PROGRESS IN APPLIED SCIENCE AND TECHNOLOGY
Faculty of Science and Technology
Rajamangala University of Technology Thanyaburi
Prog Appl Sci Tech. 2024; 14(2):12-15
ISSN (Print): 2730-3012
ISSN (Online): 2730-3020
https://ph02.tci-thaijo.org/index.php/past

Research Article

Received: March 22, 2024
Revised: June 12, 2024
Accepted: June 25, 2024

DOI: 10.60101/past.2024.253316

Some Properties of Subspaces over Residue Class Rings

Juthamas Sangwisat and Siripong Sirisuk*
Department of Mathematics and Statistics, Faculty of Science and Technology, Thammasat University, Pathum Thani 12120, Thailand
*E-mail: siripong@mathstat.sci.ac.th

Abstract

Let $\mathbb{Z}_{p^s}$ denote the residue class ring where p is a prime number and s is a positive integer. For $n \geq 1$, a free submodule of the $\mathbb{Z}_{p^s}$-module $\mathbb{Z}_{p^s}^n$ that has a basis is called a subspace of $\mathbb{Z}_{p^s}^n$. In this paper, we present some properties of subspaces regarding their dimensions and the joins of subspaces of $\mathbb{Z}_{p^s}^n$.

Keywords: Submodule, Subspace, Dimension, Residue Class Ring

1. Introduction

Let p be a prime number and s a positive integer. The ring $\mathbb{Z}_{p^s}$ of integers modulo p^s is known as the *residue class ring*. In particular, when $s = 1$, $\mathbb{Z}_p$ forms a finite field. Residue class rings play a crucial role in various mathematical areas, including coding theory, computer science, and algebraic graph theory. Numerous works have explored codes over residue class rings (1-4). Additionally, several types of graphs focus exclusively on residue class rings, such as Grassmann graphs (5,6), bilinear form graphs (7-9), and symplectic graphs (10,11). Moreover, $\mathbb{Z}_{p^s}$ plays an important role in algebraic structure since it is a Galois ring, a finite chain ring, a principal ideal ring, and a commutative local ring (12-15). The ideals of $\mathbb{Z}_{p^s}$ are in the chain

$$\{0\} = p^s\mathbb{Z}_{p^s} \subsetneq p^{s-1}\mathbb{Z}_{p^s} \subsetneq \cdots \subsetneq p\mathbb{Z}_{p^s} \subsetneq \mathbb{Z}_{p^s}.$$

It is clear that $p\mathbb{Z}_{p^s}$ is the unique maximal ideal of $\mathbb{Z}_{p^s}$, which is denoted by J_{p^s}. Note that $J_{p^s} = \{0\}$ if and only if $s = 1$. Also, u is a unit in $\mathbb{Z}_{p^s}$ if and only if $u \notin J_{p^s}$. Moreover, $|p^i\mathbb{Z}_{p^s}| = p^{s-i}$ for all $i = 0,1,\ldots,s$.

Let n be a positive integer. Consider the $\mathbb{Z}_{p^s}$-module $\mathbb{Z}_{p^s}^n$. The zero vector in $\mathbb{Z}_{p^s}^n$ is denoted by $\vec{0}$. A set $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_m\}$ of vectors in $\mathbb{Z}_{p^s}^n$ is said to be *linearly independent* if for any $a_1, a_2, \ldots, a_m$ in $\mathbb{Z}_{p^s}$, $a_1\vec{x}_1 + a_2\vec{x}_2 + \cdots + a_m\vec{x}_m = \vec{0}$ implies $a_1 = a_2 = \cdots = a_m = 0$. The *dimension* of a submodule X of $\mathbb{Z}_{p^s}^n$, denoted by $\dim(X)$, is the number of vectors in a linearly independent subset of X with maximum cardinality. For vectors $\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_m$ in $\mathbb{Z}_{p^s}^n$, one can show that the set $\{a_1\vec{x}_1 + a_2\vec{x}_2 + \cdots + a_m\vec{x}_m \mid a_i \in \mathbb{Z}_{p^s}\}$ is a submodule of $\mathbb{Z}_{p^s}^n$ which is denoted by $\langle \vec{x}_1, \vec{x}_2, \ldots, \vec{x}_m \rangle$. If $X = \langle \vec{x}_1, \vec{x}_2, \ldots, \vec{x}_m \rangle$ is the submodule of $\mathbb{Z}_{p^s}^n$ of dimension m generated by a linearly independent set $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_m\}$, then X is called an *m-subspace* or *subspace* of $\mathbb{Z}_{p^s}^n$, and the set $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_m\}$ is called a *basis* of X. The 0-subspace is defined to be $\{\vec{0}\}$ with a basis $\emptyset$. In addition, subspaces of $\mathbb{Z}_{p^s}^n$ are also referred to as free submodules and free linear codes. It is

worth noting that when $s = 1$, the subspaces of the $\mathbb{Z}_{p^s}$-module $\mathbb{Z}_{p^s}^n$ coincide with the usual subspaces of a vector space $\mathbb{Z}_p^n$ over the field $\mathbb{Z}_p$. Note that the module $\mathbb{Z}_{p^s}^n$ possesses a standard basis $\{\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n\}$ where $\vec{e}_i = (e_{i1}, e_{i2}, \dots, e_{in})$ with $e_{ii} = 1$ and $e_{ij} = 0$ for all $i \neq j$. Therefore, $\dim(\mathbb{Z}_{p^s}^n) = n$.

Next, Huang et al. (6) introduced the concept of joins of two subspaces. Let X and Y be subspaces of $\mathbb{Z}_{p^s}^n$. A *join* of X and Y is defined to be a subspace of $\mathbb{Z}_{p^s}^n$ containing both X and Y. A *minimum join* is a join with minimum dimension. The set of minimum joins of X and Y, denoted by $X \vee Y$. We write $\dim(X \vee Y)$ for the dimension of a minimum join of X and Y. If Z is the unique minimum join of X and Y, that is, $X \vee Y = \{Z\}$, we write $X \vee Y = Z$ for convenience.

According to the various properties of residue class rings, this paper aims to present some fundamental properties of submodules, subspaces and joins of two subspaces of $\mathbb{Z}_{p^s}^n$. Our findings contribute to deeper understanding of these algebraic structures and their applications in various mathematical areas.

2. Main Results

In this section, we first present some properties of submodules and subspaces of $\mathbb{Z}_{p^s}^n$ regarding their dimensions. Next, we study some properties of joins of two subspaces. Some examples are also provided.

Proposition 2.1 If X is an m-subspace of $\mathbb{Z}_{p^s}^n$, then $|X| = p^{sm}$.

Proof. Assume that X is an m-subspace of $\mathbb{Z}_{p^s}^n$ with a basis $\{\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m\}$. Let $\vec{x} \in X$. Suppose that $\vec{x} = a_1\vec{x}_1 + a_2\vec{x}_2 + \cdots + a_m\vec{x}_m = b_1\vec{x}_1 + b_2\vec{x}_2 + \cdots + b_m\vec{x}_m$ for some $a_i, b_i \in \mathbb{Z}_{p^s}$. It follows that $(a_1 - b_1)\vec{x}_1 + (a_2 - b_2)\vec{x}_2 + \cdots + (a_m - b_m)\vec{x}_m = \vec{0}$. Since $\{\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m\}$ is linearly independent, we obtain that $a_i = b_i$ for all $i = 1,2, \dots, m$. This implies that any $\vec{x}$ in X can be uniquely expressed as $\vec{x} = a_1\vec{x}_1 + a_2\vec{x}_2 + \cdots + a_m\vec{x}_m$, where $a_i \in \mathbb{Z}_{p^s}$. Hence, any $\vec{x}$ in X depends on the unique choices of $\{a_1, a_2, \dots, a_m\}$. Since there are p^s choices for each a_i where $i = 1,2, \dots, m$, the number of vectors in X is $(p^s)^m = p^{sm}$. □

Example 1 In $\mathbb{Z}_4^2$, $X = \langle(1,2), (1,0)\rangle = \{(0,0), (1,0), (2,0), (3,0), (0,2), (1,2), (2,2), (3,2)\}$ is a submodule of $\mathbb{Z}_4^2$ but it is not a subspace of $\mathbb{Z}_4^2$ since $|X| \neq 2^{2m}$ for any positive integer m, by Proposition 2.1.

We see that a submodule of $\mathbb{Z}_{p^s}^n$ may not be a subspace, although it has a dimension. However, if X is a submodule (which may not be a subspace) of $\mathbb{Z}_{p^s}^n$ with $\dim(X) = m$, then X contains an m-subspace of $\mathbb{Z}_{p^s}^n$. This is proved in the following proposition.

Proposition 2.2 If X is a submodule of $\mathbb{Z}_{p^s}^n$ with $\dim(X) = m$, then X contains an m-subspace of $\mathbb{Z}_{p^s}^n$.

Proof. Assume that X is a submodule of $\mathbb{Z}_{p^s}^n$ with $\dim(X) = m$. Let $\{\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m\}$ be a linearly independent set in X with maximum cardinality. Then $Y = \langle\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m\rangle$ is an m-subspace of $\mathbb{Z}_{p^s}^n$. Thus, X contains an m-subspace Y. □

Furthermore, we obtain the following proposition.

Proposition 2.3 Let X and Y be submodules of $\mathbb{Z}_{p^s}^n$ such that $X \subseteq Y$. Then:

1. $\dim(X) \leq \dim(Y)$.
2. If Y is a subspace and $\dim(X) = \dim(Y)$, then $X = Y$.

Proof. 1. Suppose that $\dim(X) = m$. Then there exists a linearly independent set S of X with $|S| = m$. Since $X \subseteq Y$, it follows that S is a linearly independent subset of Y. Thus, $\dim(Y) \geq |S| = m$. Therefore, $\dim(X) \leq \dim(Y)$.

2. Assume that Y is a subspace and $\dim(X) = \dim(Y) = m$. By Proposition 2.1, we obtain that $|Y| = p^{sm}$. Since X is a submodule with $\dim(X) = m$, by Proposition 2.2, X contains an m-subspace Z of $\mathbb{Z}_{p^s}^n$. Again, by Proposition 2.1, $|Z| = p^{sm}$. Now, observe that $Z \subseteq X \subseteq Y$, and $|Z| = p^{sm} = |Y|$. Therefore, $X = Y$. □

Since $\dim(\mathbb{Z}_{p^s}^n) = n$, we immediatly obtain the following corollary.

Corollary 2.4 If X is a submodule of $\mathbb{Z}_{p^s}^n$, then $\dim(X) \leq n$.

Example 2 Consider a submodule $X = \langle(1,2),(1,0)\rangle$ of $\mathbb{Z}_4^2$. Note that Example 1 shows that X is not a subspace. However, its dimension always exists. To find it, we note that $\dim(X) \leq 2$ by Corollary 2.4. Suppose that $\dim(X) = 2$. Let $\{\vec{x}, \vec{y}\}$ be a linearly independent set in X. Then $Z = \langle\vec{x}, \vec{y}\rangle$ is a 2-subspace of $\mathbb{Z}_4^2$. By Proposition 2.1, $|Z| = 16$. It follows that $16 = |Z| \leq |X| = 8$, a contradiction. Thus, $\dim(X) \leq 2$. Note that $\{(1,0)\}$ is a linearly independent set in X. Therefore, $\dim(X) = 1$.

We next characterize submodules with dimension 0. The following lemma is necessary for this purpose.

Lemma 2.5 (16) Let $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_{p^s}^n$. Then $\{\vec{x}\}$ is a linearly independent set if and only if $x_j \notin J_{p^s}$ for some $j \in \{1,2,\ldots,n\}$.

Theorem 2.6 Let X be a submodule of $\mathbb{Z}_{p^s}^n$. Then $\dim(X) = 0$ if and only if $X \subseteq J_{p^s}^n$, where $J_{p^s}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in J_{p^s}\}$.

Proof. Assume that $\dim(X) = 0$. Let $\vec{x} = (x_1, x_2, \ldots, x_n) \in X$. Suppose $x_i \notin J_{p^s}$ for some $i \in \{1,2,\ldots,n\}$. By Lemma 2.5, $\{\vec{x}\}$ is a linearly independent set in X. Then $\dim(X) \geq 1$, which is a contradiction. Thus, $x_i \in J_{p^s}$ for all $i = 1,2,\ldots,n$. Hence, $\vec{x} \in J_{p^s}^n$. Therefore, $X \subseteq J_{p^s}^n$.

Conversely, assume that $\dim(X) > 0$. Then there exists a linearly independent vector $\vec{x} = (x_1, x_2, \ldots, x_n)$ in X. By Lemma 2.5, $x_j \notin J_{p^s}$ for some $j \in \{1,2,\ldots,n\}$. Hence, $\vec{x} \notin J_{p^s}^n$. Thus, $X \nsubseteq J_{p^s}^n$. □

Proposition 2.7 Let X and Y be distinct subspaces of $\mathbb{Z}_{p^s}^n$. If $\dim(X) = \dim(Y) = m > 0$, then $\dim(X \cap Y) < m$.

Proof. Assume that $\dim(X) = \dim(Y) = m > 0$. Since $X \cap Y$ is a submodule of X and Y, we obtain that $\dim(X \cap Y) \leq \dim(X) \leq m$ by Proposition 2.3 (1). Suppose $\dim(X \cap Y) = m$. According to Proposition 2.3 (2), we obtain that $X = X \cap Y = Y$, a contradiction. Thus, $\dim(X \cap Y) < m$. □

Next, we study some properties of joins of subspaces. Recall that a join of two subspaces X and Y is a subspace of $\mathbb{Z}_{p^s}^n$ containing both X and Y. In general, a join is not necessarily unique.

Example 3 Consider subspaces of $\mathbb{Z}_4^3$.
1. Let $X = \langle(0,0,1)\rangle$ and $Y = \langle(0,2,1)\rangle$ be subspaces in $\mathbb{Z}_4^3$. Then $\langle(0,0,1),(0,1,0)\rangle$ and $\langle(0,0,1),(2,1,0)\rangle$ are the minimum joins of X and Y, i.e.,
$X \vee Y = \{\langle(0,0,1),(0,1,0)\rangle, \langle(0,0,1),(2,1,0)\rangle\}$.
It follows that $\dim(X \vee Y) = 2$.
2. If $X = \langle(0,0,1)\rangle$ and $Y = \langle(1,2,0)\rangle$, then $X \vee Y = \langle(2,0,1),(1,2,0)\rangle$, so that $\dim(X \vee Y) = 2$.
3. If $X = \langle(0,0,1)\rangle$ and $Y = \langle(0,1,2),(1,0,0)\rangle$, then $X \vee Y = \mathbb{Z}_4^3$, so that $\dim(X \vee Y) = 3$.

Note that for submodules X and Y of $\mathbb{Z}_{p^s}^n$, $X + Y = \{\vec{x} + \vec{y} \mid \vec{x} \in X \text{ and } \vec{y} \in Y\}$ is a submodule of $\mathbb{Z}_{p^s}^n$. Moreover, it is the unique join when $s = 1$ as illustrated in the following proposition.

Proposition 2.8 If X and Y are subspaces of $\mathbb{Z}_p^n$, then $X \vee Y = X + Y$.

Proof. It is clear that $X + Y$ is a subspace of $\mathbb{Z}_p^n$ containing X and Y. Then $X + Y$ is a join of X and Y. Also, if W is a minimum join of X and Y, then $X + Y = W$. It implies that $X + Y$ is the unique minimum join. As a result, $X \vee Y = X + Y$. □

More properties on $X \vee Y$ are studied as follows.

Theorem 2.9 Let X and Y be subspaces of $\mathbb{Z}_{p^s}^n$. Then $\dim(X \vee Y) = n$ if and only if $X \vee Y = \mathbb{Z}_{p^s}^n$.

Proof. It is clear that, if $X \vee Y = \mathbb{Z}_{p^s}^n$, then $\dim(X \vee Y) = n$. Assume that $\dim(X \vee Y) = n$. Let W be a minimum join of X and Y. Then $\dim(W) = n$. Since W is an n-subspace of $\mathbb{Z}_{p^s}^n$, it follows from Proposition 2.3 (2) that $W = \mathbb{Z}_{p^s}^n$. Thus, $X \vee Y = \mathbb{Z}_{p^s}^n$. □

Proposition 2.10 Let X and Y be subspaces of $\mathbb{Z}_{p^s}^n$ such that $X \subseteq Y$. Then:
1. $X \vee Y = Y$.
2. $\dim(X \vee Z) \leq \dim(Y \vee Z)$ for all subspace Z of $\mathbb{Z}_{p^s}^n$.

Proof. 1. Since $X \subseteq Y$, it is evident that Y is a subspace containing both of X and Y with the minimum dimension. That is, $Y \in X \vee Y$. Therefore, $\dim(X \vee Y) = \dim(Y)$. Suppose there is another minimum join, denoted as W, of X and Y. Then $Y \subseteq W$. As $\dim(Y) = \dim(X \vee Y) = \dim(W)$, by Proposition 2.3 (2), $Y = W$. Thus, Y is the unique maximum join of X and Y, i.e., $X \vee Y = Y$.
2. Let Z be a subspace of $\mathbb{Z}_{p^s}^n$. Assume that $W \in Y \vee Z$, i.e., W is a subspace containing Y and Z, and $\dim(W) = \dim(Y \vee Z)$. Since $X \subseteq Y$, it implies that W is a join of X and Z. Then $\dim(X \vee Z) \leq \dim(W) = \dim(Y \vee Z)$. □

Proposition 2.11 If X, X', Y and Y' are subspaces of $\mathbb{Z}_{p^s}^n$ such that $X \subseteq X'$ and $Y \subseteq Y'$, then $\dim(X \vee Y) \leq \dim(X' \vee Y')$.

Proof. Assume $X \subseteq X'$ and $Y \subseteq Y'$. Let $Z' \in X' \vee Y'$. Then $X \subseteq X' \subseteq Z'$ and $Y \subseteq Y' \subseteq Z'$, i.e., Z' is a join of X and Y. Now, let $Z \in X \vee Y$. Thus, $\dim(X \vee Y) = \dim(Z) \leq \dim(Z') = \dim(X' \vee Y')$. □

In conclusion, the study of subspaces over residue class rings enhances our understanding of linear algebra in modular arithmetic. In addition, submodules and subspaces are known as linear codes and free linear codes in coding theory, respectively. Therefore, this knowledge is crucial for applications such as error-correcting codes and cryptography. Future research could explore more advanced properties of these subspaces and their practical implications.

Declaration of Conflicting Interests
The authors declared that they have no conflicts of interest in the research, authorship, and this article's publication.

References

1. Calderbank AR, McGuire G, Kumar PV, Helleseth T. Cyclic codes over $\mathbb{Z}_4$, locator polynomials and Newton's identities. IEEE Trans Inform Theory. 1996;42:217-26.
2. Helleseth T. Codes over $\mathbb{Z}_4$. In: Alt, H. (eds) Computational Discrete Mathematics. Lecture Notes in Computer Science, vol 2122. Berlin, Heidelberg: Springer; 2001.
3. Van Lint JH. Codes over $\mathbb{Z}_4$. In: Introduction to Coding Theory. Graduate Texts in Mathematics, vol 86. Berlin, Heidelberg: Springer; 1999.
4. Kyureghyan G, Kwon SM. Codes over the ring $\mathbb{Z}_p^s$: Bounds on the minimum distance. Finite Fields Appl. 2010; 16(2):144-163.
5. Huang LP, Lv B, Wang K. Automorphisms of Grassmann graphs over a residue class ring. Discrete Math. 2020;343(4):111693.
6. Huang, LP, Lv B, Wang K. Erdos-Ko-Rado theorem, Grassmann graphs and p^s-Kneser graphs for vector spaces over a residue class ring. J Comb Theory Ser A. 2019;164:125-158.
7. Guo J. Erdos-Ko-Rado theorem for matrices over residue class rings. Graphs Combin. 2021;37(6):1-14.
8. Huang LP. Generalized bilinear forms graphs and MRD codes over a residue class ring. Finite Fields Appl. 2018;51:306-324.
9. Huang LP, Su H, Tang G, Wang JB. Bilinear forms graphs over residue class rings. Linear Algebra Appl. 2017;253:13-32.
10. Li F, Wang K, Guo J. More on symplectic graphs modulo p^n. Linear Algebra Appl. 2017;438(6):2651-2660.
11. Meemark Y, Prinyasart T. On symplectic graphs modulo p^n. Discrete Math. 2011;311(17):1874-1878.
12. McDonald BR. Finite Rings with Identity. New York: Marcel Dekker; 1974.
13. McDonald BR. Geometric Algebra over Local Rings. New York: Marcel Dekker; 1976.
14. McCoy NH.: Rings and Ideals. Washington, DC: The Mathematical Association of America; 1948.
15. Wan ZX. Lectures on Finite Fields and Galois Rings. Singapore: World Scientific Publishing Company; 2003.
16. Sirisuk S, Meemark Y. Generalized symplectic graphs and generalized orthogonal graphs over finite commutative rings. Linear Multilinear Algebra. 2019; 67(12):2427-2450.

