RESEARCH ARTICLE • OPEN ACCESS

Lattice Constructions in Euclidean Space $\mathbb{R}^n$ and Its Subspaces

Zahira Najmatul Hayyah, Edi Kurniadi, and Anita Triska

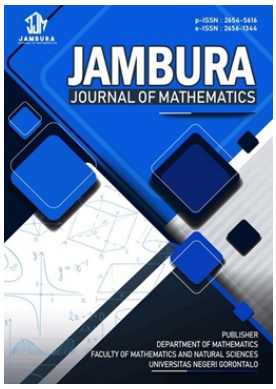
JAMBURA
JOURNAL OF MATHEMATICS

Volume 8, Issue 1, Pages 87–92, February 2026

Received 19 December 2025, Revised 2 February 2026, Accepted 11 February 2026, Published 16 February 2026

To Cite this Article : Z. N. Hayyah, E. Kurniadi, and A Triska,"Lattice Constructions in Euclidean Space $\mathbb{R}^n$ and Its Subspaces ", *Jambura J. Math*, vol. 8, no. 1, pp. 87–92, 2026, *https://doi.org/10.37905/jjom.v8i1.36272*

JOURNAL INFO • JAMBURA JOURNAL OF MATHEMATICS



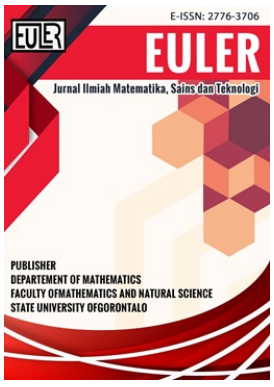
Homepage	:	http://ejurnal.ung.ac.id/index.php/jjom/index
Journal Abbreviation	:	Jambura J. Math.
Frequency	:	Biannual (February and August)
Publication Language	:	English (preferable), Indonesia
DOI	:	https://doi.org/10.37905/jjom
Online ISSN	:	2656-1344
Editor-in-Chief	:	Hasan S. Panigoro
Publisher	:	Department of Mathematics, Universitas Negeri Gorontalo
Country	:	Indonesia
OAI Address	:	http://ejurnal.ung.ac.id/index.php/jjom/oai
Google Scholar ID	:	iWLjgaUAAAAJ
Email	:	info.jjom@ung.ac.id

JAMBURA JOURNAL • FIND OUR OTHER JOURNALS

Jambura Journal of Biomathematics

Jambura Journal of Mathematics Education

Jambura Journal of Probability and Statistics



EULER : Jurnal Ilmiah Matematika, Sains, dan Teknologi

Jambura Journal of Mathematics, Volume 8, Issue 1, Pages 87–92, February 2026 https://doi.org/10.37905/jjom.v8i1.36272

Research Article

Check for updates

Lattice Constructions in Euclidean Space $\mathbb{R}^n$ and Its Subspaces

Zahira Najmatul Hayyah[1,*], **Edi Kurniadi**[1], **Anita Triska**[1]

[1]*Department of Mathematics, Universitas Padjadjaran, Sumedang 45363, Indonesia*

ARTICLE HISTORY
Received 19 December 2025
Revised 2 February 2026
Accepted 11 February 2026
Published 16 February 2026

KEYWORDS
Lattice construction
Standard basis
Vector space
Euclidean space
Subspace
$\mathbb{Z}^n$

ABSTRACT. *A lattice is a discrete subgroup of n-dimensional Euclidean space that serves as a fundamental object of study in Algebra and the Geometry of Numbers. This structure has significant applications in various fields, particularly in lattice-based cryptography and coding theory. This paper aims to present the formal construction of lattices for n-dimensional Euclidean space $\mathbb{R}^n$ and its linear subspaces by analyzing the formal definitions and essential properties of lattices. The main results of this research lie in two main results which are presented in several propositions. First, the set $\mathbb{Z}^n$ of standard integer points is proven to be a lattice in n-dimensional space with respect to the standard basis of $V \subseteq \mathbb{R}^n$. Second, the set of integer points whose last component is zero is proven to be a lattice within $(n-1)$-dimensional non-trivial subspaces. Indeed, in this case, the obtained lattice is not equal to $\mathbb{Z}^n$. Moreover, it also discussed the lattices of a non-standard basis for V. Explicitly, this work contributes a rigorous formal verification that integer structures within subspaces, such as $\mathbb{Z}^{n-1} \times \{0\}$, retain fundamental lattice properties even under non-standard basis constructions.*

1. Introduction

The Euclidean space $\mathbb{R}^n$ is one of the most fundamental mathematical objects studied in linear algebra and geometry. Although this space is continuous, the study of its discrete subgroups has opened up a field of research known as the Geometry of Numbers [1]. This field studies the interaction between convex bodies and discrete structures and provides a framework for analyzing geometric and arithmetic properties [2]. Central to this field is the concept of a lattice, which can be understood as the set of linear combinations of a linearly independent set in the Euclidean space $\mathbb{R}^n$ whose coefficients are all integers.

Formally, a lattice L in $\mathbb{R}^n$ is defined as the set of all integer linear combinations of a set of linearly independent basis vectors [3]. Furthermore, when $L \subseteq \mathbb{R}^n$, it is called a lattice in $\mathbb{R}^n$. The practical importance of lattices has grown in recent decades, particularly due to their applications in computer science and engineering [4]. In modern cryptography, the security of most post-quantum cryptographic schemes, including frameworks such as Learning with Errors (LWE) and NTRU-based systems, relies on the assumed computational difficulty of lattice problems, such as the Shortest Vector Problem (SVP), to withstand potential quantum-computing attacks [4–7]. The urgency of lattice research has intensified following the National Institute of Standards and Technology (NIST) post-quantum cryptography standardization process. Recently, lattice-based algorithms such as ML-KEM and ML-DSA have been finalized as global standards due to their robust security and efficiency [8, 9]. These schemes utilize module-lattice structures to achieve an optimal balance between key size and computational speed [10, 11]. Besides cryptography, lattices are fundamental to coding theory for devising efficient error-correcting codes [12], particularly for securing next-generation wireless networks such as 6G [13].

Although lattices have various advanced applications, the formal construction of a lattice remains a necessary first step. Therefore, this paper focuses on the formal construction and verification of lattice properties in $\mathbb{R}^n$ and its subspaces. The first objective is to formally prove that the set $\mathbb{Z}^n$ satisfies the definition of a lattice in $\mathbb{R}^n$. Subsequently, the analysis is extended to a linear subspace $V \subseteq \mathbb{R}^n$. In addition, this study demonstrates how the set $\mathbb{Z}^{n-1} \times \{0\}$ can be constructed and proven to be a lattice within the chosen subspace

$$V = \text{Span}\{e_1, e_2, e_3, \ldots, e_{n-1}\},$$

where $\{e_i\}$ represents the standard basis vectors.

While classical references such as [1] or [3] establish the general theory of the geometry of numbers, the explicit construction of lattices within specific linear subspaces is often treated summarily. This paper complements these standard works by contributing a structured and pedagogical exposition focused specifically on foundational lattice constructions in Euclidean spaces and their subspaces.

2. Methods

This study uses both a literature review and a theoretical and analytical approach based on linear algebra and the geometry of numbers to explore the concept of lattices. The research aims to provide a clear understanding of how lattices are constructed in $\mathbb{R}^n$. Before presenting the findings, the theoretical framework that supports the study and outlines the key ideas and definitions necessary for understanding the results is discussed.

*Corresponding Author.

Email : zahira22001@mail.unpad.ac.id (Z. N. Hayyah)
Homepage : http://ejurnal.ung.ac.id/index.php/jjom/index / E-ISSN : 2656-1344

Definition 1. [14] A vector space V over a field F is a commutative group $(V,+)$ whose elements are called vectors, with a distinguished element of V, denoted by $\vec{0}$ and called the zero vector, together with a scalar multiplication of vectors by elements of F satisfying the following conditions. For all $u, v \in V$ and all $\alpha, \beta \in F$,

1. $\alpha v \in V$,
2. $1v = v$,
3. $0v = \vec{0}$,
4. $\alpha(u+v) = \alpha u + \alpha v$,
5. $(\alpha+\beta)v = \alpha v + \beta v$,
6. $(\alpha\beta)v = \alpha(\beta v)$.

A vector space over $\mathbb{R}$ is called a real vector space. The vector spaces $\mathbb{R}^n$ are usually referred to as the n-dimensional Euclidean space. In this paper, V refers to a real vector space over $\mathbb{R}$.

Definition 2. [14] A subspace of a vector space V is a subset $U \subseteq V$ for which U is a vector space using the same operations of addition and scalar multiplication defined on V.

Lemma 1. *[14] A nonempty subset $U \subseteq V$ of a vector space V is a subspace of V if and only if*

1. *whenever $u_1, u_2 \in U$, then $u_1 + u_2 \in U$,*
2. *whenever $\alpha \in F$ and $u \in U$, then $\alpha u \in U$.*

Example 1. The set $W = \{(a,0) \mid a \in \mathbb{R}\}$ is a subspace of the vector space $\mathbb{R}^2$, while the set $X = \{(a,1) \mid a \in \mathbb{R}\}$ is not a subspace of $\mathbb{R}^2$.

Definition 3. [15] Let $v_1, v_2, \ldots, v_n$ be vectors in a vector space V. A vector v is said to be a linear combination of $v_1, v_2, \ldots, v_n$ if there exist scalars $c_1, c_2, \ldots, c_n$ such that v can be written as $v = c_1v_1 + c_2v_2 + \cdots + c_nv_n$.

Example 2. Let $v_1 = \begin{pmatrix}1\\2\end{pmatrix}, v_2 = \begin{pmatrix}2\\3\end{pmatrix}$ be vectors in a vector space V. A vector $v = \begin{pmatrix}4\\7\end{pmatrix}$ is a linear combination of v_1, v_2 because there exist scalars $c_1 = 2$ and $c_2 = 1$ such that $v = 2v_1 + v_2 = 2\begin{pmatrix}1\\2\end{pmatrix} + \begin{pmatrix}2\\3\end{pmatrix}$.

Definition 4. [15] Let $v_1, v_2, \ldots, v_n$ be vectors in a vector space V. A set $S = \{v_1, v_2, \ldots, v_n\}$ is said to span V if every $v \in V$ can be written as a linear combination of $v_1, v_2, \ldots, v_n$. This is denoted by $V = \text{Span}(S)$.

Example 3. The set $S = \left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$ spans the vector space $V = \mathbb{R}^2$ because every $v \in V$ can be written as a linear combination of these vectors.

Definition 5. [14] A collection of vectors $v_1, v_2, \ldots, v_n$ is said to be linearly independent if whenever $c_1v_1 + c_2v_2 + \cdots + c_nv_n = \vec{0}$, then necessarily $c_1 = c_2 = \cdots = c_n = 0$.

Example 4. The set $S = \left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$ is linearly independent because the equation $c_1\begin{pmatrix}1\\0\end{pmatrix} + c_2\begin{pmatrix}0\\1\end{pmatrix} = \vec{0}$ is satisfied only if $c_1 = 0$ and $c_2 = 0$.

Definition 6. [14] A set of vectors $\{v_1, v_2, \ldots, v_n\}$ in a vector space V is called a basis for V if

1. $v_1, v_2, \ldots, v_n$ are linearly independent,
2. $\text{Span}\{v_1, v_2, \ldots, v_n\} = V$.

The number of vectors in a basis is called the dimension of V.

Example 5. The set $S = \left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$ is a basis for $\mathbb{R}^2$ because it is linearly independent and $\text{Span}(S) = \mathbb{R}^2$.

Definition 7. [16] Let $\{v_1, v_2, \ldots, v_k\}$ be a linearly independent set of vectors in $\mathbb{R}^n$ and let

$$V = \langle v_1, v_2, \ldots, v_k \rangle$$

be the vector subspace of $\mathbb{R}^n$ spanned by these vectors. The lattice L generated by $v_1, v_2, \ldots, v_k$ consists of all integer linear combinations of these vectors, that is,

$$L = \{p_1v_1 + p_2v_2 + \cdots + p_kv_k \mid p_i \in \mathbb{Z}\}.$$

A lattice in $\mathbb{R}^n$ is a subset $L \subseteq \mathbb{R}^n$ which is generated by some set of linearly independent vectors in $\mathbb{R}^n$.

3. Results and Discussion

The results of this research are presented in the form of propositions describing the construction of lattices within $\mathbb{R}^n$

and its subspace. Before detailing the proofs, it is crucial to note the mathematical significance of these structures: they demonstrate how lattice properties, such as full-rank or non-full-rank, are preserved or altered when restricted to specific linear subspaces. The first results stated in Proposition 1 and Proposition 2, which describe the construction of lattices from non-trivial proper subspaces with respect to the standard basis, are presented below. Specifically, in Proposition 1, it is proved that the lattice $\mathbb{Z}^n$ is generated by the standard basis of $\mathbb{R}^n$.

Proposition 1. *Let $\mathbb{R}^n$ be a vector space over $\mathbb{R}$ with the standard basis $S = \{e_1, e_2, \ldots, e_n\}$, where*

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

with 1 in the i-th component and $1 \leq i \leq n$. Then $\mathbb{Z}^n$ is a lattice in $\mathbb{R}^n$.

Proof. By Definition 6, S is a standard basis of $\mathbb{R}^n$ such that S is a set of linearly independent vectors that spans $\mathbb{R}^n$. By Definition 4, choose $V = \mathbb{R}^n = \operatorname{Span} S$. Then, by Definition 7, a lattice L is defined as the set of all integer linear combinations (Definition 3) of the vectors in S:

$$\begin{aligned} L &= \{p_1e_1 + p_2e_2 + p_3e_3 + \cdots + p_ne_n \mid p_i \in \mathbb{Z}\} \\ &= \left\{ \begin{pmatrix} p_1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ p_2 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ p_3 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ p_n \end{pmatrix} \;\middle|\; p_i \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_n \end{pmatrix} \;\middle|\; p_i \in \mathbb{Z} \right\} = \mathbb{Z}^n \subseteq \mathbb{R}^n. \end{aligned}$$

Thus, $\mathbb{Z}^n$ is a lattice in $\mathbb{R}^n$, as it is generated by the integer linear combinations of the linearly independent standard basis vectors in S.

□

As a consequence, based on the fact that $\mathbb{R}^n \simeq M(n, R)$, a lattice for $M(n, R)$ is also obtained, which will be proved using Proposition 1.

Proposition 2. *Let $M(n, R)$ be a vector space over R with the standard basis $S = \{E_{11}, E_{12}, \ldots, E_{1n}, \ldots, E_{nn}\}$, where E_{ij} denotes a matrix consisting of 1 in the (i, j)-th entry and 0 elsewhere. Then, $\mathbb{Z}^{n^2}$ is a lattice in $\mathbb{R}^{n^2}$.*

Proof. Let us construct the map defined by

$$\psi : M(n, \mathbb{R}) \ni A = (a_{ij}) \mapsto v = (a_{11}, \ldots, a_{nn}) \in \mathbb{R}^{n^2}.$$

This map ψ is a vector space isomorphism, which implies that the underlying vector space is isomorphic to $\mathbb{R}^{n^2}$ and has dimension n^2. However, from Proposition 1, it is obtained that a lattice L can be constructed based on Definition 7 as

$$\begin{aligned} L &= \{p_{11}a_{11} + p_{12}a_{12} + p_{13}a_{13} + \cdots + p_{nn}a_{nn} \mid p_{ij} \in \mathbb{Z},\ 1 \leq i, j \leq n\} \\ &= \left\{ \begin{pmatrix} p_{11} \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ p_{12} \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ p_{13} \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ \vdots \\ p_{1n} \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ p_{nn} \end{pmatrix} \right| \\ &\quad p_{ij} \in \mathbb{Z},\ 1 \leq i, j \leq n\} \\ &= \left\{ \begin{pmatrix} p_{11} \\ p_{12} \\ p_{13} \\ \vdots \\ p_{nn} \end{pmatrix} \;\middle|\; p_{ij} \in \mathbb{Z},\ 1 \leq i, j \leq n \right\} = \mathbb{Z}^{n^2} \subseteq \mathbb{R}^{n^2}. \end{aligned}$$

Thus, $\mathbb{Z}^{n^2}$ is a lattice in $\mathbb{R}^{n^2}$, as it is generated by the integer linear combinations of the linearly independent standard basis vectors in S. □

The second result is stated in Proposition 3, provides lattice constructions for subspaces of the Euclidean space $\mathbb{R}^n$.

Proposition 3. *Let $\mathbb{R}^n$ be a vector space over $\mathbb{R}$ with a set*

$$S = \{e_1, e_2, \ldots, e_{n-1}\}, \quad e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

where 1 is in the i-th component and $1 \leq i \leq n-1$, which is a linearly independent set in $\mathbb{R}^n$. Let

$$V = \{(a_1, a_2, \ldots, a_{n-1}, 0) \mid a_i \in \mathbb{R}\} \subseteq \mathbb{R}^n.$$

Then, $\mathbb{Z}^{n-1} \times \{0\} \simeq \mathbb{Z}^{n-1}$ is a lattice. However, since this lattice has rank $n-1$, it is not a full-rank lattice in $\mathbb{R}^n$.

Proof. By Definition 5, S is linearly independent in $\mathbb{R}^n$. Choose $V = \operatorname{Span} S$, which is

$$V = \{(a_1, a_2, a_3, \ldots, a_{n-1}, 0) \mid a_i \in \mathbb{R}\} \subseteq \mathbb{R}^n,$$

according to Definition 2. Then, a lattice L is defined by

$$L = \{V = p_1e_1 + p_2e_2 + p_3e_3 + \cdots + p_{n-1}e_{n-1} \mid p_i \in \mathbb{Z}\}$$

$$= \left\{ \begin{pmatrix} p_1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ p_2 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ p_3 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ p_{n-1} \\ 0 \end{pmatrix} \middle| \, p_i \in \mathbb{Z} \right\}$$

$$= \left\{ \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_{n-1} \\ 0 \end{pmatrix} \middle| \, p_i \in \mathbb{Z} \right\}$$

$$= \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \times \{0\}$$

$$= \mathbb{Z}^{n-1} \times \{0\} \cong \mathbb{Z}^{n-1} \subseteq \mathbb{R}^n.$$

Thus, $\mathbb{Z}^{n-1}$ is also a lattice, as it generated by the integer linear combinations of the linearly independent standard basis vectors in S. □

Next, the discussion turns to detailed examples illustrating the process of constructing lattices in $\mathbb{R}^n$. These examples aim to demonstrate the practical application of the theoretical results presented in the preceding propositions and to provide a concrete understanding of how lattices can be systematically generated.

Example 6. In this example, it is constructed a lattice with respect to non-zero trivial subspace with standard basis in $\mathbb{R}^2$.

By Definition 1, let $\mathbb{R}^2$ be a vector space over $\mathbb{R}$. Then, choose

$$S = \left\{ \vec{v}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \vec{v}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\},$$

a standard basis of $\mathbb{R}^2$ and $V = \mathbb{R}^2 = \operatorname{span} S$. Then, the lattice is given by

$$\begin{aligned} L &= \{p_1\vec{v}_1 + p_2\vec{v}_2 \mid p_1, p_2 \in \mathbb{Z}\} \\ &= \left\{ \begin{pmatrix} p_1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ p_2 \end{pmatrix} \middle| \, p_1, p_2 \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \middle| \, p_1, p_2 \in \mathbb{Z} \right\} \\ &= \mathbb{Z}^2. \end{aligned}$$

Example 7. In this example, it is constructed a lattice with respect to non-zero trivial subspace with standard basis in $\mathbb{R}^3$.

Let $\mathbb{R}^3$ be a vector space over $\mathbb{R}$. Then, choose

$$S = \left\{ \vec{v}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \vec{v}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \vec{v}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\},$$

a standard basis of $\mathbb{R}^3$ and $V = \mathbb{R}^3 = \operatorname{span} S$. Then, the lattice L is defined by

$$\begin{aligned} L &= \{p_1\vec{v}_1 + p_2\vec{v}_2 + p_3\vec{v}_3 \mid p_1, p_2, p_3 \in \mathbb{Z}\} \\ &= \left\{ \begin{pmatrix} p_1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ p_2 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ p_3 \end{pmatrix} \middle| \, p_1, p_2, p_3 \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \middle| \, p_1, p_2, p_3 \in \mathbb{Z} \right\} \\ &= \mathbb{Z}^3. \end{aligned}$$

In addition, besides constructing lattices with respect to non-zero trivial subspaces using the standard basis in $\mathbb{R}^n$, it is also possible to construct lattices with respect to non-zero trivial subspaces using a non-standard basis. The following two examples illustrate lattices constructed with respect to non-zero trivial subspaces using non-standard basis in $\mathbb{R}^2$ and $\mathbb{R}^3$.

Example 8. In this example, it is constructed a lattice with respect to non-zero trivial subspace with non-standard basis in $\mathbb{R}^2$.

Let $\mathbb{R}^2$ be a vector space over $\mathbb{R}$. Then, choose

$$S = \left\{ \vec{v}_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \vec{v}_2 = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right\},$$

a basis of $\mathbb{R}^2$ and $V = \mathbb{R}^2 = \operatorname{span} S$. Then, the lattice L is defined by

$$\begin{aligned} L &= \{p_1\vec{v}_1 + p_2\vec{v}_2 \mid p_1, p_2 \in \mathbb{Z}\} \\ &= \left\{ \begin{pmatrix} p_1 \\ 2p_1 \end{pmatrix} + \begin{pmatrix} 2p_2 \\ 3p_2 \end{pmatrix} \middle| \, p_1, p_2 \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} p_1 + 2p_2 \\ 2p_1 + 3p_2 \end{pmatrix} \middle| \, p_1, p_2 \in \mathbb{Z} \right\}. \end{aligned}$$

Indeed $L \subseteq \mathbb{Z}^2$. To prove that $\mathbb{Z}^2$ is contained in L, let $\begin{pmatrix} k_1 \\ k_2 \end{pmatrix} \in \mathbb{Z}^2$ and let

$$\begin{aligned} \begin{pmatrix} p_1 + 2p_2 \\ 2p_1 + 3p_2 \end{pmatrix} = \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} &\iff \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} \\ &\iff \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \frac{1}{3-4} \begin{pmatrix} 3 & -2 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} \\ &= \begin{pmatrix} -3 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \end{pmatrix}. \end{aligned}$$

Therefore, it is obtained that

$$\begin{aligned} p_1 &= -3k_1 + 2k_2, \\ p_2 &= 2k_1 - k_2, \end{aligned}$$

are contained in $\mathbb{Z}$. In other words, $\begin{pmatrix} k_1 \\ k_2 \end{pmatrix} \in L$. Thus, L can

be defined by

$$L = \left\{ \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} \middle| \, k_1 = p_1 + 2p_2,\ k_2 = 2p_1 + 3p_2,\ k_1, k_2, p_1, p_2 \in \mathbb{Z} \right\} = \mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z}^2.$$

Example 9. In this example, it is constructed a lattice with respect to non-zero trivial subspace with non-standard basis in $\mathbb{R}^3$.

Let $\mathbb{R}^3$ be a vector space over R. Then, choose

$$S = \left\{ \bar{v}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \bar{v}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\},$$

a linearly independent set of vectors in $\mathbb{R}^3$ and

$$V = \left\{ \begin{pmatrix} a \\ b \\ 0 \end{pmatrix} \middle| \, a, b \in R \right\} \subseteq \mathbb{R}^3.$$

By Lemma 1, V is a subspace of $\mathbb{R}^3$ (Definition 2). Here,

$$V = \langle S \rangle = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle.$$

Then, the lattice L is defined by

$$\begin{aligned} L &= \{ p_1\bar{v}_1 + p_2\bar{v}_2 \mid p_1, p_2 \in \mathbb{Z} \} \\ &= \left\{ \begin{pmatrix} p_1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ p_2 \\ 0 \end{pmatrix} \middle| \, p_1, p_2 \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} p_1 \\ p_2 \\ 0 \end{pmatrix} \middle| \, p_1, p_2 \in \mathbb{Z} \right\} \\ &= \mathbb{Z} \times \mathbb{Z} \times \{0\} \cong \mathbb{Z}^2. \end{aligned}$$

Example 10. This example demonstrates a set that is not a lattice. Consider the set

$$A = \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} \middle| \, a \in \mathbb{R} \right\}.$$

To show that A is not a lattice, let

$$S = \left\{ \bar{v}_1 = \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right\},$$

be a linearly independent set of vectors in $\mathbb{R}^2$, and let

$$V = \{ (a, 0) \mid a \in \mathbb{R} \} \subseteq \mathbb{R}^2, \quad V = \left\langle \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right\rangle.$$

The lattice L is defined by

$$L = \{ p_1\bar{v}_1 \mid p_1 \in \mathbb{Z} \} = \left\{ \begin{pmatrix} 2p_1 \\ 0 \end{pmatrix} \middle| \, p_1 \in \mathbb{Z} \right\}.$$

Choose

$$u = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in A.$$

Equating u to an arbitrary element of L yields

$$\begin{aligned} \begin{pmatrix} 2p_1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 2p_1 &= 1 \\ p_1 &= \frac{1}{2}. \end{aligned}$$

Since $\frac{1}{2} \notin \mathbb{Z}$, it follows that $u \notin L$. This implies that the set A is not a lattice.

4. Conclusion

This paper has presented the formal construction of lattices in the Euclidean space $\mathbb{R}^n$ and its linear subspaces. The study has focused on the fundamental constructions that serve as a foundation for further research on lattices. Based on the discussion, two main conclusions can be drawn. The set $\mathbb{Z}^n$ has been proven to be a lattice in $\mathbb{R}^n$ which is shown by defining it as the set of all integer linear combinations of the standard basis vectors $\{e_1, e_2, e_3, \ldots, e_n\}$. Moreover, the set $\mathbb{Z}^{n-1} \times \{0\}$ has also been proved to be a lattice within the $(n-1)$-dimensional subspace $V = \text{Span}\{e_1, e_2, e_3, \ldots, e_{n-1}\}$. This shows how lattices can be constructed within subspaces of a lower dimension than the ambient Euclidean space.

However, this study is currently limited to Euclidean settings. To address these limitations, future research can explore applications in discrete geometry or extend these formal constructions to non-Euclidean settings to further test the generalizability of the proposed framework.

Author Contributions. **Zahira Najmatul Hayyah**: Conceptualization, writing-original draft preparation, formal analysis. **Edi Kurniadi**: Conceptualization, supervision, validation, writing-review and editing. **Anita Triska**: Supervision, writing-review and editing. All authors have reviewed and approved the final published version of this paper.

Acknowledgement. The authors acknowledge the contributions of all those who contributed in this study and the preparation of the manuscript. We extend our sincere appreciation to the editor and reviewers for their valuable insights and support in refining this paper.

Funding. This research received no external funding.

Conflict of interest. The authors declare no conflict of interest.

Data availability. Not applicable.

References

[1] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, 1st ed., Classics in Mathematics. Berlin, Heidelberg: Springer-Verlag, 1997. doi: 10.1007/978-

3-642-62035-5.
[2] P. M. Gruber, *Convex and Discrete Geometry*, 1st ed., Grundlehren der mathematischen Wissenschaften. Berlin, Heidelberg: Springer-Verlag, 2007. doi: 10.1007/978-3-540-71133-9.
[3] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Grundlehren der mathematischen Wissenschaften. New York, NY: Springer, 1999. doi: 10.1007/978-1-4757-6568-7.
[4] C. Peikert, "A decade of lattice cryptography," *Found. Trends Theor. Comput. Sci.*, vol. 10, no. 4, pp. 283–424, 2016, doi: 10.1561/0400000074.
[5] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*. New York, NY: Springer, 2002, doi: 10.1007/978-1-4615-0897-7.
[6] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*. New York, NY: Springer, 2008, doi: 10.1007/978-0-387-77993-5.
[7] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017, doi: 10.1038/nature23461.
[8] G. Alagic *et al.*, "Status report on the third round of the NIST post-quantum cryptography standardization process," NIST Interagency Rep., Sep. 2022, doi: 10.6028/NIST.IR.8413-upd1.
[9] NIST, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, Federal Information Processing Standards Publication (FIPS) 203, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2024, doi: 10.6028/NIST.FIPS.203.
[10] NIST, *Module-Lattice-Based Digital Signature Standard*, Federal Information Processing Standards Publication (FIPS) 204, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2024, doi: 10.6028/NIST.FIPS.204.
[11] V. Lyubashevsky, "Lattice-based digital signatures," *Natl. Sci. Rev.*, vol. 8, no. 9, Sep. 2021, Art. no. nwab077, doi: 10.1093/nsr/nwab077.
[12] W. Ebeling, *Lattices and Codes: A Course Partially Based on Lectures by F. Hirzebruch*, 2nd rev. ed. Wiesbaden: Vieweg, 2013.
[13] J. P. Jayaprabha and G. Srivastava, "Lattice-based cryptographic frameworks for securing 5G and 6G communication networks: A comprehensive performance analysis," *J. Emerg. Technol. Innov. Res.*, vol. 11, no. 1, pp. h790–h794, Jan. 2024. [Online]. Available: http://www.jetir.org/papers/JETIR2401796.pdf.
[14] B. Jacob, *Linear Algebra: A Study Guide and Solutions Manual for Students and Instructors*. Oxford, 1990.
[15] E. Kurniadi, E. Carnia, and H. S. Supian, *Aljabar Linear Edisi Pertama*. Bandung, Indonesia: Unpad Press, 2023. [Online]. Available: https://press.unpad.ac.id
[16] G. Baumslag, B. Fine, M. Kreuzer, and G. Rosenberger, *A Course in Mathematical Cryptography*. Berlin, Germany: De Gruyter, 2015. doi: 10.1515/9783110372779.