectors then by theorem 2.1.26, each $e_i, e_j \in B$, $\exists$ a $\lambda \in \mathbb{Z}_p^*$ such that $e_i + e_j\lambda \in Q$. Then by Definition 2.1.3 $-$ $(e)$, $\forall\ \alpha, \beta \in \mathbb{Z}_p$, $\exists$ a $\gamma \in \mathbb{Z}_p$ such that $(e_i+e_j\lambda)\alpha+(e_i+e_j\lambda)\beta = (e_i+e_j\lambda)\gamma$. Simplifying the last equation we have

$$\begin{aligned}(e_i+e_j\lambda)\alpha+(e_i+e_j\lambda)\beta &= (e_i+e_j\lambda)\gamma\\ (0,\dots,1,0,\dots,\lambda^{l_j},0,\dots,0)\alpha+(0,\dots,1,0,\dots,\lambda^{l_j},0,\dots,0)\beta &= (0,\dots,1,0,\dots,\lambda^{l_j},0,\dots,0)\gamma\\ (0,\dots,\alpha^{l_i},0,\dots,\lambda^{l_j}\alpha^{l_j},0,\dots,0)+(0,\dots,\beta^{l_i},0,\dots,\lambda^{l_j}\beta^{l_j},0,\dots,0) &= (0,\dots,\gamma^{l_i},0,\dots,\lambda^{l_j}\gamma^{l_j},0,\dots,0)\\ (0,\dots,\alpha^{l_i}+\beta^{l_i},0,\dots,\lambda^{l_j}(\alpha^{l_j}+\beta^{l_j}),0,\dots,0) &= (0,\dots,\gamma^{l_i},0,\dots,\lambda^{l_j}\gamma^{l_j},0,\dots,0),\end{aligned}$$

which implies that $\alpha^{l_i}+\beta^{l_i} = \gamma^{l_i}$ and $\alpha^{l_j}+\beta^{l_j} = \gamma^{l_j}$ for all $i, j \in \{1,2,\dots,n\}$. Thus for all $i, j \in \{1,2,\dots,n\}$, $(\alpha^{l_i}+\beta^{l_i})^{l_j} = (\alpha^{l_j}+\beta^{l_j})^{l_i}$. By Theorem 3.2.1, $l_i \equiv l_j \pmod{p-1}$. Thus for all $\alpha \in \mathbb{Z}_p$, $\phi_i(\alpha) = \alpha^{l_i} = \alpha^{l_j} = \phi_j(\alpha)$. □

Next we look at how Lemma 3.2.2 can be used in conjunction with the Decomposition Theorem to find the canonical direct decomposition of the near vector spaces we have constructed.

Let $(V, G) = (\mathbb{Z}_p^n, \mathbb{Z}_p)$ be a near vector space, for some $n \in \mathbb{N}$, $n > 1$ and $p$ a prime.
Let $\bigcup_{k=1}^{m} A_k$ be a partition of the set $J = \{1,2,\dots,n\}$ such that

$$A_k := \{j \in J \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_j(\alpha) = \phi_k(\alpha)\}. \tag{3.2.1}$$

Then we have that the $A_k$ are nonempty and mutually disjoint for $k \in \{1,2,\dots,m\}$.

**3.2.3 Lemma.** ((Howell et al., 2019), Lemma 5.11)

In the case of the near vector space defined above we have that:

$(a)$ The quasi-kernel, $Q(V) = \bigcup_{k=1}^{m} \mathcal{V}_k$
where $\mathcal{V}_k = \{(a_1, 0, \dots, 0, a_i, 0, \dots, 0) \mid a_i \in \mathbb{Z}_p \text{ is in position } i \text{ with } i \in A_k, \text{ for } k \in \{1,\dots,m\}\}$.

$(b)$ $\mathcal{V}_k$ is a regular subspace of $V$ for $k = 1, \ldots, m$.

$(c)$ $V = \oplus_{k=1}^{m} \mathcal{V}_k$ is the canonical decomposition of $V$.

**3.2.4 Example.** Let $(V, G) = ((\mathbb{Z}_{11})^5, \mathbb{Z}_{11})$ be a near vector space and let $\alpha \in G$ be an endomorphism on $V$ defined as

$$(v_1, v_2, v_3, v_4, v_5)\alpha := (v_1\alpha^3, v_2\alpha^3, v_3\alpha^7, v_4\alpha^7, v_5\alpha^7)$$

for all $(v_1, v_2, v_3, v_4, v_5) \in V$.

We obtain the set $A_j := \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \phi_j(\alpha)\}$ for $j \in J = \{1, 2, 3, 4, 5\}$.

$$\begin{aligned} A_1 &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \phi_1(\alpha)\} \\ &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \alpha^3\} \\ &= \{1, 2\} \end{aligned}$$

$$\begin{aligned} A_2 &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \phi_2(\alpha)\} \\ &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \alpha^3\} \\ &= \{1, 2\} \end{aligned}$$

$$\begin{aligned} A_3 &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \phi_3(\alpha)\} \\ &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \alpha^7\} \\ &= \{3, 4, 5\} \end{aligned}$$

$$\begin{aligned} A_4 &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \phi_4(\alpha)\} \\ &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \alpha^7\} \\ &= \{3, 4, 5\} \end{aligned}$$

$$\begin{aligned} A_5 &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \phi_5(\alpha)\} \\ &= \{i \in I \mid \forall\ \alpha \in \mathbb{Z}_p, \phi_i(\alpha) = \alpha^7\} \\ &= \{3, 4, 5\}. \end{aligned}$$

We have that $A_1 = A_2$ and $A_3 = A_4 = A_5$. Thus $A_1 \cup A_3$ is a partition of $J = \{1, 2, 3, 4, 5\}$, where $A_1$ and $A_3$ mutually disjoint and nonempty.

Next we determine $\mathcal{V}_k$ for $k = 1, 3$.

$$\begin{aligned} V_1 &= \{\{(a_1, 0, \ldots, 0, a_i, 0, \ldots, 0) \mid a_i \in \mathbb{Z}_p \text{ is in position } i \text{ with } i \in A_1\} \\ &= \{(a_1, a_2, 0, 0, 0) \mid a_1, a_2 \in \mathbb{Z}_p\} \end{aligned}$$

$$\begin{aligned} V_3 &= \{\{(a_1, 0, \ldots, 0, a_i, 0, \ldots, 0) \mid a_i \in \mathbb{Z}_p \text{ is in position } i \text{ with } i \in A_3\} \\ &= \{(0, 0, a_3, a_4, a_5) \mid a_3, a_4, a_5 \in \mathbb{Z}_p\}. \end{aligned}$$

Then by Lemma 3.2.3, $Q(V) = V_1 \cup V_3$, $V_1$ and $V_3$ are regular subspaces of $V$, and $V = V_1 \oplus V_3$ is the canonical direct decomposition of $V$.

**3.2.5 Theorem.** *((Howell, 2018), Theorem 4.5) Let $(V, G) = (\mathbb{Z}_p^n, \mathbb{Z}_p)$ be a near vector space with scalar multiplication defined for all $\alpha \in \mathbb{Z}_p$ by*

$$(v_1, \ldots, v_n)\alpha := (v_1\phi_1(\alpha), \ldots, v_n\phi_n(\alpha)),$$

*where $n \in \mathbb{N},\ n \geq 1,\ p$ a prime, $(v_1, \ldots, v_n) \in V$ and the $\phi_i$ $(i = 1, 2, \ldots, n)$ are automorphisms of $(\mathbb{Z}_p, \cdot)$. Then the following are equivalent*

$(a)$ *$Q(V) = V$;*

$(b)$ *$V$ is regular;*

$(c)$ *$\forall\ i, j \in J = \{1, \ldots, n\}$ and $\lambda \in \mathbb{Z}_p,\ \phi_i(\lambda) = \phi_j(\lambda)$.*

*Proof.* $(a) \Rightarrow (b)$ Suppose that $Q(V) = V$. Let $u, v \in Q(V)\backslash\{0\} \subseteq V$, and let $\lambda \in G^*$. Since $\lambda$ is an endomorphism on $V,\ v\lambda \in V$. Then $u + v\lambda \in V$ since $(V, +)$ is a group. Thus $u + v\lambda \in Q(V)$, and $u\ cp\ v$ by Definition 2.1.15. Therefore, by Definition 2.1.24, $V$ is regular.

$(b) \Rightarrow (c)$ We suppose that $V$ is regular. Then by Lemma 3.2.2, $\forall\ i, j \in J = \{1, \ldots, n\}$ and $\lambda \in \mathbb{Z}_p,\ \phi_i(\lambda) = \phi_j(\lambda)$.

$(c) \Rightarrow (a)$ Suppose that $\forall\ i, j \in J = \{1, \ldots, n\}$ and $\alpha \in \mathbb{Z}_p,\ \phi_i(\alpha) = \phi_j(\alpha)$. Then by Equation 3.2.1, the set $I = \{1, 2, \ldots, n\}$ cannot be partitioned, thus $A_1 = I$. By Lemma 3.2.3$(a)$, $Q(V) = \mathcal{V}$ where $\mathcal{V} = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{Z}_p\}$. We have that $V = \mathcal{V}$ by Lemma 3.2.3$(c)$. Thus $Q(V) = V$. □

**3.2.6 Theorem.** *((Howell, 2018), Theorem 4.6) Let $(V, G) = (\mathbb{Z}_p^n, \mathbb{Z}_p)$ be a near vector space with scalar multiplication defined for all $\alpha \in \mathbb{Z}_p$ by*

$$(v_1, \ldots, v_n)\alpha := (v_1\phi_1(\alpha), \ldots, v_n\phi_n(\alpha)),$$

*where $n \in \mathbb{N},\ n \geq 1,\ p$ a prime, $(v_1, \ldots, v_n) \in V$ and the $\phi_j$ $(j = 1, 2, \ldots, n)$ are automorphisms of $(\mathbb{Z}_p, \cdot)$. If $Q(V) \neq V$ and $V = V_1 \oplus \cdots \oplus V_m$ is the canonical direct decomposition of $V$, then $Q(V) = Q_1 \cup \cdots \cup Q_m$ where $Q_k = V_k$ for each $k \in \{1, \ldots, m\}$.*

*Proof.* Suppose that $Q(V) \neq V$ and $V = V_1 \oplus \cdots \oplus V_m$ is the canonical direct decomposition of $V$. Then by Lemma 3.2.3$(a)$,

$$Q(V) = \bigcup_{k=1}^{m} \mathcal{V}_k,$$

where $\mathcal{V}_k = \{(a_1, 0, \ldots, 0, a_i, 0, \ldots, 0) \mid a_i \in \mathbb{Z}_p$ is in position $i$ with $i \in A_k,$ for $k \in \{1, \ldots, m\}\}$.
We observe that the defintion given above partitions $Q(V)\backslash\{0\}$ into sets, $\mathcal{V}_1 = \mathcal{V}_1\backslash\{0\}, \ldots, \mathcal{V}_m = \mathcal{V}_m\backslash\{0\}$ of mutually compatible vectors.
Let $B \subset Q(V)$ be the canonical basis of $V$, and let $B_k := B \cap \mathcal{V}_k$ for $k \in \{1, \ldots, m\}$. We consider $V_k := \langle B_k \rangle$ which comprises of linear combinations of elements of $B_k$, and thus generates elements of the form $\mathcal{V}_k$. So we have that $\mathcal{V}_k = V_k$ for each $k \in \{1, \ldots, m\}$. Hence, we set $Q_k = \mathcal{V}_k$ for each $k \in \{1, \ldots, m\}$. □

**3.2.7 Theorem.** *((Rodtes and Chomjun, 2017), Theorem 3.2) Let $(V_1, G_1) = (\mathbb{Z}_p^n, \mathbb{Z}_p)$ and $(V_2, G_2) = (\mathbb{Z}_p^n, \mathbb{Z}_p)$ be near vector spaces, where the actions of $G_1$ and $G_2$ on $\mathbb{Z}_p^n$ are determined by some suitable sequences, say $(S_1)$ and $(S_2)$ respectively, for $p$ a prime and $n \in \mathbb{N},\ n \geq 1$. Then $(V_1, G_1) \cong (V_2, G_2)$ if and only if there is a $q \in S_1$ such that $S_1 = qS_2$ and for each $j = 1, \ldots, N$, where $N = |S_1| = |S_2|$, the occurrences of $qq'_j \in (S_1)$ and $q'_j \in (S_2)$ are the same.*

**3.2.8 Example.** Let $(V_1, G_1) = ((\mathbb{Z}_{11})^5, \mathbb{Z}_{11})$ be a near vector space and let $\eta \in G_1$ be an endomorphism on $V_1$ defined as

$$(x_1, x_2, x_3, x_4, x_5)\eta := (x_1\eta^3, x_2\eta^3, x_3\eta^9, x_4\eta^9, x_5\eta^9),$$

for $(x_1, x_2, x_3, x_4, x_5) \in V$.

It can be seen that the action of $G_1$ on $V_1$ is determined by the suitable sequence, say $(S_1) = (3, 3, 9, 9, 9)$ (see Example 3.1.5).

Let $(V_2, G_2) = ((\mathbb{Z}_{11})^5, \mathbb{Z}_{11})$ be a near vector space and let $\tau \in G_2$ be an endomorphism on $V_2$ defined as

$$(y_1, y_2, y_3, y_4, y_5)\tau := (y_1\tau, y_2\tau, y_3\tau^3, y_4\tau^3, y_5\tau^3).$$

It can be seen that the action of $G_2$ on $V_2$ is determined by the suitable sequence, say $(S_2) = (1, 1, 3, 3, 3)$ (see Example 3.1.5).

Let $N = |S_1| = |S_2| = 5$. We choose $q = 3 \in S_2$. We have that $S_1 = qS_2$. We observe that the number of occurrences of $q'_j \in (S_2)$ is the same as that of $qq'_j \in (S_1)$ for each $j = 1, \ldots, N$. Then by Theorem 3.2.7, $(V_1, G_1) \cong (V_2, G_2)$.

# 4. Conclusion

The main aim of this study was to discuss the construction and decomposition of finite-dimensional near vector spaces constructed using copies of $\mathbb{Z}_p$ for $p$ a prime.

We studied the notion of suitable sequences with respect to $\mathbb{Z}_p$ for $p$ a prime and used these in conjunction with van der Walt's result to show how to construct near vector spaces using copies of $\mathbb{Z}_p$ for $p$ a prime. We then studied the quasi-kernel of these near vector spaces and how they decompose according to André's Decomposition Theorem.

We used the result by Rodtes and Chomjun to check when two finite-dimensional near vector spaces constructed over $\mathbb{Z}_p$ for $p$ a prime are isomorphic.

Finally, we gave algorithms for the generation of suitable sequences and the decomposition of the near vector spaces we studied.

# Acknowledgements

I want to appreciate God almighty for His faithfulness, love and grace in my life especially during the course of my stay at AIMS.

My heartfelt gratitude goes to my supervisor, Dr Karin-Therese Howell for her time, dedication, meticulous care and advice from the beginning to the completion of this work. I would like to extend my gratitude to my co-supervisors, Dr Janko Böhm and Dr Magdaleen Marais for their guidance and assistance through out the course of this essay.

My profound gratitude goes to Prof Neil Turok, Prof Barry Green, Prof Jeff Sanders and the entire AIMS family. Special thanks to Dr Kenneth Dadedzi for his advice, encouragement and support.

My immeasurable appreciation goes to my beloved dad, Mr Ogu Emeka, my siblings, uncles and aunts for their love, support and encouragement. Many thanks to a friend turned brother, my mentor, Dr Chimere Anabanti for his guidance and encouragement.

# References


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

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

Dorfling, S., Howell, K.-T., and Sanon, S. The decomposition of finite-dimensional near-vector spaces. *Communications in Algebra*, 46(7):3033–3046, 2018.

Howell, K.-T. *Contributions to the theory of near vector spaces*. PhD thesis, University of the Free State, 2007.

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

Howell, K.-T. Near-vector spaces determined by finite fields and their fibrations. Submitted, 2018.

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

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

Howell, K.-T. and Sanon, S. P. On spanning sets and generators of near-vector spaces. *Turkish Journal of Mathematics*, 42(6):3232–3241, 2018.

Howell, K.-T., Chistyakov, D., and Sanon, S. On representation theory and near-vector spaces. *Linear and Multilinear Algebra*, 67(7):1495–1510, 2019.

Karzel, H. Fastvektorräume, unvollständige fastkörper und ihre abgeleiteten geometrischen strukturen. *Mitt. Math. Sem. Giessen*, 166:127–139, 1984.

Rodtes, K. and Chomjun, W. On the number of near-vector spaces determined by finite fields. *Journal of Algebra*, 492:90–101, 2017.

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