ON SOME DECOMPOSITIONS OF MATRICES

PEERAPHAT GATEPHAN

A Thesis Submitted to the Graduate School of Naresuan University
in Partial Fulfillment of the Requirements
for the Doctor of Philosophy Degree in Mathematics
March 2025

This thesis entitled "On some decompositions of matrices"

by Peeraphat Gatephan

has been approved by the Graduate School as partial fulfillment of the requirements for the Doctor of Philosophy Degree in Mathematics of Naresuan University

Oral Defense Committee

..... Chair

(Associate Professor Tanadon Chaobankoh, Ph.D.)

..... Advisor

(Associate Professor Kijti Rodtes, Ph.D.)

Teerapong Suksumran ..... External Examiner

(Associate Professor Teerapong Suksumran, Ph.D.)

Chakkrid Klin-eam ..... Internal Examiner

(Associate Professor Chakkrid Klin-eam, Ph.D.)

Ekkachai Laysirikul ..... Internal Examiner

(Assistant Professor Ekkachai Laysirikul, Ph.D.)

Approved

Krongkarn Chootip .....

(Associate Professor Krongkarn Chootip, Ph.D.)

Dean of the Graduate School

- 6 MAR 2025

ACKNOWLEDGEMENT

First and foremost, I am extremely grateful to my advisor, Associate Professor Kijti Rodtes, for his invaluable advice, continuous support, and patience during my Ph.D. studies. His constant guidance and feedback helped me throughout the entire research and thesis writing process.

Furthermore, I would like to thank my thesis committees, Associate Professor Tanadon Chaobankoh, Associate Professor Teerapong Suksumran, Associate Professor Chakkrid Klin-eam, and Assistant Professor Ekkachai Laysirikul for their interest in my work and their valuable comments and suggestions.

I would like to express our sincere gratitude for the financial support from the Full Scholarship Application Form for High Potential Graduate Students, Naresuan University. Additionally, I would like to thank the Department of Mathematics, Faculty of Science, Naresuan University, for facilitating places and others that are useful for support this thesis.

Finally, I would like to express my heartfelt gratitude to my parents, professors, and friends for their unwavering encouragement and support throughout my studies. They have supported me through good times and bad, making my university experience rich and wonderful. In addition, I would also like to take a moment to acknowledge myself for the determination, perseverance, and hard work that I have put into completing this thesis.

Peeraphat Gatephan

Title	ON SOME DECOMPOSITIONS OF MATRICES
Author	Peeraphat Gatephan
Advisor	Associate Professor Kijti Rodtes, Ph.D.
Academic Paper	Ph.D. Dissertation in Mathematics, Naresuan University, 2024.
Keywords	Matrices decomposition, Quadratic ring of integers, Ring with involution, Hermitian matrices, Idempotent factorization, Diophantine equations, Dieudonné determinant

ABSTRACT

This thesis investigates specific matrix decompositions within a specific algebraic structure. The research has been divided into two stages, based on algebraic structure, as follows:

For matrices over division rings, we prove that every $n \times n$ matrix over a division ring, whose center contains at least $n+2$ elements, can possibly be expressed as a product of three diagonalizable matrices. This thesis presents a necessary and sufficient condition for the decomposition of a square matrix over a division ring into a product of four Hermitian matrices and a special diagonalizable matrix. Furthermore, we demonstrate that the Dieudonné determinant of Hermitian matrices over a division ring is the commutator class that includes an element in the fixed field, which is located inside the division ring.

For matrices over the quadratic ring of integers, we present a necessary and sufficient condition for the decomposition of a specific 2×2 singular matrix into a product of two idempotent matrices in a particular form. Applying the Florida transform and Kronecker symbol, we derive a required condition for decomposing a matrix into the specific form.

LIST OF CONTENTS

Chapter Page

CHAPTER I

INTRODUCTION

In mathematics, linear algebra is a branch originating from the method of solving systems of m linear equations with n variables, such as:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m. \end{aligned} \tag{1.1.1}$$

In order to efficiently verify and solve the previously mentioned systems, matrix theory is a widely used tool for solving systems of linear equations in linear algebra. This method provides a systematic means to express the previously provided system of equations in the structure of a matrix equation as follows:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}. \tag{1.1.2}$$

This form can be succinctly expressed as the equation $Ax = b$, where A is an $m \times n$ matrix, x is an $n \times 1$ matrix, and b is an $m \times 1$ matrix. This transformation simplifies the system and facilitates the application of matrix techniques for analyzing and solving the system of linear equations. For instance, when considering an $n \times n$ invertible matrix A, it becomes evident that the system in equation (1.1.1) yields a unique solution for each variable, specifically expressed as $x = A^{-1}b$. Nevertheless, a general system of equations may consist of a system with no solutions, a system with a unique solution, or a system with infinitely many solutions. This offers a challenge for mathematicians in their efforts to develop tools that assess the feasibility of various systems of equations. One of the most powerful methods in matrix theory for solving linear systems is matrix factorization. The majority of effectively executed factorizations can be expressed as products of matrices, the characteristics for which have been extensively analyzed.

Through the application of Gauss elimination, a given matrix A can be expressed as the product of a lower triangular matrix and an upper triangular matrix (refer to Section 2.4 for further details). This process of factorization is referred to as "LU decomposition". If we can express a square $n \times n$ matrix A admit LU decomposition, then the equation $Ax = b$ can be reformulated as $LUx = b$. By defining $Ux = y := \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, the equation $Ax = b$ is transformed into $Ly = b$, corresponding to the system of variables in y. By transforming the equation $Ly = b$ into a system of linear equations, we obtain the following equations:

$$\begin{aligned} l_{11}y_1 &= b_1 \\ l_{21}y_1 + l_{22}y_2 &= b_2 \\ l_{31}y_1 + l_{32}y_2 + l_{33}y_3 &= b_3 \\ &\vdots \\ l_{n1}y_1 + l_{n2}y_2 + \cdots + l_{nn}y_n &= b_n, \end{aligned} \tag{1.1.3}$$

where $L = (l_{ij})$. The authors in [1] demonstrate that Equation (1.1.3) provides the value of y_i for each $i = 1, \ldots, n$. The value of y has been established. Therefore, the equation $Ux = y$ can also yield a solution for x.

In Section 2.4, it has been shown that not all matrices over complex numbers can be expressed as the product of a lower triangular matrix and an upper triangular matrix. In 1986, Ahmed Ramzi Sourour extended the existing restriction to non-scalar invertible matrices. He [2] proposed that any non-scalar invertible matrix can be expressed as a product of a lower triangularizable matrix and a simultaneously upper triangularizable matrix. In addition, the eigenvalues of each of these triangularizable matrices can be determined (refer to Theorem 2.4.10 for further details).

However, it is essential to recognize that not all matrices satisfy the requirements established by Sourour's theory. It is a widely accepted fact that all non-scalar invertible matrices over fields can be expressed in rational canonical form, as demonstrated in Theorem 2.4.9. In 1969 Radjavi [3] proved that any square matrix over the complex numbers can be expressed as a product of four Hermitian matrices if and only if the determinant of the matrix is a real number, utilizing

the rational canonical form of matrices. Recently, Nan and You have extended the factorization of sourour matrices by covering a particular group of matrices over division rings (referring to Theorem 3.1.2). The results inspired us to extend our investigation into the factorization of matrices over division rings.

In particular, when the matrix A in Equation (1.1.2) is an idempotent matrix ($A^2 = A$), this matrix holds significant importance in relation to Cochran's Theorem in statistics (see [4]). In [5], the authors presented numerous applications of idempotent, including its relevance to Hamilton-Jacobi-Bellman equations, dynamic optimization, the Fokker-Planck equation, and stationary Schrödinger. Applying the minimal polynomial, it can be determined that the only invertible idempotent matrix is the identity matrix. It is important to note that not every singular matrix is idempotent. However, Erdos [6] established that any singular matrix over fields can be expressed as a product of idempotent matrices (referring to Theorem 2.4.14).

For a nonsingular square matrix A, the matrix A is said to have "idempotent factorization" if it can be expressed as a product of idempotent matrices. Let us examine the scenario where the matrix A in Equation (1.1.2) is in the form $C_1C_2\cdots C_k$ where C_i is an idempotent matrix for $i = 1, 2, \ldots, k$. In this context, we can analyze the implications and properties that arise from this formulation. The following equations can be explored:

$$\begin{aligned} Ax &= b \\ C_1C_2\cdots C_kx &= b \\ (C_1)\,C_1C_2\cdots C_kx &= (C_1)\,b \\ (C_1C_1)\,C_2\cdots C_kx &= C_1b \\ C_1C_2\cdots C_kx &= C_1b \\ b &= C_1b. \end{aligned}$$

The above equations indicate that for the product of idempotent matrices $A = C_1\cdots C_k$, the equation $Ax = b$ will have a solution x_0 if and only if the condition $C_1b = b$ is satisfied.

One may also investigate the subsequent equations:

$$\begin{aligned} b &= Ax \\ &= C_1 \cdots C_{k-1} C_k x \\ &= C_1 \cdots C_{k-1} \left(C_k C_k\right) x \\ &= C_1 \cdots C_{k-1} C_k \left(C_k x\right) \\ &= A\left(C_k x\right). \end{aligned}$$

The above equations provide demonstrate that if x_0 satisfies the equation $Ax = b$, then the transformation $C_k x_0$ will also yield a solution to the equation.

In accordance with the study of idempotent factorization matrices over fields, there is a focus on the investigation of idempotent factorization matrices within specific integral domains. This includes research on Euclidean domains by Alahmadi in [7], Bézout Domains by Ruitenburg in [8], as well as unique factorization domains, projective-free domains, and PRINC domains discussed in [9] and [10]. In 2020, Cossu and Zanardo [10] researched the idempotent factorization of 2×2 column-row matrices over quadratic ring of integers. Moreover, in the same paper, they claimed that non-column-row matrices of size 2×2 can possibly be written as the product of two specific idempotent matrices (see Problem 4.1.2). This conjecture (Problem 4.1.2) inspires an investigation into the idempotent factorization of matrices over quadratic ring of integers.

This thesis has been structured as follows: Chapter II presents necessary definitions along with notations required for this thesis. We also provide some fundamental properties of matrices over division rings and the quadratic ring of integers. The literature reviews concerning the fundamental decomposition of matrices over fields are also presented in the final section of this chapter. Chapter III investigates some decomposition of matrices over division rings. In that chapter, the definition of Hermitian matrices over division rings and its Dieudonné determinant will be provided. In the last section of chapter III, we introduce enhanced methods for expressing matrix decomposition as a product of diagonalizable matrices and as a product of hermitian matrices together with a diagonalizable matrix where its Dieudonné determinant equals 1. Chapter IV explores a special class of non-column-row matrices and provides a necessary and sufficient

condition on idempotent factorization of matrices over quadratic ring of integers. Finally, Chapter V provides the conclusion of this thesis.

CHAPTER II

PRELIMINARIES

This chapter presents fundamental definitions and theorems useful to this thesis and is organized into four sections. Section 2.1 explains the definitions and basic concepts of rings, division rings, integral domains, and fields. In Section 2.2, we investigate the definition and specific properties of matrices defined over a division ring. Section 2.3 investigates the quadratic ring of integers, addressing its definitions and related concepts, such as Diophantine equations and the Kronecker symbol. Finally, Section 2.4 offers a thorough examination of existing literature concerning the fundamental theorem for the decomposition of matrices over complex numbers.

This thesis defines the fundamental mathematical symbols as follows: define the symbols $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ to denote the sets of all positive integers, integers, rational numbers, real numbers, and complex numbers, respectively. For natural numbers n and m, the set of all $n \times m$ matrices, as well as the set of all $n \times n$ matrices, with each entry being an element of the complex numbers $\mathbb{C}$, is denoted by $\mathbb{M}_{n\times m}(\mathbb{C})$ and $\mathbb{M}_n(\mathbb{C})$, respectively. Let $n \in \mathbb{N}$. The set of all $n \times 1$ matrices over the field of complex numbers $\mathbb{C}$ will be stated in the form of $\mathbb{C}^n$.

2.1 Basic Notations and Definitions

The abstract notation of abstract algebra will be the first topic that we address in the following. However, in order to simplify the process of reading, we will also provide some instances of definitions that the majority of people are probably well familiar with. The proofs and additional characteristics of the definitions discussed in this section are available in the fundamental abstract algebra textbook (refer to [11–15]).

In [11], a set is defined as a collection of objects. For instance, the set of natural numbers, represented as $\mathbb{N}$, includes the objects $1, 2, 3, \ldots$ and is formally defined as $\mathbb{N} = \{1, 2, 3, \ldots\}$. For any set S, the objects that consist of S are referred to as elements. An element x is represented as $x \in S$ when it belongs to the set S; on the other hand, if it does not belong, it is indicated as $x \notin S$. As an example, $5 \in \mathbb{N}$ whereas $-5 \notin \mathbb{N}$. An empty set is defined as a set that contains no elements, which is represented by the symbol $\emptyset$. Conversely, a set that contains at least one element is referred to as a nonempty set. Let S, T be any sets. A set T is called a subset of S if every element of T is contained within S, which is denoted as $T \subset S$; conversely, if this condition is not met, it is represented as $T \not\subset S$. The Cartesian product of S and T is the set $S \times T = \{(s, t) : s \in S \text{ and } t \in T\}$. The relation $*$ from S to T is a subset of $S \times T$ and is denoted by $s * t$ if $(s, t) \in *$; otherwise, it is denoted as $s \not* t$. A function $f : S \to T$ is a relation such that for each $s \in S$, there exists a unique $t \in T$ such that $s\, f\, t$ and denoted by $f(s) = t$. A function f is said to be **one-to-one (injective)** if the condition $f(s_1) = f(s_2)$ implies that $s_1 = s_2$ for all $s_1, s_2 \in S$. Additionally, the function f is called **onto (surjective)** if for every $t \in T$, there exists an element $s \in S$ such that $f(s) = t$. A function that acts with both one-to-one and onto properties is referred to as **bijective**. A binary operation on S can be defined as a function that maps the Cartesian product $S \times S$ to the set S. A function f is an **involution** function on a nonempty set S if $f(f(x)) = x$ for all $x \in S$. For instance, addition $(+)$ and multiplication $(\times)$ are both binary operations on $\mathbb{Z}$.

A nonempty set G together with a binary operation $*$; $(G, *)$, is said to be a **group** under the operation $*$ if it satisfies the following conditions:

(G1) $a * b \in G$ for all $a, b \in G$,

(G2) $(a * b) * c = a * (b * b)$ for all $a, b, c \in G$,

(G3) there exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$,

(G4) for any $a \in G$, there exists $b \in G$ such that $a * b = b * a = e$.

The element e in (G3) is unique and is called the identity of the group G under $*$ and the element b in (G4) is also unique and is called the inverse of a and

denoted by $b =: a^{-1}$. A group $(G, *)$ (G for short) is called an **abelian group** if the equation $a * b = b * a$ holds for all elements $a, b \in G$. For instance, $(\mathbb{Z}, +)$ is an abelian group under addition while $(\mathbb{Z}, \times)$ does not form a group. However, $\mathbb{Z}^{\times} := \mathbb{Z} \setminus \{0\}$ is not a group under multiplication. In an algebraic structure of nonempty sets S, T together with a binary operation $+_S, +_T$, respectively, a function $f : S \to T$ is called a **homomorphism** function if $f(x +_S y) = f(x) +_T f(y)$ for all $x, y \in S$. A function f is called an **automorphism** function if f is a bijective homomorphism function into itself.

In [11], a nonempty set R equipped with two binary operations, addition $+$ and multiplication $\times$; namely, $(R, +, \times) =: R$ is defined as a **ring** if it satisfies the following conditions.

(R1) $(R, +)$ is an abelian group under addition,

(R2) if $a, b \in R$, then $a \times b =: ab \in R$ (closure under multiplication),

(R3) if $a, b, c \in R$, then $(ab)\,c = a\,(bc)$ (associativity of multiplication),

(R4) if $a, b, c \in R$, then $a\,(b + c) = ab + ac$ (left distributive law),

(R5) if $a, b, c \in R$, then $(a + b)\,c = ac + bc$ (right distributive law).

Specifically, we denote the additive identity of a ring R as 0, and the additive inverse of an element a in R as $-a$. For instance, $(\mathbb{N}, +, \times)$ serves as an example of a ring. The **center** of R, denoted $Z(R)$, is defined as the set $\{z \in R : az = za \text{ for all } a \in R\}$. This set comprises all elements that commute with every element in R. A ring R is defined as a **ring with identity** if it contains a unique element, denoted by 1, such that $1a = a1 = a$ for all $a \in R$. For any ring R, it is clear that 1 and 0 belong to $Z(R)$. For elements $a, b \in R$, a divides b if there exists $c \in R$ such that $b = ac$ and denoted by $a \mid b$; otherwise, $a \nmid b$. In an algebraic structure of rings with identities R, S together with binary operations $+_R, \cdot_R$ and $+_S, \cdot_S$, respectively, a function $f : R \to S$ is called **ring homomorphism** (homomorphism for short) if $f(a +_R b) = f(a) +_S f(b)$, $f(a \cdot_R b) = f(a) \cdot_S f(b)$ and $f(1_R) = 1_S$ for all $a, b \in R$. A homomorphism f is a **ring automorphism** (automorphism for short) if f is a bijective homomorphism from

R into itself. An automorphism f of R is called an **anti-automorphism** function if $f(a \cdot_R b) = f(b) \cdot_R f(a)$ for all $a, b \in R$. Moreover, an element $a \in R$ is said to be a **unit** if there exists an element $b \in R$ such that $ab = ba = 1$. Based on the provided definition, we assign b as the **inverse** of a, represented as a^{-1}. Denote $R^\times$ the set of all units in R. For instance, the set of all unit elements in $\mathbb{Z}$ is $\{-1, 1\}$ while the set of all unit in $\mathbb{N}$ is $\{1\}$. Additionally, every nonzero element in $\mathbb{R}$ is a unit element in $\mathbb{R}$. A ring R is called a **division ring** (or **skew field**) if it holds an identity element and every nonzero element is a unit. A ring R is said to be a **commutative ring** if $ab = ba$ for all $a, b \in R$. In the context of a commutative ring with identity R, R is said to be a **field** if every nonzero element within R serves as a unit. For any nonzero element a in commutative ring R, a is said to be a **zero divisor** if there exists a nonzero element $b \in R$ such that $ab = 0$. For instance, in $\mathbb{Z}_6$, the element 3 is a zero divisor since $3 \times 2 = 0$ while 5 is not a zero divisor. A commutative ring R is defined as an **integral domain** if every nonzero element in R is not a zero divisor; that is, R contains no zero divisors. It is widely understood that every finite integral domain is actually a field. In particular, if the identity element $1 = 0$, then, $a = 1a = 0a = 0$, for any $a \in R$. This implies that $R = \{0\}$. For instance, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all examples of fields while $\mathbb{Z}$ fails to meet the criteria for a field and is rather divided as an integral domain.

Let $S \subset R$. A subset S of R is said to be a subring of R if S is a ring under the same addition and multiplication as in R. A subring I of R is said to be an **ideal** if I satisfies the absorption property; namely, $ri, ir \in I$ for all $r \in R$ and for all $i \in I$. For ideals I and J of R, the $I + J = \{i + j : i \in I, j \in J\}$ and $IJ = \{i_1j_1 + i_2j_2 + \cdots + i_nj_n : i_k \in I, j_k \in J, n \in \mathbb{N}\}$ are also ideals of R. It is true that if a unit exists in an ideal I of R, then $I = R$. The set $\langle a_1 \rangle_L = \{ra_1 : r \in R\}$ is an ideal of R and is referred to as a **left principal ideal**, with a_1 playing as the generator. Similarly, the set $\langle a_1 \rangle_R = \{a_1r : r \in R\}$ also forms an ideal of R, referred to as a **right principal ideal**, with a_1 serving as the generator. The set $\langle a_1 \rangle = \{\sum_{i=1}^{n} r_i a_1 s_i : r_i, s_i \in R, n \in \mathbb{N}\}$ is an ideal of R and is referred to as a **two sided principal ideal**, where a_1 represents the generator.

For a commutative ring R, an ideal that is generated by a single element is said to be a **principal ideal**. Additionally, for any commutative ring R, the set $\langle a_1, a_2, \ldots, a_k \rangle = \{\sum_{i=1}^{n} r_i a_i : r_i \in R, n \in \mathbb{N}\}$ is also an ideal of R and is referred to as a **finitely generated ideal**, as it is generated by $a_1, a_2, \ldots, a_k$. For instance, $\langle 2 \rangle = \{2a : a \in \mathbb{Z}\}$, which stands for the set of all even numbers, is a principal ideal of $\mathbb{Z}$.

Let R be an integral domain. An element $a \in R$ is said to be an **irreducible element** if it is a non-zero element that is not a unit and cannot be expressed as the product of two non-unit elements. For instance, in $\mathbb{Z}$, the number 8 is reducible because it can be expressed as the product of 2 and 4; namely $8 = 2 \times 4$. An element a in R is said to be a **prime element** if, for $b, c \in R$, the condition $a \mid bc$ necessitates that either $a \mid b$ or $a \mid c$ holds true. A prime element can be exemplified by a prime number within the set of integers, $\mathbb{Z}$. In complex number $\mathbb{C}$, the number 3 is not a prime element, since $3 = \left(2 + \sqrt{-5}\right)\left(2 - \sqrt{-5}\right)$. The specific class of integral domains are outlined as follows. In [16], the integral domain R is said to be a **Euclidean Domain** if there is an integer-value function defined on $K^{\times} = K \setminus \{0\}$; namely $\varepsilon : K^{\times} \to \mathbb{N} \cup \{0\}$, such that, for $a, b \in K^{\times}$,

(i) $\varepsilon(a) \leq \varepsilon(ab)$,

(ii) there exist $q, r \in K$ such that $a = bq + r$ and either $r = 0$ or $\varepsilon(r) < \varepsilon(b)$.

The definition of special class of integral domains is presented in [17]: For any integral domain R, if every ideal of R is principal, then R is said to be a **principal ideal domain**. A ring R is said to be a **Bézout domain** when every finitely generated ideal is a principal ideal. While a **Prüfer domain** is characterized by the property that every finitely generated ideal is invertible. An ideal I_1 is said to be an **invertible ideal** if there exists another ideal I_2 for which the product $I_1 I_2 = R$. An integral domain R is said to be a **unique factorization domain** if every non-zero element of R which is not a unit can be written as a finite product of irreducible elements of R. For instance, $\mathbb{Z}$ can be considered as an example of a unique factorization domain. The standard division method in integers is just formalized by the following theorem.

Theorem 2.1.1. *[18, Division Algorithm] Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then, there exist unique $q, r \in \mathbb{Z}$ such that*

$$a = bq + r \text{ and } 0 \leq r < |b|.$$

Let $a, b \in \mathbb{Z}$ be nonzero. The **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, is described as the largest positive integer that divides both a and b. For any common factor x of a and b, it follows that $c \mid \gcd(a, b)$. In order to find the greatest common divisor of any two large numbers, Euclid, a Greek mathematician, provided the algorithm for computing the greatest common divisor of two integers by using the division algorithm as the following theorem.

Theorem 2.1.2. *[19, Euclidean Algorithm] Let $a, b \in \mathbb{Z}$ be nonzero. Then, there exist unique $q_i, r_i \in \mathbb{Z}$ such that*

$$r_i = r_{i+1}q_{i+1} + r_{i+2} \text{ and } 0 < r_{i+2} < r_{i+1}$$

for $i = 0, 1, \ldots, n-2$ where $r_0 = a, r_1 = b$ and $r_{n+1} = 0$. Moreover, $\gcd(a, b) = r_n$, where r_n the last nonzero remainder from the above algorithm.

Application of the Euclidean Algorithm (Theorem 2.1.2) leads us to the subsequent theory.

Theorem 2.1.3. *[18, Extended Euclidean Algorithm] Let $a, b \in \mathbb{Z}$ be nonzero. Then, there are integers x and y such that*

$$\gcd(a, b) = ax + by.$$

On the other hand, if $\gcd(a, b) =: d \mid n$, then there exists $t \in \mathbb{Z}$ such that $n = dt$. This implies that

$$\begin{aligned} n &= dt \\ &= (ax + by)\, t \\ &= axt + byt =: aX + bY, \end{aligned}$$

where $X = xy$ and $Y = yt$. The equation $n = aX + bY$ is known as a **Linear Diophantine equation** in two variables (X and Y). The extended Euclidean algorithm indicates that the linear Diophantine equation $n = aX + bY$ has a solution if and only if $\gcd(a, b) \mid n$. In addition, if (x_0, y_0) is a solution of $n = ay + by$, then the set of all solutions is

$$\left\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x = x_0 + \frac{kb}{d}, y = y_0 - \frac{ka}{d}, \exists k \in \mathbb{Z}\right\}.$$

The following section will provide fundamental definitions in linear algebra and matrix theory. The proofs and additional properties of the definitions discussed can be located in general textbooks such as: [14, 20–22]. Let V be a nonempty set and $\mathbb{F}$ be a field. The set V is defined as a **vector space** over F if it is equipped with a binary operation of addition $+$ and a scalar multiplication $\cdot\,(\cdot : \mathbb{F} \times V \to V)$ that conforms to the following conditions:

(V1) $u + v \in V$ for all $u, v \in V$,

(V2) $cv \in V$ for all $v \in V$ and $c \in \mathbb{F}$,

(V3) $(u + v) + w = u + (v + w)$ for all $u, v, w \in V$,

(V4) $u + v = v + u$ for all $u, v \in V$

(V5) there is $0 \in V$ such that $0 + v = v$ for all $v \in V$,

(V6) for any $v \in V$, there exists $-v \in V$ such that $v + (-v) = 0$,

(V7) $c(u + v) = cu + cv$ for all $u, v \in V$ and $c \in \mathbb{F}$,

(V8) $(a + b)v = av + bv$ for all $v \in V$ and $a, b \in \mathbb{F}$,

(V9) $(ab)v = a(bv)$ for all $v \in V$ and $a, b \in \mathbb{F}$,

(V10) $1v = v$ for all $v \in V$.

The elements in V are referred to as **vectors**, while the elements in $\mathbb{F}$ are referred to as **scalars**. For instance, the set of all matrices $\mathbb{C}^n$ is a vector space over $\mathbb{C}$. Let S be a subset of V. The set S is said to be a subspace of V if it is also a

vector space over $\mathbb{F}$. The set span(S) consists of all finite linear combinations of vectors in S, defined as follows:

$$\text{span}(S) = \{a_1 s_1 + a_2 s_2 + \cdots + a_n s_n : a_i \in \mathbb{F}, v_i \in V, n \in \mathbb{N}\}.$$

It has been proven that span(S) is a subspace of V. Let $B = \{v_1, v_2, \ldots, v_n\}$ be a subset of V. The set B is said to be **linearly independent** if the equation $c_1 v_1 + \cdots + c_n v_n = 0$ holds true, then $c_i = 0$ for each i; otherwise, if this condition does not hold, then S is considered linearly dependent. If the set B is linearly independent and span$(B) = V$, then the set B is called a basis of V, and we denote the dimension of V as n, expressed as $\dim(V) = n$.

2.2 Matrices over division rings

To prevent any possibility of confusion for readers, it is important to mention that the symbol K in this thesis denotes a division ring, with its center represented as $Z(K)$ and $K^\times = K \backslash \{0\}$. An element $x \in K$ is said to be a **central element** if $xy = yx$ for all $y \in K$. For any $a \in K$, an element a is said to be a commutator element if $a = xyx^{-1}y^{-1}$ for some $x, y \in K^\times$. The **commutator subgroup** of K is the subgroup under multiplication that is generated by all commutator elements and is denoted by K^c. Denote $A = (a_{ij}) \in \mathbb{M}_{m\times n}(K)$ the matrix in the form

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

It is important to keep in mind that in a division ring K, the operation of multiplication is not restricted to the commutative property. This gap highlights the necessity of expanding the core matrix operations, as outlined in [23]: Let $A = (a_{ij}), B = (b_{ij}) \in \mathbb{M}_{m\times n}(K)$.

1. The **addition** of matrices.

   If $C = (c_{ij})$ is obtained by the sum of A and B, namely, $C = A + B$, then

   $$c_{ij} = a_{ij} + b_{ij}, \text{ for all } i, j.$$

2. The **scalar multiplication** of a matrix by an element in K.
   If $C = (c_{ij})$ is obtained by the scalar product of A by the element $c \in K$ from the left, namely $C = cA$, then

$$c_{ij} = ca_{ij}, \text{ for all } i, j.$$

   Similar, the scalar product of A by the element $c \in K$ from the right, namely, $C = Ac$, is defined as follows: $c_{ij} = a_{ij}c$ for all i, j.

3. The **multiplication** of matrices.
   Let $D = (d_{ij}) \in \mathbb{M}_{n\times l}(K)$. If $C = (c_{ij})$ is obtained by the product of A and D; namely $C = AD$, then $C \in \mathbb{M}_{m\times l}$ with

$$c_{ij} = \sum_{k=1}^{n} a_{ik}d_{kj}, \text{ for all } i, j.$$

4. The **direct sum** of matrices.
   If $C = (c_{ij})$ is obtained by the direct sum of A and B, then C is the block diagonal matrix where A and B appear as diagonal blocks, and the remaining entries are zero, namely, $C = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} =: A \oplus B$.

5. The **transpose** of a matrix.
   By interchanging rows and columns of a matrix A, we obtain the transpose of A, denote A^t as follow:

$$A^t = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}.$$

For matrices $A, B \in \mathbb{M}_n(K)$ and scalar $a \in K$, the following properties hold: $(A^t)^t = A$, $(A+B)^t = A^t + B^t$, and $(aA)^t = aA^t$. It is important to be aware that the equation $(AB)^t = B^tA^t$ generally does not hold, since the elements in K do not necessarily commute with one another in multiplicative operations. For any square matrix $X \in \mathbb{M}_n(K)$, if there is a $Y \in \mathbb{M}_n(K)$ such that $XY = YX = I_n$, then Y is referred to as the inverse of X and is represented by $Y =: X^{-1}$. Furthermore,

it can be concluded that X is an invertible matrix. For matrices $A, B \in \mathbb{M}_n(K)$, it follows that the inverse of the product is given by $(AB)^{-1} = B^{-1}A^{-1}$, and the inverse of the inverse is expressed as $(A^{-1})^{-1} = A$. Let $v_1, v_2, \ldots, v_r \in K^n$ be r rows vectors. They are called **linearly dependent** over K if there exist $a_1, a_2, \ldots, a_r \in K$ which all are not zero such that

$$a_1v_1 + a_2v_2 + \cdots + a_rv_r = 0.$$

Let $w_1, w_2, \ldots, w_r \in \mathbb{M}_{n\times 1}(K)$ be r column vectors. They are called linearly dependent over K if there exist $b_1, b_2, \ldots, b_r \in K$ which all are not zero such that

$$w_1b_1 + w_2b_2 + \cdots + w_rb_r = 0.$$

Otherwise, they are **linearly independent**. For any $A \in \mathbb{M}_{n\times m}(K)$, we define the **row rank** of A as r if A contains r linearly independent row vectors. Similarly, we define the **column rank** of A as s if A contains s linearly independent column vectors. In [23], it is shown that the row rank and column rank of matrix A are equal. The row rank and column rank of A are referred to as the **rank** of A, denoted by rank(A). Denote $\mathrm{GL}_n(K)$ the **general linear group** of degree n over K, which consists of all invertible matrices in $\mathbb{M}_n(K)$. Let $X, Y \in \mathbb{M}_{m\times n}(K)$ be matrices. The matrices X and Y are defined to be **equivalent** if there exist matrices $P \in \mathrm{GL}_m(K)$ and $Q \in \mathrm{GL}_n(K)$ such that

$$X = PYQ.$$

It is not hard to see that two matrices are equivalent if and only if they have the same rank. Furthermore, for any matrix $A \in \mathbb{M}_{m\times n}(K)$ with rank r, the matrix A is equivalent to $\begin{pmatrix} I_r & \\ & 0_{m-r\times n-r} \end{pmatrix}$. In [23], they also showed that the $n \times n$ matrix A is invertible if and only if the condition rank$(A) = n$ holds. Let $a \in K$ and let $\pi \in S_n$ be a permutation. In this thesis, we define the following matrices for consistent use throughout the contents of the thesis.

1. $E_{ij}(a)$ is the matrix that is obtained by substituting a for the ij entry in the identity matrix of size n,

2. P_π is a matrix obtained by permuting the rows of the identity matrix according to the permutation π of the number 1 to n; namely $P_\pi = (\delta_{i,\pi(j)})$ where δ is the Kronecker delta symbol.

The following propositions relate to the two matrices discussed above.

Proposition 2.2.1. *[24] Let $a, b \in K$ and $\pi, \sigma \in S_n$. Then, for $i, j \in \mathbb{N}$,*

1. $E_{ij}(a)E_{ij}(b) = E_{ij}(a+b)$.
2. $E_{ij}(0) = I_n$.
3. $(E_{ij}(a))^{-1} = E_{ji}(-a)$.
4. $P_\pi P_\sigma = P_{\pi\sigma}$.
5. $(P_\pi)^{-1} = p_{\pi^{-1}} = (P_\pi)^t$.

Lemma 2.2.2. *[24] Let $A = (a_{ij}) \in \mathbb{M}_n(K), a \in K$ and $\pi \in S_n$. Then, for $i \neq j$, the following are transforming from A by $E_{ij}(a)$ and P_π.*

1. *$E_{ij}(a)A$ is a matrix that applies the left multiple of a from the $j-$th row to the $i-$th row;*
2. *$AE_{ij}(a)$ is a matrix that applies the right multiple of a from the $i-$th column to the $j-$th column;*
3. *$P_\pi A$ $\left(A(P_\pi)^{-1}\right)$ is a matrix that applies moving the $i-$th row (column) into the position $\pi(i)-$th row (column).*

Let $A, B \in \mathbb{M}_n(K)$. In [25], the matrices A and B are **conjugate (similar)** if there exists $X \in \mathrm{GL}_n(K)$ such that $A = XBX^{-1}$. A matrix $A \in \mathbb{M}_n(K)$ is said to be a **diagonalizable matrix** if A is conjugate to a diagonal matrix; namely, there exists $X \in \mathrm{GL}_n(K)$ such that $A = XDX^{-1}$ where $D = \mathrm{diag}(a_1, \ldots, a_n)$ is a diagonal matrix. For any square matrix $A \in \mathbb{M}_n(K)$, A is said to be a central matrix if $AX = XA$ for all $X \in \mathbb{M}_n(K)$.

Theorem 2.2.3. *(cf. [26]) Let $A \in \mathbb{M}_n(K)$ be a central matrix. Then, $A = aI_n$ for some $a \in Z(K)$.*

Proof. Let $A = (a_{ij})$ be a central matrix in $\mathbb{M}_n(K)$. Then, $AX = XA$ for all $X \in \mathbb{M}_n(K)$. Since $E_{ii}(x)A = AE_{ii}(x)$ for $1 \leq i \leq n$ and for any $x \in K$, we have that a_{ii} is a central element in $Z(K)$ for all $i = 1, \ldots, n$. Let $D_k = (d_{ij}) \in \mathbb{M}_n(K)$ be a diagonal matrix with $d_{kk} = 1$ and zero otherwise. Since $D_kA = AD_k$ for all $k = 1, \ldots, n$, we have that A is a diagonal matrix. Moreover, for $1 \leq i, j \leq n$, $AE_{ij}(1) = E_{ij}(1)A$ implies that $a_{ii} = a_{jj}$ and hence, $A = aI_n$ for some $a \in Z(K)$. □

The following section outlines the fundamental concepts of the definition of determinant for matrices over division rings. For matrices over commutative rings R with identity 1_R, the determinant is the unique alternating R-multilinear form that sends I_n to 1_R. For matrices over non-commutative rings, a generalization of the determinant of matrices over division rings was proposed by Dieudonné [27] in 1943. The following theorems are necessary to define a determinant function on matrices over a division ring.

Theorem 2.2.4. *[24, Bruhat normal form] Let K be a division ring and $A \in \mathrm{GL}_n(K)$. Then, there exists a unique diagonal matrix D and a unique $\pi \in S_n$ such that*

$$A = LDP_\pi U,$$

where L is a lower triangular matrix and U is an upper triangular matrix with 1 as its diagonal entries, $D = \mathrm{diag}(u_1, \ldots, u_n)$ with $u_i \in K^\times$.

Based on Theorem 2.2.4, the following definition is defined:

Definition 2.2.5. [24] Let K be a division ring. The function $\delta et : \mathbb{M}_n(K) \to K$ defined by

$$\delta et(A) := \begin{cases} 0 & \text{if } A \notin GL_n(K) \\ sgn(\pi) \prod_{i=1}^{n} u_i \neq 0 & \text{if } A \in GL_n(K), \end{cases}$$

where u_i's are the (non-vanishing) diagonal elements of the matrix D and π is the permutation of the Bruhat normal form of A.

According to Theorem 1.6 in [28], this function is zero for all singular matrices in $\mathbb{M}_n(K)$. It is sufficient for determining the determinant for matrices in $GL_n(K)$. It is important to note that this determinant function requires the multiplicative property, specifically that $\det(AB) = \det(A)\det(B)$ holds for all $A, B \in \mathbb{M}_n(K)$. Let $a_1, a_2, b_1, b_2 \in K^\times$ and let $A = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}, B = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} \in \mathbb{M}_2(K)$. Through direct calculation, we have that $AB = \begin{pmatrix} a_1b_1 & 0 \\ 0 & a_2b_2 \end{pmatrix}$. According to Definition 2.2.5, it follows that $\delta et(A) = a_1a_2$, $\delta et(B) = b_1b_2$, and $\delta et(AB) = a_1b_1a_2b_2$. We observed that, in general, $\delta et(A)\delta et(B) \neq \delta et(AB)$, due to the non-commutative structure of K. However, by the simple calculation, it is evident that

$$\begin{aligned} a_1a_2b_1b_2 &= a_1\left(b_1a_2a_2^{-1}b_1^{-1}\right)a_2b_1b_2 \\ &= a_1b_1a_2\left(a_2^{-1}b_1^{-1}a_2b_1\right)b_2 \\ &= a_1b_1a_2C_1b_2 \\ &= a_1b_1a_2\left(b_2C_1C_1^{-1}b_2^{-1}\right)C_1b_2 \\ &= a_1b_1a_2b_2\left(C_1C_2\right), \end{aligned}$$

where $C_1 = a_2^{-1}b_1^{-1}a_2b_1, C_2 = C_1^{-1}b_2^{-1}C_1b_2$ are commutator elements in K; namely, $C_1, C_2 \in K^c$. The determinant function of matrices over a division ring, particularly the **Dieudonné determinant**, functions as a group surjective homomorphism expressed as

$$\mathrm{Det} : \mathrm{GL}_n(K) \to \left[K^\times\right] := K^\times/K^c$$

which is induced by the function δet as outlined in Definition 2.2.5 (see Definition 3 (page 135) in [24] for further information). So, for $A \in \mathrm{GL}_n(K)$, we denote $\mathrm{Det}(A) = \{ax : x \in K^c\} =: [a]$ for some $a \in K^\times$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$. If $a \neq 0$, then we have

$$\begin{aligned} A &= \begin{pmatrix} a & 0 \\ c & d - ca^{-1}b \end{pmatrix}\begin{pmatrix} 1 & -a^{-1}b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ ca^{-1} & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d - ca^{-1}b \end{pmatrix}\begin{pmatrix} 1 & -a^{-1}b \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Consequently, $\mathrm{Det}(A) = [a\,(d - ca^{-1}b)] = [ad - aca^{-1}b]$. If $a = 0$, then

$$A := \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & 0 \\ d & c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 \\ db^{-1} & 1 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Consequently, $\mathrm{Det}(A) = [-bc]$. The Dieudonné determinants had been extensively investigated in [28]. The following is a list of properties that we will use in our thesis (see the details and proofs in [28]):

Proposition 2.2.6. *Let $A, B \in \mathbb{M}_n(K)$.*

(D1) The Dieudonné determinant is a multiplicative function; namely, $\mathrm{Det}(AB) = \mathrm{Det}(A)\,\mathrm{Det}(B)$, *for* $A, B \in \mathbb{M}_n(K)$.

(D2) The Dieudonné determinant of any singular matrix is identically 0.

(D3) The Dieudonné determinant is invariant under elementary row (column) operations.

(D4) $\mathrm{Det}\,(A \oplus B) = [ab]$ *for* $A \in \mathbb{M}_m(K), B \in \mathbb{M}_n(K)$ *with* $\mathrm{Det}(A) = [a]$ *and* $\mathrm{Det}(B) = [b]$ *for some* $a, b \in K^\times$.

(D5) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$. $\mathrm{Det}(A) = \begin{cases} [ad - aca^{-1}b] & \text{if } a \neq 0, \\ [-bc] & \text{if } a = 0. \end{cases}$

For matrices $A \in \mathbb{M}_r(K)$ and $B \in \mathbb{M}_s(K)$ with $\mathrm{Det}(A) = [a]$ and $\mathrm{Det}(B) = [b]$ for some $a, b \in K^\times$, it can be observed that $A \oplus B = (A \oplus I)\,(I \oplus B)$. According to Theorem 3.16 in [28], Brenner showed that $\mathrm{Det}(I \oplus B) = [b]$. In addition, the author [28] provided that $\mathrm{Det}(A \oplus B) = [\pm ab]$ where the factor ± 1 indicates the sign of a permutation from the factorization of $A \oplus I$ and $I \oplus B$ as a product of elementary matrices. However, the factor ± 1 is in fact only 1, since we can apply a similarity to transform $A \oplus I$ into $I \oplus A$; namely, $Y^{-1}\,(A \oplus I_s)\,Y = (I_s \oplus A)$ where $A \in \mathbb{M}_r(K)$ and $Y = \begin{pmatrix} 0 & I_r \\ I_s & 0 \end{pmatrix}$. By applying Lemma 3.14 in [28] which

asserts that $\mathrm{Det}\,(I_s \oplus A) = \mathrm{Det}(A)$ and the multiplicative property of Dieudonné determinant, Proposition 2.2.6 (D4) is obtained.

Let $L = (l_{ij}) \in \mathrm{GL}_n(K)$ be a lower triangular matrix. Consequently, l_{ii} is a non-zero element for every $i = 1, \ldots, n$. By applying Theorem 2.2.4, we identify that $L = \widetilde{L}D$, where $\widetilde{L}$ is a lower triangular matrix with all diagonal entries equal to 1, and $D = \mathrm{diag}(l_{11}, l_{22}, \ldots, l_{nn})$. By Definition 2.2.5, we have that $\delta et(L) = \prod_{i=1}^{n} l_{ii}$. Thus, $\mathrm{Det}(L) = [l_{11}l_{22}\cdots l_{nn}]$, representing the commutator class that refers to the product of all diagonal entries of L. Similarly, for any upper triangular matrix $U = (u_{ij}) \in \mathbb{M}_n(K)$, $\mathrm{Det}(U) = [u_{11}u_{22}\cdots u_{nn}]$.

2.3 Quadratic ring of integers

In mathematics, the complex numbers have a complex structure. They are both an algebraically closed field (every nonzero polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$) and a commutative algebra over $\mathbb{R}$. Additionally, each rational number $\frac{a}{b}$, for $a, b \in \mathbb{Z}$ with $b \neq 0$, is algebraic since it is a root of a polynomial $bx - a = 0$. Also, $\pm\sqrt{2}$ are algebraic over $\mathbb{R}$, since they are roots of $x^2 - 2 = 0$. The following is the definition of special numbers in complex numbers.

Definition 2.3.1. [29] Let $a \in \mathbb{C}$. Then,

- a is said to be an **algebraic number** if it is a root of a polynomial equation whose coefficients are integers,
- a is said to be an **algebraic integer** if it is a root of a monic polynomial whose coefficients are integers,
- a is said to be a **quadratic number** if it is a root of a polynomial of degree two whose coefficients are integers,
- a is said to be a **quadratic integer** if it is a root of a monic polynomial of degree two whose coefficients are integers.

In [30], many elements of the complex quadratic numbers are collected as follows: Let $D \in \mathbb{Z} \setminus \{0, 1\}$ be a square-free integer. Then, the set

$$\mathcal{K} := \mathbb{Q}\left(\sqrt{D}\right) = \left\{a + b\sqrt{D} : a, b \in \mathbb{Q}\right\}$$

is called a **quadratic number field**. In particular, we refer to a real quadratic number field if $D > 0$ and an imaginary quadratic number field if $D < 0$. Let $\alpha = a + b\sqrt{D} \in \mathcal{K}$. Then, in [30], α is a root of $P_\alpha(x) = x^2 - 2ax + a^2 - Db^2 \in \mathbb{Q}[x]$. It is straightforward to confirm that $\alpha' = a - b\sqrt{D}$ serves as a root of $P_\alpha(x)$ as well. Furthermore, α' has been identified as the **conjugate** of α. The following maps are defined on $\mathcal{K}$. Let $\alpha = a + b\sqrt{D} \in \mathcal{K}$ where D is a square-free integer. In [30], the expression for the **norm** of α is given by $\|\alpha\| = \alpha\alpha' = a^2 - Db^2$. The **trace** of α is given by $\mathrm{Tr}_{\mathcal{K}}(\alpha) = \alpha + \alpha' = 2a$. The **discriminant** of α is defined as $\mathrm{dics}(\alpha) = (\alpha - \alpha')^2 = 4Db^2$. For instance, the conjugate, the norm and the discriminant of $\alpha = 2 + \sqrt{3} \in \mathbb{Q}\left(\sqrt{3}\right)$ are

$$\begin{aligned}
\alpha' &= 2 - \sqrt{3}, \\
\|\alpha\| &= \alpha\alpha' = \left(2 + \sqrt{3}\right)\left(2 - \sqrt{3}\right) = 2^2 - 3 = 1, \\
\mathrm{Tr}_{\mathcal{K}}(\alpha) &= \alpha + \alpha' = \left(2 + \sqrt{3}\right) + \left(2 - \sqrt{3}\right) = 4, \\
\mathrm{disc}(\alpha) &= 4\,(3)\,(1^2) = 12,
\end{aligned}$$

respectively. Then, the subsequent property was obtained through direct computation.

Proposition 2.3.2. *[30] Let $\alpha, \beta \in \mathcal{K}$. Then, we have*

1. $\|\alpha\beta\| = \|\alpha\| \cdot \|\beta\|$.
2. $\mathrm{Tr}_{\mathcal{K}}(\alpha + \beta) = \mathrm{Tr}_{\mathcal{K}}(\alpha) + \mathrm{Tr}_{\mathcal{K}}(\beta)$.
3. $\|\alpha\| = 0$ *if and only if* $\alpha = 0$.
4. $\mathrm{disc}(\alpha) = 0$ *if and only if* $\alpha \in \mathbb{Q}$.

The set of all integral elements in $\mathcal{K}$, namely, the **quadratic ring of integer** $\mathcal{O}_{\mathcal{K}}$ of a quadratic number field $\mathcal{K}$, can be expressed explicitly depending on D as the following theorem.

Theorem 2.3.3. *[30] The integral elements in $\mathcal{K}$ are given by*

$$\mathcal{O}_{\mathcal{K}} = \begin{cases} \left\{a + b\sqrt{D}\right\} & \text{if } D \equiv 2,3 \pmod 4, \\ \left\{\frac{a+b\sqrt{D}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\} & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

In particular, $\mathcal{O}_{\mathcal{K}}$ is an integral domain.

For each $\alpha = a+b\sqrt{D} \in \mathcal{O}_{\mathcal{K}}$, the norm $\|\alpha\| = a^2 - Db^2$ operates as a Euclidean function. It has been established in [12] for negative integers and in [31] for positive integers that $\mathcal{O}_{\mathcal{K}}$ is a Euclidean domain for the values

$$D = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Furthermore, it is demonstrated in [32] that no other ring of quadratic integers exists that is Euclidean with the norm providing as a Euclidean function. For each $\alpha = a + b\sqrt{D} \in \mathcal{O}_{\mathcal{K}}$, it is understood that $\|\alpha\| = a^2 - Db^2$. On the other hand, when we establish a square-free integer D and indicate specific integers $\|\alpha\| =: N$, the challenge of determining the existence of integers $a, b \in \mathbb{Z}$ that satisfy the equation $a^2 + b^2D = N$ reduces to addressing a specific type of Diophantine equation, referred to as **generalized Pell's equations**. A necessary condition for the solvability of generalized Pell's equations is outlined below.

Lemma 2.3.4. *[33] If the equation $x^2 - Dy^2 = N$ has a solution $x, y \in \mathbb{Z}$, then $u^2 \equiv D \pmod{Q_0}$ has a solution where $Q_0 = |N|$.*

In number theory, the Legendre symbol is defined as a function that can be represented in the following. Let p be an odd prime integer and $a \in \mathbb{Z}$. In [30], the Legendre symbol of a and p defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is congruent to a perfect square modulo } p \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not congruent to any perfect square modulo } p \\ 0 & \text{if } a \equiv 0 \pmod p. \end{cases}$$

The **Kronecker symbol** serves as a generalization of the Legendre symbol for all integers, and it can be expressed as follows.

Definition 2.3.5. Let $a, b \in \mathbb{Z}$. The Kronecker symbol of a and b is

$$\left(\frac{a}{b}\right) = \begin{cases} 1 & \text{if } a \text{ is congruent to a perfect square modulo } b, \\ -1 & \text{if } a \text{ is not congruent to any perfect square modulo } b, \\ 0 & \text{if } a \equiv 0 \pmod{b}. \end{cases}$$

From the aforementioned definitions and Lemma 2.3.4, we derive the following necessary instruments.

Lemma 2.3.6. *Let $N, D \in \mathbb{Z}$ which D is square-free. If $\left(\frac{D}{|N|}\right) = -1$, then the equation $x^2 - Dy^2 = N$ has no integer solutions.*

The subsequent are the fundamental properties about the Kronecker symbol.

Proposition 2.3.7. *[34] Let $p, q \in \mathbb{Z}$. Then, the following statements are true.*

1. $\left(\frac{-1}{q}\right) = 1$ *if and only if* $q = 4n + 1$.
2. $\left(\frac{2}{q}\right) = 1$ *if and only if* $q = 8n \pm 1$.
3. *For any odd prime* q, $\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \pmod{q}$. *(Euler's criterion)*
4. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ *(quadratic reciprocal law).*

2.4 Literature Review

This section presents the standard factorization of matrices over complex numbers, as documented in various textbooks, including [14, 21, 22]. In this section, we define $\overline{\cdot}$ to represent the complex conjugate of the complex number $\mathbb{C}$, the operation $*$ to denote the conjugate transpose operator of a complex matrix, and the scalar function $\det : \mathbb{M}_n(\mathbb{C}) \to \mathbb{C}$ as the standard determinant function for matrices over complex numbers. A matrix $A \in \mathbb{M}_n(\mathbb{C})$ is defined as nonsingular if there exists a matrix $B \in \mathbb{M}_n(\mathbb{C})$ such that the equation $AB = BA = I_n$ holds true; otherwise, it is singular. Let us denote $\mathrm{GL}_n(\mathbb{C})$ as the collection of nonsingular $n \times n$ matrices over $\mathbb{C}$. Additionally, we will identify $\mathrm{SL}_n(\mathbb{C})$ as the subgroup

consisting of nonsingular matrices that possess a determinant equal to 1. We will begin by recalling the fundamental definitions of various types of matrices, for any $A = (a_{ij}) \in \mathbb{M}_n(\mathbb{C})$,

- A is a diagonal matrix if $a_{ij} = 0$ for all $i \neq j$.
- A is a scalar matrix if $a_{ii} = a$ for some $a \in \mathbb{C}$ and $a_{ij} = 0$ for all $i \neq j$.
- A is a normal matrix if $AA^* = A^*A$,
- A is a hermitian matrix if $A = A^*$,
- A is a positive semidefinite (PSD) matrix if $x^*Ax \geq 0$ for all $x \in \mathbb{C}^n$,
- A is a positive definite (PD) matrix if $x^*Ax > 0$ for all nonzero vector $x \in \mathbb{C}^n$,
- A is a unitary matrix if $AA^* = A^*A = I_n$,
- A is a symmetric matrix if $A^t = A$,
- A is an orthogonal matrix if $A^tA = AA^t = I_n$.
- A is an idempotent matrix if $A^2 = A$.
- A is an involution matrix if $A^2 = I_n$.
- A is a nilpotent matrix if $A^k = 0$ for some $k \in \mathbb{N}$.
- A is a unipotent matrix if $(A - I_n)^k = 0$ for some $k \in \mathbb{N}$.

Let $A \in \mathbb{M}_n(\mathbb{C})$. A nonzero vector $x \in \mathbb{C}^n$ is said to be an **eigenvector** of A corresponding to the **eigenvalue** $\lambda \in \mathbb{C}$ if $Ax = \lambda x$. In matrix factorization, one decomposition that explicates important features, such as the eigenvalues and eigenvectors of the matrix, is the diagonalizability. The matrix A is said to be a **diagonalizable** matrix if A is similar to a diagonal matrix; namely, there exists

$X \in \mathbb{M}_n(\mathbb{C})$ such that

$$X^{-1}AX = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix} =: \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n), \tag{2.4.1}$$

for some $\lambda_i \in \mathbb{C}$. Furthermore, for each column vector v_i of the matrix X, v_i is an eigenvector corresponding to eigenvalue λ_i. In general, not all square matrices are diagonalizable. The necessary and sufficient condition that delineates the diagonalizability of a matrix, as stated in [14], is that a matrix $A \in \mathbb{M}_n(\mathbb{C})$ is diagonalizable if and only if there exists a basis for $\mathbb{C}^n$ formed completely of eigenvectors of A. In particular, when the matrix X in the Equation (2.4.1) is a unitary matrix, the decomposition is said to be unitary diagonalizable. For any $A \in \mathbb{M}_n(\mathbb{C})$, a matrix A is said to be a **unitary diagonalizable** matrix if there exists a unitary matrix $U \in \mathrm{GL}_n(\mathbb{C})$ such that

$$A = UDU^*$$

where $D = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ for some $\lambda_i \in \mathbb{C}$. A unitary diagonalizable matrix can be exemplified by a set of all normal matrices, as outlined in the subsequent theorem:

Theorem 2.4.1. *[22, Spectral Decomposition] Let $A \in \mathbb{M}_n(\mathbb{C})$ with all eigenvalues $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$. Then,*

A is a normal matrix if and only if $A = UDU^*$,

where $U \in \mathbb{M}_n(\mathbb{C})$ is a unitary matrix and $D = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$. In particular,

A is a Hermitian matrix if and only if A is normal and λ_i are real numbers

and

A is a PD (PSD) if and only if A is Hermitian and λ_i are positive (nonnegative)

for all $i = 1, \ldots, n$.

According to the aforementioned theory, by extracting the square root of the eigenvalue λ_i of a Hermitian matrix A, we would observe that

$$\begin{aligned} A &= U^*DU \\ &= U^*\left(\sqrt{D}\right)^2 U \\ &= U^*\sqrt{D}\sqrt{D}U \\ &= U^*\sqrt{D}\left(UU^*\right)\sqrt{D}U \\ &= \left(U^*\sqrt{D}U\right)\left(U^*\sqrt{D}U\right) \\ &= \left(U^*\sqrt{D}U\right)\left(U^*\sqrt{D}U\right) =: B^2. \end{aligned}$$

Assuming that A is Hermitian, according to Theorem 2.4.1, all λ_i are real, and hence, $\sqrt{\lambda_i}$ is also real. Based on Theorem 2.4.1, we can conclude that B is a Hermitian matrix. Applying the similar procedure to a positive semidefinite matrix and a positive definite matrix yields the subsequent result.

Theorem 2.4.2. *[22, Uniqueness of Square Root] Let* $A \in \mathbb{M}_n(\mathbb{C})$. *If* A *is a Hermitian matrix, a positive definite matrix, or a positive semidefinite matrix, then there exists a unique Hermitian matrix, a positive definite matrix, or a positive semidefinite matrix, respectively,* $B \in \mathbb{M}_n(\mathbb{C})$ *such that* $A = B^2$.

In this context, the matrix B in Theorem 2.4.1 is referred to as the **square root** of A and is denoted by $A^{\frac{1}{2}}$. For any matrix $A \in \mathbb{M}_n(\mathbb{C})$, it is straightforward to observe that A^*A is a positive semidefinite matrix. According to Theorem 2.4.1, all eigenvalues of A^*A are nonnegative real numbers. Consequently, for each i, $\sqrt{\lambda_i(A^*A)}$ is defined as a **singular value** of A and is denoted by $\sigma_i(A)$. The following decomposition has been well-known in linear algebra.

Theorem 2.4.3. *[22, Singular Value Decomposition] Let* $A \in \mathbb{M}_{m\times n}(\mathbb{C})$ *with nonzero singular value* $\sigma_1, \ldots, \sigma_r$. *Then, there exists unitary matrix* $U \in \mathbb{M}_n(\mathbb{C})$ *and unitary matrix* $V \in \mathbb{M}_n(\mathbb{C})$ *such that*

$$A = U \begin{pmatrix} D_r & 0 \\ 0 & 0 \end{pmatrix} V,$$

where $D_r = \mathrm{diag}(\sigma_1, \ldots, \sigma_r,)$ *and the block matrix is of size* $m \times n$.

In particular, when $A \in \mathbb{M}_n(\mathbb{C})$, both U and V are unitary matrices of size $n \times n$. Then, we have

$$A = UDV = U(VV^*)DV = (UV)(V^*DV) =: WP,$$

where W is unitary matrix and P is positive semidefinite, as will be demonstrated in the following theorem.

Theorem 2.4.4. *[22, Polar Decomposition] Let $A \in \mathbb{M}_n(\mathbb{C})$. Then,*

$$A = WP = P^*V,$$

for some positive semidefinite matrix P and unitary matrices W, V.

Moreover, this theorem suggests that, for any $A \in \mathbb{M}_n(\mathbb{C})$,

"A is a product of two normal matrices".

The decomposition of matrices into a product of Hermitian matrices was introduced by Heydar Radjavi in 1968, as the following theorem:

Theorem 2.4.5. *[3] Let $A \in \mathbb{M}_n(\mathbb{C})$. Then,*

A is a product of four Hermitian matrices if and only if $\det(A)$ *is real.*

The key instrument for demonstrating Theorem 2.4.5, as outlined in [3], as the following theorem.

Theorem 2.4.6. *[3] Let $A \in \mathbb{M}_n(\mathbb{F})$. Then,*

A is a product of two symmetric matrices over $\mathbb{F}$.

The next results relate to the decomposition of matrices into a product of positive definite (or semidefinite) matrices.

Theorem 2.4.7. *[35, 36] Let $A \in \mathbb{M}_n(\mathbb{C})$. Then,*

1. *A is a product of four positive definite matrices if and only if* $\det(A) > 0$ *and A is not a scalar aI_n where $a \leq 0$.*
2. *A is a product of five positive definite matrices if and only if* $\det(A) > 0$.

However, Taussky [37] established the necessary and sufficient condition for decomposing any matrix into a product of two positive semidefinite matrices: for any $A \in \mathbb{M}_n(\mathbb{C})$, A can be expressed as a product of two positive semidefinite matrices if and only if A is diagonalizable and possesses nonnegative eigenvalues. Furthermore, the following findings were made public by Wu in 1988. In [38], Wu established that the following propositions are equivalent: for any $A \in \mathbb{M}_n(\mathbb{C})$,

1. $A = XY$ for some positive semidefinite matrices X, Y,
2. $A = XY$ for some positive definite matrix X and positive semidefinite matrix Y,
3. A is similar to a nonnegative matrix.

In the same paper, Wu additionally provided that, for any singular matrix A,

$$A \text{ is a product of four nonnegative matrices,}$$

and four is the smallest such number.

It is important to note that not every square matrix possesses the property of diagonalizability. Nonetheless, every matrix defined over the complex numbers has a **Jordan canonical form**. For any $\lambda \in \mathbb{C}$, a matrix $J_n(\lambda) \in \mathbb{M}_n(\mathbb{C})$ is defined as a Jordan block if

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}.$$

The theorem presented in [22] articulates that:

Theorem 2.4.8. *Let $A \in \mathbb{M}_n(C)$. Then, there exists a matrix $P \in \mathrm{GL}_n(\mathbb{C})$ such that*

$$PAP^{-1} = J_{n_1}(\lambda_1) \oplus \cdots \oplus J_{n_r}(\lambda_r),$$

where $n_1 + \cdots + n_r = n$ and λ_i represent the eigenvalues of A.

To investigate matrices with characteristic polynomials that split, it is possible to derive the Jordan canonical form of a matrix over a splitting field, where each polynomial can be expressed as a product of linear factors (in the form $x - a$ for some element a in a field). In general, a polynomial does not have to be expressed as a product of linear factors, and additionally, matrices are not required to have eigenvalues. However, for any matrix $A \in \mathbb{M}_n(\mathbb{F})$, the characteristic polynomial $f(x)$ of the matrix A factors uniquely as $f(x) = (-1)^n (\phi_1(x))^{n_1} \cdots (\phi_k(x))^{n_k}$, where the $\phi_i(x)$ are all distinct irreducible monic polynomials for $1 \leq i \leq k$ and $n_1 + \cdots + n_k = n$. For $a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}$, the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{k-1} \end{pmatrix}$$

is called the **companion matrix** of the monic polynomial $x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$. For a field that is not a splitting field, every square matrix over the field possesses a rational canonical form, as stated in the following theorem from [22]:

Theorem 2.4.9. *[22] Every matrix over fields is similar to a direct sum of companion matrices.*

The previously mentioned theorems highlight the decomposition of matrices via the application of eigenvalues, eigenvectors, or the characteristic polynomial. In mathematics, the lower-upper (LU) decomposition involves factoring a square matrix into the product of a lower triangular matrix and an upper triangular matrix; specifically, a matrix A admits LU decomposition if $A = LU$ for some a lower triangular matrix L and an upper triangular matrix U. It is important to

note that certain matrices cannot be represented as the product of L and U. For instance, we now assume that there exist $a, b, c, d, e, f \in \mathbb{C}$ such that

$$S := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}.$$

By direct calculation, we have that

$$\begin{aligned} 0 &= ad \\ 1 &= ae \\ 1 &= bd \\ 0 &= be + cf. \end{aligned}$$

Given that $ad = 0$, it follows that either $a = 0$ or $d = 0$. If $a = 0$, this leads to a contradiction, as it implies $1 = ae = 0$. Likewise, if $d = 0$, it presents a contradiction that $1 = bd = 0$. Therefore, it can be concluded that S cannot allow LU decomposition. In 1986, Sourour [2] generated unexpected progress by expanding the LU decomposition for applying to any nonsingular matrices over fields in the following form:

Theorem 2.4.10. *[2] Let $A \in \mathbb{M}_n(\mathbb{F})$ be a non-scalar invertible matrix over a field $\mathbb{F}$ and let $a_i, b_i \in \mathbb{F}$, for $1 \leq i \leq n$, such that $\det(A) = \prod_{i=1}^{n} a_i b_i$. There exist matrices $B, C \in \mathbb{M}_n(\mathbb{F})$ with eigenvalues $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, respectively, such that $A = BC$. Additionally, matrices B and C can be determined such that B is lower triangularizable and C is simultaneously upper triangularizable.*

Furthermore, Theorem 2.4.10 can be applied in presenting several matrix factorizations, such as Ballantine's theorem in Theorem 2.4.7. Applying Theorem 2.4.10, he further established the conclusion presented in [39] which asserts that for every matrix $A \in \mathbb{M}_n(\mathbb{F})$ with $\det(A) = 1$,

A is a product of three unipotent matrices.

Additionally, he reproved the decomposition presented in [39], demonstrating that

if A is a nonsingular matrix, then A is a product of two unipotent matrices.

For a field $\mathbb{F}$, the collection of commutator elements of matrices over the field $\mathbb{F}$ is $\{XYX^{-1}Y^{-1} : X, Y \in \mathrm{GL}_n(\mathbb{F})\}$. Moreover, Theorem 2.4.10 can be utilized to substantiate the following assertions, as outlined in [40–42] as follows: Let $A \in \mathrm{SL}_n(\mathbb{F})$. Consequently, the subsequent statements hold true.

1. If $\mathbb{F}$ has at least $n+1$ elements, then A is a commutator of matrices in $\mathrm{GL}_n(\mathbb{F})$.
2. If $\mathbb{F}$ has at least $n+2$ elements and A is a non-scalar matrix, then A is a commutator of matrices in $\mathrm{SL}_n(\mathbb{F})$.
3. If $\mathbb{F}$ has at least $n+3$ elements and A is a non-scalar matrix, then A is a commutator of matrices with arbitrarily prescribed nonzero elements.

In the same paper, he [2] presented a novel proof of the matrix decomposition originally provided in [43] as follows: Let $\mathbb{F}$ be a field containing at least $n+2$ elements, and let $A \in \mathbb{M}_n(\mathbb{F})$. It follows that,

if $\det(A) = \pm 1$, then A is a product of at most four involution matrices.

The reviews indicate that a widely accepted strategy for matrix decomposition involves defining matrices as products of other matrices, each factor made distinct by their significance and extensive study support. The following section outlines the commonly used factorization of matrices over complex numbers and fields into a product of specific matrices. It is important to note that not every square matrix possesses the property of diagonalizability. However, every square matrix over a field $\mathbb{F}$, where the characteristic of $\mathbb{F}$ is not 2 and $\mathbb{F} \neq \mathbb{F}_3$, can be expressed as a product of two diagonalizable matrices, as demonstrated in the following theorem.

Theorem 2.4.11. *[44] Let $\mathbb{F}$ be any field such that $\mathrm{char}(\mathbb{F}) \neq 2$ and $\mathbb{F} \neq \mathbb{F}_3$. Then,*

every square matrices over $\mathbb{F}$ is a product of two diagonalizable matrices.

In particular, ever square matrices over $\mathbb{F}_3$ is a product of three diagonalizable matrices, and in general the number three is minimal.

According to the theorem in 2.4.6, the decomposition of matrices over complex numbers as a product of symmetric matrices was specifically again dealt with by Bosch in 1986. By using Jordan normal form, he [45] also proved the following theorem.

Theorem 2.4.12. *[45] Let $A \in \mathbb{M}_n(\mathbb{C})$. Then,*

A is a product of two complex symmetric matrices.

Moreover, for any $A \in \mathbb{M}_n(\mathbb{R})$, A is a product of two real symmetric matrices.

The decomposition of matrices into a product of unitary matrices was investigated by Tôyama in 1949, resulting in the statement of the following theorem.

Theorem 2.4.13. *[46] Let $A \in \mathbb{M}_n(\mathbb{C})$ be a unitary matrix. Then,*

A is a commutators of unitary matrices if and only if $\det(A) = 1$.

Furthermore, the decomposition of matrices into products of commutators, where each component is a unipotent matrix, has been investigated. According to the following statement, Baodong Zheng [47] was the first mathematician to study it in 2002. Let $\mathbb{F}$ represent either the set of complex numbers or the set of real numbers. Then,

every matrix $A \in \mathrm{SL}_n(\mathbb{F})$ can be expressed as a product of no more than two commutators of involutions.

Afterwards, in 2021, Hou [48] showed that for any $A \in \mathrm{SL}_n(\mathbb{C})$,

A can be expressed as a product involving no more than two commutators formed from unipotent matrices,

each factor having an index of 2. The investigation of matrix decomposition into a product of nilpotent matrices was conducted by Wu [49]. In 1987, Wu stated that for any $A \in \mathbb{M}_n(\mathbb{C})$ that is singular and not 2×2 nilpotent, then

A is a product of two nilpotent matrices whose rank both equal to rank(A).

After that, Botha investigated the decomposition of matrices into a product of nilpotent matrices with specified ranks as outlined in [50]. He established that, for any $A \in \mathbb{M}_n(\mathbb{C})$ that is singular and not 2×2 nilpotent and for any natural numbers such that n_1, n_2 satisfy $\text{null}(A) \geq n_1, n_2 \geq 1$ and $n_1 + n_2 \geq \text{null}(A)$, then

$$A \text{ is similar to } N_1 N_2,$$

where the last $(n_1 + n_2 - n)-$column of N_1 and the last $(n_1 + n_2 - n)-$row of N_2 are zero and $\text{null}(A) = n$.

The decomposition of matrices into a product of idempotent matrices was introduced by Erdos in 1967, expressed in the following theorem.

Theorem 2.4.14. *[6] Let $A \in \mathbb{M}_n(\mathbb{C})$ be singular. Then,*

A is a product of idempotent matrices.

His work initiated the exploration of integral domains R that satisfy the property ID_n; specifically, for any singular matrix $A \in \mathbb{M}_n(R)$, A can be represented as a product of idempotent matrices. After that, there are generalizations of idempotent factorization matrices over fields to matrices over some special types of integral domains, such as Euclidean domains by Alahmadi in [7], Bézout Domains by Ruitenburg in [8], unique factorization domains, projective-free domains and PRINC domains in [9] and [10]. The challenge of decomposing invertible matrices into products of elementary factors has been a notable focus of investigation throughout the years. The assignment of defining integral domains R that satisfy the property GE_n; specifically, for any nonsingular matrix $A \in \mathbb{M}(\mathbb{R})$, A can be represented as a product of elementary matrices. The theorem has been demonstrated using elementary matrices as outlined in [22]. Specifically, for any matrix $A \in \mathbb{M}_n(\mathbb{C})$, it holds that

A can be expressed as a product of elementary matrices if and only if A is nonsingular.

Furthermore, in the context of any Bézout Domain R, it can be observed that the property ID_2 leads to the conclusion that ID_n holds true, while the property GE_2 similarly results in the implication that GE_n is valid for all $n \geq 0$ (refer to [8,51] for further elaboration). Their research was driven by the exploration of idempotent factorization of 2×2 matrices within the ring of integers of a quadratic number field, as pursued by Cozzu and Zanardo. The authors demonstrated that any column-row matrix can be expressed as a product of idempotent matrices. The authors also examined the idempotent factorization of 2×2 matrices in a specific form, as detailed in section 4.1.

CHAPTER III

DECOMPOSITION OF MATRICES OVER DIVISION RING

This chapter is organized into three distinct sections. In Section 3.1, we provide some decomposition of matrices over division rings. In Section 3.2, we define Hermitian matrices and analyze several of their essential properties. In Section 3.3, we provide improvements to the current theory and lemmas to support subsequent advancements in our studies. Furthermore, we provide a matrix factorization expressed as the product of three diagonalizable matrices. Additionally, we outline the essential and adequate conditions for matrix factorization of a non-central matrix into a product of four Hermitian matrices and one diagonalizable matrix, where the Dieudonné determinant corresponds to the commutator class including one. We denote K as a division ring with its center $Z(K)$, where $K^{\times} = K \setminus \{0\}$, and let K^c represent the commutator subgroup of K. For elements $a, b \in K$, we define a to be conjugate to b if there exists an element $x \in K^{\times}$ such that $a = xbx^{-1}$.

3.1 Some decomposition of matrices over division rings

The topic of matrix decomposition over division rings possesses a substantial historical background, encompassing a variety of different kinds of factors. This chapter presents a concise overview of the research, which is detailed briefly in the following sections. It is important to note that any matrix $A \in \mathbb{M}_n(K)$ can have a maximum of n eigenvalues that are not conjugate (refer to [25] for further information). Furthermore, if A possesses n nonconjugate eigenvalues, it follows that A is diagonalizable. The subsequent criteria represent essential conditions for the diagonalizability of specific categories of matrices.

Lemma 3.1.1. ([52, Lemma 3.2] and [25, Cf. Theorem 8.2.3]) *Let $n \geq 1$. If A is a lower or upper triangular matrix with pairwise nonconjugate diagonal entries $a_{11}, a_{22}, \ldots, a_{nn} \in K$ and all except at most one algebraic over $Z(K)$, then A is similar to the diagonal matrix* $\mathrm{diag}(a_{11}, a_{22}, \ldots, a_{nn})$.

In addition to the diagonalizable matrix, the decomposition of matrices into a generalized Jordan canonical form was provided by Đoković in [53]. A square matrix A is a generalized Jordan matrix if A is a matrix of the form

$$\begin{pmatrix} a & b & 0 & \cdots & 0 \\ 0 & a & b & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a & b \end{pmatrix}$$

where $b \notin \{ax - xa : x \in K\}$. Among the most popular subjects in matrices over division algebra is the decomposition of matrices into a product of commutators. However, in order to investigate the decomposition of matrices as a product of commutators, a more basic decomposition of the matrix is necessary. In 2019, Egorchenkova and Gordeev [54] showed the following result: Let $n \geq 2$. Then, for any non-central matrix $A \in \mathrm{GL}_n(K)$, there exist $\alpha_i \in K^\times$ for $i = 1, \ldots, n$, $P \in \mathrm{GL}_n(K)$, a lower triangular matrix L, an upper triangular matrix U with all diagonal entries of L and U equal to 1 such that

$$PAP^{-1} = LDU$$

where $D = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$. In the same paper, they [54] also showed that any non-central matrices in $\mathrm{SL}_n(K)$ is a product of less than or equal to $\lceil \frac{c}{n-2} \rceil$ where c is the supremum of the smallest integer n such that any elements in K^c can be written as a product of n commutator elements in K, is called the commutator width, and $\lceil \cdot \rceil$ is the ceil function for $n \geq 3$. After that, in 2023, Bien et al. [55] demonstrated the following result: Let K be a finite-dimensional division ring and n be a positive integer. If K is algebraically closed, then every matrix in $\mathrm{SL}_n(K)$ is a commutator of elements from $\mathrm{SL}_n(K)$. Following that, Bien et al. [52] modified the factorization of matrices over finite dimension division algebra over its center to the following: Let $n \geq 2$. Then, for any non-central matrix $A \in \mathrm{SL}_n(K)$, there

exist $P \in \mathrm{GL}_n(K)$, a lower triangular matrix L, an upper triangular matrix U with all diagonal entries of L and U equal to 1 such that

$$PAP^{-1} = LUD_s,$$

where $D_s = \mathrm{diag}(1, \ldots, 1, s)$ for some $s \in K^c$. In the same paper, they [52] also showed that the first two factors of the above factorization are a product of at most two commutators of two involutions. Furthermore, they [52] established that the commutator width of involutions in $\mathrm{GL}_n(K)$, denoted as $\omega_I(\mathrm{GL}_n(K))$, is bounded above by $2+3\omega(K^\times)$, where $\omega(K^\times)$ indicates the commutator width of $K^\times$. This result holds under the conditions that either $\mathrm{char}(K) \neq 2$ or $\mathrm{char}(D) = 2$ with $n \geq 3$. In the case where $\mathrm{char}(K) = 2$ and $n = 2$, it follows that $\omega_I(\mathrm{GL}_n(K)) \leq 2 + 6\omega(K^\times)$.

According to Theorem 2.4.10, Nan and You, in 2007, established the decomposition of non-central matrices over finite-dimensional division algebra, as outlined in the subsequent theorem:

Theorem 3.1.2. *[56, Theorem 2.1] Let $A \in \mathbb{M}_n(K)$ be a non-central invertible matrix and $\alpha_i, \beta_i \in K$ for $i = 1 \ldots, n$, such that $\mathrm{Det}(A) = \prod_{j=1}^{n}[\alpha_j \beta_j]$. Then, there exist a lower triangular matrix $L \in \mathbb{M}_n(K)$ and an upper triangular matrix $U \in \mathbb{M}_n(K)$ such that*

$$PAP^{-1} = LU,$$

where $P \in \mathrm{GL}_n(K)$. Furthermore, L and U can be chosen so that elements in the main diagonal of L are $\alpha_1, \ldots, \alpha_n$ and of U are $\beta_1, \ldots, \beta_n c_n$ where $c_n \in K^c$.

Applying Theorem 3.1.2, it has been shown that for any matrix formed as $A = A_1 \oplus \begin{pmatrix} 1 \end{pmatrix} \in \mathrm{SL}_{n+1}(K)$ where $A_1 \in \mathrm{SL}_n(K)$, the matrix A can be represented as the product of four involutions in $\mathrm{SL}_{n+1}(K)$.

3.2 Hermitian matrices over division rings

Let $- : K \to K$ be an anti-automorphism, which is an involution with $-(a) = \overline{a}$ and let $F = \{a \in K : \overline{a} = a\}$ be a subset of K. Define the **trace** map

$\mathrm{Tr} : K \to F$ by $\mathrm{Tr}(a) = a + \overline{a}$ for all $a \in K$. The following proposition is a list of some properties of the relationship between K and F.

Proposition 3.2.1. *Let K be a division ring with an involution $\overline{\cdot}$ and $F = \{a \in K : \overline{a} = a\} \subseteq K$. Then,*

1. $0, 1 \in F$
2. *If $a \in F$, then $a^{-1} \in F$.*
3. *If $a \in Z(K)^{\times}$, then $\overline{a} \in Z(K)$.*
4. $a + \overline{a}, a\overline{a}, \overline{a}a \in F$ *for all* $a \in K$.

Proof. Let $a \in K$. Consequently, we observe that $\overline{a} \cdot 1 = \overline{a} = \overline{1 \cdot a} = \overline{a} \cdot \overline{1}$. Based on this analysis, we can deduce that $1 = \overline{1}$, indicating that 1 belongs to the set F. In the same way, it follows that $0 \in F$. If $a \in F$, then $\overline{a} = a$. Through direct computation, we establish that $a \cdot a^{-1} = 1 = \overline{1} = \overline{a^{-1} \cdot a} = \overline{a} \cdot \overline{a^{-1}}$. Since $\overline{a} = a$, we have $a^{-1} = \overline{a^{-1}}$, indicating that a^{-1} belongs to F. If $a \in Z(K)^{\times}$, then $ab = ba$ for all $b \in K$. For any $\overline{b} \in K$, we have $\overline{a \cdot \overline{b}} = \overline{\overline{b}} \cdot \overline{a} = b \cdot \overline{a}$ and $\overline{\overline{b} \cdot a} = \overline{a} \cdot \overline{\overline{b}} = \overline{a} \cdot b$. Since a is in the center of K, $\overline{a \cdot \overline{b}} = \overline{\overline{b} \cdot a}$, and this implies that $\overline{a} \in Z(K)^{\times}$. Since K is an abelian group, it follows that $\overline{a + \overline{a}} = \overline{a} + \overline{\overline{a}} = \overline{a} + a = a + \overline{a}$. Through direct computation, we find that $\overline{a \cdot \overline{a}} = \overline{\overline{a}} \cdot \overline{a} = a \cdot \overline{a}$ and $\overline{\overline{a} \cdot a} = \overline{a} \cdot \overline{\overline{a}} = \overline{a} \cdot a$. This indicates that $a + \overline{a}, a\overline{a}, \overline{a}a \in F$. □

The following are some examples of division rings with an involution:

Example 3.2.2. [23, 57]

(1) For $a, b \in \mathbb{R}$, the complex conjugate of the complex number $\mathbb{C}$, represented as $\overline{a + bi} = a - bi$, functions as an involution of $\mathbb{C}$, with $\mathbb{R}$ playing as the fixed field.

(2) An involution $- : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ defined by $-(a) = a^q$ for all $a \in \mathbb{F}_{q^2}$, where q is a prime power. The fixed field of this involution is $\mathbb{F}_q$.

(3) Let $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ be the division ring of real quaternions characterized by the properties $i^2 = j^2 = k^2 = ijk = -1$. For $a, b, c, d \in \mathbb{R}$, an involution of $\mathbb{H}$ is defined by $\overline{a + bi + cj + dk} = a - bi - cj - dk$ with the fixed field $\mathbb{R}$.

(4) Let $\mathbb{F}$ be a field of characteristic n with $n \neq 2$ and $a, b \in \mathbb{F}^\times$. The quaternion algebra $\left(\frac{a,b}{\mathbb{F}}\right) = \mathbb{F} \oplus \mathbb{F}i \oplus \mathbb{F}j \oplus \mathbb{F}ij$ where $i^2 = a, j^2 = b$ and $ij = -ji$. For $a_1, a_2, a_3, a_4 \in \mathbb{F}$, an involution of $\left(\frac{a,b}{\mathbb{F}}\right)$ is defined by $\overline{a_1 + a_2 i + a_3 j + a_4 ij} = a_1 - a_2 i - a_3 j - a_4 ij$ with the fixed field $\mathbb{F}$.

(5) Let $\mathbb{F}$ be a field of characteristic 2 and $a, b \in \mathbb{F}^\times$. The quaternion algebra $\left(\frac{a,b}{\mathbb{F}}\right) = \mathbb{F} \oplus \mathbb{F}i \oplus \mathbb{F}j \oplus \mathbb{F}ij$ where $i^2 + i = a, j^2 = b$ and $ij = ji + j$. For $a_1, a_2, a_3, a_4 \in \mathbb{F}$, an involution of $\left(\frac{a,b}{\mathbb{F}}\right)$ is defined by $\overline{a_1 + a_2 i + a_3 j + a_4 ij} = a_1 + a_2 (1 + i) + a_3 j + a_4 ij$ whose fixed field is $\mathbb{F} \oplus \mathbb{F}j \oplus \mathbb{F}ij$.

In the context of Example 3.2.2 (1), we are able to observe that F can be viewed as the field of real numbers when K is a field of complex numbers and $\overline{\cdot}$ is the complex conjugate. The definition of a Hermitian matrix is thus defined as follows.

Definition 3.2.3. [23] Let $A = (a_{ij}) \in \mathbb{M}_n(K)$. Then, A is said to be a **Hermitian matrix** over K on the involution $\overline{\cdot}$ if

$$A = \overline{A^t} =: A^*$$

where $\overline{A} = (\overline{a_{ij}})$. Any two Hermitian matrices $A, B \in \mathbb{M}_n(K)$, A and B, are said to be **cogredient** if there exists $X \in \mathrm{GL}_n(K)$ such that $A = X^* B X$.

Denote by $\mathcal{H}_n(K)$ the set of all $n \times n$ Hermitian matrices over K equipped with the involution $\overline{\cdot}$. In [23,57,58], it is consistently assumed that F serves as a subfield of K, which is contained in $Z(K)$. Additionally, the authors assume that the function trace Tr is characterized as surjective; specifically, for any element $a \in F$, there exists $x \in K$ such that $a = x + \overline{x}$. Given these conditions, it is feasible for every Hermitian matrix to be transformed into a simpler form through cogredience transformation as the following: Let K be a division ring with an

involution $\overline{\cdot}$ such that F is a subfield of K, which is a subset of $Z(K)$, and the map Tr is surjective. Let $A \in \mathcal{H}_n(K)$. Then,

$$A \text{ is cogredient to a diagonal matrix } D = \operatorname{diag}\{a_1, \ldots, a_r, 0, \ldots, 0\}$$

where $a_i \in F^\times$ for $i = 1, \ldots, r$ and r is equal to the rank of A.

As outlined in the previous discussion, a gap exists between Hermitian matrices and their associated Dieudonné determinant. In this context, we now assume that F is closed under multiplication. Through direct verification, it can be shown that F forms a nonempty subfield of K, containing 0 and 1 as the additive and multiplicative identities, respectively. Under this assumption, we arrive at the following result:

Theorem 3.2.4. *Let $A \in \mathcal{H}_n(K)$. Then, $\operatorname{Det}(A) = [a]$ for some $a \in F$.*

Proof. Let $A \in \mathcal{H}_n(K)$. There is nothing to prove if A is a singular matrix. Now, suppose that A is non-singular. If A is a central matrix, then $A = \operatorname{diag}(a, a, \ldots, a)$ for some $a \in F$. Then, $\operatorname{Det}(A) = [a^n]$ with $a^n \in F$ because F is closed under multiplication. If A is a non-central matrix, we proceed with the proof by induction on n. For $n = 1$, we have $A = (a)$ for some $a \in K$ and thus $\operatorname{Det}(A) = [a]$. Since A is Hermitian, $a \in F$. For $n = 2$, we can write $A = \begin{pmatrix} a & b \\ \overline{b} & c \end{pmatrix}$. If $a = 0$, then, according to Proposition 2.2.6 (D5), $\operatorname{Det}(A) = [-\overline{b}b]$. We can conclude that $-\overline{b}b \in F$, since $\overline{-\overline{b}b} = -\overline{b}\,\overline{\overline{b}} = -\overline{b}b$. If $a \neq 0$, then, according to Proposition 2.2.6 (D5), $\operatorname{Det}(A) = [ac - a\overline{b}a^{-1}b] = [a(c - \overline{b}a^{-1}b)]$. It is evident that $a, c - \overline{b}a^{-1}b \in F$, and consequently, $a(c - \overline{b}a^{-1}b) \in F$, as we have assumed that F is closed under multiplication. For $n = 3$, we denote

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ \overline{a_{12}} & a_{22} & a_{23} \\ \overline{a_{13}} & \overline{a_{23}} & a_{33} \end{pmatrix}.$$

If $a_{11} \neq 0$, we can apply row and column operations to obtain the following:

$$A' = X_1 A X_1^* = (a_{11}) \oplus A_2,$$

where X_1 is a product of elementary matrices corresponding to the elimination of the first column by a_{11} and $A_2 \in \mathcal{H}_2(K)$. Since $(A')^* = (X_1 A X_1^*)^* = X_1 A^* X_1^* = X_1 A X_1^* = A'$, it follows that A' is Hermitian. Consequently, both (a_{11}) and A_2 are also Hermitian. Thus, $a_{11} \in F$, and through the process of induction, we establish that $\mathrm{Det}(A_2) = [a]$ for a specific $a \in F$. Therefore, according to Property 2.2.6 (D3) and (D4), we have $\mathrm{Det}(A) = [a_{11}a]$ with $a_{11}a \in F$. If $a_{11} = 0$ and $a_{12} \neq 0$, applying row operations leads us to the conclusion that

$$\begin{aligned} A' &= X_2 A X_2^* \\ &= \begin{pmatrix} 0 & a_{12} \\ \overline{a_{12}} & a_{22} \end{pmatrix} \oplus \left(a_{33} - \overline{a_{13}}\,\overline{a_{12}}^{-1} a_{23} - \overline{a_{23}} a_{12}^{-1} a_{13} - \overline{a_{13}}\,\overline{a_{12}}^{-1} a_{22} a_{12}^{-1} a_{13} \right), \end{aligned}$$

where X_2 is a product of elementary matrices corresponding to the elimination of the first column by $\overline{a_{12}}$ and the elimination of the second column (except a_{22}) by a_{12}. Considering the fact that A' is Hermitian, it implies that the two direct summands in A' are also Hermitian. Based on our assumption, we have that $f := (a_{33} - \overline{a_{13}}\,\overline{a_{12}}^{-1} a_{23} - \overline{a_{23}} a_{12}^{-1} a_{13} - \overline{a_{13}}\,\overline{a_{12}}^{-1} a_{22} a_{12}^{-1} a_{13}) \in F$ and through induction, it follows that $-\overline{a_{12}} a_{12} \in F$. According to Proposition 2.2.6 (D3), (D4), and (D5), we derive that $\mathrm{Det}(A) = [\overline{a_{12}} a_{12} \cdot f]$ with $\overline{a_{12}} a_{12} \cdot f \in F$. It is important to note that a non-singular matrix A does not include any rows that are entirely composed of zeros. Given that a_{11} and a_{12} are both equal to zero, it follows that a_{13} must be non-zero. Now, we can assume that

$$A = \begin{pmatrix} 0 & 0 & a_{13} \\ 0 & a_{22} & a_{23} \\ \overline{a_{13}} & \overline{a_{23}} & a_{33} \end{pmatrix}.$$

Through direct computation, we determine that

$$\begin{aligned} A' &= E_{31}(-a_{23}a_{13}^{-1}) P_{(2\,3)} A P_{(2\,3)} E_{13}(\overline{-a_{23}a_{13}^{-1}}) \\ &= E_{31}(-a_{23}a_{13}^{-1}) \begin{pmatrix} 0 & a_{13} & 0 \\ \overline{a_{13}} & a_{33} & \overline{a_{23}} \\ 0 & a_{23} & a_{22} \end{pmatrix} E_{13}(\overline{-a_{23}a_{13}^{-1}}) \\ &= \begin{pmatrix} 0 & a_{13} & 0 \\ \overline{a_{13}} & a_{33} & 0 \\ 0 & 0 & a_{22} \end{pmatrix}. \end{aligned}$$

Consequently, based on Proposition 2.2.6 (D3), (D4), and (D5), we can derive that $\mathrm{Det}(A) = \mathrm{Det}(A') = [\overline{a_{13}}a_{13}a_{22}]$. Applying comparable reasoning as in the previous instances, we have $\overline{a_{13}}a_{13}a_{22} \in F$.

We will consider that for any Hermitian matrix $A \in \mathcal{H}_n(K)$, the determinant of A can be expressed as $\mathrm{Det}(A) = [a]$ for a specific element $a \in F$. Consider the matrix $B = (b_{ij})$ belonging to the space $\mathcal{H}_{n+1}(K)$. If $b_{11} \neq 0$, then

$$B' = XBX^* = \left(b_{11}\right) \oplus B_2,$$

where X represents a product of elementary matrices that are associated with the elimination of the first column by b_{11} and $B_2 \in \mathcal{H}_n(K)$. Through the process of hypothesis induction and employing analogous reasoning to that of the preceding paragraph, we conclude that $\mathrm{Det}(B) = [b_{11}b]$ where $b_{11}b \in F$. If $b_{11} = 0$, then there must be a $b_{1k} \neq 0$ for some $k \in \{2, 3, \ldots, n\}$ (since B is invertible), which implies that $\overline{b_{1k}} \neq 0$. By swapping the 2^{nd} row with the k^{th} row and the 2^{nd} column with the k^{th} column, we obtain that

$$B' = P_{(2\,k)}BP_{(2\,k)} = \begin{pmatrix} 0 & b_{1k} & X \\ \overline{b_{1k}} & b_{kk} & \\ & \overline{X^t} & B_2 \end{pmatrix}.$$

Let Y represent a product of elementary matrices that correspond to the elimination of the first column using $\overline{b_{1k}}$ and the second column (excluding b_{kk}) using b_{1k}. Through direct calculation, it can be established that

$$B'' = YB'Y^* = \begin{pmatrix} 0 & b_{1k} \\ \overline{b_{1k}} & b_{kk} \end{pmatrix} \oplus B_2',$$

where $B_2' \in \mathcal{H}_{n-1}(K)$. Once more, employing analogous reasoning, we find that $\mathrm{Det}(B) = [\overline{b_{1k}}b_{1k}b_2']$ for some $b_2' \in F$, where $\mathrm{Det}(B_2') = [b_2']$. Given that F is closed, it follows that $\mathrm{Det}(B) = [f']$ for a specific element $f' \in F$. □

3.3 Main tools and their applications

We begin our discussion by developing on a result reported by Nan and You in [56], which suggested that if A is a non-central matrix, then A can be shown

to be similar to a matrix whose first column is represented as $\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \end{pmatrix}^t$, applicable for $n \geq 2$. Their concepts are additionally applied in the exposition of this lemma.

Lemma 3.3.1. *Let $n \geq 2$ and let $A \in \mathbb{M}_n(K)$ be a non-central nonzero matrix. Then, A is similar to the matrix with the first column being $\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \end{pmatrix}^t$.*

Proof. We divide the proof into 3 cases involving the matrix A as follows.
Case 1: Assume that $A = \text{diag}(a, \ldots, a)$ for some $a \in K \backslash Z(K)$. Since $a \notin Z(K)$, there exists $x \neq 0$ such that $ax \neq xa$; i.e., $(ax - xa)^{-1}$ exists. So, we obtain that

$$E_{12}(-a)E_{22}\left((xa - ax)^{-1}\right) E_{21}(x)AE_{21}(-x)E_{22}\left(xa - ax\right) E_{12}(a)$$

has its first column as $\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \end{pmatrix}^t$.
Case 2: Assume that $A = \text{diag}(a_{11}, \ldots, a_{nn})$ with $a_{ii} \neq a_{jj}$ for some $i \neq j$. By direct row and column operations via $P_{(1\,i)}$ and $P_{(2\,j)}$, we can assume that $a_{11} \neq a_{22}$. Hence, we also obtain that the matrix

$$E_{12}(-a)E_{22}\left((a_{11} - a_{22})^{-1}\right) E_{21}(x)AE_{21}(-x)E_{22}(a_{11} - a_{22})E_{12}(a)$$

has its first column as $\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \end{pmatrix}^t$.
Case 3: Assume that $A = (a_{ij})$ is not a diagonal matrix. Since A is a nonzero matrix, there exists $a_{ij} \in K^\times$ with $i \neq j$. By direct row and column operations via $P_{(1\,j)}$ and $P_{(2\,i)}$, we can assume that $a_{21} \neq 0$. Set $X = \text{diag}(1, a_{ij}^{-1}, 1, \ldots, 1)$. Then,

$$XAX^{-1} = \begin{pmatrix} a'_{11} & \\ 1 & \\ a'_{31} & * \\ \vdots & \\ a'_{n1} & \end{pmatrix} := A'.$$

Let Y be a product of elementary matrices corresponding to the elimination of the first column by the $(2,1)-$entry. Thus, $YA'Y^{-1}$ has its first column as $\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \end{pmatrix}^t$. □

Utilizing Lemma 3.3.1, we can extend Theorem 3.1.2 by including singular non-zero non-central matrices, as shown in the following theorem.

Theorem 3.3.2. *Let $A \in \mathbb{M}_n(K)$ be a singular nonzero non-central matrix and $\alpha_i, \beta_i \in K^\times$ for $1 \leq i < n$. Then, there exist a lower triangular matrix L, an upper triangular matrix U, and $P \in \mathrm{GL}_n(K)$ such that*

$$PAP^{-1} = LU.$$

Furthermore, L and U can be chosen so that the elements in the main diagonal of L are $\alpha_1, \ldots, \alpha_r, 0, \ldots, 0$ and of U are $\beta_1, \ldots, \beta_r, 0, \ldots, 0$ for some $r < n$.

Proof. Induction is employed with respect to n. The outcome is clear for $n = 1$. Let $A \in \mathbb{M}_2(K)$, which is a singular, nonzero, and non-central matrix. According to Lemma 3.3.1, it follows that A is similar to the matrix $\begin{pmatrix} 0 & a_{12} \\ 1 & a_{22} \end{pmatrix}$. Next, we define $P = \begin{pmatrix} 1 & \alpha_1\beta_1 \\ 0 & 1 \end{pmatrix}$, leading us to the conclusion that

$$PAP^{-1} = \begin{pmatrix} \alpha_1\beta_1 & b_{12} \\ 1 & b_{22} \end{pmatrix}.$$

Since A is singular, we can apply Propositions (D2), (D3), and (D5) to obtain the following conclusions:

$$0 = \alpha_1\beta_1 b_{22} - \alpha_1\beta_1(\alpha_1\beta_1)^{-1}b_{12} = \alpha_1\beta_1 b_{22} - b_{12}.$$

To clarify, $b_{22} = \beta_1^{-1}\alpha_1^{-1}b_{12}$. So, we can decompose the matrix PAP^{-1} as follows:

$$\begin{pmatrix} \alpha_1\beta_1 & b_{12} \\ 1 & b_{22} \end{pmatrix} = \begin{pmatrix} \alpha_1 & 0 \\ \beta_1^{-1} & 0 \end{pmatrix} \begin{pmatrix} \beta_1 & \alpha_1^{-1}b_{12} \\ 0 & 0 \end{pmatrix}.$$

Assume that the theorem holds true for all singular nonzero non-central matrices of size smaller than n for $2 \leq n$. Let $A \in \mathbb{M}_n(K)$ be a singular nonzero non-central matrix. According to Lemma 3.3.1, it follows that A is similar to

$$A_0 := \begin{pmatrix} 0 & \\ 1 & \\ 0 & * \\ \vdots & \\ 0 & \end{pmatrix}.$$

Next, we define $P_0 = P \oplus I_{n-2}$. Subsequently, through the application of direct row and column operations, we arrive at the conclusion that

$$P_0 A_0 P_0^{-1} = \begin{pmatrix} \alpha_1\beta_1 & & \\ 1 & & \\ 0 & * & \\ \vdots & & \\ 0 & & \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 & Y \\ X & T \end{pmatrix} =: A_1$$

where $X = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^t$. Through the application of row and column operations on the block matrix, we derive that

$$A_1 = \begin{pmatrix} 1 & 0 \\ X\beta_1^{-1}\alpha_1^{-1} & I_{n-1} \end{pmatrix} \begin{pmatrix} \alpha_1\beta_1 & 0 \\ 0 & T - X\alpha_1^{-1}\beta_1^{-1}Y \end{pmatrix} \begin{pmatrix} 1 & \beta_1^{-1}\alpha_1^{-1}Y \\ 0 & I_{n-1} \end{pmatrix}.$$

According to Property 2.2.6 (D2), (D3), and (D4), we conclude that

$$\mathrm{Det}(A) = [\alpha_1\beta_1] \cdot \mathrm{Det}(T - X\alpha_1^{-1}\beta_1^{-1}Y) = 0.$$

Since $\alpha_1, \beta_1 \neq 0$, it can be concluded that $\mathrm{Det}(T - X\alpha_1^{-1}\beta_1^{-1}Y) = 0$.

Now, if $T - X\alpha_1^{-1}\beta_1^{-1}Y$ is a central matrix, then $T - X\alpha_1^{-1}\beta_1^{-1}Y) = aI_{n-1}$ for some $a \in Z(K)$. Since $\mathrm{Det}(T - X\alpha_1^{-1}\beta_1^{-1}Y) = [a^{n-1}] = 0$, we conclude that $a = 0$; that is, $T - X\alpha_1^{-1}\beta_1^{-1}Y = 0$ is a zero matrix. Consequently, we find that

$$A_1 = \begin{pmatrix} \alpha_1 & 0 \\ X\beta_1^{-1} & 0_{n-1\times n-1} \end{pmatrix} \begin{pmatrix} \beta_1 & \alpha_1^{-1}Y \\ 0 & 0_{n-1\times n-1} \end{pmatrix},$$

representing a multiplication of a lower triangular matrix and an upper triangular matrix.

Specifically, if $T - X\alpha_1^{-1}\beta_1^{-1}Y$ is a non-central matrix, then, according to the induction hypothesis, there exists $P_1 \in \mathrm{GL}_{n-1}(K)$ such that

$$T - X\alpha_1^{-1}\beta_1^{-1}Y = P_1 \begin{pmatrix} \alpha_2 & & \\ \vdots & \ddots & \\ * & \cdots & 0 \end{pmatrix} \begin{pmatrix} \beta_2 & \cdots & * \\ & \ddots & \vdots \\ & & 0 \end{pmatrix} P_1^{-1}.$$

Then,

$$
\begin{aligned}
A_1 &= \begin{pmatrix} 1 & 0 \\ X\beta_1^{-1}\alpha_1^{-1} & P_1 \end{pmatrix} \begin{pmatrix} \alpha_1 & & & \\ 0 & \alpha_2 & & \\ \vdots & \vdots & \ddots & \\ 0 & * & \cdots & 0 \end{pmatrix} \begin{pmatrix} \beta_1 & 0 & \cdots & 0 \\ & \beta_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & 0 \end{pmatrix} \begin{pmatrix} 1 & \beta_1^{-1}\alpha_1^{-1}Y \\ 0 & P_1^{-1} \end{pmatrix} \\
&= \begin{pmatrix} 1 & \\ & P_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ P_1^{-1}X\beta_1^{-1}\alpha_1^{-1} & I_{n-1} \end{pmatrix} \begin{pmatrix} \alpha_1 & & & \\ 0 & \alpha_2 & & \\ \vdots & \vdots & \ddots & \\ 0 & * & \cdots & 0 \end{pmatrix} \\
&\times \begin{pmatrix} \beta_1 & 0 & \cdots & 0 \\ & \beta_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & 0 \end{pmatrix} \begin{pmatrix} 1 & \beta_1^{-1}\alpha_1^{-1}YP_1 \\ 0 & I_{n-1} \end{pmatrix} \begin{pmatrix} 1 & \\ & P_1^{-1} \end{pmatrix} \\
&= \begin{pmatrix} 1 & \\ & P_1 \end{pmatrix} \begin{pmatrix} \alpha_1 & & & \\ * & \alpha_2 & & \\ \vdots & \vdots & \ddots & \\ * & * & \cdots & 0 \end{pmatrix} \begin{pmatrix} \beta_1 & * & \cdots & * \\ & \beta_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & 0 \end{pmatrix} \begin{pmatrix} 1 & \\ & P_1^{-1} \end{pmatrix}.
\end{aligned}
$$

Since A_1 is similar to A, the conclusion has been validated. Since $\mathrm{Det}(A) = 0$, it follows that $r < n$. □

According to Lemma 3.1.1, the diagonal entries $a_{11}, a_{22}, \ldots, a_{nn} \in K$ of A are pairwise nonconjugate, indicating that there can be at most one zero among them. The following lemma suggests that this condition can be relaxed:

Lemma 3.3.3. *Let $l, n \in \mathbb{N}$ with $l < n$ and $A \in \mathbb{M}_n(K)$. Let us consider the matrix A defined as follows: $A = \begin{pmatrix} A_{11} & 0 \\ A_{21} & 0 \end{pmatrix}$, where A_{11} is a lower triangular matrix belonging to $\mathbb{M}_l(K)$, or $A = \begin{pmatrix} A_{11} & A_{12} \\ 0 & 0 \end{pmatrix}$ where A_{11} is an upper triangular matrix in $\mathbb{M}_l(K)$. If all diagonal entries $a_{11}, a_{22}, \ldots, a_{ll}$ of A_{11} are pairwise nonconjugate elements in K and all except at most one are algebraic over $Z(K)$, then A is similar to the diagonal matrix* $\mathrm{diag}(a_{11}, \ldots, a_{ll}, 0, \ldots, 0)$.

Proof. Since A_{11} meets the criteria outlined in Lemma 3.1.1, it follows that there exists a matrix $P \in \mathrm{GL}_l(K)$ for which the equation $PA_{11}P^{-1} = D$ holds true where $D = \mathrm{diag}(a_{11}, \ldots, a_{ll})$. Therefore, we conclude that

$$\begin{pmatrix} P & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} A_{11} & 0 \\ A_{21} & 0 \end{pmatrix} \begin{pmatrix} P^{-1} & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} D & 0 \\ A_{21}P^{-1} & 0 \end{pmatrix}.$$

Through direct computation working with row and column operations, we obtain that

$$\begin{pmatrix} I & 0 \\ -A_{21}P^{-1}D^{-1} & I \end{pmatrix} \begin{pmatrix} D & 0 \\ A_{21}P^{-1} & 0 \end{pmatrix} \begin{pmatrix} I & 0 \\ A_{21}P^{-1}D^{-1} & I \end{pmatrix} = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}.$$

This means that $\begin{pmatrix} A_{11} & 0 \\ A_{21} & 0 \end{pmatrix}$ exhibits similarity to the diagonal matrix $D \oplus 0$.

Applying the same technique, it can be proved that $A = \begin{pmatrix} A_{11} & A_{12} \\ 0 & 0 \end{pmatrix}$ is similar to the diagonal matrix $D \oplus 0$. □

It is important to note that if K is an infinite division ring that has a finite dimension over its center, then the cardinality of the center, denoted as $|Z(K)|$, must be infinite. This fact suggests that K contains an infinite number of pairwise nonconjugate elements, as any distinct elements within $Z(K)$ are nonconjugate. The classification of division rings with finite dimension over their center serves as a significant area of interest in the examination of matrix decompositions over division rings (refer to [52,59–61]). Additionally, Duang and Son [62] extended the idea of division rings as discussed in [52] to division rings with infinite dimensions over their center, while still requiring infinite centers. However, in the context of an infinite division ring, there exists a division ring with a center that is a finite field (Proposition 2.3.5 in [25]). In this situation, it is not possible to clearly determine the number of elements in K that are pairwise nonconjugated. Therefore, the number of pairwise nonconjugate elements in the division ring K seems to be a probable assumption.

After this paragraph, we will run under the assumption that F is a subset of $Z(K)$. The factorization may include an additional matrix component. The

subsequent conclusions can be derived from the lemmas and theorems that have been previously discussed.

Theorem 3.3.4. *Let $A \in \mathbb{M}_n(K)$. If $Z(K)$ has at least $n+2$ elements, then A is a product of three diagonalizable matrices. In particular, if K is a field containing at least $n+2$ elements, then A is a product of two diagonalizable matrices.*

Proof. Let $A \in \mathbb{M}_n(K)$. If A is a central matrix, then it follows that A must be diagonal. Consequently, it can be expressed as a product of three diagonalizable matrices, specifically the two identity matrices and A itself. Assume that A is a non-central matrix. If A is non-singular, then $\mathrm{Det}(A) = [a]$ for some $a \in K^\times$. We can now select unique nonzero elements from $Z(K)$ that are pairwise nonconjugate, as well as nonconjugate to both a and 1; specifically, $\alpha_1, \ldots, \alpha_{n-1} \in Z(K)$. According to Theorem 3.1.2, it can be established that there exists a matrix $P \in \mathrm{GL}_n(K)$ such that $PAP^{-1} = LU$, where L is specified as a lower triangular matrix with diagonal entries $\alpha_1, \ldots, \alpha_{n-1}, a$, while U is defined as an upper triangular matrix with diagonal entries $\alpha_{n-1}^{-1}, \ldots, \alpha_1^{-1}, x$ for some $x \in K^c$. Since $\alpha_1, \ldots, \alpha_{n-1}, a$ are pairwise conjugate and $\alpha_1, \ldots, \alpha_{n-1}$ are algebraically closed over $Z(K)$, we can apply Lemma 3.1.1 to conclude that L is diagonalizable. If x is not conjugate to α_i for all $i = 1, \ldots, n$, then, by applying Lemma 3.1.1, it follows that U is composed of diagonalizable matrices. If x is conjugate to α_j for some $j \in \{1, \ldots, n\}$, a direct computation yields that

$$U = \begin{pmatrix} \alpha_1^{-1} & \cdots & * & * \\ 0 & \ddots & \vdots & \vdots \\ 0 & \cdots & \alpha_{n-1}^{-1} & * \\ 0 & \cdots & 0 & x \end{pmatrix} = \begin{pmatrix} \alpha_1^{-1} & \cdots & * & * \\ 0 & \ddots & \vdots & \vdots \\ 0 & \cdots & \alpha_{n-1}^{-1} & * \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & x \end{pmatrix} =: BC. \tag{3.3.1}$$

By applying Lemma 3.1.1 once more, we can deduce that the matrices B and C offer diagonalizability. Therefore, $A = P^{-1}LBCP = (P^{-1}LP)(P^{-1}BP)(P^{-1}CP)$ is the product of multiplying three diagonalizable matrices.

If A is a singular matrix, it is possible to choose distinct and pairwise nonconjugate elements $\alpha_1, \ldots, \alpha_r \in Z(K)^\times$ for some $r < n$. In similar ways, applying Theorem 3.1.2, one can state the existence of a matrix $P \in \mathrm{GL}_n(K)$ such that

the equation $PAP^{-1} = LU$ holds true. Here, L represents a lower triangular matrix with diagonal entries $\alpha_1, \ldots, \alpha_r, 0, \ldots, 0$, while U denotes an upper triangular matrix with diagonal entries $\alpha_r^{-1}, \ldots, \alpha_1^{-1}, 0, \ldots, 0$. According to Lemma 3.3.3, it follows that both L and U are diagonalizable, which implies that A can be expressed as a product of two diagonalizable matrices.

Specifically, if K is a field with a minimum number of $n+2$ elements, then the commutator subgroup K^c consists only of the identity element $1 \in K$. This suggests the factor C in the equation (3.3.1) is equivalent to the identity matrix. Therefore, any matrix A can be expressed as the product of two diagonalizable matrices. □

According to Theorem 2.4.5, they [3] showed that a matrix $A \in \mathbb{M}_n(\mathbb{C})$ can be expressed as a product of four Hermitian matrices if and only if $\det(A) = a$ for some $a \in \mathbb{R}$. It is important to observe that the commutator elements within the field $\mathbb{C}$ consist only of the identity element 1. When extending the factorization over $\mathbb{C}$ to division rings with involution and employing the Dieudonné determinant, it is necessary to address commutator subgroups, which may not be trivial.

Theorem 3.3.5. *Let $A \in \mathbb{M}_n(K)$ be a non-central matrix. If F contains at least $n+2$ pairwise nonconjugate elements, then*

$$A = H_1H_2H_3H_4T \quad \textit{if and only if} \quad \mathrm{Det}(A) = [a] \textit{ for some } a \in F,$$

where $H_i \in \mathcal{H}_n(K)$ for all $i = 1, \ldots, 4$ and T is a diagonalizable matrix with $\mathrm{Det}(T) = [1]$. In particular, if A is singular, then A is a product of four Hermitian matrices.

Proof. Let $A \in \mathbb{M}_n(K)$. Assume that $A = H_1H_2H_3H_4T$ for some $H_1, H_2, H_3, H_4 \in \mathcal{H}_n(K)$ and T is a diagonalizable matrix with $\mathrm{Det}(T) = [1]$. According to Theorem 3.2.4, for each index $i = 1, 2, 3, 4$, it follows that $\mathrm{Det}(H_i) = [h_i]$ for a corresponding element $h_i \in F$. The result indicates that $\mathrm{Det}(A) = [h_1][h_2][h_3][h_4][1] = [h_1h_2h_3h_4 \cdot 1]$ Since F is closed under multiplication, it follows that $\mathrm{Det}(A) = [a]$ for some element a in F.

Conversely, we consider the assumption that $\mathrm{Det}(A) = [a]$ for a specific $a \in F$. In this context, we organize our proof into two separate instances concerning A. For a nonsingular matrix A, determined by our assumption, we can select pairwise nonconjugate nonzero elements in F, making sure none of them are conjugate to a or 1; specifically, $\alpha_1, \ldots, \alpha_{n-1} \in F$. According to Theorem 3.1.2, it can be established that there exists a matrix $P \in \mathrm{GL}_n(K)$ such that the equation $PAP^{-1} = LU$ holds true where L is described as a lower triangular matrix with diagonal entries $\alpha_1, \ldots, \alpha_{n-1}, a$, while U is defined as an upper triangular matrix with diagonal entries $\alpha_{n-1}^{-1}, \ldots, \alpha_1^{-1}, x$, where x belongs to K^c. That is, $A = P^{-1}LUP = (P^{-1}LP)(P^{-1}UP)$. If $x \notin F$, then

$$U = \begin{pmatrix} \alpha_1^{-1} & \cdots & * & * \\ 0 & \ddots & \vdots & \vdots \\ 0 & \cdots & \alpha_{n-1}^{-1} & * \\ 0 & \cdots & 0 & x \end{pmatrix} = \begin{pmatrix} \alpha_1^{-1} & \cdots & * & * \\ 0 & \ddots & \vdots & \vdots \\ 0 & \cdots & \alpha_{n-1}^{-1} & * \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & x \end{pmatrix} =: BD_x.$$

Since $\alpha_1, \ldots, \alpha_{n-1}, a \in F \subseteq Z(K)$, it follows that $\alpha_1, \ldots, \alpha_{n-1}, a$ are algebraic over $Z(K)$. According to Lemma 3.1.1, we can identify matrices $S, T \in \mathrm{GL}_n(K)$ such that the transform $P^{-1}LP = SD_LS^{-1}$ holds, where $D_L = \mathrm{diag}(\alpha_{n-1}^{-1}, \ldots, \alpha_1^{-1}, a)$. Similarly, we have $P^{-1}BP = TD_BT^{-1}$ with $D_B = \mathrm{diag}(\alpha_1, \ldots, \alpha_{n-1}, 1)$. Thus, we conclude that

$$\begin{aligned} A &= SD_LS^{-1}TD_BT^{-1}PD_xP^{-1} \\ &= S\left(S^*(S^*)^{-1}\right)D_LS^{-1}T\left(T^*(T^*)^{-1}\right)D_BT^{-1}PD_xP^{-1} \\ &= (SS^*)\left(\left(S^{-1}\right)^* D_LS^{-1}\right)(TT^*)\left(\left(T^{-1}\right)^* D_BT^{-1}\right)\left(PD_xP^{-1}\right),. \end{aligned}$$

It follows that A is a product of four Hermitian matrices and one diagonalizable matrix along with its Dieudonné determinant, represented as

$$\mathrm{Det}(PD_xP^{-1}) = \mathrm{Det}(P)\,\mathrm{Det}(D_x)\,\mathrm{Det}(P^{-1}) = [p][1][p^{-1}] = [1].$$

Furthermore, if $x \in F$ and x is nonconjugate to α_i for every i, then the diagonal entries of U exhibit pairwise nonconjugacy. According to Lemma 3.1.1, it can be concluded that U possesses the property of being diagonalizable. By applying the same technique as previously described, eliminating the factor D_x, we can deduce that A is the result of multiplying four Hermitian matrices.

For a singular matrix A, we choose distinct and pairwise nonconjugate nonzero elements $\alpha_1, \ldots, \alpha_r \in F^\times$. According to Theorem 3.1.2, it follows that $A = PLP^{-1}PUP^{-1}$ for some $P \in \mathrm{GL}_n(K)$, where L is a lower triangular matrix with diagonal entries $\alpha_1, \ldots, \alpha_r, 0, \ldots, 0$, and U is an upper triangular matrix with diagonal entries $\alpha_r^{-1}, \ldots, \alpha_1^{-1}, 0, \ldots, 0$. Since $\alpha_1, \ldots, \alpha_r$ are algebraic over $Z(K)$, it follows from Lemma 3.3.3 that there exist matrices $S, T \in \mathrm{GL}_n(K)$ such that the equation $PLP^{-1} = SD_LS^{-1}$ holds, where $D_L = \mathrm{diag}(\alpha_1, \ldots, \alpha_r, 0, \ldots, 0)$. Additionally, we have $PUP^{-1} = TD_UT^{-1}$, with $D_U = \mathrm{diag}(\alpha_1^{-1}, \ldots, \alpha_r^{-1}, 0, \ldots, 0)$. By integrating $(S^*(S^*)^{-1})$ and $(T^*(T^*)^{-1})$ into the aforementioned process, we are able to determine that A can be expressed as a product of four Hermitian matrices. □

Applying Theorem 3.3.5, we derive a condition for expressing one's any central matrices as a product of Hermitian matrices that are as follows:

Theorem 3.3.6. *Let $A = \mathrm{diag}(a, \ldots, a) \in \mathbb{M}_n(K)$ be a central matrix. If F contains at least $n+2$ pairwise nonconjugate elements, then*

$$A = H_1H_2H_3H_4H_5T \quad \textit{if and only if} \quad \mathrm{Det}(A) = [f] \textit{ for some } f \in F$$

where $H_i \in \mathcal{H}_n(K)$ for all $i = 1, \ldots, 5$ and T is a diagonalizable matrix with $\mathrm{Det}(T) = [1]$.

Proof. Let us consider the expression $A = H_1H_2H_3H_4H_5T$, where $H_1, \ldots, H_5$ are elements of $\mathcal{H}_n(K)$ and T is a diagonalizable matrix with the property that $\mathrm{Det}(T) = [1]$. Applying the same reason demonstrated in the proof of Theorem 3.3.5, it follows that $\mathrm{Det}(A) = [f]$ for a specific element $f \in F$.

We will continue under the assumption that $\mathrm{Det}(A) = [f]$ for a certain $f \in F$. When $f = 1$, there is no further evidence required. If $f \in F \setminus \{1\}$, then $[a^n] = [f]$, leading to the conclusion that $a^n = fx$ for some $x \in K^c$. This also implies that

$a = fa^{1-n}x$. Then,

$$\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} = \begin{pmatrix} f & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \begin{pmatrix} a^{1-n}x & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} =: D_f B.$$

Since $f \neq 1$, it follows that $x \neq a^n$, which leads to the conclusion that $a^{1-n}x \neq a$. This suggests that B is a non-central matrix and that $\mathrm{Det}(B) = [1]$. According to Theorem 3.3.5, it follows that $B = H_1H_2H_3H_4T$ represents the product of four Hermitian matrices and one diagonalizable matrix, in which $\mathrm{Det}(T) = [1]$. Since $f \in F$, it follows that D_f is a Hermitian matrix. Consequently, A can be expressed as a product of five Hermitian matrices and one diagonalizable matrix, with the Dieudonné determinant equal to $[1]$. □

Specifically, when $A = aI_n$ is a central matrix and a meets particular requirements, the factorization presented in Theorem 3.3.6 can be simplified as noted in the following propositions.

Proposition 3.3.7. *Let $a \in Z(K) \setminus F$ and $n \in \mathbb{N}$. The following statements are true.*

(*i*) *aI_n cannot be written as a product of two Hermitian matrices.*

(*ii*) *If $a^2 \in F$, then aI_2 is a product of three Hermitian matrices.*

(*iii*) *If $a^2 \in F$, then aI_{2n} is a product of three Hermitian matrices.*

(*iv*) *If $a^n \in F$, then aI_n is a product of four Hermitian matrices.*

Proof. (*i*) Let us consider the equation $aI_n = H_1H_2$, where H_1 and H_2 are elements of the space $\mathcal{H}_n(K)$. Since $a \notin F$, it follows that $a \neq 0$. This indicates that H_1 and H_2 belong to the group $\mathrm{GL}_n(K)$. Consequently, we arrive at the equation $H_2 = H_1^{-1}aI_n = aI_nH_1^{-1}$. Since H_2 is Hermitian, we have the following:

$$aI_nH_1^{-1} = H_2 = H_2^* = \overline{a}I_nH_1^{-*} = \overline{a}I_nH_1^{-1}.$$

That is, $H_1^{-1} = a^{-1}\overline{a}H_1^{-1}$. Since H_1^{-1} is a nonzero matrix, it follows that there exists a nonzero element $h_{ij} =: h \neq 0$ such that the equation $h = a^{-1}\overline{a}h$ holds true. This indicates that $a = \overline{a}$, leading to a contradiction.

(*ii*) Let us consider the case where a^2 belongs to the field F; specifically, we have the equation $a\,a = \overline{a}\,\overline{a}$. Since $a \neq 0$, we can deduce that $a\overline{a}^{-1} = a^{-1}\overline{a} = \overline{a}a^{-1} = \overline{\overline{a}^{-1}a} = \overline{a\overline{a}^{-1}}$, indicating that $a\overline{a}^{-1} \in F$. Through direct decomposition, we obtain that,

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & a \\ \overline{a} & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \overline{a}^{-1}a \end{pmatrix}.$$

It is easy to see that $\begin{pmatrix} 0 & a \\ \overline{a} & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \overline{a}^{-1}a \end{pmatrix}$ are Hermitian matrices. Hence, aI_2 is a product of three Hermitian matrices.

(*iii*) We now examine aI_{2n} represented as $\underbrace{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \oplus \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}}_{n \text{ blocks}}$.

According to (*ii*), it follows that every block of aI_{2n} can be expressed as a product of three Hermitian matrices. This indicates that aI_{2n} can also be expressed as a product of three Hermitian matrices; specifically,

$$\underbrace{\begin{pmatrix} 0 & a \\ \overline{a} & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & a \\ \overline{a} & 0 \end{pmatrix}}_{n \text{ blocks}} \times \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{n \text{ blocks}} \times \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & \overline{a}^{-1}a \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 1 & 0 \\ 0 & \overline{a}^{-1}a \end{pmatrix}}_{n \text{ blocks}}.$$

(*iv*) Examine the following matrix product:

$$aI_n = \begin{pmatrix} 0 & a & 0 & \cdots & 0 \\ 0 & 0 & a & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a \\ a & 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} := BC.$$

Let $D = \text{diag}(a^n, a^{n-1}, \ldots, a)$. Observe that

$$D^{-1}BD = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a^n & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Since $a^n \in F$, it follows that both $D^{-1}BD$ and C are matrices defined over the field F. Since F is a field, it has been demonstrated in [3] that $D^{-1}BD$ and C can be expressed as a product of two symmetric matrices over F, which consequently implies that they also represent a product of two Hermitian matrices over K. This indicates that aI_n can be expressed as a product of four Hermitian matrices. □

According to Example 3.2.2 (3.), the following is an immediate consequence of Theorem 3.3.5.

Corollary 3.3.8. *Let $\mathbb{H}$ be the real quaternion division ring and $A \in \mathbb{M}_n(\mathbb{H})$. Then,*

$$A = H_1H_2H_3H_4T \quad \textit{if and only if} \quad \text{Det}(A) = [a] \textit{ for some } a \in \mathbb{R},$$

where $H_i \in \mathcal{H}_n(\mathbb{H})$ for all $i = 1, \ldots, 4$ and T is a diagonalizable matrix with $\text{Det}(T) = [1]$. In particular, if A is singular, then A is a product of four Hermitian matrices.

Proof. If A is a central matrix, then $A = aI_n$ for some $a \in \mathbb{R}$, and hence A is hermitian. If A is a nonsingular non-central matrix, by Theorem 3.3.5, A is a product of four Hermitian matrices and one diagonalizable matrix where the Dieudonné determinant is [1]. If A is a singular non-central matrix, by Theorem 3.3.5, A is a product of four Hermitian matrices. □

Remark 3.3.9. Let K denote the field of complex numbers $\mathbb{C}$. It follows that the commutator subgroup of $\mathbb{C}$ is $\{1\}$. This indicates that the matrix T in Theorem 3.3.5 runs as the identity matrix, leading to the Dieudonné determinant

in accordance with the standard determinant. For any matrix A belonging to $\mathbb{M}_n(\mathbb{C})$,

A is a product of four Hermitian matrices if and only if $\det(A) = a$ for some $a \in \mathbb{R}$.

CHAPTER IV

DECOMPOSITION OF MATRICES OVER QUADRATIC RING OF INTEGERS

This chapter comes with two sections. In the first section, we provide a unique category of non-column-row matrix as well as a requirement that an element in $\mathcal{O}_\mathcal{K}$ must be satisfied for belonging in each entry of each matrix in this classification. In the second section, we provide the factorization of a matrix into the product of two idempotent matrices in a certain configuration. In the last section, we also provide conjectures on the factorization of a matrix into two idempotent matrices based on specific cases.

4.1 A special class of non-column-row matrices

In this section, we will begin by examining the following definition of a column-row matrix. Let R be a ring. In [9], a matrix $A \in \mathbb{M}_2(R)$ is said to be a **column-row** matrix if there exist $a, b, x, y \in R$ such that

$$A = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} ax & ay \\ bx & by \end{pmatrix}.$$

Furthermore, in [9], Cossu and Zanardo showed that if $A \in \mathbb{M}_2(R)$ is a singular matrix and the ideal generated by the elements in the first row is a principal ideal, then A is said to be a column-row matrix. Subsequently, in [17], they reached the following conclusions regarding the column-row matrix.

Theorem 4.1.1. *[17] Let $\mathcal{O}_\mathcal{K}$ be the ring of integers over any real quadratic number field. Any column-row matrix over $\mathcal{O}_\mathcal{K}$ is a product of idempotent matrices over $\mathcal{O}_\mathcal{K}$. In particular, every singular matrix in $\mathbb{M}_2(\mathcal{O}_\mathcal{K})$ having at least one row or column whose elements generate a principal ideal is a product of idempotent matrices over $\mathcal{O}_\mathcal{K}$.*

In the same paper, they [17] also explored the factorization of certain special matrices over $\mathcal{O}_{\mathcal{K}}$ in the form

$$A(p,z) := \begin{pmatrix} p & z \\ \overline{z} & \frac{\|z\|}{p} \end{pmatrix}$$

where p is a prime integer, which is an irreducible but not prime element in $\mathcal{O}_{\mathcal{K}}$ and $z \in \mathcal{O}_{\mathcal{K}}$ such that the ideal generated by p, z, $\langle p, z\rangle$, is a non-principal ideal. The authors additionally determined the following problem within the same paper.

Problem 4.1.2. [17] Let p be a prime integer which is irreducible but not prime in $\mathcal{O}_{\mathcal{K}}$ and $z \in \mathcal{O}_{\mathcal{K}}$ be such that $\langle p, z\rangle$ is a non-principal ideal. Does the factorization

$$A(p,z) = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix} \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & 1-\overline{a} \end{pmatrix}, \tag{4.1.1}$$

for some $a, b, c \in \mathcal{O}_{\mathcal{K}}$ with $a(1-a) = bc$, always hold true?

In this thesis, we constantly denote D as a positive square-free integer and p as a prime number that is irreducible but not prime in $\mathcal{O}_{\mathcal{K}}$. A characterization of $z \in \mathcal{O}_{\mathcal{K}}$ for which $\langle p, z\rangle$ is non-principal can be determined via the set $I_p(D)$ (*the set of all non unit $z \in \mathcal{O}_{\mathcal{K}}$ for which $z \notin \langle p\rangle$ but there exists $m \notin \langle p\rangle$ such that $zm \in \langle p\rangle$*) for a given D and p as described above. Exactly, this concept points out that

Proposition 4.1.3. *For any element $z \in \mathcal{O}_{\mathcal{K}}$, we have $z \in I_p(D)$ if and only if $\langle p, z\rangle$ is a non-principal ideal.*

Proof. Let $z \in I_p(D)$ and assume for a contradiction that $\langle p, z\rangle = \langle c\rangle$ for some $c \in \mathcal{O}_{\mathcal{K}}$. Since $z \in I_p(D)$, there exists $m \notin \langle p\rangle$ such that $zm = pl$ for some $m, l \in \mathcal{O}_{\mathcal{K}}$. Since $p \in \langle p, z\rangle = \langle c\rangle$, there exists $a \in \mathcal{O}_{\mathcal{K}}$ such that $p = ca$. By using the fact that p is an irreducible element, we have that c or a must be a unit in $\mathcal{O}_{\mathcal{K}}$. If c is a unit, then $\langle c\rangle = \mathcal{O}_{\mathcal{K}}$. So, $1 \in \langle c\rangle = \langle p, z\rangle$; namely, there exist $x, y \in \mathcal{O}_{\mathcal{K}}$ such that $px + zy = 1$. Then,

$$m = pxm + zmy = pxm + ply = p(xm + ly) \in \langle p\rangle,$$

which is a contradiction. However, if a is a unit, then $\langle p \rangle = \langle ca \rangle = \langle c \rangle$. This means that $c = pn$ for some $n \in \mathcal{O}_K$. Since $\langle p, z \rangle = \langle c \rangle$, there exist $x, y \in \mathcal{O}_K$ such that $px + z = cy$. Then, we have

$$z = cy - px = pny - px = p(ny - x) \in \langle p \rangle,$$

which is a contradiction. Thus, $\langle p, z \rangle$ is a non-principal ideal.

On the other hand, we suppose that $\langle p, z \rangle$ is a non-principal ideal and assume for a contradiction that $z \notin I_p(D)$. By assumption, we have $zm \notin \langle p \rangle$, for any element $m \in \mathcal{O}_K$ such that $m \notin \langle p \rangle$. Since $z \notin \langle p \rangle$, $\overline{z} \notin \langle p \rangle$. By choosing $m = \overline{z}$, we conclude that $k := zm = \|z\| \notin \langle p \rangle$; i.e., $k \in \mathbb{Z}$ and $\gcd(p, k) = 1$. Then, Theorem 2.1.3, there exist $x, y \in \mathbb{Z}$ such that

$$1 = px + ky = px + z\overline{z}y \in \langle p, z \rangle.$$

This implies that $\langle p, z \rangle$ is a principal ideal, which is a contradiction. So, $z \in I_p(D)$. □

Additionally, we prove the following proposition.

Proposition 4.1.4. *Let $z \in I_p(D)$. Then, the following statements are true.*

(1) $p \mid \|z\|$ and

(2) $\overline{z} \in I_p(D)$.

Moreover, for any integer $t \in \mathbb{Z}$,

$$\left(\mathbb{Z} \cup \mathcal{O}_K^\times \cup t\mathcal{O}_K^\times\right) \cap I_p(D) = \emptyset.$$

Proof. Let $z \in I_p(D)$. To prove (1), we assume for a contradiction that $p \nmid \|z\|$. This argument suggests that $\gcd(p, \|z\|) = 1$. Consequently, according to Theorem 2.1.3, there are integers x, y such that $px + \|z\|y = 1$. That is, $px + z\overline{z}y = 1$ and hence, $\langle p, z \rangle = \langle 1 \rangle$ is a principal ideal, resulting in a contradiction with Proposition 4.1.3.

In order to prove (2), we again suppose for the interest of contradiction that $\overline{z} \notin I_p(D)$. According to Proposition 4.1.3, $\langle p, \overline{z} \rangle$ forms a principal ideal, hence implying that $\langle p, z \rangle$ is also a principal ideal, resulting in a contradiction.

For the last statement, we propose a contradiction that there exists $a \in (\mathbb{Z} \cup \mathcal{O}_K^\times \cup t\mathcal{O}_K^\times) \cap I_p(D)$ for some $t \in \mathbb{Z}$. If $a \in \mathbb{Z}$, then $a^2 = \|a\|$ and by (1), we have $p \mid a^2$. So, $p \mid a$ and thus $a \in \langle p \rangle$. This shows that $a \notin I_p(D)$; therefore ti is a contradiction. If $a \in \mathcal{O}_K^\times$, then $\langle p, a \rangle$ is principal; that is, $a \notin I_p(D)$, which implies a contradiction. Finally, we suppose that $a = tu$ for some $u \in \mathcal{O}_K^\times$. If $p \mid t$, then $\langle p, a \rangle = \langle p, t \rangle = \langle p \rangle$, a contradiction. Furthermore, if $p \nmid t$, then $p \nmid \|a\|$, as confirmed by

$$t^2 = \|t\| = \|t\|\|u\| = \|tu\| = \|a\|.$$

So, by (1), $a \notin I_p(D)$, which leads to a contradiction. □

It is important to observe that $A(p, \overline{z}) = A(p, z)^t$, and the continued existence of idempotent factorization under the transpose operator allows us to conclude that:

Remark 4.1.5. For $z \in I_p(D)$, $A(p, z)$ admits a factorization of the form (4.1.1) if and only if $A(p, \overline{z})$ admits a factorization of the form (4.1.1).

The following examples are examples of non-column-row matrices whose admit idempotent factorization is in the form (4.1.1).

Example 4.1.6. [10]

$$\begin{pmatrix} 3 & 1+\sqrt{10} \\ 1-\sqrt{10} & -3 \end{pmatrix} = \begin{pmatrix} 2+2\sqrt{10} & 7+\sqrt{10} \\ -6 & -1-2\sqrt{10} \end{pmatrix} \begin{pmatrix} 2-2\sqrt{10} & -6 \\ 7-\sqrt{10} & -1+2\sqrt{10} \end{pmatrix}$$

$$\begin{pmatrix} 2 & \sqrt{10} \\ -\sqrt{10} & -5 \end{pmatrix} = \begin{pmatrix} 6+2\sqrt{10} & 4+\sqrt{10} \\ -10-3\sqrt{10} & -5-2\sqrt{10} \end{pmatrix} \begin{pmatrix} 6-2\sqrt{10} & -10+3\sqrt{10} \\ 4-\sqrt{10} & -5+2\sqrt{10} \end{pmatrix}.$$

4.2 Idempotent factorization over quadratic ring of integers

In this section, we focus on the conditions under which $A(p,z)$, for each $z \in I_p(D)$, satisfies the decomposition defined by the equation (4.1.1). In particular, we firstly investigate the idempotent factorization of $A(p,z)$, for $z = a+b\sqrt{D}$, by using the information form z and p as in the following form:

$$A(p,z) = \begin{pmatrix} z & x \\ \frac{\|z\|}{p} & 1-z \end{pmatrix} \begin{pmatrix} \overline{z} & \frac{\|z\|}{p} \\ \overline{x} & 1-\overline{z} \end{pmatrix}, \tag{4.2.1}$$

for some $x \in \mathcal{O}_\mathcal{K}$. The following equations are necessary for this particular form of decomposition via simple computation for $x = a + b\sqrt{D}$:

$$\begin{aligned} p &= \|z\| + \|x\|, \\ z &= z\frac{\|z\|}{p} + x(1-\overline{z}), \\ \frac{\|z\|}{p} &= \left(\frac{\|z\|}{p}\right)^2 + \frac{\|1-z\|}{p}, \qquad (4.2.2) \\ z(1-z) &= x\frac{\|z\|}{p}. \qquad (4.2.3) \end{aligned}$$

Note that $\|1-z\| = \|z\| - 2a + 1$. By multiplying the equation (4.2.2) by p, we get that

$$\begin{aligned} p\|z\| &= \|z\|^2 + p^2\|z\| - 2p^2a + p^2 \\ 0 &= \|z\|^2 + (p^2-p)\|z\| - 2pa + p^2. \end{aligned}$$

We can solve the quadratic Diophantine equations by using the techniques for such problems, as both $\|z\|$ and a are variables, to get that

$$\begin{aligned} \|z\| &= p(2pt+1) \\ a &= 2p^2t^2 + pt(p+1) + \frac{p+1}{2}, \end{aligned}$$

for some $t \in \mathbb{Z}$. Since $\|z\| = a^2 - Db^2$, by direct computation, we have

$$Db^2 = 4p^4t^4 + 4p^3t^3(p+1) + 2p^2t^2(p+1) + pt(p+1)^2 + p^2t^2(p+1)^2 + \left(\frac{p+1}{2}\right)^2 - 2p^2t - p.$$

Under the assumption that a is an integer, it follows that $p \equiv 3 \pmod 4$. This implies that $Db^2 \equiv \left(\frac{p+1}{2}\right)^2 - 2p^2t - p \pmod 4$. Hence,

$$Db^2 \equiv 2t+1 \pmod 4.$$

Since $x^2 \equiv 0, 1 \pmod 4$ for every $x \in \mathbb{Z}$, we are going to investigate b^2 in the following two cases. A contradiction will result if $b^2 \equiv 0 \pmod 4$, since $2t+1 = 4h$ for some $h \in \mathbb{Z}$. In particular, if $b^2 \equiv 1 \pmod 4$ and $D \equiv 3 \pmod 4$, then we have $t \equiv 1, 3 \pmod 4$. By Equation (4.2.3), we get that, for $x = m + n\sqrt{D}$,

$$\begin{aligned} z(1-z) &= \left(m+n\sqrt{D}\right)\frac{\|z\|}{p} \\ a+b\sqrt{D}-a^2-Db^2-2ab\sqrt{D} &= \left(m+n\sqrt{D}\right)\frac{\|z\|}{p} \\ -p+\frac{a-2Db^2}{\|z\|}+\frac{b-2ab}{\|z\|} &= m+n\sqrt{D}. \end{aligned}$$

It can be readily confirmed that, specifically for the case when $p = 3$, the norm $\|z\| = 18t+3$. By direct computation, $\|z\| \mid a - 2Db^2 = -648t^4 - 864t^3 - 414t^2 - 48t$ and $\|z\| \mid 1 - 2a = -36t^2 - 24t - 3$; namely, $\frac{a-2Db^2}{\|z\|}, \frac{b-2ab}{\|z\|} \in \mathbb{Z}$. By these computations, we obtain the following examples:

Example 4.2.1. When $p = 3$ and $t = 5$, we have

$$\begin{pmatrix} 3 & 512+\sqrt{262,051} \\ 512-\sqrt{262,051} & 31 \end{pmatrix} = \\ \begin{pmatrix} 512+\sqrt{262,051} & 5,627+11\sqrt{262,051} \\ 31 & -511-\sqrt{262,051} \end{pmatrix} \begin{pmatrix} 512-\sqrt{262,051} & 31 \\ 5,627-11\sqrt{262,051} & -512+\sqrt{262,051} \end{pmatrix}.$$

Example 4.2.2. When $p = 3$ and $t = 3$, we have

$$\begin{pmatrix} 3 & 200+\sqrt{39,943} \\ 200-\sqrt{39,943} & 19 \end{pmatrix} = \\ \begin{pmatrix} 200+\sqrt{39,943} & -4,197+21\sqrt{39,943} \\ 19 & -199-\sqrt{39,943} \end{pmatrix} \begin{pmatrix} 200-\sqrt{39,943} & 19 \\ -4,197-21\sqrt{39,943} & -199+\sqrt{39,943} \end{pmatrix}.$$

According to Example 4.1.6, we customize the structure presented in equation (4.2.1) to the following form: For any element $z \in I_p(D)$ with $\|z\| = -p^2$,

$$A(p,z) = \begin{pmatrix} \alpha z & x \\ -\alpha p & 1-\alpha z \end{pmatrix} \begin{pmatrix} \alpha\overline{z} & -\alpha p \\ \overline{x} & 1-\alpha\overline{z} \end{pmatrix}, \tag{4.2.4}$$

for some $x \in \mathcal{O}_{\mathcal{K}}$. We note that $\|1-\alpha z\| = \alpha^2\|z\| - 2\alpha z_1 + 1 = -\alpha^2 p^2 - 2\alpha z_1 + 1$. By direct computation, we have:

$$\begin{aligned} p &= \alpha^2\|z\| + \|x\| \\ z &= \alpha^2 zp + z(1-\alpha z) \\ -p &= \alpha^2 p^2 + \|1-\alpha z\| \qquad (4.2.5) \\ \alpha z(-\alpha z) &= -x\alpha p. \qquad (4.2.6) \end{aligned}$$

According to Equation (4.2.5), it follows that $-p = \alpha^2 p^2 + (-\alpha^2 p^2 - 2\alpha z_1 + 1)$. This indicates that $2\alpha z_1 = 1+p$, leading to the conclusion that $\alpha = \frac{1+p}{2z_1}$. We now assume that $\alpha \in \mathbb{Z}$. For any element $x = x_1 + x_2\sqrt{D}$, by Equation (4.2.6), we have

$$\begin{aligned} -z(1-\alpha z) &= -(x_1+x_2)p \\ z_1 - \alpha(z_1^2 - Dz^2) + (z_2 - 2\alpha z_1 z_2)\sqrt{D} &= px_1 + px_2\sqrt{D}. \end{aligned}$$

So, we have that

$$\begin{aligned} -x_1 &= \frac{z_1 - \left(\frac{1+p}{2z_1}\right)(2z_1^2+p^2)}{p} \\ &= \frac{2z_1^2 - (2z_1^2 + p^2 + 2pz_1^2 + p^3)}{2z_1 p} \\ &= \frac{-2pz_1^2 - p^2(p+1)}{2pz_1} = -z_1 - \frac{p(p+1)}{2z_1} \in \mathbb{Z}, \end{aligned}$$

and

$$-x_2 = \frac{z_2 - 2z_1 z_2 \alpha}{p} = \frac{z_2 - \frac{2z_1 z_2(1+p)}{2z_1}}{p} = \frac{z_2 - z_2(p-1)}{p} = -z_2 \in \mathbb{Z}.$$

Determined by the previous discussion, we can derive the following observation.

Remark 4.2.3. Let p be a prime integer that is irreducible but not prime in $\mathcal{O}_{\mathcal{K}}$ and $z = z_1 + z_2\sqrt{D} \in I_p(D)$ with $\|z\| = -p^2$. If $z_1 \mid \frac{1+p}{2}$, then $A(p,z)$ admits idempotent factorization in the form (4.2.4).

Example 4.2.4.

$$\begin{pmatrix} 19 & 1+\sqrt{362} \\ 1-\sqrt{362} & -19 \end{pmatrix} = \begin{pmatrix} 10+10\sqrt{362} & 191+\sqrt{362} \\ -190 & -9-10\sqrt{362} \end{pmatrix} \begin{pmatrix} 10-10\sqrt{362} & -190 \\ 191-\sqrt{362} & -9+10\sqrt{362} \end{pmatrix}.$$

Usually, one can additionally determine directly that $A(p,z)$ can be represented as a product of two idempotent matrices in the following way:

$$A(p,z) = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix} \begin{pmatrix} d & e \\ f & 1-d \end{pmatrix}$$

if and only if

$$\begin{aligned} p &= ad+bf \\ z &= ae+b(1-d) \\ \overline{z} &= cd+f(1-a) \\ k := \frac{\|z\|}{p} &= ce+(1-a)(1-d) \\ a(1-a) &= bc \\ d(1-d) &= ef, \end{aligned}$$

for some $a,b,c,d,e,f \in \mathcal{O}_K$. Some of the above relations are redundant, which can be reduced to the following lemma:

Lemma 4.2.5. *Let $z \in I_p(D)$. For elements $a,b,c,d,e,f \in \mathcal{O}_K$, we have that*

$$A(p,z) = BC \text{ where } B := \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix} \text{ and } C := \begin{pmatrix} d & e \\ f & 1-d \end{pmatrix},$$

are idempotent matrices if and only if

$$p = ad+bf \tag{4.2.7}$$

$$z(1-a) = kb \tag{4.2.8}$$

$$\overline{z}a = pc \tag{4.2.9}$$

$$zd = pe \tag{4.2.10}$$

$$\overline{z}(1-d) = kf. \tag{4.2.11}$$

Proof. Since B, C are idempotent, $BA(p,z) = A(p,z)$ and $A(p,z)C = A(p,z)$. For $BA(p,z) = A(p,z)$ we have $(B-I)A(p,z) = 0$. Then,

$$\begin{aligned}
(a-1)p &= -b\overline{z} && (4.2.12)\\
(a-1)z &= -bk && (4.2.13)\\
cp &= a\overline{z} && (4.2.14)\\
cz &= bk && (4.2.15)\\
a(1-a) &= bc. && (4.2.16)
\end{aligned}$$

We should note that (4.2.12) is the result of multiplying (4.2.13) by $\overline{z}$, while (4.2.14) is derived from (4.2.15) multiplied by $\overline{z}$. Additionally, (4.2.16) is derived from (4.2.13) and (4.2.14). The previous relationships can be simplified to:

$$\begin{aligned}
(1-a)z &= kb\\
\overline{z}a &= pc.
\end{aligned}$$

In an equivalent way, applying the same procedure to $A(p,z)(I-C) = 0$ yields the following relations:

$$\begin{aligned}
(1-d)\overline{z} &= kf\\
zd &= pe.
\end{aligned}$$

On the other hand, we assume that the equations (4.2.7) to (4.2.11) hold true. Therefore, the multiplication of equations (4.2.8) and (4.2.9) illustrates that B is an idempotent matrix. The equations (4.2.10) and (4.2.11) illustrate that C qualifies as an idempotent matrix. By multiplying equations (4.2.9), (4.2.10), and (4.2.11) by $1-a$, $1-d$, and e, respectively, and applying the subsequent equations:

$$\begin{aligned}
\overline{z} &= cd + (1-a)f\\
z &= ae + b(1-d)\\
k &= ce + (1-a)(1-d),
\end{aligned}$$

thereby concluding the proof. □

Within the framework of D, the quadratic ring of integers $\mathcal{O}_\mathcal{K}$ can be explicitly defined in respect to the quadratic number field $\mathcal{K}$. We divide our computation into two separate cases according to the variable D.

case 1: $D \equiv 1 \pmod 4$ with z in the form $\frac{z_1+z_2\sqrt{D}}{2}$ and $z_1 \equiv z_2 \pmod 2$

case 2: $D \equiv 1, 2, 3 \pmod 4$ and $z = z_1 + z_2\sqrt{D}$ for some $z_1, z_2 \in \mathbb{Z}$.

To establish necessary and sufficient conditions for the idempotent factorization of a matrix $A(p, z) \in \mathbb{M}_2(\mathcal{O}_\mathcal{K})$ into two idempotent matrices, it is sufficient, according to Lemma 4.2.5, to establish the existence of elements $a, b, c \in \mathcal{O}_\mathcal{K}$ that satisfy equations (4.2.8) and (4.2.9), as well as $d, e, f \in \mathcal{O}_\mathcal{K}$ corresponding to equations (4.2.10) and (4.2.11). Additionally, the elements a, d, b, f have to fulfill the conditions described in equation (4.2.7).

Case 1: The existence of $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Z}$ with $a_1 \equiv a_2 \pmod 2$, $b_1 \equiv b_2 \pmod 2$, and $c_1 \equiv c_2 \pmod 2$ must be established is equivalent to

$$\begin{aligned}\left(\frac{z_1 + z_2\sqrt{D}}{2}\right)\left(1 - \frac{a_1 + a_2\sqrt{D}}{2}\right) &= k\left(\frac{b_1 + b_2\sqrt{D}}{2}\right)\\ \left(\frac{z_1 - z_2\sqrt{D}}{2}\right)\left(\frac{a_1 + a_2\sqrt{D}}{2}\right) &= p\left(\frac{c_1 + c_2\sqrt{D}}{2}\right),\end{aligned}$$

and is equivalent to

$$\begin{aligned} z_1a_1 - z_2Da_2 \quad -2pc_1 \qquad\qquad\qquad\quad &= 0\\ -z_2a_1 + z_1a_2 \qquad\quad -2pc_2 \qquad\qquad &= 0\\ z_1a_1 + z_2a_2D \qquad\qquad +2kb_1 \qquad &= 2z_1\\ z_2a_1 + z_1a_2 \qquad\qquad\qquad\quad +2kb_2 \;&= 2z_2.\end{aligned}$$

To determine the existence of $a_1, a_2, c_1, c_2, b_1, b_2 \in \mathbb{Z}$, we initially solve the previously mentioned system of linear equations (with variables $a_1, a_2, b_1, b_2, c_1, c_2$) with the Gauss-Jordan elimination algorithm (over $\mathcal{K}$) and subsequently focus strictly on integral solutions. The row-reduced echelon matrix for the previously

mentioned system is obtained by direct computation as follows:

$$\left(\begin{array}{cccccc|c} 1 & 0 & 0 & 0 & \frac{z_1}{2p} & \frac{-z_2D}{2p} & 2 \\ 0 & 1 & 0 & 0 & \frac{-z_2}{2p} & \frac{z_1}{2p} & 0 \\ 0 & 0 & 1 & 0 & \frac{z_1^2+z_2^2D}{4p^2} & \frac{-2z_1z_2D}{4p^2} & \frac{z_1}{p} \\ 0 & 0 & 0 & 1 & \frac{-2z_1z_2}{4p^2} & \frac{z_1^2+z_2^2D}{4p^2} & \frac{-z_2}{p} \end{array}\right).$$

Then, for integers $b_1, b_2 \in \mathbb{Z}$ with $b_1 \equiv b_2 \pmod 2$, we have that

$$a_1 = \frac{4p - z_1b_1 + z_2b_2D}{2p} \tag{4.2.17}$$

$$a_2 = \frac{z_2b_1 - z_1b_2}{2p} \tag{4.2.18}$$

$$c_1 = \frac{-(z_1^2 + z_2^2D)b_1 + 2z_1z_2Db_2 + 4z_1p}{4p^2} \tag{4.2.19}$$

$$c_2 = \frac{2z_1z_2b_1 - (z_1^2 + z_2^2D)b_2 - 4z_2p}{4p^2}. \tag{4.2.20}$$

We observe that since $z_1 \equiv z_2 \pmod 2$ and $b_1 \equiv b_2 \pmod 2$, it implies that $a_1 \equiv a_2 \pmod 2$ and $c_1 \equiv c_2 \pmod 2$. In a similar way, by repeating the previously mentioned procedure using equations (4.2.10) and (4.2.11), for integers $f_1, f_2 \in \mathbb{Z}$, we likewise obtain that

$$d_1 = \frac{4p - z_1f_1 - z_2f_2D}{2p}$$

$$d_2 = \frac{z_2f_1 + z_1f_2}{2p}$$

$$e_1 = \frac{-(z_1^2 + z_2^2D)b_1 - 2z_1z_2Df_2 + 4z_1p}{4p^2}$$

$$e_2 = \frac{2z_1z_2b_1 + (z_1^2 + z_2^2D)f_2 - 4z_2p}{4p^2}.$$

Remark that since $z_1 \equiv z_2 \pmod 2$ and $f_1 \equiv f_2 \pmod 2$, we have $d_1 \equiv d_2 \pmod 2$ and $e_1 \equiv e_2 \pmod 2$. By relation (4.2.7), $a = (a_1 + a_2\sqrt{D})/2, b = (b_1 + b_2\sqrt{D})/2, d = (d_1 + d_2\sqrt{D})/2$ and $f = (f_1 + f_2\sqrt{D})/2$ must satisfy the condition C_1:

$$0 = (p+k)b_1f_1 + (p+k)Db_2f_2 - z_1(b_1 + f_1) + z_2(b_2 - f_2) + 4p - 4p^2$$

$$0 = 4p^2(b_2f_1 + b_1f_2) + z_1^2(b_2f_1 + b_1f_2) - z_2^2D(b_2f_1 + b_1f_2) - 4pz_1(b_2 + f_2) + 4pz_2(b_1 - f_1).$$

Case 2: The existence of $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Z}$ must be established is equivalent to

$$\begin{aligned}(z_1 + z_2\sqrt{D})(1 - a_1 - a_2\sqrt{D}) &= k(b_1 + b_2\sqrt{D}) \\ (z_1 - z_2\sqrt{D})(a_1 + a_2\sqrt{D}) &= p(c_1 + c_2\sqrt{D}),\end{aligned}$$

and is equivalent to

$$\begin{array}{llllll} z_1a_1 - z_2Da_2 & -pc_1 & & & = & 0 \\ -z_2a_1 + z_1a_2 & & -pc_2 & & = & 0 \\ z_1a_1 + z_2a_2D & & & +kb_1 & = & z_1 \\ z_2a_1 + z_1a_2 & & & +kb_2 & = & z_2. \end{array}$$

By direct computations, the row-reduced echelon form of the previously mentioned system is

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \frac{z_1}{p} \quad \frac{-z_2D}{p} & 1 \\ 0 & 1 & 0 & 0 & \frac{-z_2}{p} \quad \frac{z_1}{p} & 0 \\ 0 & 0 & 1 & 0 & \frac{z_1^2+z_2^2D}{p^2} \quad \frac{-2z_1z_2D}{p^2} & \frac{z_1}{p} \\ 0 & 0 & 0 & 1 & \frac{-2z_1z_2}{p^2} \quad \frac{z_1^2+z_2^2D}{p^2} & \frac{-z_2}{p} \end{array}\right).$$

Then, for integers $b_1, b_2 \in \mathbb{Z}$, we have

$$a_1 = \frac{p - z_1b_1 + z_2b_2D}{p} \tag{4.2.21}$$

$$a_2 = \frac{z_2b_1 - z_1b_2}{p} \tag{4.2.22}$$

$$c_1 = \frac{-(z_1^2 + z_2^2D)b_1 + 2z_1z_2Db_2 + z_1p}{p^2} \tag{4.2.23}$$

$$c_2 = \frac{2z_1z_2b_1 - (z_1^2 + z_2^2D)b_2 - z_2p}{p^2}. \tag{4.2.24}$$

In the same way, we were able to determine that for integers $f_1, f_2 \in \mathbb{Z}$ by repeating the process described above with equations (4.2.10) and (4.2.11).

$$\begin{aligned} d_1 &= \frac{p - z_1f_1 - z_2f_2D}{p} \\ d_2 &= \frac{-z_2f_1 - z_1f_2}{p} \\ e_1 &= \frac{-(z_1^2 + z_2^2D)f_1 - 2z_1z_2Df_2 + z_1p}{p^2} \\ e_2 &= \frac{-2z_1z_2f_1 - (z_1^2 + z_2^2D)f_2 + z_2p}{p^2}. \end{aligned}$$

By relation (4.2.7) with $a = a_1 + a_2\sqrt{D}, b = b_1 + b_2\sqrt{D}, d = d_1 + d_2\sqrt{D}$ and $f = f_1 + f_2\sqrt{D}$ must satisfy the condition C_2:

$$\begin{aligned} 0 &= (p+k)b_1f_1 + (p+k)Db_2f_2 - z_1(b_1+f_1) + z_2(b_2-f_2) + p - p^2 \\ 0 &= p^2(b_2f_1+b_1f_2) + z_1^2(b_2f_1+b_1f_2) - z_2^2D(b_2f_1+b_1f_2) - pz_1(b_2+f_2) + pz_2(b_1-f_1). \end{aligned}$$

In the two cases discussed, specifically when $f_1 = b_1$ and $f_2 = -b_2$, this comes from $a = \overline{d}$ and $b = \overline{f}$. This suggests that the conditions C_1 and C_2 have been changed as follows:

$$0 = (p+k)b_1^2 - (p+k)Db_2^2 - 2z_1b_1 + 2z_2b_2D + 4p - 4p^2, \quad (4.2.25)$$

and

$$0 = (p+k)b_1^2 - (p+k)Db_2^2 - 2z_1b_1 + 2z_2Db_2 + p - p^2, \quad (4.2.26)$$

respectively, where $k = \|z\|/p$. We now provide a necessary and sufficient condition for the idempotent factorization in the form of equation (4.1.1), expressed through a system of quadratic Diophantine equations, compared to a system of equations within the ring of integers.

Theorem 4.2.6. *Let $z \in I_p(D)$. Then, $A(p,z)$ is a product of two idempotent matrices as in equation (4.1.1) if and only if*

case 1: the system of equations (4.2.17) to (4.2.20) and (4.2.25) has an integral solution,

case 2: the system of equations (4.2.21) to (4.2.24) and (4.2.26) has an integral solution.

The previously mentioned theorem suggests that, generally, the condition for idempotent factorization depends on the five equations. For each of the variables p, D, and $z \in I_p(D)$, only one equation is sufficient to determine the idempotent factorization.

Corollary 4.2.7. *Let $D \equiv 2 \pmod 4$ and $k \equiv 3 \pmod 4$. Let $z \in I_2(D)$ in which $\|z\| = 2k$. Then, $A(2,z)$ is a product of two idempotent matrices as in the equation (4.1.1) if and only if the quadratic Diophantine equation*

$$0 = (2+k)b_1^2 - (2+k)Db_2^2 - 2z_1b_1 + 2z_2Db_2 - 2 \quad (4.2.27)$$

has an integer solution.

Proof. Suppose that $A(2,z)$ can be written as a product of two idempotent matrices of the form in equation (4.1.1). According to Theorem 4.2.6, in case 2 with $p=2$, we can deduce from the equation (4.2.26) that the equation (4.2.27) has an integral solution.

On the reverse side, we suppose that the equation (4.2.27) has a solution. Based on $k \equiv 3 \pmod 4$, it follows that $\|z\| \equiv 2 \pmod 4$. Let $z = z_1 + z_2\sqrt{D}$. Thus, $z_1^2 + 2z_2^2 \equiv 2 \pmod 4$, suggesting that $z_1 \equiv 0 \pmod 2$ and $z_2 \equiv 1 \pmod 2$. The fact that the equation (4.2.27) has a solution $b_1, b_2 \in \mathbb{Z}$, it follows that $0 \equiv b_1^2 + 2b_2^2 + 2 \pmod 4$. This implies that $b_1 \equiv 0 \pmod 2$ and $b_2 \equiv 1 \pmod 2$. We can now express

$$z_1 = 2h_1,\ z_2 = 2h_2+1,\ b_1 = 2h_3,\ b_2 = 2h_4+1 \text{ and } D = 4h_5+2$$

for some $h_1, h_2, h_3, h_4, h_5 \in \mathbb{Z}$. According to equations (4.2.21) to (4.2.24), we obtain that the following are all integers:

$$\begin{aligned}
a_1 &= 1 - 2h_1h_3 + (2h_5+1)(2h_4+1)(2h_2+1) \\
a_2 &= h_3(2h_2+1) - h_1(2h_4+1) \\
c_1 &= -h_3(2h_1^2 + (2h_2+1)^2(2h_5+1)) + 2h_1(2h_2+1)(2h_4+1)(2h_5+1) + h_1 \\
c_2 &= 2h_1h_3(2h_2+1) - h_1^2(2h_4+1) - (2h_2+1)(2h_2h_5 + h_2 + h_5 + 1).
\end{aligned}$$

□

Example 4.2.8. For $p=2$ and $z=\sqrt{10}$, we have that a solution of the quadratic Diophantine equation $-3x^2 + 20y^2 + 20y - 2 = 0$ is $x=4$ and $y=1$. Then, according to Corollary 4.2.7, we note that

$$h_1 = h_2 = h_4 = 0, h_3 = 2, h_5 = 2.$$

Hence, by direct calculation, we have

$$\begin{pmatrix} 2 & \sqrt{10} \\ -\sqrt{10} & -5 \end{pmatrix} = \begin{pmatrix} 6+2\sqrt{10} & 4+\sqrt{10} \\ -10-3\sqrt{10} & -5-2\sqrt{10} \end{pmatrix} \begin{pmatrix} 6-2\sqrt{10} & -10+3\sqrt{10} \\ 4-\sqrt{10} & -5+2\sqrt{10} \end{pmatrix}.$$

In order to demonstrate that conjecture 4.1.2 holds true for $z \in I_p(D)$ with $\|z\| = -p^2$, the following lemmas are required.

Lemma 4.2.9. *Let $z \in I_p(D)$ with $\|z\| = -p^2$. Then,*

$$\gcd(z_1, z_2 D) = 1,$$

for $z = z_1 + z_2\sqrt{D}$ or $z = (z_1 + z_2\sqrt{D})/2$ where $z_1, z_2 \equiv 1 \pmod 2$.

Proof. In this proof, we categorize our statement into two distinct circumstances based on the structure of z. In the beginning, our focus is on $z = z_1 + z_2\sqrt{D} \in I_p(D)$. Let $d = \gcd(z_1, z_2 D)$. Therefore, d is a divisor of z_1, and d is also a divisor of $z_2 D$. This suggests that

$$d \mid \left(z_1^2 - D z_2^2\right),$$

where $z_1^2 - D z_2^2 = -p^2$. The possible values of d are $1, p, p^2$. If $d = p$, then p divides z_1 and p divides $z_2 D$. This shows that $p^2 \mid D z_2^2$, given that $p^2 \mid z_1^2$ and $p^2 \mid (z_1^2 - D z_2^2)$. If $p \nmid D$, then $p^2 \mid z_2^2$, which implies $p \mid z_2$; consequently, $p \mid z$, leading to a contradiction. However, if $p \mid D$, then $p \mid z_2^2$, resulting in a contradiction. If $d = p^2$, then $p^2 \mid z_1$ and $p^2 \mid z_2 D$. Assuming that D is square-free, it follows that $p \mid z_1$ and $p \mid z_2$, leading to a contradiction. Consequently, it could be determined that $d = 1$.

In the alternative case, where $D \equiv 1 \pmod 4$ and z is expressed as $\frac{z_1 + z_2\sqrt{D}}{2}$ with $z_1, z_2 \equiv 1 \pmod 2$, it follows that $z_1^2 - z_2^2 D = -4p^2$. We have determined that $d \mid (z_1^2 - D z_2^2)$ where $z_1^2 - D z_2^2 = -4p^2$, where $d = \gcd(z_1, z_2 D)$. The possible values of d are $1, 2, p, 2p, 4p, p^2, 2p^2, 4p^2$. If $2 \mid d$, then $2 \mid z_1$, which contradicts the fact that $z_1 \equiv 1 \pmod 2$. If $p \mid d$, then $p \mid z_1$ and $p \mid z_2 D$. This indicates that $p \mid z_2$, given that $p^2 \mid z_1^2$ and $p^2 \mid (z_1^2 - D z_2^2)$, with D being square-free, leading to a contradiction. This suggests a $d = 1$. □

The following lemma demonstrates that if $z \in I_2(D)$, then $\|z\| \neq -4$.

Lemma 4.2.10. *Let $z \in \mathcal{O}_K$ with $\|z\| = -4$. Then, $\langle 2, z \rangle$ is a principal ideal.*

Proof. We have now established the assumption that $z_1^2 - D z_2^2 = -4$. We first examine a case in which D is an odd square-free integer.

Case1: z_1 is an even number. Consequently, z_2 must be even, indicating that $z \in \langle 2 \rangle$. Therefore, it implies that $\langle 2, z \rangle = \langle 2 \rangle$ is a principal ideal.

Case2: z_1 is an odd integer. So, z_2 must be odd. Then, there exist $m, n \in \mathbb{Z}$ such that

$$\begin{aligned} -4 &= (2m+1)^2 - D(2n+1)^2 \\ &= 4m^2 + 4m - 1 + D(-4n^2 - 4n - 1) \\ &= 4(m^2 - Dn^2 + m - nD) + 1 - D. \end{aligned}$$

So, $D \equiv 1 \pmod 4$. Now, we obtain that

$$\begin{aligned} z = z_1 + z_2\sqrt{D} &= (2m+1) + (2n+1)\sqrt{D} \\ &= 2\left(m + n\sqrt{D} + \left(\frac{1+\sqrt{D}}{2}\right)\right) \\ &\in \langle 2 \rangle. \end{aligned}$$

Next, we turn to a case in which D is an even square-free integer. Given the condition that $z_1^2 - Dz_2^2 = -4$, it follows that z_1 must be an even integer. If z_2 is also even, the evidence is complete. If z_2 is odd, then there are integers m and n such that

$$\begin{aligned} -4 &= 4m^2 - D(4n^2 + 4n + 1) \\ &= 4(m^2 - Dn^2 - Dn) - D. \end{aligned}$$

Therefore, $D \equiv 0 \pmod 4$, resulting in a contradiction. □

According to Lemma 4.2.10, the prime numbers referenced in the following theorem are indeed odd.

Theorem 4.2.11. *Let $z \in I_p(D)$ with $\|z\| = -p^2$. Then,*

$A(p, z)$ can be written into the form of equation (4.1.1).

Proof. In this proof, we partition the proof into two sections based on the form of z: $z = (z_1 + z_2\sqrt{D})/2$ and $z = z_1 + z_2\sqrt{D}$, where $z_1, z_2 \in \mathbb{Z}$. By Theorem 4.2.6 with $k = \|z\|/p = -p$, for $z = \frac{z_1 + z_2\sqrt{D}}{2}$, the equation (4.2.25) becomes

$$2p - 2p^2 = z_1 b_1 - z_2 b_2 D.$$

By applying Theorem 2.1.3 and Lemma 4.2.9, there exist $x, y \in \mathbb{Z}$ such that $1 = z_1 x + (-z_2 D)y$. For each $m \in \mathbb{Z}$, we let

$$\begin{aligned} b_1 &= 2x(p - p^2) - z_2 m D \\ b_2 &= 2y(p - p^2) - m z_1. \end{aligned}$$

When we consider $D \equiv 1 \pmod 4$ and $z_1 \equiv z_2 \pmod 2$, this implies that $b_1 \equiv b_2 \pmod 2$. By substituting b_1, b_2 in the equation (4.2.17), we obtain that

$$\begin{aligned} a_1 &= \frac{4p - z_1(2x(p - p^2) - z_2 m D) + z_2(2y(p - p^2) - m z_1)D}{2p} \\ &= \frac{4p - z_1(2x(p - p^2) + z_2(2y(p - p^2))D}{2p} \\ &= 2(1 - \frac{1-p}{2} z_1 x + \frac{1-p}{2} z_2 D y) \in \mathbb{Z}. \end{aligned}$$

Similarly, by substituting b_1, b_2 in the equation (4.2.18), we obtain the following:

$$\begin{aligned} a_2 &= \frac{z_2(2x(p - p^2) - z_2 m D) - z_1(2y(p - p^2) - m z_1)}{2p} \\ &= \frac{-4mp^2 + z_2(2x(p - p^2)) - z_1(2y(p - p^2))}{2p} \\ &= -2mp + z_2 x(1 - p)) - z_1(y(1 - p)) \\ &= 2(-mp + z_2 x \frac{1-p}{2} - z_1 y \frac{1-p}{2}) \in \mathbb{Z}. \end{aligned}$$

The assumption is that p is an odd integer, then $(1 - p)/2 \in \mathbb{Z}$. Therefore, $a_1 \equiv a_2 \pmod 2$. This is important to note that $z_1^2 + z_2^2 D = 2z_1^2 + 4p^2$, when $\|z\| = (z_1^2 - z_2^2 D)/4 = -p^2$. Then, by substituting b_1, b_2 in equation (4.2.19), we obtain the following:

$$\begin{aligned} c_1 &= \frac{-(z_1^2 + z_2^2 D)(2x(p - p^2) - z_2 m D) + 2z_1 z_2 D(2y(p - p^2) - m z_1)) + 4p z_1}{4p^2} \\ &= \frac{-(2z_1^2 + 4p^2)(2x(p - p^2) - z_2 m D) + 2z_1 z_2 D(2y(p - p^2) - m z_1)) + 4p z_1}{4p^2} \\ &= \frac{-4z_1^2 x(p - p^2) + 2z_1^2 z_2 m D - 8p^2 x(p - p^2) + 4p^2 z_2 m D + 4z_1 z_2 D y(p - p^2) - 2z_1^2 z_2 m D + 4p z_1}{4p^2} \\ &= \frac{-4z_1^2 x(p - p^2) - 8p^2 x(p - p^2) + 4p^2 z_2 m D + 4z_1 z_2 D y(p - p^2) + 4p z_1}{4p^2} \\ &= \frac{4p z_1(-z_1 x(1 - p) + z_2 D y(1 - p) + 1) - 8p^2 x(p - p^2) + 4p^2 z_2 m D}{4p^2} \\ &= \frac{4p^2 z_1 - 8p^2 x(p - p^2) + 4p^2 z_2 m D}{4p^2} \\ &= z_1 - 2x(p - p^2) + z_2 m D \in \mathbb{Z}. \end{aligned}$$

It is important to note that $z_1^2 + z_2^D = -4p^2 + 2z_2^2 D$, when $\|z\| = -p^2$. Then, by substituting b_1, b_2 in equation (4.2.20), we obtain the following:

$$\begin{aligned}
c_2 &= \frac{2z_1z_2(2x(p-p^2) - z_2mD) - (z_1^2 + z_2^2D)(2y(p-p^2) - mz_1)) - 4pz_2}{4p^2} \\
&= \frac{2z_1z_2(2x(p-p^2) - z_2mD) - (-4p^2 + 2z_2^2D)(2y(p-p^2) - mz_1)) - 4pz_2}{4p^2} \\
&= \frac{4z_1z_2x(p-p^2) - 2z_1z_2^2mD + 8p^2y(p-p^2) - 4p^2mz_1 - 4z_2^2yD(p-p^2) + 2z_1z_2^2Dm - 4pz_2}{4p^2} \\
&= \frac{4z_1z_2x(p-p^2) + 8p^2y(p-p^2) - 4p^2mz_1 - 4z_2^2yD(p-p^2) - 4pz_2}{4p^2} \\
&= \frac{4pz_2(z_1x(1-p) - z_2Dy(1-p) - 1) + 8p^2y(p-p^2) - 4p^2mz_1}{4p^2} \\
&= \frac{-4p^2z_2 + 8p^2y(p-p^2) - 4p^2mz_1}{4p^2} \\
&= -z_2 + 2y(p-p^2) - mz_1 \in \mathbb{Z}.
\end{aligned}$$

Since $z_1 \equiv z_2 \pmod 2$, it follows that $c_1 \equiv c_2 \pmod 2$ for every integer $m \in \mathbb{Z}$. According to Theorem 4.2.6, $A(p, z)$ possesses an idempotent factorization in the form of Equation (4.1.1).

In case 2, by Theorem 4.2.6 with $k = -p$, $z = z_1 + z_2\sqrt{D}$, and $\|z\| = -p^2$, the equation (4.2.26) is transformed into the following:

$$\frac{-p(p-1)}{2} = z_1b_1 - z_2Db_2.$$

Once again, Theorem 2.1.3 and Lemma 4.2.9 demonstrate that there exist $x, y \in \mathbb{Z}$ such that $1 = z_1x + (-z_2D)y$. Now, for any integer $m \in \mathbb{Z}$, we have

$$\begin{aligned}
b_1 &= \frac{xp(1-p)}{2} - z_2mD \\
b_2 &= \frac{yp(1-p)}{2} - mz_1.
\end{aligned}$$

By substituting b_1, b_2 into Equation (4.2.21), we obtain that

$$\begin{aligned}
pa_1 &= p - z_1(\frac{xp(1-p)}{2} - z_2mD) + z_2(\frac{yp(1-p)}{2} - mz_1)D \\
pa_1 &= p - z_1\frac{xp(1-p)}{2} + z_2\frac{yp(1-p)}{2} \\
pa_1 &= p + \frac{p(1-p)}{2} \\
a_1 &= 1 + \frac{p-1}{2} \in \mathbb{Z}.
\end{aligned}$$

Similarly, by substituting b_1, b_2 into equation (4.2.22), we also obtain that

$$
\begin{aligned}
pa_2 &= z_2(\frac{xp(1-p)}{2} - z_2mD) - z_1(\frac{yp(1-p)}{2} - mz_1) \\
pa_2 &= pz_2x\frac{1-p}{2} - pz_1y\frac{1-p}{2} + m(z_1^2 - z_2^2D) \\
pa_2 &= pz_2x\frac{1-p}{2} - pz_1y\frac{1-p}{2} - mp^2 \\
a_2 &= z_2x\frac{1-p}{2} - z_1y\frac{1-p}{2} - mp \in \mathbb{Z}.
\end{aligned}
$$

Denote that $z_1^2 + z_2^2D = 2z_1^2 + p^2$, because $\|z\| = z_1^2 - z_2^2D = -p^2$. Then, by substituting b_1, b_2 in equation (4.2.23), we obtain that

$$
\begin{aligned}
p^2c_1 &= -(z_1^2 + z_2^2D)(\frac{xp(1-p)}{2} - z_2mD) + 2z_1z_2D(\frac{yp(1-p)}{2} - mz_1) + z_1p \\
p^2c_1 &= -(2z_1^2 + p^2)(\frac{xp(1-p)}{2} - z_2mD) + 2z_1z_2D(\frac{yp(1-p)}{2} - mz_1) + z_1p \\
p^2c_1 &= -2z_1^2x\frac{p(1-p)}{2} - p^2x\frac{p(1-p)}{2} + mp^2z_2D + 2z_1z_2Dy\frac{p(1-p)}{2} + z_1p \\
p^2c_1 &= -2z_1(z_1x\frac{p(1-p)}{2} - z_2Dy\frac{p(1-p)}{2}) + z_1p + p^2(-x\frac{p(1-p)}{2} + mz_2D) \\
p^2c_1 &= z_1p(p-1) + z_1p + p^2(-x\frac{p(1-p)}{2} + mz_2D) \\
p^2c_1 &= p^2(z_1 - x\frac{p(1-p)}{2} + mz_2D) \\
c_1 &= z_1 - x\frac{p(1-p)}{2} + mz_2D \in \mathbb{Z}.
\end{aligned}
$$

Since $\|z\| = -p^2$, it follows that $z_1^2 + z_2^2D = -p^2 + 2z_2^2D$. Then, by substituting b_1, b_2 in equation (4.2.24), we obtain the following:

$$
\begin{aligned}
p^2c_2 &= 2z_1z_2(\frac{xp(1-p)}{2} - z_2mD) - (z_1^2 + z_2^2D)(\frac{yp(1-p)}{2} - mz_1) - z_2p \\
p^2c_2 &= 2z_1z_2x\frac{p(1-p)}{2} + p^2(y\frac{p(1-p)}{2} - mz_1) - 2z_2^2Dy\frac{p(1-p)}{2} - pz_2 \\
p^2c_2 &= p^2(y\frac{p(1-p)}{2} - mz_1) + 2z_2(z_1x\frac{p(1-p)}{2} - z_2Dy\frac{p(1-p)}{2}) - pz_2 \\
p^2c_2 &= p^2(y\frac{p(1-p)}{2} - mz_1) + 2z_2(z_1x\frac{p(1-p)}{2} + z_2p(1-p) - pz_2 \\
p^2c_2 &= p^2(y\frac{p(1-p)}{2} - mz_1) + 2z_2(z_1x\frac{p(1-p)}{2} - z_2p^2 \\
c_2 &= y\frac{p(1-p)}{2} - mz_1 - z_2 \in \mathbb{Z}.
\end{aligned}
$$

By Theorem 4.2.6, we can conclude that $A(p, z)$ admits an idempotent factorization in the form of Equation (4.1.1). □

According to Theorem 4.2.6, it is evident that the idempotent factorization in Cossu and Zanardo's conjecture is unable to be unique by selecting a different integer m. An additional example of factoring $A(3, 1+\sqrt{10})$, different than the one in Example 4.1.6, is there:

$$\begin{aligned}
A(3,1+\sqrt{10}) &= \begin{pmatrix} 2+5\sqrt{10} & 17+2\sqrt{10} \\ -16+\sqrt{10} & -1-5\sqrt{10} \end{pmatrix} \begin{pmatrix} 2-5\sqrt{10} & -16-\sqrt{10} \\ 17-2\sqrt{10} & -1+5\sqrt{10} \end{pmatrix} \\
&= \begin{pmatrix} 2-19\sqrt{10} & -36-6\sqrt{10} \\ 64-7\sqrt{10} & -1+19\sqrt{10} \end{pmatrix} \begin{pmatrix} 2+19\sqrt{10} & 64+7\sqrt{10} \\ -36+6\sqrt{10} & -1-19\sqrt{10} \end{pmatrix} \\
&= \begin{pmatrix} 2+8\sqrt{10} & 27+3\sqrt{10} \\ -26+2\sqrt{10} & -1-8\sqrt{10} \end{pmatrix} \begin{pmatrix} 2-8\sqrt{10} & -26-2\sqrt{10} \\ 27-3\sqrt{10} & -1+8\sqrt{10} \end{pmatrix} \\
&= \begin{pmatrix} 2-4\sqrt{10} & -13-1\sqrt{10} \\ 14-2\sqrt{10} & -1+4\sqrt{10} \end{pmatrix} \begin{pmatrix} 2-4\sqrt{10} & 14+2\sqrt{10} \\ -13+1\sqrt{10} & -1+4\sqrt{10} \end{pmatrix},
\end{aligned}$$

etcetera. If A is idempotent, then for every invertible matrix X, the matrix $X^{-}AX$ is also idempotent. The following observation inspired us to regard z as the fundamental solution of generalized Pell's equations.

Remark 4.2.12. Let $z \in I_p(D)$. If $A(p,z)$ admits idempotent factorization, then $A(p,zx)$ does also, for any element $x \in \mathcal{O}_{\mathcal{K}}$ with $\|x\| = 1$.

Proof. Let $x \in \mathcal{O}_{\mathcal{K}}$ with $\|x\| = 1$. It follows that $x\overline{x} = 1$. This indicates that $\overline{x} = x^{-1}$. Assume that $A(p,z) = B_1 B_2 \cdots B_m$ for some idempotent matrices B_i for $i = 1, \ldots, m$. Set $X = \operatorname{diag}(1, x)$. Then, $X^{-1} = \operatorname{diag}(1, \overline{x})$. By direct computation, we have

$$\begin{aligned}
A(p,zx) &= X^{-1}A(p,z)X \\
&= X^{-1}\left(B_1 B_2 \cdots B_m\right)X \\
&= X^{-1}B_1\left(XX^{-1}\right)B_2\left(XX^{-1}\right)\cdots\left(XX^{-1}\right)B_m X \\
&= \left(X^{-1}B_1 X\right)\left(X^{-1}B_2 X\right)\cdots\left(X^{-1}B_m X\right)
\end{aligned}$$

is a product of idempotent matrices. □

From this observation, we derive that for the given $\tilde{z}_k := \left(1+\sqrt{10}\right)\cdot\left(19+6\sqrt{10}\right)^k$ for $k \in \mathbb{Z}$, the matrix $A(3, \tilde{z}_k)$ admits idempotent factorization in the form given by (4.1.1).

In 2021, Matthews and Robertson [63] presented a novel method for solving the binary quadratic Diophantine equation $ax^2 + bxy + cy^2 + dx + ey + f = 0$ by converting it into the **Florida transform** in the following equation:

$$as_2^2X^2 + br_2s_2XY + cr_2^2Y^2 = M,$$

where $M = -r_2^2s_2^2\left(ae^2 - bde + cd^2 + f\Delta_1\right)/\Delta_1$, $r_1/r_2 = \alpha/\Delta_1$ and $s_1/s_2 = \beta/\Delta_1$, so that $\gcd(r_1, r_2) = \gcd(s_1, s_2) = 1$, when $\Delta_1 = b^2 - 4ac, \alpha = 2cd - be$ and $\beta = 2ae - db$. By applying the Florida transform to equation (4.2.26), we get that, for any $z \in I_p(D)$,

$$X^2 - DY^2 = (p + k - 1)p^2, \tag{4.2.28}$$

where $\gcd(p + k, z_1) = \gcd(p + k, z_2) = 1$. Utilizing Lemma 2.3.6, we derive the following corollary.

Corollary 4.2.13. *Let $z \in I_p(D)$ with $D \equiv 2, 3 \pmod 4$. Suppose that $p \nmid D$ and $\gcd(p + k, z_1) = \gcd(p + k, z_2) = 1$. If the Kronecker symbol of $\left(\frac{D}{|p+k-1|}\right) = -1$, then $A(p, z)$ cannot be written in the form (4.1.1).*

Proof. According to Lemma 2.3.6, if $\left(\frac{D}{|p+k-1|}\right) = -1$, then the congruence $x^2 \equiv D \pmod{|p + k - 1|}$ does not have a solution. Consequently, the equation (4.2.28) also does not have a solution. This shows that the equation (4.2.26) does not have a solution. According to Theorem 4.2.6, $A(p, z)$ cannot be expressed in the form (4.1.1). □

It is important to observe that the Kronecker symbol $\left(\frac{10}{|7|}\right) = -1$. According to Corollary 4.2.13, it follows that $A(3, 5 + \sqrt{10})$ and $A(3, -5 + \sqrt{10})$ cannot be represented in the form (4.1.1). Furthermore, for $z \in I_p(D)$ with $D \equiv 2 \pmod 4$, we provide an example demonstrating that $A(p, z)$ cannot be decomposed in the form (4.1.1) as the following.

Corollary 4.2.14. *Let $z \in I_p(D)$ with $D \equiv 2 \pmod 4$, $p \equiv 3 \pmod 4$ and $p + \|z\|/p \equiv 2 \pmod 4$. Then, $A(p, z)$ cannot be written in the form (4.1.1).*

Proof. Assuming that we have $p - p^2 \equiv 2 \pmod 4$ and $\|z\| \equiv 1 \pmod 4$. Therefore, the equation $p - p^2 = 4t + 2$ holds for some integer $t \in \mathbb{Z}$. This implies that

$\frac{p-p^2}{2} \equiv 1 \pmod 2$. With regard to $\|z\| \equiv 1 \pmod 4$, it follows that z_1 is an odd integer. According to Equation (4.2.26), it follows that

$$0 \equiv 2b_1^2 + 2z_1b_1 + 2 \pmod 4.$$

This suggests that $2 \equiv 2(b_1(b_1 + z_1)) \pmod 4$. For integers b_1 and z_1, in which z_1 is an odd integer, it follows that $b_1(b_1 + z_1) \equiv 0, 2 \pmod 4$. This implies $2 \equiv 0 \pmod 4$, leading to a contradiction. Therefore, there are no integers b_1, b_2 that satisfy the equation (4.2.26). According to Theorem 4.2.6, it can be concluded that $A(p, z)$ cannot be written in the form (4.1.1). □

For example, when $z = 1 + 2\sqrt{10}$ and $p = 3$, the conditions of Corollary 4.2.14 are satisfied, indicating that $A(3, 1 + 2\sqrt{10})$ cannot be written in the form (4.1.1). Moreover, if we assume that $A(3, 1+2\sqrt{10})$ is a product of two idempotent matrices, namely,

$$A(3, 1+2\sqrt{10}) = \begin{pmatrix} a_1 + a_2\sqrt{10} & b_1 + b_2\sqrt{10} \\ c_1 + c_2\sqrt{10} & 1 - a_1 - a_2\sqrt{10} \end{pmatrix} \begin{pmatrix} d_1 + d_2\sqrt{10} & e_1 + e_2\sqrt{10} \\ f_1 + f_2\sqrt{10} & 1 - d_1 - d_2\sqrt{10} \end{pmatrix},$$

for some $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2, f_1, f_2 \in \mathbb{Z}$, then by Lemma 4.2.5, the equation system:

$$3 = a_1d_1 + 10a_2d_2 + b_1f_1 + 10b_2f_2, \tag{4.2.29}$$

$$0 = d_1a_2 + d_2a_1 + b_1f_2 + b_2f_1, \tag{4.2.30}$$

$$b_1 = \frac{1 - a_1 - 20a_2}{-13}, \qquad e_1 = \frac{d_1 + 20d_2}{3},$$
$$b_2 = \frac{2 - 2a_1 - a_2}{-13}, \qquad e_2 = \frac{2d_1 + d_2}{3},$$
$$c_1 = \frac{a_1 - 20a_2}{3}, \qquad f_1 = \frac{1 - d_1 + 20d_2}{-13},$$
$$c_2 = \frac{-2a_1 + a_2}{3}, \qquad f_2 = \frac{-2 + 2d_1 - d_2}{-13},$$

must have an integral solution. Utilizing the modulo technique to resolve the aforementioned system of equations, it is imperative that we have

$$a_1 = 39l - 7a_2 - 12$$
$$d_1 = 39n + 7d_2 + 27,$$

for some $l, n \in \mathbb{Z}$. So, we have that b_1, b_2 are in terms of l, a_2 and f_1, f_2 are in terms of n, d_2. By substituting the values a_1, a_2, d_1, d_2 into the equations (4.2.29) and (4.2.30), we obtain a system of Diophantine equations that

$$\begin{aligned} 3 &= 1170nl + 210ld_2 + 819l - 210na_2 - 345n - 147a_2 - 65d_2 - 242 \\ 0 &= 30ld_2 - 12n + 21a_2 - 11d_2 + 30na_2 - 8. \end{aligned}$$

Unexpectedly, according to an online calculator for Diophantine equations in [64], we find that the given system of equations does not have a solution that is an integer. Therefore, it follows that no two idempotent matrices over $\mathbb{Z}[\sqrt{10}]$ can be expressed as a product of $A(3, 1 + 2\sqrt{10})$. We have also used this method on several additional matrices, such as $A(7, 13 + 2\sqrt{10}), A(3, \sqrt{15})$ and $A(7, \sqrt{77})$, which cannot be expressed as a product of two idempotent matrices. Based on these scenarios, we are compelled to believe that:

Problem 4.2.15. Let $z \in I_p(D)$. If $\begin{pmatrix} p & z \\ \overline{z} & k \end{pmatrix}$ can be written as a product of two idempotent matrices, then $\begin{pmatrix} p & z \\ \overline{z} & k \end{pmatrix}$ is a product of idempotent in the form (4.1.1).

CHAPTER V

DISCUSSION AND CONCLUSION

This thesis examines the decomposition of matrices whose entries belong to two distinct algebraic structures, divided into specific cases, with the following decomposition methods outlined:

This thesis enhances current approaches for the application of matrices over a division ring, specifically focusing on their use with singular matrices in the relevant context. By applying these lemmas, we demonstrate that if the center of a division ring contains at least $n + 2$ elements, then any $n \times n$ matrix over the division ring can be expressed as a product of three diagonalizable matrices (Theorem 3.3.4). Furthermore, we establish that the Dieudonné determinant of any Hermitian matrix over a division ring is a class represented by an element in a fixed field (Theorem 3.2.4). We demonstrate that if the center of a division ring contains at least $n + 2$ elements, then any non-central matrices over division rings can be expressed as a product of four Hermitian matrices and a diagonalizable matrix, where the Dieudonné determinant belongs to a class containing 1 (Theorem 3.3.5). Additionally, any central matrices over division rings can be represented as a product of five Hermitian matrices and a diagonalizable matrix, with the Dieudonné determinant also belonging to a class containing 1 (Theorem 3.3.6).

For matrices over the quadratic ring of integers, we present a necessary and sufficient condition for the decomposition of any 2×2 singular matrix of a form $A(p, z)$ into a product of two idempotent matrices as in the form (4.1.1) (Theorem 4.2.6). In certain specific instances, we establish that the idempotent factorization is valid when an equation possesses an integral solution (Corollary 4.2.7). We also demonstrate that the idempotent factorization in the form (4.1.1) may not be unique. By applying the Florida transform and Kronneker symbol, we obtain a necessary condition (Corollary 4.2.13).

Future research could benefit from an examination of the definitions asso-

ciated with positive or nonnegative elements within a division ring with involution. Additionally, investigating the concepts of positive definite matrices and positive semidefinite matrices in the framework of a division ring would be interesting. Moreover, the investigation of idempotent factorization of square matrices over the quadratic ring of integers has yet to yield a final answer regarding the general case of $n \times n$ matrices. In the scenario of 2×2 matrices, it is evident that clear factorization is not guaranteed in general cases, as illustrated in Problem 4.2.15 of this thesis.

REFERENCES

REFERENCES

1. Ashraf M, De Filippis V, Siddeeque MA. Advanced Linear Algebra with Applications. Singapore: Springer; 2022.

2. Sourour AR. A factorization theorem for matrices. Linear and Multilinear Algebra. 1986;19(2):141-147.

3. Radjavi H. Products of hermitian matrices and symmetries. Proceedings of the American Mathematical Society. 1969;21(2):369-372.

4. Gentle JE. Matrix Algebra: Theory Computations and Applications in Statistics. 2nd ed. Switzerland: Springer International Publishing; 2017.

5. Kolokoltsov VN, Maslov VP. Idempotent analysis and its applications. Netherlands: Springer Netherlands; 2013.

6. Erdos JA. On products of idempotent matrices. Glasgow Mathematical Journal. 1967;8(2):118-122.

7. Alahmadi A, Jain SK, Leroy A. Decomposition of singular matrices into idempotents. Linear and Multilinear Algebra. 2014;62(1):13-27.

8. Ruitenburg W. Products of idempotent matrices over Hermite domains. Semigroup Forum. 1993;46(3):371-378.

9. Salce L, Zanardo P. Products of elementary and idempotent matrices over integral domains. Linear Algebra and its Applications. 2014;452:130-152.

10. Cossu L, Zanardo P. Factorizations into idempotent factors of matrices over Prüfer domains. Communications in Algebra. 2019;47(4):1818-1828.

11. Lee GT. Abstract algebra: An introductory course. Switzerland: Springer International Publishing; 2018.

12. Dummit DS, Foote RM. Abstract algebra. New Jersey : John Wiley and Sons; 2004.

13. Fraleigh JB. A first course in abstract algebra. 8th ed. Massachusetts: Pearson Education; 2003.

14. Friedberg SH, Insel AJ, Spence LE. Linear Algebra. 4th ed. New Jersey: Pearson Education; 2003.

15. Hungerford TW. Abstract Algebra: An Introduction. 3rd ed. Massachusetts: Cengage Learning; 2014.

16. Rogers K. The axioms for Euclidean domains. The American Mathematical Monthly. 1971;78(10):1127-1128.

17. Cossu L, Zanardo P. Idempotent factorizations of singular 2×2 matrices over quadratic integer rings. Linear and Multilinear Algebra. 2022;70(2):297-309.

18. Trifković M. Algebraic theory of quadratic numbers. New York: Springer+Business Media; 2013.

19. Rosen KH. Elementary number theory. 6th ed. Massachusetts: Pearson Education; 2011.

20. Lay DC, Lay SR, McDonald JJ. Linear Algebra and Its Applications. 5th ed. USA: Pearson Education; 2016.

21. Strang G. Introduction to Linear Algebra. 5th ed. USA: Wellesley-Cambridge Press; 2016.

22. Zhang F. Matrix theory: basic results and techniques. New York: Springer Science+Business Media; 2011.

23. Wan, Z. X. Geometry of matrices: in memory of professor LK Hua (1910–1985). Singapore: World Scientific; 1996.

24. Draxl PK. Skew fields. New York: Cambridge University Press; 1983.

25. Cohn PM. Skew fields, Theory of general division rings. New York: Cambridge University Press; 1998.

26. Centre of a matrix ring are diag$\{a, a, ..., a\}$ with $a \in Z(R)$ [Internet]. Mathematics Stack Exchange. Available from: https://math.stackexchange.com/questions/284043/centre-of-a-matrix-ring-are-operatornamediag-a-a-a-with-a-i

27. Dieudonné J. Les déterminants sur un corps non commutatif. Bulletin de la Société Mathématique de France. 1943;71:27-45.

28. Brenner JL. Applications of the Dieudonné determinant. Linear algebra and its applications. 1968;1(4):511-536.

29. Jarvis F. Algebraic number theory. Switzerland: Springer International Publishing; 2014.

30. Lemmermeyer F. Quadratic number fields. Switzerland: Springer International Publishing; 2021.

31. Lemmermeyer F. The Euclidean algorithm in algebraic number fields. Expositiones Mathematicae. 1995;13:385-416.

32. LeVeque WJ. Topics in Number Theory, volumes I and II.New York: Dover Publications; 1956.

33. Matthews K. The Diophantine Equation $x^2 - Dy^2 = N$, $D > 0$. Expositiones Mathematicae. 2000;18(4):323-332.

34. Stillwell J. Elements of number theory. New York: Springer; 2003.

35. Ballantine CS. Products of positive definite matrices. III. Journal of Algebra. 1968 10(2):174-182.

36. Ballantine CS. Products of positive definite matrices. IV. Linear Algebra and its Applications. 1970;3(1):79-114.

37. Taussky O, Parker WV. 4846. The American Mathematical Monthly. 1960;67(2):192-193.

38. Wu PY. Products of positive semidefinite matrices. Linear Algebra and Its Applications. 1988;111:53-61.

39. Fong CK, Sourour AR. The group generated by unipotent operators. Proceedings of the American Mathematical Society. 1986;97(3):453-458.

40. SHODA VK. Einige sätze über matrizen. InJapanese journal of mathematics: transactions and abstracts. The Mathematical Society of Japan. 1636(13):361-365.

41. Thompson RC. Commutators in the special and general linear groups. Transactions of the American Mathematical Society. 1961;101(1):16-33.

42. Thompson RC. Commutators of matrices with prescribed determinant. Canadian Journal of Mathematics. 1968;20:203-221.

43. Gustafson WH, Halmos PR, Radjavi H. Products of involutions. Linear Algebra and Its Applications. 1976;13(1–2):157–162.

44. Botha JD. Products of diagonalizable matrices. Linear algebra and its applications. 1998;273(1-3):65-82.

45. Bosch AJ. The factorization of a square matrix into two symmetric matrices. The American Mathematical Monthly. 1986;93(6):462-464.

46. Tôyama H. On commutators of matrices. In Kodai mathematical seminar reports, Department of Mathematics, Tokyo Institute of Technology. 1949;5-6(1):1-2

47. Zheng B. Decomposition of matrices into commutators of involutions. Linear algebra and its applications. 2002;347(1-3):1-7.

48. Hou X. Decomposition of matrices into commutators of unipotent matrices of index 2. The Electronic Journal of Linear Algebra. 2021;37:31-34.

49. Wu PY. Products of nilpotent matrices. Linear Algebra and its applications. 1987;96:227-232.

50. Botha JD. Factorization of a singular matrix into nilpotent matrices with prescribed ranks. Linear and Multilinear Algebra. 1994;38(1-2):145-150.

51. Laffey TJ. Products of idempotent matrices. Linear and Multilinear Algebra. 1983;14(4):309-314.

52. Bien MH, Dung TH, Ha NT, Son TN. Decompositions of matrices over division algebras into products of commutators. Linear Algebra and its Applications. 2022;646:119-131.

53. Đoković DŽ. Inner derivations of division rings and canonical Jordan form of triangular operators. Proceedings of the American Mathematical Society. 1985;94(3):383-386.

54. Egorchenkova EA, Gordeev NL. Products of commutators on a general linear group over a division algebra. Journal of Mathematical Sciences. 2019;243(4):561-572.

55. Bien MH, Lam PL, Mai VT. Commutators in special linear groups over certain division rings. Ukrainian Mathematical Journal. 2023;75(3):376-386.

56. Nan J, You H. Products of Involutions in Steinberg Group over Skew Fields. Chinese Annals of Mathematics, Series B. 2007;28:253-264.

57. Huang LP. Geometry of $n \times n$ ($n \geq 3$) Hermitian matrices over any division ring with an involution and its applications. Communications in Algebra®. 2008;36(6):2410-2438.

58. Huang L. Geometry of 2×2 Hermitian matrices over any division ring. Science in China Series A: Mathematics. 2009;52(11):2404-2418.

59. Bien MH, Son TN, Thuy PT, Truong LQ. Products of unipotent matrices of index 2 over division rings. Acta Mathematica Hungarica. 2024;173(1):74-100.

60. Danchev PV, Dung TH, Son TN. Products of traceless and semi-traceless matrices over division rings and their applications. International Journal of Algebra and Computation. 2024;34(03):331-349.

61. Ha NT, Nam PH, Son TN. Products of commutators of involutions in skew linear groups. Acta Mathematica Vietnamica. 2024;49(2):253-263.

62. Dung TH, Son TN. On Kursov's theorem for matrices over division rings. Linear Algebra and its Applications. 2025;704:218-230.

63. Matthews KR, Robertson JP. On solving a binary quadratic Diophantine equation. Rocky Mountain Journal of Mathematics. 2021;51(4):1369-1385.

64. Matthews, K. QUADRATIC DIOPHANTINE EQUATIONS AND FUNDAMENTAL UNIT BCMATH PROGRAMS [Internet]. Available from: http://www.numbertheory.org/php/main_pell.html