Scientific Research Publishing

Advances in Pure Mathematics, 2023, 13, 11-33
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

Near-Vector Spaces Constructed over $\mathbb{Z}_p$, for p a Prime

Kelone Tefoetsile[1*], Jeromy Kalunga[2*], Mathews Zimba[2], James Muchinga[3], Saviour Chibeti[4], Henry M. Phiri[4]

[1]Department of Mathematics and Statistical Sciences, Bostwana International University of Science and Technology, Palaype, Botswana
[2]Department of Mathematics, Copperbelt University, Kitwe, Zambia
[3]Departrment of Natural Science, Levy Mwanawasa Medical University, Lusaka, Zambia
[4]Economics Department, University of Lusaka, Lusaka, Zambia
Email: kelone.tefoetsile@gmail.com, jeromy.kalunga@cbu.ac.zm, jeromy@aims.ac.za

How to cite this paper: Tefoetsile, K., Kalunga, J., Zimba, M., Muchinga, J., Chibeti, S. and Phiri, H.M. (2023) Near-Vector Spaces Constructed over $\mathbb{Z}_p$, for p a Prime. *Advances in Pure Mathematics*, **13**, 11-33.
https://doi.org/10.4236/apm.2023.131002

Received: November 9, 2022
Accepted: January 25, 2023
Published: January 28, 2023

Abstract

The purpose of this paper is to construct near-vector spaces using a result by Van der Walt, with $\mathbb{Z}_p$ for p a prime, as the underlying near-field. There are two notions of near-vector spaces, we focus on those studied by André [1]. These near-vector spaces have recently proven to be very useful in finite linear games. We will discuss the construction and properties, give examples of these near-vector spaces and give its application in finite linear games.

Keywords

Vector Spaces, Near Vector Spaces, Regularity, Compatibility, Fields, Near-Fields, F-Group and Quasi-Kernel

1. Introduction

In the early 20th century, the American mathematician Leonard Eugene Dickson wondered what structure would arise if one axiom in the list of axioms of a division ring was removed. Dickson discovered that there are near-fields which fulfill all axioms of a division ring except one distributive law. In this essay we will be using right near-fields.

Near-vector spaces are less linear than traditional vector spaces. The ones we are interested in were first introduced by André in the paper [1]. There are a few different notions of near-vector spaces, those studied by André, Beidleman [2] and Karzel [3]. André used right near-fields to study near-vector spaces. It was later shown by van der Walt, that an arbitrary finite-dimensional near-vector

*Co-first author.

space can be constructed using a finite number of near-fields [1]. This construction has been used in order to characterize all finite-dimensional near-vector spaces by taking copies of $\mathbb{Z}_p$, for p a prime [4].

In this paper we discuss near-vector spaces constructed over $\mathbb{Z}_p$ in terms of their quasi-kernels and regularity. Regularity is a central notion in the study of near-vector spaces. In [1] the Decomposition Theorem states that every near-vector space can be written as a direct sum of maximal regular subspaces. Thus regular subspaces are considered the building blocks for near-vector spaces. The importance of the Decomposition Theorem is in the decomposition of complex structures into small, simpler structures which are convenient to work with.

André's near-vector spaces have various applications in Finite Linear Games and Cryptography to mention a few.

This paper is organized in three chapters. In Chapter 2 we give basic definitions and examples which lead to the concept of a near-vector space. In Chapter 3 we show how near-vector spaces are constructed over $\mathbb{Z}_p$ using a result by van der Walt. We determine the quasi-kernels $Q(V)$ of our near-vector spaces and decompose them into maximal regular subspaces using the Decomposition Theorem. We give necessary conditions needed to show when two near-vector spaces are isomorphic (Lemma 3.8). This is something new that has not been provided in any literature before. We observed that if (V,F) is a near-vector space of dimension n, *i.e.* $V=F^n$, then the number of Q_i's in the Decomposition Theorem is less or equal to n (Lemma 3.11). A proof was provided. In Chapter 4 we look at an application of near-vector spaces over $\mathbb{Z}_p$ to finite linear games and consider some examples.

2. Preliminary Material and Examples

This chapter focuses on the fundamentals of near-vector spaces.

2.1. Basic Definitions

Recall the following definitions.

Definition 2.1. [5] A set V is said to be a right vector space over a division ring F, if $(V,+)$ is an abelian group and, if for each $\alpha\in F$ and $v\in V$, there is a unique element $v\alpha\in V$ such that the following conditions hold for all $\alpha,\beta\in F$ and all $u,v\in V$:

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

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

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

d) $v1=v$.

The elements of V are called vectors, whereas elements of F are called scalars. And the operation that acts on (or combines) a scalar α and a vector v to form the vector $v\alpha$ is called *scalar multiplication*.

Remark 2.2.

a) A vector space V is said to be closed under both operations, by this we mean:

i) Closed under addition: If $u,v\in V$ then $u+v\in V$.

ii) Closed under multiplication: If $u\in V,\alpha\in F$ then $u\alpha\in V$.

b) A division ring F can be regarded as a set of endomorphisms of V by defining $f_\alpha(u):=u\alpha$ for all $u\in V$ and $\alpha\in F$.

c) If (V,F) is a vector space, then for every $\alpha,\beta\in F$ and for each $u\in V$, there exists $\gamma\in F$ such that $u\alpha+u\beta=u\gamma$.

d) If the scalars are *real*, then V is called a *real vector space* while if the scalars are *complex*, V is called a *complex vector space*.

The following are examples of (real) vector spaces.

Example 2.3. For $n\geq 1$, $\mathbb{R}^n=\{(x_1,x_2,\cdots,x_n)\,|\,x_1,x_2,\cdots,x_n\in\mathbb{R}\}$, is a vector space with usual (point-wise) addition and multiplication.

Example 2.4. For $n\geq 1$, $P_n=\left\{\sum_{i=0}^{n}a_ix^i\,|\,a_0,a_1,\cdots,a_n\in\mathbb{R}\right\}$, the set of polynomials of degree at most n is a vector space.

Example 2.5. The set $\mathcal{F}$ of all real-valued functions defined on the real line with operations

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

and

$$(cf)(x):=cf(x),$$

for all $f,g\in\mathcal{F},c\in\mathbb{R}$, is a vector space over $\mathbb{R}$.

Definition 2.6. [6] Let V be a vector space over F. Let V' be a subset of V. Then V' is called a subspace of V if it is itself a vector space with the induced operations of V.

Before we define what a near-vector space is, we need the following.

Definition 2.7. [7] A *right near-ring* is a triple $(N,+,\cdot)$ which satisfies:

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

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

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

N is a near-field if $(N\setminus\{0\},\cdot)$ is also a group.

2.2. Near-Vector Spaces

Definition 2.8. [8] A pair (V,F) is called a *near-vector space* if:

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

b) F contains the endomorphisms $0,id$ and $-id$.

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

d) If $u\alpha=u\beta$ with $u\in V$ and $\alpha,\beta\in F$, then $\alpha=\beta$ or $u=0$, *i.e.* F acts fixed point free (fpf) on V.

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

$$Q(V)=\{u\in V\,|\,\forall\alpha,\beta\in F,\exists\gamma\in F \text{ such that } u\alpha+u\beta=u\gamma\}. \tag{1}$$

Remark 2.9.

a) Since $-id\in F$, $(V,+)$ is an abelian group, *i.e.*

$$u+v=(-u)(-1)+(-v)(-1)=(-u-v)(-1)=(-(v+u))(-1)=v+u.$$

b) If $\alpha \in F$ then $0\alpha=0$ and $(-u)\alpha=-(u\alpha)$ since α is an endomorphism of *V*.

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

Lemma 2.10. [1] *Let* (V,F) *be a near-vector space. Then the quasi-kernel* $Q(V)$ *has the following properties*:

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

b) For $u \in Q(V)\setminus\{0\}$, γ *in* Equation (1) *is uniquely determined by* α *and* β.

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

d) *If* $u \in Q(V)$ *and* $\lambda_i \in F$, *for* $i \in \{1,2,\cdots,n\}$, *then* $\sum_{i=1}^{n} u\lambda_i = u\eta \in Q(V)$ *for some* $\eta \in F$ *and for all positive numbers n.*

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

Proof.

a) Let $\alpha,\beta \in F$ and take any $\gamma \in F$. Then $0\alpha+0\beta=0\gamma$. Hence, $0 \in Q(V)$.

b) Let $u \in Q(V)\setminus\{0\}$ and $\alpha,\beta \in F$. Then there exist γ such that $u\alpha+u\beta=u\gamma$. That is, $u(\alpha+\beta)=u\gamma$. So by Definition 2.8-(d), $u=0$ or $\alpha+\beta=\gamma$. But $u \neq 0$. So, $\alpha+\beta=\gamma$.

c) Let $u \in Q(V)$ and $\lambda \in F$. Suppose $\lambda=0$. Then $u\lambda=u0=0 \in Q(V)$ (by (a) above). Now suppose $\lambda \neq 0$. Let $\alpha,\beta \in F$. Then $\lambda\alpha,\lambda\beta \in F$. Since $u \in Q(V)$, then there exist γ such that

$$u(\lambda\alpha)+u(\lambda\beta)=u\gamma=u\lambda\lambda^{-1}\gamma, \text{ since } \lambda\lambda^{-1}=1.$$

So $(u\lambda)\alpha+(u\lambda)\beta=(u\lambda)(\lambda^{-1}\gamma)$. That is, $u\lambda \in Q(V)$. Hence, $uF \subseteq Q(V)$.

d) Let $u \in Q(V)$ and $\lambda_i \in F, 1 \leq i \leq n$. Want to show that $\sum_{i=1}^{n} u\lambda_i = u\eta \in Q(V)$. We prove this by induction. That is,

i) Base case: For $n=1$, we have $\sum_{i=1}^{1} u\lambda_i = u\lambda \in Q(V)$ (by (c) above).

ii) Inductive step: Assume $\sum_{i=1}^{k} u\lambda_i = u\eta \in Q(V)$. We need to show that $\sum_{i=1}^{k+1} u\lambda_i \in Q(V)$. That is,

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

Therefore, by induction we conclude that $\sum_{i=1}^{n} u\lambda_i = u\eta \in Q(V)$ for some $\eta \in F$ and for all *n*, where *n* is a positive number.

e) Let $u \in Q(V)\setminus\{0\}$ and $\alpha,\beta \in F$. Then by Remark 2.9-(b), $\beta(-1)=-\beta \in F$ since *F* is a set of endomorphisms of *V*. So there exist $\gamma \in F$ such that $u\alpha+u(-\beta)=u\gamma$, *i.e.* $u\alpha-u\beta=u\gamma$.

□

Example 2.11. Every near-field is a near-vector space over itself.

Example 2.12. Let $(V,F)=(\mathbb{R}^2,\mathbb{R})$. Then (V,F) is a near-vector space with scalar multiplication defined by

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

for all $(x_1,x_2)\in\mathbb{R}^2,\alpha\in\mathbb{R}$. It is not a vector space over $\mathbb{R}$. To see that it is not a vector space over $\mathbb{R}$, let $(x_1,x_2)\in\mathbb{R}^2$. Then for $\alpha,\beta\in\mathbb{R}$, we get the following two equations

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

and

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

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

Definition 2.13. [9] Let (V,F) be a near-vector space. A subset V' of $Q(V)$ is said to be *linearly independent* if for all $\alpha_1,\alpha_2,\cdots,\alpha_n\in F$ and $v_1,v_2,\cdots,v_n\in V'$,

$$v_1\alpha_1+v_2\alpha_2+\cdots+v_n\alpha_n=0$$

implies that

$$\alpha_1=\alpha_2=\cdots=\alpha_n=0.$$

A subset V' is a generating system of $Q(V)$ if for all $v\in Q(V)$ there exist $\alpha_1,\alpha_2,\cdots,\alpha_n\in F$ and $v_1,v_2,\cdots,v_n\in V'$ such that

$$v=v_1\alpha_1+v_2\alpha_2+\cdots+v_n\alpha_n.$$

A basis for $Q(V)$ is defined to be a basis for V and the cardinality of the basis is the dimension of V.

Remark 2.14. A near-vector space (V,F) is said to be a finite-dimensional near-vector space if it is of finite dimension.

Lemma 2.15. [9] *Let V be a near-vector space and let $B=\{u_i\mid 1\leq i\leq n\}$ be a basis of $Q(V)$. Then each $v\in V$ is a unique linear combination of elements of B, i.e. there exists $\lambda_i\in F$, with $\lambda_i\neq 0$ for at most a finite number of $i\in\{1,2,\cdots,n\}$, which are uniquely determined by v and B, such that*

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

Proof. See [9]. □

Example 2.16. The near-vector space from Example 2.12 has basis $B=\{(1,0),(0,1)\}$. Therefore, $(\mathbb{R}^2,\mathbb{R})$ is a 2-dimensional near-vector space.

Definition 2.17. [10] If (V,F) is a near-vector space and $\varnothing\neq V'\subseteq V$ is such that V' is the subgroup of $(V,+)$ generated additively by

$$XF=\{x\alpha\mid x\in X,\alpha\in F\},$$

where X is a independent subset of $Q(V)$, then we say that (V',F) is a sub-

space of (V,F), or simply V' is a subspace of V if F is clear from the context.

Remark 2.18.

a) If (V',F) is a subspace of (V,F), then X is a basis of V'.

b) (V',F) is a subspace of (V,F) if and only if V' is closed under addition and multiplication.

Example 2.19. Every near-vector space is a subspace of itself.

Next we define what it is meant when two near-vector spaces are said to be isomorphic.

Definition 2.20. [6] Two near-vector spaces (V_1,F_1) and (V_2,F_2) are said to be isomorphic if there are group isomorphisms $\phi:(V_1,+)\to(V_2,+)$ and $\psi:(F_1^*,\cdot)\to(F_2^*,\cdot)$ such that

$$\phi(u\alpha)=\phi(u)\psi(\alpha),$$

for all $u\in V_1$ and $\alpha\in F_1^*$. We write $(V_1,F_1)\cong(V_2,F_2)$.

To further investigate the structure of near-vector spaces, we need to understand what is meant when two non-zero elements of the quasi-kernel $Q(V)$ are compatible and when a near-vector space is regular.

Definition 2.21. [9] The elements u and $v\in Q(V)\setminus\{0\}$ are *compatible* (u cp v), if there exists a $\lambda\in F\setminus\{0\}$ such that

$$u+v\lambda\in Q(V).$$

Definition 2.22. [1] Let (V,F) be a near-vector space such that $V=\{0\}$ or $Q(V)\neq\{0\}$. Let $u\in Q(V)\setminus\{0\}$. Define the operation $+_u$ on F by

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

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

Lemma 2.23. [1] *Two non-zero elements of the quasi-kernel $Q(V)$ are compatible if and only if there exists a $\lambda\in F\setminus\{0\}$ such that*

$$+_u=+_{v\lambda}.$$

Proof. See [9]. □

Theorem 2.24. [9] The compatibility relation is an equivalence relation on $Q(V)\setminus\{0\}$.

Proof.

a) Reflexivity: Let $u\in Q(V)\setminus\{0\}$. Then by Lemma 2.10-(d), $u+u\lambda\in Q(V)\setminus\{0\}$ for $\lambda\in F^*$. Thus u cp u.

b) Symmetry: Suppose u and v are compatible, then u cp v, with $u,v\in Q(V)\setminus\{0\}$. Then there exists $\lambda\in F^*$ such that $u+v\lambda\in Q(V)$. We need to show that v cp u. Since u and v are elements of $Q(V)\setminus\{0\}$, $(u+v\lambda)\lambda^{-1}=u\lambda^{-1}+v=v+u\lambda^{-1}\in Q(V)$ for $\lambda^{-1}\in F^*$. Thus, v and u are compatible, *i.e.* v cp u.

c) Transitivity: Let $u,v,w\in Q(V)\setminus\{0\}$ and suppose u cp v and v cp w. Then by Lemma 2.23 $+_u=+_{v\lambda}$ and $+_v=+_{w\eta}$ for $\lambda,\eta\in F^*$. We need to show that $+_u=+_{w\mu}$ for some $\mu\in F^*$. Firstly, define $\alpha+_{u\lambda}\beta:=\left(\alpha^{\lambda}+_u\beta^{\lambda}\right)^{\lambda^{-1}}$. So,

$$\begin{aligned}\alpha +_u \beta &= \alpha +_{v\lambda} \beta \\ &= \left(\alpha^{\lambda} +_v \beta^{\lambda}\right)^{\lambda^{-1}} \\ &= \left(\alpha^{\lambda} +_{w\eta} \beta^{\lambda}\right)^{\lambda^{-1}} \\ &= \alpha +_{w\eta\lambda} \beta \\ &= \alpha +_{w\mu} \beta, \text{ for } \mu = \eta\lambda \in F^*.\end{aligned}$$

Hence, v cp w.

Therefore, the compatibility relation is an equivalence relation on $Q(V)\setminus\{0\}$.

□

Theorem 2.25. [9] Let u, v and $u+v \in Q(V)\setminus\{0\}$. Then

a) u cp v, and

b) u cp $u+v$.

Proof.

a) Since $u+v \in Q(V)$, by Definition 2.21 u and v are compatible with $\lambda = 1$.

b) Set $v = u\alpha$ for $\alpha \in F^*$. Then u cp $u+v$ since $u+(u+v) = u+(u+u\alpha) \in Q(V)$ for $\lambda = 1$ (by Lemma 2.10-(d)).

□

Definition 2.26. [9] A near-vector space V is called a regular near-vector space if any two vectors of $Q(V)\setminus\{0\}$ are compatible.

Theorem 2.27. [9] A near-vector space V is regular if and only if there exists a basis which consists of mutually pairwise compatible vectors.

Proof. Suppose a near-vector space V is regular. Then, by Definition 2.26, any two non-zero elements of the quasi-kernel $Q(V)$ are compatible. Therefore, every basis of $Q(V)$ (also a basis of V) consists of mutually pairwise compatible vectors.

Conversely, let V be a near-vector space. Let B be a basis of V consisting of mutually pairwise compatible vectors. Let $u \in Q(V)\setminus\{0\}$. Then u can be written as a unique linear combination of elements of B (Lemma 2.15). Suppose $u = \sum_{i=1}^{n} u_i\lambda_i$ where $u_i \in B$ and $\lambda_i \in F^*$ for all $i \in \{1, 2, \cdots, n\}$. Let

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

Then $u = u' + u_n\lambda_n \in Q(V)\setminus\{0\}$. Since $u \in Q(V)\setminus\{0\}$ then for every $\alpha, \beta \in F$, there exists a $\gamma \in F$ such that

$$\begin{aligned}u\alpha + u\beta &= (u' + u_n\lambda_n)\alpha + (u' + u_n\lambda_n)\beta \\ &= u'\alpha + u_n\lambda_n\alpha + u'\beta + u_n\lambda_n\beta \\ &= u'\alpha + u'\beta + u_n\lambda_n\alpha + u_n\lambda_n\beta \\ &= (u' + u_n\lambda_n)\gamma \\ &= u'\gamma + u_n\lambda_n\gamma.\end{aligned}$$

But $u_n \notin \{u_1, u_2, \cdots, u_{n-1}\}$. Thus, by uniqueness, $u_n\lambda_n\alpha + u_n\lambda_n\beta = u_n\lambda_n\gamma$ and $u'\alpha + u'\beta = u'\gamma$, which implies that $u' \in Q(V)$.

It still remains to check if u and u' are compatible.

If $u'=0$ then $u=u_n\lambda_n$ and by Lemma 2.10-(d), $u_n+u_n\lambda_n\in Q(V)$. Thus u_n cp $u_n\lambda_n$. If $u_n\neq 0$ then by Theorem 2.25, $u_n\lambda_n$ cp $u'+u_n\lambda_n$ since $u',u_n\lambda_n$ and $u'+u_n\lambda_n=u_n\lambda_n+u'$ are elements of $Q(V)$. But u_n cp $u_n\lambda_n$ by Lemma 2.10-(d). Therefore, by transitivity (Theorem 2.24), u_n cp u. But by assumption u_n is compatible with every element of B. Therefore, u is compatible with every element of B by transitivity (Theorem 2.24). Thus if $v,w\in Q(V)\setminus\{0\}$ then v cp u_i and w cp u_i with any $u_i\in B$ since $u\in Q(V)\setminus\{0\}$ was chosen arbitrarily. Hence again, by transitivity (Theorem 2.24), v cp w. Thus every two non-zero elements of $Q(V)$ are compatible. Therefore, a near-vector space V is regular. □

Definition 2.28. [5] The near-vector space (V,F) is said to be the direct sum of the 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

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

b) $W_i\cap(W_1+W_2+\cdots+W_{i-1}+W_{i+1}+\cdots+W_n)=\{0\}$ for each i.

We then have the following important theorem by André.

Theorem 2.29. (**The Decomposition Theorem**) [11] Every near-vector space V is the direct sum of regular near-vector spaces $V_i(i\in I)$ such that each $u\in Q(V)\setminus\{0\}$ lies in precisely one direct summand V_i. The subspaces V_i are maximal regular near-vector spaces.

We note that if V is regular, it is the only maximal regular subspace. The Decomposition Theorem means that every non-regular near-vector space (V,F) is a direct sum of disjoint maximal regular near-vector subspaces V_i, for $i\in\{1,2,\cdots,n\}$, such that

$$V=V_1\oplus V_2\oplus\cdots\oplus V_n.$$

We will not prove this theorem here. A proof can be found in [11]. The following is the procedure described in the proof on how V is decomposed into its maximal regular near-vector subspaces:

a) Partition $Q(V)\setminus\{0\}$ into sets Q_i of mutually pairwise compatible vectors.

b) Let $B\subseteq Q(V)\setminus\{0\}$ be a basis of V and let $B_i:=B\cap Q_i$.

c) Let $V_i:=\langle B_i\rangle$ be the subspace of V generated by B_i. Then each V_i is a maximal regular subspaces of V and V is a direct sum of those V_i's.

As a result of Theorem 2.29, we have the following theorem.

Theorem 2.30. (**The Uniqueness Theorem**) [9] There exists only one direct decomposition of a near-vector space into maximal regular near subspaces.

Definition 2.31. [9] The uniquely determined direct decomposition of a near-vector space V into maximal regular subspaces, is called the canonical direct decomposition of V.

3. Construction of Near-Vector Spaces over $\mathbb{Z}_p$, for p a Prime

In this chapter we characterize all finite-dimensional near-vector spaces over

$\mathbb{Z}_p$ where p is prime and we use Van der Walt's Theorem, also known as the Construction Theorem, to construct these near-vector spaces.

3.1. Automorphisms of $\mathbb{Z}_p$

Before we get into constructing near-vector spaces, we start by understanding the basic structure of $\mathbb{Z}_p$, for p a prime. We know that $\mathbb{Z}_p$ is a group under addition. For a prime p, let

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{0,1,\cdots,p-1\}.$$

Then $\mathbb{Z}_p$ is a field under addition and multiplication modulo p. That is, $\mathbb{Z}_p$ is a field with additive identity zero, multiplicative identity one, additive inverse $-x$ and multiplicative inverse x^{-1} for every $x \in \mathbb{Z}_p$. The inverse of $x \in \mathbb{Z}_p$ is an element, denoted by x^{-1}, satisfying

$$xx^{-1} = x^{-1}x = 1 \bmod p.$$

All $x \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ are invertible. Thus, $\mathbb{Z}_p^*$ is a set of invertible elements in $\mathbb{Z}_p$ and the inverse of its elements can be computed using

$$x^{-1} = x^{p-2} \bmod p.$$

We know that $\mathbb{Z}_p^*$ is a cyclic group under multiplication. That is, there exists $x \in \mathbb{Z}_p^*$ such that

$$\mathbb{Z}_p^* = \langle x \rangle = \{x^n \mid 1 \le n \le p-1\} = \{x^1, x^2, \cdots, x^{p-1}\}.$$

Such an element x is called a generator of $\mathbb{Z}_p^*$. Being cyclic implies that $(\mathbb{Z}_p^*, \cdot)$ is an abelian group.

Lemma 3.1. [9] *Let q be a positive integer. Each element of $\mathbb{Z}_p$ has a q-th root in $\mathbb{Z}_p$ if and only if* $\gcd(q, p-1) = 1$.

Proof. Suppose that every element of $\mathbb{Z}_p$, $x \in \mathbb{Z}_p$, has a q-th root in $\mathbb{Z}_p$. Let $x_1, x_2, \cdots, x_{p-1}$, non-zero elements of $\mathbb{Z}_p$, be q-th roots of $1, 2, \cdots, p-1$, respectively. That is,

$$x_n^q \equiv n \bmod p, \tag{2}$$

where x_n is a non-zero elements of $\mathbb{Z}_p$, in a particular order, for $n \in \{1, 2, \cdots, p-1\}$. Suppose that $d \mid (p-1)$, where $d > 1$. We know that if p is a prime number and $d \mid (p-1)$, then the congruence,

$$x^d - 1 \equiv 0 \bmod p$$

has exactly d solutions [12]. That is, there exists distinct $y_i \in \mathbb{Z}_p, 1 \le i \le d$, such that

$$y_i^d \equiv 1 \bmod p. \tag{3}$$

From Equation (3), we get $y_i^d = pr + 1$ for some integer r. If $d \mid q$, then $q = dt$ for some integer t. That is, $y_i^q = (y_i^d)^t = (pr+1)^t$. Using the binomial formula, we get

$$y_i^q = \sum_{i=0}^{t} \binom{t}{i} (1)^{t-i} (pr)^i = 1 + \sum_{i=1}^{t} \binom{t}{i} (pr)^i.$$

That is,

$$y_i^q = 1 + \sum_{i=1}^{t} \binom{t}{i} p^{i-1} p r^i = 1 + p \sum_{i=1}^{t} \binom{t}{i} p^{i-1} r^i = 1 + pm,$$

where m is an integer. Thus, $y_i^q \equiv 1 \bmod p, 1 \le i \le d$. This contradicts the fact that there is only one element of $\mathbb{Z}_p$, $x \in \mathbb{Z}_p$, with $x^q \equiv 1 \bmod p$ (from Equation (2)). Hence, if $d \mid (p-1)$ and $d > 1$, then $d \nmid q$. Therefore, $\gcd(q, p-1) = 1$.

Conversely, suppose that $\gcd(q, p-1) = 1$. Then by [[12], Theorem 2.3], $aq + b(p-1) = 1$ for some $a, b \in \mathbb{Z}$. Let $x \in \mathbb{Z}_p, x \neq 0$ (note that $x = 0$ has a q-th root being itself). Note that for every element of $\mathbb{Z}_p$, $x \in \mathbb{Z}_p$, $\gcd(x, p) = 1$. Since $\gcd(x, p) = 1$, by Fermat's Theorem,

$$x^{p-1} \equiv 1 \bmod p.$$

Thus

$$x^{b(p-1)} \equiv 1^b \equiv 1 \bmod p,$$

which implies that

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

That is,

$$x \equiv \left(x^a\right)^q \bmod p.$$

Hence, x has a q-th root in $\mathbb{Z}_p$, namely x^a. Therefore, each element of $\mathbb{Z}_p$ has a q-th root in $\mathbb{Z}_p$ if and only if $\gcd(q, p-1) = 1$. □

The above lemma leads to the following lemma which makes use of the Galois Field $\left(GF\left(p^r\right), +, \cdot\right)$ of order p^r.

Lemma 3.2. [13] *The mapping* $\psi : GF\left(p^r\right)^* \to GF\left(p^r\right)^*$ *is an automorphism of the group* $\left(GF\left(p^r\right)^*, \cdot\right)$ *if and only if there exists* $q \in \mathbb{Z}$, *with* $1 \le q \le p^r - 1$ *and* $\gcd\left(q, p^r - 1\right) = 1$, *such that* $\psi(x) = x^q$ *for all* $x \in GF\left(p^r\right)^*$.

Proof. Since $\left(GF\left(p^r\right), +, \cdot\right)$ is a finite field, $\left(GF\left(p^r\right)^*, \cdot\right)$ is a cyclic group. That is, there exists $x \in GF\left(p^r\right)^*$ such that $GF\left(p^r\right)^* = \langle x \rangle = \left\{x^n \mid 1 \le n \le p^r - 1\right\} = \left\{x, x^2, \cdots, x^{p^r-1}\right\}$. Let $\psi(x) = x^k$, for some $k \in \left\{1, 2, \cdots, p^r - 2\right\}$. Note that we cannot have $k = p^r - 1$ since $\psi(x) = x^k = x^{p^r-1} = 1$ for all $x \in GF\left(p^r\right)^*$. That is, ψ won't be surjective. Then $\psi\left(x^i\right) = x^{ik}$ for some $i \in \left\{1, 2, \cdots, p^r - 1\right\}$. But $\langle x \rangle = \left\{x^i \mid 1 \le i \le p^r - 1\right\} = GF\left(p^r\right)^*$, so is $\left\langle x^k \right\rangle = \left\{x^{ik} \mid 1 \le i \le p^r - 1\right\} = GF\left(p^r\right)^*$, since ψ is bijective on $GF\left(p^r\right)^*$. This means that every element of $GF\left(p^r\right)^*$ has a k-th root in $GF\left(p^r\right)^*$ and by Lemma 3.1, $\gcd\left(k, p^r - 1\right) = 1$. Take $k = q$.

Conversely, suppose that there exists $q \in \mathbb{Z}$, with $1 \le q \le p^r - 1$ and $\gcd\left(q, p^r - 1\right) = 1$, such that $\psi(x) = x^q$ for all $x \in GF\left(p^r\right)^*$. We know that

$\left(GF\left(p^r\right)^*,\cdot\right)$ is a cyclic group and let a be its generator. That is, a^q is also a generator of $GF\left(p^r\right)^*$ since $1\le q\le p^r-1$ and $\gcd\left(q,p^r-1\right)=1$. Since a^q is a generator of $GF\left(p^r\right)^*$, then for any $x\in GF\left(p^r\right)^*$, there exists $1\le k\le p^r-1$, such that $a^{qk}=x$. Thus, ψ is surjective. Let $x,y\in GF\left(p^r\right)^*$, such that $x^q=y^q$. Then there exists $1\le k,t\le p^r-1$, such that $x=a^k$ and $y=a^t$. That is, $a^{qk}=a^{qt}$ which implies that $k=t$ and $x=y$. Hence, ψ is injective. Thus, ψ is bijective. Also for any $x,y\in GF\left(p^r\right)^*$, we have $\psi(xy)=\psi(x)\psi(y)$. Therefore, ψ is an automorphism of $\left(GF\left(p^r\right)^*,\cdot\right)$. □

3.2. Van Der Walt's Theorem

The following theorem describes how arbitrary finite-dimensional near-vector spaces can be constructed.

Theorem 3.3. [8] Let $(V,+)$ be a group and let $F:=D\cup\{0\}$, where D is a fixed point free group of automorphisms of V. Then (V,F) is a finite-dimensional near-vector space if and only if there exist a finite number of near-fields $F_1,F_2,\cdots,F_n$, semigroup isomorphism $\psi_i:(F,\circ)\to(F_i,\cdot)$, and an additive group isomorphism $\phi:V\to F_1\oplus F_2\oplus\cdots\oplus F_n$ such that if $\phi(v)=(x_1,x_2,\cdots,x_n)$, then

$$\phi(v\alpha)=\left(x_1\psi_1(\alpha),x_2\psi_2(\alpha),\cdots,x_n\psi_n(\alpha)\right),$$

for all $v\in V,\alpha\in F$.

We will not prove the theorem here, see [14] for more details. We only show how it is used in constructing near-vector spaces over $\mathbb{Z}_p$, for p a prime. The following is a brief step by step approach on how to construct near-vector spaces over $\mathbb{Z}_p$ using Theorem 3.3 and making use of Lemma 3.2.

Let $\left(\mathbb{Z}_p,+,\cdot\right)$ be a field with p a prime. Then

1). Set $(V,F)=\left(\left(\mathbb{Z}_p\right)^n,\mathbb{Z}_p\right)$ where n is the dimension of our near-vector space. That is,

$$V=\left\{\left(x_1,\cdots,x_n\right)\mid x_i\in\mathbb{Z}_p \text{ for } 1\le i\le n\right\}.$$

2). List all $q\in\{1,2,\cdots,p-1\}$ such that $\gcd(q,p-1)=1$.

3). For each i, list all automorphisms, $\psi_i(\alpha)=\alpha^{q_i}$, where $q_i\in\{1,2,\cdots,p-1\}$ and $\gcd(q_i,p-1)=1$ for $\alpha\in\mathbb{Z}_p$.

4). Define scalar multiplication by

$$\begin{aligned}\left(x_1,x_2,\cdots,x_n\right)\alpha&:=\left(x_1\psi_1(\alpha),x_2\psi_2(\alpha),\cdots,x_n\psi_n(\alpha)\right)\\&=\left(x_1\alpha^{q_1},x_2\alpha^{q_2}\cdots,x_n\alpha^{q_n}\right),\end{aligned}$$

for all $\left(x_1,x_2,\cdots,x_n\right)\in\left(\mathbb{Z}_p\right)^n$ and $\alpha\in\mathbb{Z}_p$.

Lemma 3.4. [13] *Let $F=GF\left(p^r\right)$ and $V=F^n$ (n-copies) be a near-vector space with scalar multiplication defined for all $\alpha\in F$ by*

$$\left(x_1,x_2,\cdots,x_n\right)\alpha:=\left(x_1\psi_1(\alpha),x_2\psi_2(\alpha),\cdots,x_n\psi_n(\alpha)\right),$$

where the ψ's are automorphisms of $(F,\cdot)$ and they can be equal. Then V is

regular if and only if for all $i,j\in\{1,2,\cdots,n\}$ *and* $\alpha\in GF\left(p^r\right)$, $\psi_i(\alpha)=\psi_j\left(\alpha^{p^l}\right)$, *for some* $l\in\{0,1,\cdots,r-1\}$.

Proof. See [13]. □

Since $\mathbb{Z}_p=GF(p)$, *i.e.* $r=1$, we have that the maximal regular subspaces of V are those for which the q_i's coincide. That is, if we have a near-vector space say, $(V,F)=\left(\left(\mathbb{Z}_{11}\right)^3,\mathbb{Z}_{11}\right)$, with scalar multiplication $(x_1,x_2,x_3)\alpha=\left(x_1\alpha,x_2\alpha^3,x_3\alpha^3\right)$. Then the canonical direct decomposition of V is $V=V_1\oplus V_2$ where $V_1=\{(x_1,0,0)\mid x_1\in F\}$ and $V_2=\{(0,x_2,x_3)\mid x_2,x_3\in F\}$. Each V_i, for $i\in\{1,2\}$, contains vectors with same type of action. By the Decomposition Theorem, those V_i's are the maximal regular subspaces of V.

The following lemma describes the decomposition of the quasi-kernel of a near-vector space constructed using copies of $\mathbb{Z}_p$.

Lemma 3.5. [15] *Suppose that* V *is a* n*-dimensional near-vector space over* $\mathbb{Z}_p$ *with* $Q(V)\neq V$ *and* $V=V_1\oplus V_2\oplus\cdots\oplus V_n$ *is the canonical decomposition of* V. *Then*

$$Q(V)=Q_1\cup Q_2\cup\cdots\cup Q_n$$

where $Q_i=V_i$ for each $i\in\{1,2,\cdots,n\}$.

Proof. See [15]. □

Consider the following example where we show that a partition across the quasi-kernel gives a near-vector space which is not regular.

Example 3.6. Let $(V,F)=\left(\left(\mathbb{Z}_{11}\right)^3,\mathbb{Z}_{11}\right)$ be a near-vector space with scalar multiplication

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

Then the quasi-kernel is $Q(V)=\{(x_1,x_2,0)\mid x_1,x_2\in F\}\cup\{(0,0,x_3)\mid x_3\in F\}$. Let $u,v\in Q(V)$. Then (V,F) is regular if u and v are compatible, u cp v. That is, there exist a $\lambda\in F^*$ such that $u+v\lambda\in Q(V)$. Take $u=(1,1,0)$ and $v=(0,0,1)$. Then

$$\begin{aligned}u+v\lambda&=(1,1,0)+(0,0,1)\lambda\\&=(1,1,0)+\left(0,0,\lambda^3\right)\\&=\left(1,1,\lambda^3\right)\notin Q(V),\text{ since }\lambda\in F^*.\end{aligned}$$

Thus, (V,F) is not a regular near-vector space.

The number of q_i's satisfying Lemma 3.2 is $\phi(p-1)$, where ϕ is the Euler's totient function. That is, for each i, there are $\phi(p-1)$ distinct possibilities for ψ.

Theorem 3.7. [9] A n-dimensional near-vector space (V,F) over $\mathbb{Z}_p$ is a vector space if and only if $q_1=q_2=\cdots=q_n=1$.

Proof. If $q_i=1$ for all i, then from Theorem 3.3 and Lemma 3.2, we get scalar multiplication as

$$(x_1,x_2,\cdots,x_n)\alpha=(x_1\alpha,x_2\alpha,\cdots,x_n\alpha)$$

which is a vector space for all $(x_1,x_2,\cdots,x_n)\in\left(\mathbb{Z}_p\right)^n$ and $\alpha\in\mathbb{Z}_p$. For any

other choices of q_i's, with $q_1 = 1$, non-isomorphic near-vector spaces are created. □

We also have

Lemma 3.8. *Let* $(V,F) = \left(\left(\mathbb{Z}_p\right)^n, \mathbb{Z}_p\right)$ *be a near-vector space. For all* $(x_1, x_2, \cdots, x_n) \in \left(\mathbb{Z}_p\right)^n$ *and* $\alpha \in F$, *let* $V_1 = \left(\mathbb{Z}_p\right)^n$ *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* $(x_1, x_2, \cdots, x_n) \in V_1$ *and* $\alpha \in \mathbb{Z}_p$. *Let* $V_2 = \left(\mathbb{Z}_p\right)^n$ *with scalar multiplication defined by* $(x_1, x_2, \cdots, x_n)\alpha = \left(x_1\alpha^{q'}, x_2\alpha^{q'}, \cdots, x_n\alpha^{q'}\right)$ *for all* $(x_1, x_2, \cdots, x_n) \in V_2$ *and* $\alpha \in \mathbb{Z}_p$, *where all* $q' \neq 1$ *and* q' *is a positive integer. Then* $(V_1, F) \cong (V_2, F)$.

Proof. To show that $(V_1, F) \cong (V_2, F)$. Define $\phi : (V_1, +) \to (V_2, +)$ by $\phi(x_1, x_2, \cdots, x_n) = \left(x_1\beta^{q'}, x_2\beta^{q'}, \cdots, x_n\beta^{q'}\right)$ and $\psi : \left(F^*, \cdot\right) \to \left(F^*, \cdot\right)$ by $\psi(\alpha) = \alpha$ for all $\alpha, \beta \in F^*$. We need to check the following.

a) If ϕ and ψ are well-defined:

Let $(x_1, x_2, \cdots, x_n) = (y_1, y_2, \cdots, y_n)$. Then

$$\begin{aligned}\phi(x_1, x_2, \cdots, x_n) &= \left(x_1\beta^{q'}, x_2\beta^{q'}, \cdots, x_n\beta^{q'}\right)\\ &= \left(y_1\beta^{q'}, y_2\beta^{q'}, \cdots, y_n\beta^{q'}\right)\\ &= \phi(y_1, y_2, \cdots, y_n).\end{aligned}$$

Let $\alpha = \beta$. Then $\psi(\alpha) = \alpha = \beta = \psi(\beta)$.

b) Checking if ϕ and ψ are bijective and, $\phi\left((x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n)\right) = \phi(x_1, x_2, \cdots, x_n) + \phi(y_1, y_2, \cdots, y_n)$ and $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$:

Let $(x_1, x_2, \cdots, x_n), (y_1, y_2, \cdots, y_n) \in \left(\mathbb{Z}_p\right)^n$ and $\alpha, \beta \in F^*$. Suppose $\phi(x_1, x_2, \cdots, x_n) = \phi(y_1, y_2, \cdots, y_n)$. Then $\left(x_1\beta^{q'}, x_2\beta^{q'}, \cdots, x_n\beta^{q'}\right) = \left(y_1\beta^{q'}, y_2\beta^{q'}, \cdots, y_n\beta^{q'}\right)$. That is, $x_1\beta^{q'} = y_1\beta^{q'}, x_2\beta^{q'} = y_2\beta^{q'}, \cdots, x_n\beta^{q'} = y_n\beta^{q'}$ which implies that $x_1 = y_1, x_2 = y_2, \cdots, x_n = y_n$ (after multiplying by $\beta^{-q'} \in F^*$, recall that F^* is a set of invertible elements in $\mathbb{Z}_p$). Thus, ϕ is injective.

Let $(y_1, y_2, \cdots, y_n) \in V_2$. Then there exist $(x_1, x_2, \cdots, x_n) \in V_1$ such that $\phi(x_1, x_2, \cdots, x_n) = (y_1, y_2, \cdots, y_n)$. Take $(x_1, x_2, \cdots, x_n) = \left(y_1\beta^{-q'}, y_2\beta^{-q'}, \cdots, y_n\beta^{-q'}\right)$ for $\beta^{-q'} \in F^*$. Then $\phi(x_1, x_2, \cdots, x_n) = \phi(y_1, y_2, \cdots, y_n)$. Thus ϕ is surjective. Therefore, ϕ is bijective. Furthermore,

$$\begin{aligned}&\phi\left((x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n)\right)\\ &= \phi(x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)\\ &= \left((x_1 + y_1)\beta^{q'}, (x_2 + y_2)\beta^{q'}, \cdots, (x_n + y_n)\beta^{q'}\right)\\ &= \left(x_1\beta^{q'} + y_1\beta^{q'}, x_2\beta^{q'} + y_2\beta^{q'}, \cdots, x_n\beta^{q'} + y_n\beta^{q'}\right)\\ &= \left(x_1\beta^{q'}, x_2\beta^{q'}, \cdots, x_n\beta^{q'}\right) + \left(y_1\beta^{q'}, y_2\beta^{q'}, \cdots, y_n\beta^{q'}\right)\\ &= \phi(x_1, x_2, \cdots, x_n) + \phi(y_1, y_2, \cdots, y_n).\end{aligned}$$

Suppose also that $\psi(\alpha) = \psi(\beta)$. Then $\alpha = \beta$. Thus ψ is injective. Let $\beta \in F^*$. Then there exist $\alpha \in F^*$ such that $\psi(\alpha) = \beta$. That is, $\alpha = \beta$. Thus

ψ is surjective. Therefore, ψ is bijective. Also $\psi(\alpha\beta)=\alpha\beta=\psi(\alpha)\psi(\beta)$.

c) Checking if $\phi\left((x_1,x_2,\cdots,x_n)\alpha\right)=\phi(x_1,x_2,\cdots,x_n)\psi(\alpha)$ for all $(x_1,x_2,\cdots,x_n)\in V_1$ and $\alpha\in F^*$:

$$\begin{aligned}\phi\left((x_1,x_2,\cdots,x_n)\alpha\right)&=\phi(x_1\alpha,x_2\alpha,\cdots,x_n\alpha)\\&=\left(x_1\alpha\beta^{q'},x_2\alpha\beta^{q'},\cdots,x_n\alpha\beta^{q'}\right)\\&=\left(x_1\beta^{q'}\alpha,x_2\beta^{q'}\alpha,\cdots,x_n\beta^{q'}\alpha\right),\text{ since } F^*\text{ is commutative}\\&=\left(x_1\beta^{q'},x_2\beta^{q'},\cdots,x_n\beta^{q'}\right)\alpha\\&=\phi(x_1,x_2,\cdots,x_n)\psi(\alpha).\end{aligned}$$

Therefore (V_1,F) is isomorphic to (V_2,F) as a near-vector space *i.e.* $(V_1,F)\cong(V_2,F)$. □

3.3. Examples

Here we construct non-isomorphic near-vector spaces by following the procedure stipulated above in constructing near-vector spaces. Recall that for all $i\in\{1,2,\cdots,n\}$, $q_i=1$ we get a vector space by Theorem 3.7 and by Lemma 3.8 we get isomorphic near-vector spaces. The quasi-kernel $Q(V)$ of each near-vector space will be investigated and we will decompose V into its maximal regular near-vector subspaces by the procedure described in the proof of Theorem 2.29.

Example 3.9. Let $(\mathbb{Z}_5,+,\cdot)$ be a field. Let $(V,F)=\left((\mathbb{Z}_5)^3,\mathbb{Z}_5\right)$. We are looking for $1\le q_i<4$ such that $\gcd(q_i,4)=1$. The candidates are $q_i\in\{1,3\}$. We can take $\psi_1(\alpha)=\alpha$ and $\psi_2(\alpha)=\psi_3(\alpha)=\alpha^3$ and the scalar multiplication can be defined as follows

$$(x_1,x_2,x_3)\alpha:=\left(x_1\psi_1(\alpha),x_2\psi_2(\alpha),x_3\psi_3(\alpha)\right)=\left(x_1\alpha,x_2\alpha^3,x_3\alpha^3\right),$$

for all $(x_1,x_2,x_3)\in V$ and $\alpha\in F$. Hence (V,F) is a near-vector space.

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

i) Let us consider $(x_1,0,0)\in V$. For $\alpha,\beta\in F$,

$$\begin{aligned}(x_1,0,0)\alpha+(x_1,0,0)\beta&=(x_1\alpha,0,0)+(x_1\beta,0,0)\\&=(x_1\alpha+x_1\beta,0,0)\\&=(x_1(\alpha+\beta),0,0)\\&=(x_1,0,0)(\alpha+\beta),\text{ with }\alpha+\beta\in F.\end{aligned}$$

Hence $(x_1,0,0)\in Q(V)$ for each $x_1\in F$.

ii) Consider $(0,x_2,x_3)\in V$. For $\alpha,\beta\in F$,

$$\begin{aligned}(0,x_2,x_3)\alpha+(0,x_2,x_3)\beta&=\left(0,x_2\alpha^3,x_3\alpha^3\right)+\left(0,x_2\beta^3,x_3\beta^3\right)\\&=\left(0,x_2\alpha^3+x_2\beta^3,x_3\alpha^3+x_3\beta^3\right)\\&=\left(0,x_2\left(\alpha^3+\beta^3\right),x_3\left(\alpha^3+\beta^3\right)\right)\\&=(0,x_2,x_3)\left(\alpha^3+\beta^3\right)^{1/3},\text{ with }\left(\alpha^3+\beta^3\right)^{1/3}\in F.\end{aligned}$$

Hence $(0,x_2,x_3)\in Q(V)$ for $x_2,x_3\in F$. Note that $(x_1,x_2,x_3)\notin Q(V)$.

iii) Consider $(x_1,x_2,0)\in V$. For $\alpha,\beta\in F$,

$$\begin{aligned}(x_1,x_2,0)\alpha+(x_1,x_2,0)\beta&=(x_1\alpha,x_2\alpha^3,0)+(x_1\beta,x_2\beta^3,0)\\&=(x_1\alpha+x_1\beta,x_2\alpha^3+x_2\beta^3,0)\\&=(x_1(\alpha+\beta),x_2(\alpha^3+\beta^3),0)\\&\neq(x_1,x_2,0)\gamma,\end{aligned}$$

for $\gamma\in F$ since in general, $(\alpha+\beta)^3\neq\alpha^3+\beta^3$. Hence $(x_1,x_2,0)\notin Q(V)$.

Note also that $(x_1,0,x_3)\notin Q(V)$ for $x_2,x_3\in F$.

Therefore, the quasi-kernel $Q(V)$ is

$$Q(V)=\{(x_1,0,0)\mid x_1\in F\}\cup\{(0,x_2,x_3)\mid x_2,x_3\in F\}.$$

Now we decompose V into its maximal regular near-vector subspaces. It is not difficult to verify that $B=\{(1,0,0),(0,1,0),(0,0,1)\}$ is a basis of the near-vector space (V,F). Let $Q^*=Q(V)\setminus\{(0,0,0)\}$. Then

$$Q^*=\{(x_1,0,0)\mid x_1\in F\}\cup\{(0,x_2,x_3)\mid x_2,x_3\in F\}\setminus\{(0,0,0)\}.$$

Partitioning Q^*, we get

$$Q_1=\{(x_1,0,0)\mid x_1\in F\}\setminus\{(0,0,0)\}$$

and

$$Q_2=\{(0,x_2,x_3)\mid x_2,x_3\in F\}\setminus\{(0,0,0)\}.$$

Now we get that

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

and

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

Let V_1 be a near-vector space generated by B_1. Then

$$V_1:=\langle B_1\rangle=\{(1,0,0)x_1\mid x_1\in F\}=\{(x_1,0,0)\mid x_1\in F\}.$$

Similarly, let V_2 be a near-vector space generated by B_2. Then

$$\begin{aligned}V_2:=\langle B_2\rangle&=\{(0,1,0)x_2+(0,0,1)x_3\mid x_2,x_3\in F\}\\&=\{(0,(x_2)^3,(x_3)^3)\mid x_2,x_3\in F\}.\end{aligned}$$

Since x_2 and x_3 are arbitrary elements in F, we can take $(x_2)^3,(x_3)^3$ as x_2' and x_3' respectively. So

$$V_2=\{(0,x_2',x_3')\mid x_2',x_3'\in F\}.$$

Therefore by the Decomposition Theorem, V_1 and V_2 are maximal regular near-vector spaces and the canonical direct decomposition of V is

$$V=V_1\oplus V_2.$$

Example 3.10. Consider the field $(\mathbb{Z}_{11},+,\cdot)$. Let $(V,F)=((\mathbb{Z}_{11})^3,\mathbb{Z}_{11})$. We

want $1 \le q_i < 10$ such that $\gcd(q_i, 10) = 1$. The candidates for q_i are $q_i \in \{1,3,7,9\}$. Therefore, we can take $\psi_1(\alpha) = \alpha$, $\psi_2(\alpha) = \alpha^3$ and $\psi_3(\alpha) = \alpha^7$. We define the scalar multiplication as follows;

$$(x_1, x_2, x_3)\alpha := (x_1\psi_1(\alpha), x_2\psi_2(\alpha), x_3\psi_3(\alpha)) = (x_1\alpha, x_2\alpha^3, x_3\alpha^7),$$

for all $(x_1, x_2, x_3) \in V$ and $\alpha \in F$. Thus, (V, F) is a near-vector space.

We now investigate the quasi-kernel $Q(V)$. The quasi-kernel is found to be

$$Q(V) = \{(x_1, 0, 0) \mid x_1 \in F\} \cup \{(0, x_2, 0) \mid x_2 \in F\} \cup \{(0, 0, x_3) \mid x_3 \in F\}.$$

We now decompose V into its maximal regular near-vector subspaces. It is not difficult to verify that $B = \{(1,0,0), (0,1,0), (0,0,1)\}$ is a basis of the near-vector space (V, F). Let $Q^* = Q(V) \setminus \{(0,0,0)\}$. Then

$$Q^* = \{(x_1, 0, 0) \mid x_1 \in F\} \cup \{(0, x_2, 0) \mid x_2 \in F\} \cup \{(0, 0, x_3) \mid x_3 \in F\} \setminus \{(0,0,0)\}.$$

Partitioning Q^*, we get

$$Q_1 = \{(x_1, 0, 0) \mid x_1 \in F\} \setminus \{(0,0,0)\},$$

$$Q_2 = \{(0, x_2, 0) \mid x_2 \in F\} \setminus \{(0,0,0)\},$$

$$Q_3 = \{(0, 0, x_3) \mid x_3 \in F\} \setminus \{(0,0,0)\}.$$

Now we get that

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

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

$$B_3 := B \cap Q_2 = \{(0,0,1)\}.$$

Let V_1, V_2 and V_3 be near-vector spaces generated by B_1, B_2 and B_3 respectively. Then

$$\begin{aligned} V_1 := \langle B_1 \rangle &= \{(1,0,0)x_1 \mid x_1 \in F\} \\ &= \{(x_1, 0, 0) \mid x_1 \in F\}, \end{aligned}$$

$$\begin{aligned} V_2 := \langle B_2 \rangle &= \{(0,1,0)x_2 \mid x_2 \in F\} \\ &= \{(0, (x_2)^3, 0) \mid x_2 \in F\} \\ &= \{(0, x_2', 0) \mid x_2' \in F\}, \text{ since } x_2 \text{ is arbitrary}, \end{aligned}$$

$$\begin{aligned} V_3 := \langle B_3 \rangle &= \{(0,0,1)x_3 \mid x_3 \in F\} \\ &= \{(0, 0, (x_3)^7) \mid x_3 \in F\} \\ &= \{(0, 0, x_3') \mid x_3' \in F\}, \text{ since } x_3 \text{ is arbitrary}. \end{aligned}$$

Therefore by the Decomposition Theorem, V_1, V_2 and V_3 are maximal regular near-vector spaces and the canonical direct decomposition of V is then

$$V = V_1 \oplus V_2 \oplus V_3.$$

From the above examples, we get the following lemma.

Lemma 3.11. *If* (V,F) *is a near-vector space of dimension n, i.e.* $V=F^n$, *then the number of* Q_i*'s in the Decomposition Theorem is less or equal to n.*

Proof. Suppose (V,F) is a near-vector space of dimension n and the number of Q_i's in the Decomposition Theorem is greater than n. Then there exist $m>n$ such that Q_m is one of the cells of partitions of $Q(V)$. By construction in the proof of the Decomposition Theorem, we have $B_m=B\cap Q_m$, where B is the basis of V, and B_m generates V_m. That is, $V_m=\langle B_m\rangle$. Also V is a direct sum of all V_i's, $i\in\{1,\cdots,m\}$, thus $\dim(V)=\dim(V_1)+\cdots+\dim(V_m)$. But $\dim(V_1)+\cdots+\dim(V_m)\geq m$ and $\dim(V)=n$, which is a contradiction since $m>n$. Therefore, the number of Q_i's in the Decomposition Theorem is less or equal to n. □

4. An Application to Finite Linear Games

There are several applications of near-vector spaces: in Finite Linear Games and Cryptography, to mention a few. In this chapter we look at the application of near-vector spaces to finite or discrete linear games.

Most of the content here is taken from [15].

A finite linear game is a problem where a physical object has a finite number of states of which can be altered by applying certain processes. By so doing, they produce finitely many outcomes. Digital systems in computer science are often of this type. Since there are only a finite number of states, we can use elements of $\mathbb{Z}_p$, for p a prime, to represent the various states.

We generalize the idea by restricting the number of finite states to $\mathbb{Z}_p$ for p a prime. But before we do that, consider the following example.

Recall that every vector space is a near-vector space. For consistency in the essay, we write scalars on the right of vectors.

Example 4.1. Five switches control five light bulbs in a row, changing the state, on or off, of the light bulb directly above it and the state of light bulbs adjacent to the left or right. Consider the figure below.

If the first and the third light bulbs are on as in **Figure 1(a)**, then pushing switch A changes the state of the system to the state in **Figure 1(b)**. If we next push switch C, the state changes to the state in **Figure 1(c)**.

We are looking for an order in which we can push the switches so that only the first, third and fifth light bulbs will be on. Assume that all light bulbs are initially off. We make use of $(\mathbb{Z}_2)^5$ over $\mathbb{Z}_2$. The vectors in $(\mathbb{Z}_2)^5$ represent the action of each switch where the elements of $\mathbb{Z}_2$ represent the action done

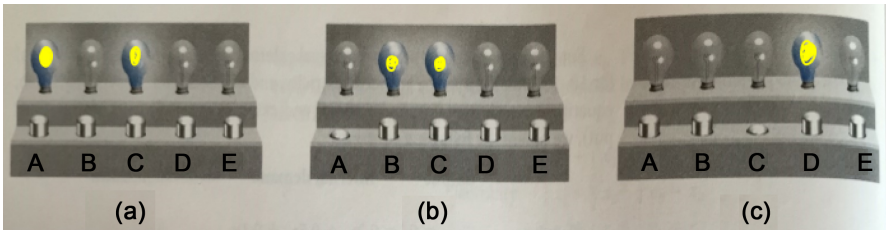

Figure 1. A row of five light bulbs controlled by five switches.

to the light bulb by a switch. Let 1 and 0 represent the *on* and *off* state of the light bulb, where $0,1 \in \mathbb{Z}_2$. Then the five switches can be represented by

$$\bar{a} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \ \bar{b} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \ \bar{c} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \ \bar{d} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \text{ and } \bar{e} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

Let $\bar{i}$ and $\bar{f}$ represent the initial and final state respectively. That is

$$\bar{i} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \text{ and } \bar{f} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

To see how we can reach the final state $\bar{f}$ (target configuration), we need to determine whether there are scalars $x_1, x_2, x_3, x_4, x_5 \in \mathbb{Z}_2$ such that $\bar{i} + \bar{a}x_1 + \bar{b}x_2 + \bar{c}x_3 + \bar{d}x_4 + \bar{e}x_5 = \bar{f}$. That is,

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} x_1 + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} x_2 + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} x_3 + \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} x_4 + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} x_5 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

We get the augmented matrix as

$$\left[\begin{array}{ccccc|c} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right].$$

Applying row operations over $\mathbb{Z}_2$ we get

$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Thus x_5 is a free variable and we have two possible solutions

$$x_1 = x_5$$

$$x_2 = 1 + x_5$$

$$x_3 = 1$$

$$x_4 = 1 + x_5.$$

When $x_5 = 0$ and $x_5 = 1$ we get the following solutions respectively

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

Therefore, we push switch $\bar{a}$ once, $\bar{c}$ once and $\bar{e}$ once to reach the target configuration.

Note that there is no way we can push the switches in such a way that only the first light bulb will be on. When a particular switch is pushed n-times, where n is an even number, the light bulb goes back to its original state. Also for any switch say $\bar{a}$, $\bar{a}n = \bar{a} + \bar{a} + \cdots + \bar{a}$ (n times).

From the above example, we can see that given n light bulbs with p possible states and a switch associated with each light bulb, the initial and final configuration or state of the system is

$$\bar{i} = \begin{bmatrix} i_1 \\ i_2 \\ \vdots \\ i_n \end{bmatrix} \text{ and } \bar{f} = \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix},$$

respectively. For the switches we have

$$\bar{s}_i = \begin{bmatrix} s_{i1} \\ s_{i2} \\ \vdots \\ s_{in} \end{bmatrix} \in \left(\mathbb{Z}_p\right)^n,$$

which captures the changes in the state of the light bulb above them. Each light bulb changes its state sequentially. The final state $\bar{f}$ corresponds to the vector addition of the initial state $\bar{i}$ and the number of times each switch is pressed (in some order). That is,

$$\bar{i} + \bar{s}_1 x_1 + \bar{s}_2 x_2 + \cdots + \bar{s}_n x_n = \bar{f},$$

where $x_1, x_2, \cdots, x_n \in \mathbb{Z}_p$. The scalar multiplication is defined for all switches $\bar{s}_i \in \left(\mathbb{Z}_p\right)^n$ and all $\alpha \in \mathbb{Z}_p$ as follows

$$\bar{s}_i \alpha = \begin{bmatrix} s_{i1} \\ s_{i2} \\ \vdots \\ s_{in} \end{bmatrix} \alpha = \begin{bmatrix} s_{i1}\alpha^q \\ s_{i2}\alpha^q \\ \vdots \\ s_{in}\alpha^q \end{bmatrix},$$

where q is a positive integer. Since we are working with near-vector spaces constructed over $\mathbb{Z}_p$ using a result by van der Walt (Theorem 3.3), then the number of times, α, a particular switch is pressed is given by the following scalar multiplication

$$\begin{bmatrix} s_{i1} \\ s_{i2} \\ \vdots \\ s_{in} \end{bmatrix} \alpha = \begin{bmatrix} s_{i1}\alpha^{q_1} \\ s_{i2}\alpha^{q_2} \\ \vdots \\ s_{in}\alpha^{q_n} \end{bmatrix},$$

where q_i, for $i \in \{1,2,\cdots,n\}$, satisfies Lemma 3.2.

Note that in Example 4.1 we used the usual multiplication (linear) where $q_i = 1$ for all $i \in \{1,2,\cdots,n\}$.

Now we consider the case where the scalar multiplication is not linear.

Example 4.2. A row of four light bulbs is controlled by four switches. Each light bulb can have five possible states, 0, 1, 2, 3 or 4, where each number represents a different state. Each switch changes the states, assuming all light bulbs were initially off, of particular light bulbs as follows

$$\overline{s}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 4 \end{bmatrix}, \ \overline{s}_2 = \begin{bmatrix} 1 \\ 2 \\ 4 \\ 0 \end{bmatrix}, \ \overline{s}_3 = \begin{bmatrix} 2 \\ 2 \\ 0 \\ 1 \end{bmatrix} \text{ and } \overline{s}_4 = \begin{bmatrix} 1 \\ 0 \\ 3 \\ 2 \end{bmatrix}.$$

Note that we are working over $\mathbb{Z}_5$ since there are five possible states. The initial state is $\overline{i} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ and suppose the final state is $\overline{f} = \begin{bmatrix} 1 \\ 3 \\ 1 \\ 3 \end{bmatrix}$. To reach the final state, we need to determine whether there are scalars $x_1, x_2, x_3, x_4 \in \mathbb{Z}_5$ such that

$$\overline{i} + \overline{s}_1 x_1 + \overline{s}_2 x_2 + \overline{s}_3 x_3 + \overline{s}_4 x_4 = \overline{f}.$$

For the case where we use the usual multiplication, suitable sequence $(1,1,1,1)$, we get scalars to be $x_1 = 2$, $x_2 = 4$, $x_3 = 0$ and $x_4 = 0$. We know that for suitable sequences $(1,1,1,1)$ and $(3,3,3,3)$ the resulting two near-vector spaces are isomorphic. But for a suitable sequence $(3,3,3,3)$, the number of times we press switches is different from how we press them with sequence $(1,1,1,1)$. With sequence $(3,3,3,3)$, we get $x_1 = 3$, $x_2 = 4$, $x_3 = 0$ and $x_4 = 0$. It is no longer the case that for any switch $\overline{s}_i$, for $i \in \{1,2,\cdots,n\}$, $\overline{s}_i n = \overline{s}_i + \overline{s}_i + \cdots + \overline{s}_i$ (n-times). Take switch $\overline{s}_2$ for example,

$$\overline{s}_2(2) = \begin{bmatrix} 1 \\ 2 \\ 4 \\ 0 \end{bmatrix} 2 = \begin{bmatrix} 2^3 \\ 2 \cdot 2^3 \\ 4 \cdot 2^3 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 2 \\ 0 \end{bmatrix},$$

whereas

$$\overline{s}_2 + \overline{s}_2 = \begin{bmatrix} 1 \\ 2 \\ 4 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \\ 4 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \\ 3 \\ 0 \end{bmatrix}.$$

This is all as a result of Lemma 3.2. Note that for the sequence $(3,3,3,3)$, $Q(V) = V$. That is, V is regular.

Example 4.3. Suppose from Example 4.2 we use suitable sequence $(1,3,3,1)$ to define the scalar multiplication. This yields the following system of equations

$$x_1 + x_2 + x_3(3) + x_4 = 1 \tag{4}$$

$$x_2^3(2) + x_3^3(2) = 3 \tag{5}$$

$$x_2^3(4) + x_4^3(3) = 1 \tag{6}$$

$$x_1(4) + x_3 + x_4(2) = 3. \tag{7}$$

Thus, we get two systems of equations, each has the same type of action.

$$x_1 + x_2 + x_3(3) + x_4 = 1 \tag{8}$$

$$x_1(4) + x_3 + x_4(2) = 3 \tag{9}$$

and

$$x_2^3(2) + x_3^3(2) = 3 \tag{10}$$

$$x_2^3(4) + x_4^3(3) = 1. \tag{11}$$

The first system is linear and the second is non-linear. Keeping in mind that $\mathbb{Z}_5$ is a field and every element of $\mathbb{Z}_5$ has an inverse in $\mathbb{Z}_5$, by doing so we get $x_1 = 2$, $x_2 = 4$, $x_3 = 0$ and $x_4 = 0$. Note that for Equation (5) and Equation (6) we used the fact that every element of $\mathbb{Z}_p$ has a q-th root in $\mathbb{Z}_p$ by Lemma 3.1. Note also that V is not regular, and observe that the quasi-kernel $Q(V)$ is

$$Q(V) = \{(x_1, 0, 0, x_4) \mid x_1, x_4 \in \mathbb{Z}_5\} \cup \{(0, x_2, x_3, 0) \mid x_2, x_3 \in \mathbb{Z}_5\} = Q_1 \cup Q_2.$$

Example 4.4. Suppose we have five possible states as in Example 4.2 with suitable sequence $(1,3,3,1)$ but this time with the following switches.

$$\overline{s_1} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \ \overline{s_2} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \ \overline{s_3} = \begin{bmatrix} 2 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \ \overline{s_4} = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 0 \end{bmatrix}.$$

The initial state is $\overline{i} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ and suppose the final state is $\overline{f} = \begin{bmatrix} 1 \\ 3 \\ 1 \\ 3 \end{bmatrix}$. We solve the following system of equations

$$x_1 + x_3(2) = 1 \tag{12}$$

$$x_2^3 + x_4^3 = 3 \tag{13}$$

$$x_2^3 + x_4^3(2) = 1 \tag{14}$$

$$x_1(2) + x_3 = 3. \tag{15}$$

We solve the same way we solved for Example 4.2 to get $x_1 = 0$, $x_2 = 0$, $x_3 = 3$ and $x_4 = 2$. Note again that the quasi-kernel is

$$Q(V) = \{(x_1, 0, 0, x_4) \mid x_1, x_4 \in \mathbb{Z}_5\} \cup \{(0, x_2, x_3, 0) \mid x_2, x_3 \in \mathbb{Z}_5\} = Q_1 \cup Q_2.$$

Also note that the switches belong to either Q_1 or Q_2.

In a nutshell, we have considered the following cases:

a) Case where $Q(V)=V$, *i.e.* V is regular. Here the scalar multiplication is linear and is of the form

$$\overline{s}_i\alpha=\begin{bmatrix} s_{i1}\alpha^q \\ s_{i2}\alpha^q \\ \vdots \\ s_{in}\alpha^q \end{bmatrix},$$

for any switch $\overline{s}_i\in(\mathbb{Z}_p)^n$ and $\alpha\in\mathbb{Z}_p$ with q satisfying Lemma 3.2. It's easy to solve for scalars if $q=1$. If $q\neq 1$, then Lemma 3.1 is of assistance in solving for scalars together with simple substitution.

b) Case where $Q(V)\neq V$, *i.e.* V is not regular. By Theorem 2.29 we can write V into its maximal regular subspaces, *i.e.* $V=V_1\oplus V_2\oplus\cdots\oplus V_n$ so as its quasi-kernel $Q(V)$ by Lemma 3.5. That is, $Q(V)=Q_1\oplus Q_2\oplus\cdots\oplus Q_n$.

c) Case where there will be more than one system to solve. The system that needs be solved is solved simultaneously in conjunction with Lemma 3.1.

d) Case where the switches belong to Q_i for some $i\in\{1,2,\cdots,n\}$. Here the rows of the coefficient matrix can be rearranged so that the system can be easier to solve.

5. Conclusion

The aim of this paper was to discuss the construction of near-vector spaces over $\mathbb{Z}_p$, for p a prime. We showed how to construct near-vector spaces using finite (right) near-fields and an important result (theorem) by van der Walt (also known as the Construction Theorem). We then used this theory to describe all finite-dimensional near-vector spaces over $\mathbb{Z}_p$, for p a prime, up to isomorphism. We also looked at their quasi-kernels and regularity. The Decomposition Theorem by André was applied on those near-vector spaces in order to get their maximal regular subspaces. We showed an application of near-vector spaces over $\mathbb{Z}_p$ to finite linear games.

Conflicts of Interest

Regarding the publication of this paper, the authors declare that, there is no conflict of interest.

References

[1] Andre, J. (1974) Lineare Algebra Uber Fastkorpern. *Mathematische Zeitschrift*, **136**, 295-313. https://doi.org/10.1007/BF01213874

[2] Beidleman, J.C. (1964) On Near-Rings and Near-Ring Modules. The Pennsylvania State University, University Park, Pennsylvania.

[3] Karzel, H. (1984) "Fastvektorraume," unvollstandige Fastkorper und ihre algeleiteten Strukturen.

[4] Howell, K.-T. and Meyer, J. (2009) Finite-Dimensional Near-Vector Spaces over Fields of Prime Order. *Communications in Algebra*, **38**, 86-93.

https://doi.org/10.1080/00927870902855549

[5] Dorfling, S., Howell, K.-T. and Sanon, S. (2018) The Decomposition of Finite-Dimensional Nearvector Spaces. *Communications in Algebra*, **46**, 3033-3046. https://doi.org/10.1080/00927872.2017.1404083

[6] Howell, K.-T. and Meyer, J. (2014) Near-Vector Spaces Determined by Finite Fields. *Journal of Algebra*, **398**, 55-62. https://doi.org/10.1016/j.jalgebra.2013.09.019

[7] Pilz, G. (1983) Near-Rings: The Theory and Its Applications. Revised Edition, Mathematics Studies 23.

[8] Howell, K.-T., Chistyakov, D. and Sanon, S. (2019) On Representation Theory and Near-Vector Spaces. *Linear and Multilinear Algebra*, **67**, 1495-1510. https://doi.org/10.1080/03081087.2018.1459449

[9] Howell, K.-T. (2007) Contributions to the Theory of Near-Vector Spaces. Ph.D. Dissertation, University of the Free State, Bloemfontein.

[10] Howell, K.-T. (2015) On Subspaces and Mappings of Near-Vector Spaces. *Communications in Algebra*, **43**, 2524-2540. https://doi.org/10.1080/00927872.2014.900689

[11] Kalunga, J., Tefoetsile, K., Phiri, H.M. and Chibeti, S. (2022) The Decomposition Theorem for Near-Vector Spaces. *International Journal of Mathematics and Its Applications*, **10**, 1-17.

[12] Burton, D.M. (2006) Elementary Number Theory. Tata McGraw-Hill Education, New York.

[13] Howell, K.-T., Chistyakov, D. and Sanon, S. (2018) On Representation Theory and Near-Vector Spaces. *Linear and Multilinear Algebra*, **67**, 1495-1510.

[14] Sanon, S.P. (2017) Contribution to the Theory of Near-Vector Spaces.

[15] Boonzaaier, L., Howell, K.-T. and Sanon, S. (2009) An Application of Finite-Dimensional Near-Vector Spaces over Fields of Prime Order in a Finite Linear Game.