กึ่งกลุ่มที่ให้โครงสร้างวงเสมือนหรือกึ่งสนามเสมือน

นายมาโนชญ์ สิริพิทักษ์เดช

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรดุษฎีบัณฑิต

สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2544
ISBN 974-03-1050-8

SEMIGROUPS ADMITTING SKEW-RING OR SKEW-SEMIFIELD STRUCTURES

Mr. Manoj Siripitukdet

A Dissertation Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Science in Mathematics

Department of Mathematics

Faculty of Science

Chulalongkorn University

Academic year 2001

ISBN 974-03-1050-8

Thesis Title	Semigroups admitting skew-ring or skew-semifield structures.
By	Mr. Manoj Siripitukdet
Field of study	Mathematics
Thesis Advisor	Associate Professor Yupaporn Kemprasit, Ph.D.
Thesis Co-advisor	Assistant Professor Amorn Wasanawichit, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Doctor's Degree

……………………………………………. Dean of Faculty of Science
(Associate Professor Wanchai Phothiphichitr, Ph.D.)

THESIS COMMITTEE

………………………………………………Chairman
(Assistant Professor Patanee Udomkavanich, Ph.D.)

……………………………………………..Thesis Advisor
(Associate Professor Yupaporn Kemprasit, Ph.D.)

……………………………………………..Thesis Co-advisor
(Assistant Professor Amorn Wasanawichit, Ph.D.)

……………………………………………..Member
(Assistant Professor Ajchara Harnchoowong, Ph.D.)

……………………………………………..Member
(Associate Professor Chaweewan Ratanaprasert, Ph.D.)

มาโนชญ์ สิริพิทักษ์เดช : กึ่งกลุ่มที่ให้โครงสร้างวงเสมือนหรือกึ่งสนามเสมือน (SEMIGROUPS ADMITTING SKEW-RING OR SKEW-SEMIFIELD STRUCTURES) อ. ที่ปรึกษา : รศ. ดร. ยุพาภรณ์ เข็มประสิทธิ์, อ. ที่ปรึกษาร่วม : ผศ.ดร. อมร วาสนาวิจิตร์ จำนวนหน้า 56 หน้า. ISBN 974-03-1050-8

กึ่งวง คือระบบ $(S, +, \cdot)$ โดยที่ $(S, +)$ และ $(S, \cdot)$ เป็นกึ่งกลุ่ม และ $\cdot$ แจกแจงบน $+$ **วงเสมือน** หมายถึง กึ่งวง $(S, +, \cdot)$ ซึ่ง $(S, +)$ เป็นกลุ่ม เราเรียกสมาชิก 0 ของกึ่งวง $S = (S, +, \cdot)$ ว่า **ศูนย์** ของ S ถ้า $x + 0 = 0 + x = x$ และ $x \cdot 0 = 0 \cdot x = 0$ ทุกสมาชิก $x \in S$ **กึ่งสนามเสมือน** คือ กึ่งวง $(S, +, \cdot)$ ซึ่งสลับที่ภายใต้การบวก มีศูนย์ 0 และ $(S \setminus \{0\}, \cdot)$ เป็นกลุ่ม

สำหรับกึ่งกลุ่ม S ให้ S^0 เป็น S ถ้า S มีศูนย์และ S มีสมาชิกมากกว่า 1 ตัว มิฉะนั้น ให้ S^0 เป็นกึ่งกลุ่ม S ที่ผนวกศูนย์ 0 เข้าไปด้วย เรากล่าวว่ากึ่งกลุ่ม S **ให้โครงสร้างวงเสมือน** ถ้ามีการดำเนินการ $+$ บน S^0 ที่ทำให้ $(S^0, +, \cdot)$ เป็นวงเสมือน เมื่อ $\cdot$ เป็นการดำเนินการบน S^0 เราให้นิยามของ**กลุ่มที่ให้โครงสร้างกึ่งสนามเสมือน**ในทำนองเดียวกัน

ให้ R เป็นวงสลับที่ ซึ่งมีเอกลักษณ์ $1 \neq 0$, $M_n(R)$ เป็นกึ่งกลุ่มของ $n \times n$ เมทริกซ์บน R ทั้งหมดภายใต้การคูณและ $G_n(R)$ เป็นกลุ่มย่อยของ $M_n(R)$ ที่ประกอบด้วย $n \times n$ เมทริกซ์บน R ที่หาตัวผกผันได้ทั้งหมด ให้ V เป็นปริภูมิเวกเตอร์บนวงการหาร, $L(V)$ เป็นกึ่งกลุ่มภายใต้การประกอบของการแปลงเชิงเส้น $\alpha : V \rightarrow V$ ทั้งหมด และ $G(V)$ เป็นกลุ่มย่อยของ $L(V)$ ที่ประกอบด้วยสมสัณฐาน $\alpha : V \rightarrow V$ ทั้งหมด ในการวิจัยนี้ เราบอกลักษณะเฉพาะของกึ่งกลุ่มย่อยหลากหลายของ $M_n(R)$ และ $L(V)$ ว่าเมื่อไรกึ่งกลุ่มย่อยเหล่านี้จะให้โครงสร้างของวงเสมือน เราพิจารณากลุ่มย่อยจำนวนมากของ $G_n(R)$ และ $G(V)$ และให้ลักษณะเฉพาะที่บอกว่ากลุ่มย่อยเหล่านี้ให้โครงสร้างของกึ่งสนามเสมือนเมื่อใด

ภาควิชา **คณิตศาสตร์**	ลายมือชื่อนิสิต...
สาขาวิชา **คณิตศาสตร์**	ลายมือชื่ออาจารย์ที่ปรึกษา..................................
ปีการศึกษา 2544	ลายมือชื่ออาจารย์ที่ปรึกษาร่วม ....

4073804423 MAJOR : MATHEMATICS
KEYWORD : SKEW-RINGS / SKEW-SEMIFIELDS / SEMIGROUPS ADMITTING SKEW-RING STRUCTURE / SEMIGROUPS ADMITTING SKEW-SEMIFIELD STRUCTURE

MANOJ SIRIPITUKDET : SEMIGROUPS ADMITTING SKEW-RING OR SKEW-SEMIFIELD STRUCTURES. THESIS ADVISOR : ASSOCIATE PROFESSOR YUPAPORN KEMPRASIT, Ph.D., THESIS COADVISOR : ASSISTANT PROFESSOR AMORN WASANAWICHIT, Ph.D., 56pp. ISBN 974-03-1050-8

A *semiring* is a system $(S, +, \cdot)$ such that $(S, +)$ and $(S, \cdot)$ are semigroups and $\cdot$ is distributive over +. By a *skew-ring* we mean a semiring $(S, +, \cdot)$ such that $(S, +)$ is a group. An element 0 of a semiring $S = (S, +, \cdot)$ is a *zero* of S if $x + 0 = 0 + x = x$ and $0 \cdot x = x \cdot 0 = 0$ for all $x \in S$. A *skew-semifield* is an additively commutative semiring $(S, +, \cdot)$ with zero 0 such that $(S\setminus\{0\}, \cdot)$ is a group.

For a semigroup S, the semigroup S^0 is defined to be S if S has a zero and S contains more than one element, otherwise, let S^0 be the semigroup S with a zero 0 adjoined. A semigroup S is said to *admit a skew-ring structure* if there exists an operation + on S^0 such that $(S^0, +, \cdot)$ is a skew-ring where $\cdot$ is the operation on S^0. A *group admitting skew-semifield structure* is defined similary.

Let R be a commutative ring with identity $1 \neq 0$, $M_n(R)$ the semigroup of all $n \times n$ matrices over R under matrix multiplication and $G_n(R)$ the subgroup of $M_n(R)$ consisting of all invertible $n \times n$ matrices over R. Let V be a vector space over a division ring, $L(V)$ the semigroup under composition of all linear transformations $\alpha : V \to V$ and $G(V)$ the subgroup of $L(V)$ consisting of all isomorphisms $\alpha : V \to V$. In this research, various subsemigroups of $M_n(R)$ and $L(V)$ are characterized when they admit a skew-ring structure. Many subgroups of $G_n(R)$ and $G(V)$ are considered. We give characterizations determining when they admit a skew-semifield structure.

Department **Mathematics**	Student's signature……………………………..
Field of Study **Mathematics**	Advisor's signature…………………………….
Academic year 2001	Co-advisor's signature ………………………...

ACKNOWLEDGEMENT

I am very grateful to late Dr. Sidney S. Mitchell, my former advisor, who kindly induced me to this research and supervised me helpfully until he passed away. To me, the most important person for my dissertation is Assoc. Prof. Dr. Yupaporn Kemprasit who continued supervising me kindly under the same topic. I am greatly indebted to her for her helpful advice in preparing and writing my dissertation. I am very thankful to my co-advisor, Assist. Prof. Dr. Amorn Wasanawichit, for his helpfulness. Moreover, I would like to thank Assist. Prof. Dr. Patanee Udomkavanich, Assist. Prof. Dr. Ajchara Harnchoowong, and Assoc. Prof. Dr. Chaweewan Ratanaprasert, the chairman and members of this dissertation. Besides, I would like to thank all of my teachers who have taught me for my knowledge and skills.

In particular, I would like to express my appreciation to my beloved parents and wife for their encouragement throughout my study.

CONTENTS

CHAPTER I

INTRODUCTION AND PRELIMINARIES

The multiplicative structure of any ring is by definition a semigroup with zero. Then it is valid to ask whether a given semigroup S has S^0 isomorphic to the multiplicative structure of some ring. If it does, we say that S admits a ring structure. If the multiplicative structure of a ring R is a group with zero, then R is a skew-field. Thus if a group G admits a ring structure, we may say that G admits a skew-field structure. Semigroups admitting ring structure have long been studied. For examples, see [9], [12], [15], [16], [17], [13], [3], [18] and [10].

By our definitions, skew-rings and skew-semifields are generalizations of rings and skew-fields, respectively. Also, the multiplicative structure of a skew-ring is a semigroup with zero and that of a skew-semifield is a group with zero. Semigroups admitting skew-ring structure and groups admitting skew-semifield structure are defined analogously and they are also valid to be studied. Matrix semigroups and semigroups of linear transformations are considered important in the area of semigroups. Also, matrix groups and groups of linear transformations are also important groups. The first section of Chapter II gives characterizations determining when some matrix semigroups admit a skew-ring structure while in the second section, we do the same way on some semigroups of linear transformations. Certain matrix groups are considered in the first section of Chapter III. They are characterized when they admit a skew-semifield structure. In the second section of Chapter III, we are concerned with some groups of linear transformations. The results of determining when they admit skew-semifield structure are provided. In our work, all matrices are over a commutative ring with identity $1 \neq 0$ and all vector spaces are over a division ring.

In the remainder of this chapter, we shall give precise definitions, notations, and basic results which will be used in Chapter II and Chapter III. Moreover, many examples are provided.

For any set X, the cardinality of X will be denoted by $|X|$. For a semigroup S, the semigroup S^0 is defined to be S if S has a zero and S contains more than one element, otherwise, let S^0 be the semigroup with a zero 0 adjoined. Observe that by the notation defined above, we have that for any group G, 0 is a zero adjoined in G^0.

A system $(S, +, \cdot)$ is called a *semiring* if $(S, +)$ and $(S, \cdot)$ are semigroups and $\cdot$ is distributive over $+$, that is, $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$ for all $x, y, z \in S$. A semiring $(S, +, \cdot)$ is said to be *additively* [*multiplicatively*] *commutative* if $(S, +)[(S, \cdot)]$ is commutative. We say that $(S, +, \cdot)$ is *commutative* if both $(S, +)$ and $(S, \cdot)$ are commutative. An element 0 of a semiring $S = (S, +, \cdot)$ is called a *zero* if $x + 0 = 0 + x = x$ and $x \cdot 0 = 0 \cdot x = 0$ for all $x \in S$. A semiring $(S, +, \cdot)$ is said to be a *skew-ring* if $(S, +)$ is a group. An element e of a skew-ring $(S, +, \cdot)$ is called a *left* [*right*] *identity* of $(S, +, \cdot)$ if $ex = x$ [$xe = x$] for all $x \in S$ and e is called an *identity* of S if it is both a left identity and a right identity of S.

The following proposition shows basic properties of skew-rings.

Proposition 1.1([2]). *Let $(S, +, \cdot)$ be a skew-ring. Then the following statements hold.*

(*i*) *$0x = x0 = 0$ for all $x \in S$ where 0 is the identity of the group $(S, +)$.*

(*ii*) *$-(-x) = x$ for all $x \in S$ where $-x$ is the inverse of x in $(S, +)$.*

(*iii*) *$x(-y) = (-x)y = -(xy)$ and $(-x)(-y) = xy$ for all $x, y \in S$.*

(*iv*) *For all $x, y, u, v \in S$, $xy + uv = uv + xy$.*

(*v*) *If $S = S^2$ where $S^2 = \{xy \mid x, y \in S\}$, then S is a ring.*

(*vi*) *If S has a left identity or a right identity, then S is a ring, hence if*

S has an identity, then S is a ring.

We shall give some examples of skew-rings which are not rings.

Example 1. Let $(S,+)$ be a group. Define a binary operation $\cdot$ on S by $x\cdot y=0$ for all $x,y\in S$ where 0 is the identity of the group $(S,+)$. Then $(S,+,\cdot)$ is clearly a skew-ring and in this case, $(S,+,\cdot)$ is called a *zero skew-ring.* If $(S,+)$ is non-abelian, then $(S,+,\cdot)$ is not a ring.

Example 2([2], page 6). Let $(R,+,\cdot)$ be a skew-ring and $M_n(R)$ the set of all $n\times n$ matrices with entries from R. Then $(M_n(R),+,\cdot)$ is a skew-ring where $+$ and $\cdot$ are the usual addition and multiplication of matrices, respectively. If $(R,+,\cdot)$ is not a ring, then $(M_n(R),+,\cdot)$ is not a ring.

The next three examples of skew-rings which are not rings follow from the following proposition. Its proof is straightforward and we omit it.

Proposition 1.2. *Let $(S,+)$ be a group. Let A be a subset of S such that*

(i) $0\in A$ where 0 is the identity of $(S,+)$,

(ii) there is an element $b\in A^c$ such that $b+b=0$ where $A^c=S\backslash A$,

(iii) $A+A^c\subseteq A^c$ and $A^c+A\subseteq A^c$ and

(iv) $A+A\subseteq A$ and $A^c+A^c\subseteq A$.

Define an operation $\cdot$ on S by

$$x\cdot y=\begin{cases}0 & \text{if} \quad x\in A \text{ or } y\in A,\\ b & \text{if} \quad x,y\in A^c.\end{cases}$$

Then $(S, +, \cdot)$ is a skew-ring and it is not a ring if $(S, +)$ is nonabelian.

Example 3. Let $G_n(\mathbb{R})$ be the set of all $n \times n$ invertible matrices over $\mathbb{R}$, $A = \{X \in G_n(\mathbb{R}) \mid \det X > 0\}$ and Z a matrix in $G_n(\mathbb{R})$ defined by

$$Z = \begin{bmatrix} -1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Define an operation $\odot$ on $G_n(\mathbb{R})$ by

$$X \odot Y = \begin{cases} I_n & \text{if } X \in A \text{ or } Y \in A, \\ Z & \text{if } X, Y \notin A. \end{cases}$$

Then $(G_n(\mathbb{R}), \oplus, \odot)$ is a skew-ring and it is not a ring if $n > 1$ where $\oplus$ is the usual multiplication of matrices and I_n is the identity $n \times n$ matrix over $\mathbb{R}$.

Example 4. Let $V_n(\mathbb{R})$ be the set of all $n \times n$ matrices X over $\mathbb{R}$ with $\det X = \pm 1$. Then $V_n(\mathbb{R})$ is a group under the usual multiplication of matrices. Let $A = \{X \mid X \in V_n(\mathbb{R}) \text{ and } \det X = 1\}$ and let Z be defined as in Example 3. Define an operation $\odot$ on $V_n(\mathbb{R})$ by

$$X \odot Y = \begin{cases} I_n & \text{if } X \in A \text{ or } Y \in A, \\ Z & \text{if } X, Y \notin A. \end{cases}$$

Then $(V_n(\mathbb{R}), \oplus, \odot)$ is a skew-ring where $\oplus$ is the usual multiplication of matrices. It is not a ring if $n > 1$.

Example 5. Let S_n be the symmetric group of degree n where $n > 1$, let $A = \{\alpha \in S_n \mid \alpha \text{ is even}\}$ and $\gamma = (1\ 2)$. Define an operation $\odot$ on S_n by

$$\alpha \odot \beta = \begin{cases} I & \text{if } \alpha \in A \text{ or } \beta \in A, \\ \gamma & \text{if } \alpha, \beta \notin A. \end{cases}$$

where I is the identity of S_n. If $\oplus$ is the composition of functions, then $(S_n, \oplus, \odot)$ is a skew-ring. It is not a ring if $n > 2$.

A semigroup S is said to *admit a ring* [*skew-ring*] *structure* if there exists a binary operation $+$ on S^0 such that $(S^0, +, \cdot)$ is a ring [skew-ring] where $\cdot$ is the operation on S^0. Let $\boldsymbol{SR}$ [$\boldsymbol{SSR}$] denote the class of all semigroups admitting ring [skew-ring] structure. Then $\boldsymbol{SR} \subseteq \boldsymbol{SSR}$. As was mentioned previously, semigroups belonging to the class $\boldsymbol{SR}$ have long been studied. We note here that by Proposition 1.1(vi) a semigroup with a left identity or right identity belonging to $\boldsymbol{SSR}$ must be in $\boldsymbol{SR}$.

An additively commutative semiring $S = (S, +, \cdot)$ with zero 0 is called a *skew-semifield* if $(S \setminus \{0\}, \cdot)$ is a group. A *semifield* is a multiplicatively commutative skew-semifield. In fact, a semifield from this definition is referred as a "semifield of zero type" in [14]. By our definition, we see that every skew-field (division ring) and every semifield is a skew-semifield. Skew-semifields are generalizations of both skew-fields and semifields. These are shown by the following examples.

Example 6([11]). Let n be a positive integer greater than 1 and S the set consisting of the zero $n \times n$ matrix and all $n \times n$ matrices over $\mathbb{R}$ of the form

$$\begin{bmatrix} a_1 & 0 & 0 & \dots & x \\ 0 & a_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{bmatrix} \quad \text{where } a_i > 0 \text{ for all } i = 1, 2, ..., n.$$

Then under the usual addition and multiplication of matrices, S is a skew-semifield but neither a semifield nor a skew-field. Note that the multiplicative inverse of the above matrix is

$$\begin{bmatrix} a_1^{-1} & 0 & 0 & \ldots & -xa_1^{-1}a_n^{-1} \\ 0 & a_2^{-1} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & a_n^{-1} \end{bmatrix}.$$

For any group G, the center of G will be denoted by $C(G)$.

A group G is said to *admit a skew-semifield structure* if there exists a binary operation $+$ on G^0 such that $(G^0, +, \cdot)$ is a skew-semifield where $\cdot$ is the operation on G^0. Let $\boldsymbol{GSSF}$ denote the class of all groups which admit a skew-semifield structure.

The following two known results are required for our work.

Proposition 1.3([11]). *If G is a group such that $a^2 = 1$ and $b^2 = 1$ for some distinct $a, b \in G\backslash\{1\}$, then $G \notin \boldsymbol{GSSF}$.*

Proposition 1.4([11]). *If G is a group such that $a^2 = 1$ and $ab \neq ba$ for some $a, b \in G\backslash\{1\}$, then $G \notin \boldsymbol{GSSF}$.*

Next, let R be a commutative ring with identity $1 \neq 0$ and $M_n(R)$ denote the multiplicative semigroup of all $n \times n$ matrices over R. Then $M_n(R)$ is a semigroup having 0 and I_n as its zero and identity, respectively where 0 and I_n denote respectively the zero $n \times n$ matrix and the identity $n \times n$ matrix over R. For $A \in M_n(R)$, the entry of A in the i^{th} row and j^{th} column will be denoted by

A_{ij}. It is known that for $A \in M_n(R)$, A is invertible over R if and only if det$A$ is an invertible element in R ([1], page 204). Let

$$G_n(R) = \{A \in M_n(R) \mid A \text{ is invertible}\}.$$

Then we have that

$$G_n(R) = \{A \in M_n(R) \mid \det A \text{ is an invertible element in } R\}$$

and $G_n(R)$ is the greatest subgroup of $M_n(R)$ having I_n as its identity. For $A \in M_n(R)$, A is called an *orthogonal matrix* if $AA^t = I_n$. A matrix $A \in M_n(R)$ is said to be a *permutation matrix* if every entry of A is either 0 or 1 and each row and each column contains exactly one 1. Let

$$\begin{aligned} O_n(R) &= \{A \in M_n(R) \mid A \text{ is orthogonal}\}, \\ P_n(R) &= \{A \in M_n(R) \mid A \text{ is a permutation matrix}\}. \end{aligned}$$

Since for every $A \in P_n(R)$, $AA^t = I_n$, we have that $P_n(R) \subseteq O_n(R)$. Clearly, both $O_n(R)$ and $P_n(R)$ are subgroups of $G_n(R)$. Next, let

$$\begin{aligned} V_n(R) &= \{A \in M_n(R) \mid \det A = \pm 1\}, \\ W_n(R) &= \{A \in M_n(R) \mid \det A = 1\}. \end{aligned}$$

Then $W_n(R) \subseteq V_n(R)$. Since detAB = det$A$det$B$ for all $A, B \in M_n(R)$ ([8], page 351), it follows that both $V_n(R)$ and $W_n(R)$ are subgroups of $G_n(R)$. Next, let

$$U_n(R) = \{A \in G_n(R) \mid A \text{ is upper triangular}\},$$

$$L_n(R) \;=\; \{A \in G_n(R) \mid A \text{ is lower triangular}\}.$$

Then $U_n(R)$ and $L_n(R)$ contain every diagonal matrix in $G_n(R)$. To show that $U_n(R)$ is a subgroup of $G_n(R)$, it is clear that for $A, B \in U_n(R)$, $AB \in U_n(R)$. Next, let $A \in U_n(R)$ be fixed. Then $A = D + C$ where

$$D \;=\; \begin{bmatrix} A_{11} & 0 & ... & 0 \\ 0 & A_{22} & ... & 0 \\ \vdots & \vdots & ... & \vdots \\ 0 & 0 & ... & A_{nn} \end{bmatrix},$$

$$C \;=\; \begin{bmatrix} 0 & A_{12} & A_{13} & ... & A_{1,n-1} & A_{1n} \\ 0 & 0 & A_{23} & ... & A_{2,n-2} & A_{2n} \\ \vdots & \vdots & \vdots & ... & \vdots & \vdots \\ 0 & 0 & 0 & ... & 0 & A_{n-1,n} \\ 0 & 0 & 0 & ... & 0 & 0 \end{bmatrix}.$$

Since A is invertible, $\det A = A_{11}A_{22}...A_{nn}$ which is invertible in $(R, \cdot)$. Thus

$$D^{-1} = \begin{bmatrix} A_{11}^{-1} & 0 & ... & 0 \\ 0 & A_{22}^{-1} & ... & 0 \\ \vdots & \vdots & ... & \vdots \\ 0 & 0 & ... & A_{nn}^{-1} \end{bmatrix}$$

and there is a unique element x in $R\backslash\{0\}$ such that $(\det A)x = 1$. For $i = 1, 2, ..., n$, set

$$\hat{A}_{ii} = A_{11}...A_{i-1,i-1}A_{i+1,i+1}...A_{nn}.$$

Let

$$P = \begin{bmatrix} x\hat{A}_{11} & 0 & ... & 0 \\ 0 & x\hat{A}_{22} & ... & 0 \\ \vdots & \vdots & ... & \vdots \\ 0 & 0 & ... & x\hat{A}_{nn} \end{bmatrix}.$$

Then $DP = PD = I_n$, so $D^{-1} = P \in U_n(R)$. Since $A \in G_n(R)$, there is $B \in G_n(R)$ such that $AB = BA = I_n$. We now have $I_n = AB = (D + C)B = DB + CB$, so $D^{-1} = D^{-1}I_n = D^{-1}(DB + CB) = B + D^{-1}CB$ which implies that $B = D^{-1} - D^{-1}CB$. For $i, j \in \{1, 2, ..., n\}$ with $i \geq j$, $C_{ij} = 0$, so

$$(D^{-1}C)_{ij} = \sum_{k=1}^{n}(D^{-1})_{ik}C_{kj} = (D^{-1})_{i1}C_{1j} + ... + (D^{-1})_{ii}C_{ij} + ... + (D^{-1})_{in}C_{nj} = 0$$

since $(D^{-1})_{ik} = 0$ for all $k \neq i$. Thus $D^{-1}C$ is of the form

$$\begin{bmatrix} 0 & \star & \star & ... & \star \\ 0 & 0 & \star & ... & \star \\ \vdots & \vdots & \vdots & ... & \vdots \\ 0 & 0 & 0 & ... & \star \\ 0 & 0 & 0 & ... & 0 \end{bmatrix},$$

that is, $(D^{-1}C)_{ij} = 0$ for all i, j with $i \geq j$. Consequently, for $j \in \{1, 2, ..., n\}$,

$$(D^{-1}CB)_{nj} = \sum_{k=1}^{n}(D^{-1}C)_{nk}B_{kj} = 0.$$

Hence $D^{-1}CB$ is of the form

$$D^{-1}CB = \begin{bmatrix} \star & ... & \star \\ \vdots & ... & \vdots \\ \star & ... & \star \\ 0 & ... & 0 \end{bmatrix}$$

and so $D^{-1} - D^{-1}CB$ is of the form

$$D^{-1} - D^{-1}CB = \begin{bmatrix} \star & ... & \star & \star \\ \vdots & ... & \vdots & \vdots \\ \star & ... & \star & \star \\ 0 & ... & 0 & \star \end{bmatrix} = B.$$

Now we see that $B_{nj} = 0$ for all $j \in \{1, 2, ..., n-1\}$. But since $(D^{-1}C)_{n-1,k} = 0$ for all $k \leq n-1$, we have that for $j \in \{1, 2, ..., n-1\}$,

$$\begin{aligned} (D^{-1}CB)_{n-1,j} &= \sum_{k=1}^{n} (D^{-1}C)_{n-1,k} B_{kj} \\ &= \sum_{k=1}^{n-1} (D^{-1}C)_{n-1,k} B_{kj} + (D^{-1}C)_{n-1,n} B_{nj} \\ &= 0 + 0 = 0. \end{aligned}$$

Hence $D^{-1}CB$ is of the form

$$D^{-1}CB = \begin{bmatrix} \star & ... & \star & \star \\ \vdots & ... & \vdots & \vdots \\ \star & ... & \star & \star \\ 0 & ... & 0 & \star \\ 0 & ... & 0 & 0 \end{bmatrix}$$

and so $D^{-1} - D^{-1}CB$ is of the form

$$D^{-1} - D^{-1}CB = \begin{bmatrix} \star & ... & \star & \star & \star \\ \vdots & ... & \vdots & \vdots & \vdots \\ \star & ... & \star & \star & \star \\ 0 & ... & 0 & \star & \star \\ 0 & ... & 0 & 0 & \star \end{bmatrix} = B.$$

By continuing this process, we have that B is of the form

$$D^{-1} - D^{-1}CB = \begin{bmatrix} \star & \star & \dots & \star & \star \\ 0 & \star & \dots & \star & \star \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots. & \star & \star \\ 0 & 0 & \dots & 0 & \star \end{bmatrix} = B.$$

Therefore $B \in U_n(R)$. This proves that $U_n(R)$ is a subgroup of $G_n(R)$.

Similarly, we can show that $L_n(R)$ is a subgroup of $G_n(R)$.

Next, let V be a vector space over a division ring R and $L(V)$ denote the semigroup under composition of all linear transformations $\alpha : V \to V$. Then the zero map 0 and the identity map 1_V on V are respectively the zero and the identity of $L(V)$. Let

$$G(V) = \{\alpha \in L(V) \mid \alpha \text{ is an isomorphism}\}.$$

Then $G(V)$ is the greatest subgroup of $L(V)$ having 1_V as its identity. Since $\mathrm{Im}\alpha\beta \subseteq \mathrm{Im}\beta$ for all $\alpha, \beta \in L(V)$, we have that $IF(V)$ is a subsemigroup of $L(V)$ where

$$IF(V) = \{\alpha \in L(V) \mid \dim(\mathrm{Im}\alpha) \text{ is finite}\}.$$

The following two subsemigroups of $L(V)$ contain $G(V)$:

$$\begin{aligned} M(V) &= \{\alpha \in L(V) \mid \alpha \text{ is one-to-one}\}, \\ E(V) &= \{\alpha \in L(V) \mid \mathrm{Im}\alpha = V\}. \end{aligned}$$

Note that $M(V) \cap E(V) = G(V)$ and $\dim V$ is finite if and only if $M(V)[E(V)] = G(V)$. Let

$$\begin{aligned} AM(V) &= \{\alpha \in L(V) \mid \dim(\mathrm{Ker}\alpha) \text{ is finite}\}, \\ AE(V)) &= \{\alpha \in L(V) \mid \dim(V/\mathrm{Im}\alpha) \text{ is finite}\}. \end{aligned}$$

Then $M(V) \subseteq AM(V)$ and $E(V) \subseteq AE(V)$. These two sets may be respectively considered as the set of all "almost one-to-one" linear transformations of V and the set of all "almost onto" linear transformations of V. To show that $AM(V)$ and $AE(V)$ are subsemigroups of $L(V)$, let $\alpha, \beta \in L(V)$. It is clear that $\mathrm{Ker}(\alpha\mid_{\mathrm{Ker}\alpha\beta}) = \mathrm{Ker}\alpha$. Since $(\mathrm{Im}\alpha \cap \mathrm{Ker}\beta)\alpha^{-1} = \mathrm{Ker}\alpha\beta$, we have $\mathrm{Im}(\alpha\mid_{\mathrm{Ker}\alpha\beta})$ $= \mathrm{Im}\alpha \cap \mathrm{Ker}\beta$. But

$$\dim(\mathrm{Ker}\alpha\beta) = \dim(\mathrm{Ker}(\alpha\mid_{\mathrm{Ker}\alpha\beta})) + \dim(\mathrm{Im}(\alpha\mid_{\mathrm{Ker}\alpha\beta})),$$

so we have

$$\begin{aligned} \dim(\mathrm{Ker}\alpha\beta) &= \dim(\mathrm{Ker}\alpha) \ + \ \dim(\mathrm{Im}\alpha \cap \mathrm{Ker}\beta) \\ &\leq \dim(\mathrm{Ker}\alpha) \ + \ \dim(\mathrm{Ker}\beta). \end{aligned} \tag{1.1}$$

Define $\beta^* : V/\mathrm{Im}\alpha \to \mathrm{Im}\beta/(\mathrm{Im}\alpha)\beta$ by

$$(v + \mathrm{Im}\alpha)\beta^* = v\beta + (\mathrm{Im}\alpha)\beta$$

for all $v \in V$. Then β^* is clearly well-defined and a linear transformation of

$V/\mathrm{Im}\alpha$ onto $\mathrm{Im}\beta/(\mathrm{Im}\alpha)\beta$. Hence

$$\dim(\mathrm{Im}\beta/(\mathrm{Im}\alpha)\beta) \leq \dim(V/\mathrm{Im}\alpha).$$

Because $\mathrm{Im}\alpha\beta \subseteq \mathrm{Im}\beta$, we have

$$V/\mathrm{Im}\beta \cong (V/\mathrm{Im}\alpha\beta)/(\mathrm{Im}\beta/\mathrm{Im}\alpha\beta),$$

which implies that

$$\dim(V/\mathrm{Im}\beta) = \dim((V/\mathrm{Im}\alpha\beta)/(\mathrm{Im}\beta/\mathrm{Im}\alpha\beta)).$$

Also, we know that

$$\dim(V/\mathrm{Im}\alpha\beta) = \dim(\mathrm{Im}\beta/\mathrm{Im}\alpha\beta) + \dim((V/\mathrm{Im}\alpha\beta)/(\mathrm{Im}\beta/\mathrm{Im}\alpha\beta)).$$

All of these facts yield the following inequality.

$$\dim(V/\mathrm{Im}\alpha\beta) \leq \dim(V/\mathrm{Im}\alpha) + \dim(V/\mathrm{Im}\beta). \tag{1.2}$$

By (1.1) and (1.2), we have that $AM(V)$ and $AE(V)$ are subsemigroups of $L(V)$. Observe that $\dim V$ is finite if and only if $AM(V)[AE(V)] = L(V)$. Moreover, if $\dim V$ is infinite, then neither $AM(V)$ nor $AE(V)$ contains a zero.

To characterize when any subsemigroup of $L(V)$ containing $G(V)$ belongs to ***SSR***, the following two known results are useful.

Proposition 1.5([10]). *Let S be a subsemigroup of $L(V)$ containing $G(V)$. If there exists an operation $\oplus$ on S^0 such that $(S^0, \oplus, \cdot)$ is a ring where $\cdot$ is the* *operation on S^0, then*

$$\ominus\alpha \;=\; \alpha \text{ for all } \alpha \in S^0 \text{ or } \ominus \alpha \;=\; -\alpha \text{ for all } \alpha \in S^0$$

where $\ominus\alpha$ is the additive inverse of α in $(S^0, \oplus, \cdot)$ and $-\alpha$ is the inverse of α under usual addition in $L(V)$.

Proposition 1.6([10]). *$G(V) \in \boldsymbol{SR}$ if and only if $\dim V \leq 1$.*

Now, let

$$\begin{aligned} OM(V) &= \{\alpha \in L(V) \mid \dim(\mathrm{Ker}\alpha) \;\text{ is infinite}\}, \\ OE(V)) &= \{\alpha \in L(V) \mid \dim(V/\mathrm{Im}\alpha) \;\text{ is infinite}\}. \end{aligned}$$

Assume that $\dim V$ is infinite. Then $0 \in OM(V)$ and $0 \in OE(V)$. Since for $\alpha, \beta \in L(V)$, $\mathrm{Ker}\alpha\beta \supseteq \mathrm{Ker}\alpha$, it follows that $\alpha\beta \in OM(V)$ for all $\alpha, \beta \in OM(V)$. Thus $OM(V)$ is a subsemigroup of $L(V)$. It may be considered as the "opposite semigroup" of $M(V)$. Since for $\alpha, \beta \in L(V)$, $\mathrm{Im}\alpha\beta \subseteq \mathrm{Im}\beta$, we have that

$$\dim(V/\mathrm{Im}\alpha\beta) \geq \dim(V/\mathrm{Im}\beta).$$

This implies that $\alpha\beta \in OE(V)$ for all $\alpha, \beta \in OE(V)$, so $OE(V)$ is a subsemigroup of $L(V)$. We can consider this semigroup as "the opposite semigroup" of $E(V)$.

Following the definition of the Baer-Levi semigroup on a countably infinite set ([5], page 14), we define

$$BL(V) = \{\alpha \in L(V) \mid \alpha \text{ is one-to-one and } \dim(V/\text{Im}\alpha) \text{ is infinite}\}$$
$$\text{where } \dim V \text{ is infinite.}$$

Then $BL(V) = M(V) \cap OE(V)$. Let B be a basis of V and let $B_1 \subseteq B$ be such that $\mid B_1 \mid = \mid B \backslash B_1 \mid = \mid B \mid$. Let $\varphi : B \to B_1$ be a bijection. Define $\eta \in L(V)$ by $v\eta = v\varphi$ for all $v \in B$. Then η is one-to-one and

$$\begin{aligned} \dim(V/\text{Im}\eta) &= \dim(V/ <B_1>) \\ &= \dim(< \{v+ <B_1> \mid v \in B\backslash B_1\} >) \\ &= \mid B\backslash B_1 \mid, \end{aligned}$$

so $\eta \in BL(V)$. Hence $BL(V)$ is a subsemigroup of $L(V)$. The following subset of $L(V)$ should be also considered:

$$OBL(V) = \{\alpha \in L(V) \mid \ \dim(\text{Ker}\alpha) \text{ is infinite and } \text{Im}\alpha = V\}$$
$$\text{where } \dim V \text{ is infinite.}$$

Then $OBL(V) = OM(V) \cap E(V)$. Let $\mu \in L(V)$ be defined by

$$v\mu = \begin{cases} v\varphi^{-1} & \text{if} \quad v \in B_1, \\ 0 & \text{if} \quad v \in B\backslash B_1. \end{cases}$$

Then $\text{Ker}\mu = < B\backslash B_1 >$ and $\text{Im}\mu = < B > = V$, so $\mu \in OBL(V)$. Hence $OBL(V)$ is a subsemigroup of $L(V)$ which can be considered as “the opposite semigroup” of $BL(V)$. Observe that neither $BL(V)$ nor $OBL(V)$ contains a zero.

For $\alpha \in L(V)$, define

$$F(\alpha) = \{v \in V \mid v\alpha = v\}.$$

Then for every $\alpha \in L(V)$, $F(\alpha)$ is a subspace of V and α is said to be *almost identical* if $\dim(V/F(\alpha))$ is finite. Next, let

$$\begin{aligned} AI(V) &= \{\alpha \in L(V) \mid \alpha \text{ is almost identical}\}, \\ GAI(V) &= \{\alpha \in G(V) \mid \alpha \text{ is almost identical}\}. \end{aligned}$$

Then $1_V \in GAI(V) \subseteq AI(V)$. To show that $AI(V)$ is a subsemigroup of $L(V)$ and $GAI(V)$ is a subgroup of $G(V)$, let $\alpha, \beta \in AI(V)$. Then $\dim(V/F(\alpha))$ is finite and $\dim(V/F(\beta))$ is finite. Note that $F(\alpha) \cap F(\beta) \subseteq F(\alpha\beta)$. Let B_0 be a basis of $F(\alpha) \cap F(\beta)$. Then there are bases B_1 of $F(\alpha)$ and B_2 of $F(\beta)$ such that $B_0 \subseteq B_1$ and $B_0 \subseteq B_2$. Thus $B_0 \subseteq B_1 \cap B_2$. It follows that $F(\alpha) \cap F(\beta) = < B_0 > \subseteq < B_1 \cap B_2 >$. Since $B_1 \cap B_2 \subseteq F(\alpha) \cap F(\beta)$, $< B_1 \cap B_2 > \subseteq F(\alpha) \cap F(\beta)$. Hence $B_1 \cap B_2$ is a basis of $F(\alpha) \cap F(\beta)$. We also have $B_1 \cup B_2$ is linearly independent. Let B be a basis of V containing $B_1 \cup B_2$. Then we have

$$B \backslash (B_1 \cap B_2) = (B \backslash B_1) \cup (B \backslash B_2),$$

and so

$$\mid B \backslash (B_1 \cap B_2) \mid \leq \mid B \backslash B_1 \mid + \mid B \backslash B_2 \mid .$$

But

$$\begin{aligned}\dim(V/F(\alpha)\cap F(\beta)) &= \dim(V/< B_1\cap B_2 >) = \mid B\backslash(B_1\cap B_2)\mid,\\ \dim(V/F(\alpha)) &= \dim(V/< B_1 >) = \mid B\backslash B_1\mid,\\ \dim(V/F(\beta)) &= \dim(V/< B_2 >) = \mid B\backslash B_2\mid\end{aligned}$$

and both $\dim(V/F(\alpha))$ and $\dim(V/F(\beta))$ are finite, so $\dim(V/F(\alpha)\cap F(\beta))$ is finite. Since $F(\alpha)\cap F(\beta)\subseteq F(\alpha\beta)$,we have $\dim(V/F(\alpha\beta))\leq \dim(V/(F(\alpha)\cap F(\beta)))$. Thus $\dim(V/F(\alpha\beta))$ is finite, so $\alpha\beta\in AI(V)$. Hence $AI(V)$ is a subsemigroup of $L(V)$. If $\alpha\in GAI(V)$, then $F(\alpha)=F(\alpha^{-1})$, so $GAI(V)$ is clearly a subgroup of $G(V)$. Note that if $\dim V$ is finite, then $AI(V)=L(V)$ and $GAI(V)=G(V)$. If $\dim V$ is infinite, $AI(V)$ does not contains a zero.

A subgroup of $G(V)$ defining by a fixed basis of V is given as follows: Let B be a basis of V. For finite distinct elements $u_1,u_2,...,u_k\in B$, let $(u_1,u_2,...,u_k)_B\in G(V)$ be defined by

$$v(u_1,u_2,...,u_k)_B=\begin{cases} u_{i+1} & \text{if} \quad v=u_i \text{ for } i=1,2,...,k-1,\\ u_1 & \text{if} \quad v=u_k,\\ v & \text{if} \quad v\in B\backslash\{u_1,u_2,...,u_k\},\end{cases}$$

and let $G_B(V)$ be the subgroup of $G(V)$ generated by the set

$$\{(u_1,u_2,...,u_k)_B \mid \ u_1,u_2,...,u_k \text{ are distinct elements of } B \text{ and } k\in\mathbb{N}\}$$

where $\mathbb{N}$ is the set of positive integers.

CHAPTER II

SEMIGROUPS ADMITTING SKEW-RING STRUCTURE

In this chapter, we divide into two sections. In the first section, we consider some matrix semigroups over a commutative ring with identity $1 \neq 0$ under usual multiplication and investigate them when they belong to the class $\boldsymbol{SSR}$. Likewise, in the second section some semigroups under composition of linear transformations of a vector space over a division ring are considered and investigated in the same way.

2.1. Matrix Semigroups

Throughout this section, let n be a positive integer, $R = (R, +, \cdot)$ a commutative ring with identity $1 \neq 0$. Recall that $M_n(R)$ is the full $n \times n$ matrix semigroup under usual multiplication and $G_n(R)$ the unit group of $M_n(R)$, that is,

$$G_n(R) = \{A \in M_n(R) \mid A \text{ is invertible}\}.$$

For $k, l \in \{1, 2, ..., n\}$, let $E^{kl} \in M_n(R)$ be defined by

$$E^{kl}_{ij} = \begin{cases} 1 & \text{if } i = k \text{ and } j = l, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\det E^{kl} = 0$ for all $k, l \in \{1, 2, ..., n\}$ if $n > 1$. As was mentioned in Chapter 1, page 7,

$$G_n(R) = \{A \in M_n(R) \mid \det A \text{ is invertible in } R\}.$$

In particular, if R is a field, then

$$G_n(R) = \{A \in M_n(R) \mid \det A \neq 0\}.$$

Then $G_n(R) \cap \{A \in M_n(R) \mid \det A = 0\} = \emptyset$. In fact, $\{A \in M_n(R) \mid \det A = 0\}$ is clearly an ideal of the semigroup $M_n(R)$. Since $(M_n(R), +, \cdot)$ is a ring where $+$ and $\cdot$ are the usual addition and multiplication of matrices, respectively, we have that $M_n(R) \in \boldsymbol{SR}$. However, the first theorem shows that if $n > 1$, then $M_n(R)$ itself is the only subsemigroup of $M_n(R)$ containing $\{A \in M_n(R) \mid \det A = 0\}$ which belongs to $\boldsymbol{SSR}$.

Theorem 2.1.1. *Let $n > 1$ and S a subsemigroup of $M_n(R)$ containing every matrix $A \in M_n(R)$ with $\det A = 0$. If $S \in \boldsymbol{SSR}$, then $S = M_n(R)$.*

Proof. First, we note that S contains the zero matrix 0 of $M_n(R)$, $|S| > 1$ and $E^{kl} \in S$ for all $k, l \in \{1, 2, ..., n\}$. Assume that there exists an operation $\oplus$ on S such that $(S, \oplus, \cdot)$ is a skew-ring where $\cdot$ is the multiplication on S. To show that $S = M_n(R)$, let $A \in M_n(R)$. Define $B, C \in M_n(R)$ by

$$B = \begin{bmatrix} A_{11} & ... & A_{1,n-1} & 0 \\ A_{21} & ... & A_{2,n-1} & 0 \\ \vdots & ... & \vdots & \vdots \\ A_{n1} & ... & A_{n,n-1} & 0 \end{bmatrix}$$

and

$$C = \begin{bmatrix} 0 & ... & 0 & A_{1n} \\ 0 & ... & 0 & A_{2n} \\ \vdots & ... & \vdots & \vdots \\ 0 & ... & 0 & A_{nn} \end{bmatrix}.$$

Then $\det B = 0 = \det C$, so $B, C \in S$. It follows that $B \oplus C \in S$. But $CE^{nn} = C$ and $BE^{nn} = 0 = CE^{k1}$ for all $k \in \{1, 2, ..., n-1\}$, so

$$(B \oplus C)E^{nn} = C \text{ and } (B \oplus C)E^{k1} = BE^{k1} \text{ for all } k \in \{1, 2, ..., n-1\}.$$

Hence for $i \in \{1, 2, ..., n\}$,

$$\begin{aligned} (B \oplus C)_{in} &= \sum_{k=1}^{n} (B \oplus C)_{ik} E^{nn}_{kn} \quad \text{since } E^{nn}_{kn} = 0 \text{ if } k \neq n \text{ and } E^{nn}_{nn} = 1 \\ &= ((B \oplus C)E^{nn})_{in} \\ &= C_{in} \ = \ A_{in} \end{aligned}$$

and for $i \in \{1, 2, ..., n\}$ and $j \in \{1, 2, ..., n-1\}$,

$$\begin{aligned} (B \oplus C)_{ij} &= \sum_{k=1}^{n} (B \oplus C)_{ik} E^{j1}_{k1} \quad \text{since } E^{j1}_{k1} = 0 \text{ if } k \neq j \text{ and } E^{j1}_{j1} = 1 \\ &= ((B \oplus C)E^{j1})_{i1} \\ &= (BE^{j1})_{i1} \\ &= \sum_{k=1}^{n} B_{ik} E^{j1}_{k1} \\ &= B_{ij} \ = \ A_{ij}. \end{aligned}$$

Consequently, $A = B \oplus C \in S$.

Hence the theorem is proved. $\square$

If I is the ideal $\{A \in M_n(R) \mid \det A = 0\}$, then $n = 1$ implies that $I^0 \cong (\mathbb{Z}_2, \cdot)$. The following corollary is obtained directly from Theorem 2.1.1 and the above fact.

Corollary 2.1.2. *The ideal $\{A \in M_n(R) \mid detA = 0\}$ of $M_n(R)$ belongs to the class* $\boldsymbol{SSR}$ *if and only if $n = 1$.*

Recall the subgroups $V_n(R)$ and $W_n(R)$ of $G_n(R)$ that

$$\begin{aligned} V_n(R) &= \{A \in G_n(R) \mid \det A = \pm 1\}, \\ W_n(R) &= \{A \in G_n(R) \mid \det A = 1\}. \end{aligned}$$

The next theorem shows that every subsemigroup of $G_n(R)$ containing $V_n(R)$ does not belong to $\boldsymbol{SSR}$ if $n > 1$. The following lemma is required.

Lemma 2.1.3. *If $A \in M_n(R)$ is such that AB=BA for every $B \in W_n(R)$, then $A = aI_n$ for some $a \in R$ where I_n is the identity $n \times n$ matrix over R.*

Proof. It is trivial if $n = 1$. Assume that $n > 1$. Let $s, t \in \{1, 2, ..., n\}$ be such that $s < t$. Define $B, C \in M_n(R)$ by

$$B_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 1 & \text{if } i = s \text{ and } j = t, \\ 0 & \text{otherwise} \end{cases}$$

and

$$C_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 1 & \text{if } i = t \text{ and } j = s, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\det B = 1 = \det C$. By assumption, $AB = BA$ and $AC = CA$. Thus

$$\begin{aligned}(AB)_{ss} &= \sum_{k=1}^{n} A_{sk}B_{ks} = A_{ss},\\ (BA)_{ss} &= \sum_{k=1}^{n} B_{sk}A_{ks} = A_{ss} + A_{ts},\\ (AC)_{tt} &= \sum_{k=1}^{n} A_{tk}C_{kt} = A_{tt}\end{aligned}$$

and

$$(CA)_{tt} = \sum_{k=1}^{n} C_{tk}A_{kt} = A_{st} + A_{tt}.$$

Consequently, $A_{ts} = A_{st} = 0$. This proves that

$$A_{st} = 0 \text{ for all distinct } s, t \in \{1, 2, ..., n\}. \tag{2.1.3.1}$$

For $k \in \{1, 2, ..., n\}$, define $D^{(k)} \in M_n(R)$ by

$$D_{ij}^{(k)} = \begin{cases} 1 & \text{if } i = j,\\ 1 & \text{if } i = 1 \text{ and } j = k,\\ 0 & \text{otherwise.}\end{cases}$$

Then $\det D^{(k)} = 1$ for all $k \in \{1, 2, ..., n\}$, so $AD^{(k)} = D^{(k)}A$ for every $k \in \{1, 2, ..., n\}$. From (2.1.3.1) and the definition of D, we have that for $i \in \{1, 2, ..., n\}$,

$$(AD^{(i)})_{1i} = \sum_{k=1}^{n} A_{1k}D_{ki}^{(i)} = A_{11}$$

and

$$(D^{(i)}A)_{1i} = \sum_{k=1}^{n} D^{(i)}_{1k} A_{ki} = A_{ii}.$$

It then follows that

$$A_{11} = A_{ii} \text{ for every } i \in \{1, 2, ..., n\}. \tag{2.1.3.2}$$

From (2.1.3.1) and (2.1.3.2), $A = aI$ where $a = A_{11}$. $\square$

Theorem 2.1.4. *If $n > 1$ and S is a subsemigroup of $G_n(R)$ containing $V_n(R)$, then S does not belong to the class **SSR**.*

Proof. Suppose that there exists an operation $\oplus$ on S^0 such that $(S^0, \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on S^0. Since $I_n \in V_n(R) \subseteq S$, by Proposition 1.1(vi), $(S^0, \oplus, \cdot)$ is a ring. Let $A \in S$ be such that $I_n \oplus A = 0$. Then for every $B \in S$,

$$B \oplus AB = (I_n \oplus A)B = 0 = B(I_n \oplus A) = B \oplus BA.$$

This implies that $AB = BA$ for every $B \in S$. By Lemma 2.1.3, $A = aI_n$ for some $a \in R$. Therefore $I_n \oplus aI_n = 0$. Next, let $C \in M_n(R)$ be defined by

$$C = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Then $C \neq I_n$, $C \neq aI_n$, $C^2 = I_n$ and $\det C = -1$. Thus $C \in V_n(R) \subseteq S$. Since $I_n \oplus aI_n = 0$ and $C \neq aI_n$, we have $I_n \oplus C \neq 0$. Because S is a subsemigroup of the group $G_n(R)$, S is cancellative. But

$$C(I_n \oplus C) = C \oplus C^2 = C \oplus I_n = I_n \oplus C$$

and $I_n \oplus C \neq 0$, so we have $C = I_n$, a contradiction.

Hence the theorem is proved. □

Corollary 2.1.5. *$G_n(R) \in \boldsymbol{SSR}$ if and only if $n = 1$ and $U_R \in \boldsymbol{SSR}$ where U_R denotes the multiplicative group of all invertible elements of R.*

Proof. If $n > 1$, then by Theorem 2.1.4, $G_n(R) \notin \boldsymbol{SSR}$. Next, assume that $n = 1$ and $U_R \notin \boldsymbol{SSR}$. But since $G_1(R) \cong U_R$, we have $G_1(R) \notin \boldsymbol{SSR}$.

Conversely, if $n = 1$ and $U_R \in \boldsymbol{SSR}$, then $U_R \cong G_1(R) \in \boldsymbol{SSR}$. □

Corollary 2.1.6. *$V_n(R) \in \boldsymbol{SSR}$ if and only if $n = 1$.*

Proof. If $n > 1$, then $V_n(R) \notin \boldsymbol{SSR}$ by Theorem 2.1.4.

Since

$$V_1^0(R) \cong (\{0, 1, -1\}, \cdot) \cong \begin{cases} (\mathbb{Z}_3, \cdot) & \text{if} \quad \text{char}R \neq 2, \\ (\mathbb{Z}_2, \cdot) & \text{if} \quad \text{char}R = 2, \end{cases}$$

the converse holds. □

The last theorem of this section shows that if $n > 2$, there is no subsemigroup of $G_n(R)$ in $\boldsymbol{SSR}$ which contains $W_n(R)$.

Theorem 2.1.7. *If $n > 2$ and S is a subsemigroup of $G_n(R)$ containing $W_n(R)$, then S does not belong to the class* $\boldsymbol{SSR}$.

Proof. Suppose that there exists an operation $\oplus$ on S^0 such that $(S^0, \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on S^0. Since $I_n \in W_n(R) \subseteq S$, $(S^0, \oplus, \cdot)$ is a ring. Let $A \in S$ be such that $I_n \oplus A = 0$. Then

$$B \oplus AB = (I_n \oplus A)B = 0 = B(I_n \oplus A) = B \oplus BA$$

for every $B \in S$, so $AB = BA$ for all $B \in S$. By Lemma 2.1.3, $A = aI_n$ for some $a \in R$.

Case 1: char$R = 2$. Let $C \in M_n(R)$ be defined by

$$C = \begin{bmatrix} 1 & 0 & 0 & \ldots & 1 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix}.$$

Then det$C = 1$, so $C \in S$. Since char$R = 2$, $C^2 = I_n$. Also, we have $C \neq I_n$ and $C \neq aI_n = A$. Thus $I_n \oplus C \neq 0$. Since S is cancellative and

$$C(I_n \oplus C) = C \oplus C^2 = C \oplus I_n = I_n \oplus C,$$

it follows that $C = I_n$, a contradiction.

Case 2: char$R \neq 2$. Then $1 \neq -1$. Let $D \in M_n(R)$ be defined by

$$D = \begin{bmatrix} -1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & -1 \end{bmatrix}.$$

Then $D^2 = I_n$ and $\det D = 1$, so $D \in S$. Since $\operatorname{char} R \neq 2$, $D \neq I_n$. Also, $D \neq aI_n = A$ because $n > 2$ and $\operatorname{char} R \neq 2$. Thus $I_n \oplus D \neq 0$. But

$$D(I_n \oplus D) = D \oplus D^2 = D \oplus I_n = I_n \oplus D,$$

so we have $D = I_n$, a contradiction. $\square$

Corollary 2.1.8. *$W_n(R) \in \boldsymbol{SSR}$ if and only if $n = 1$.*

Proof. If $n > 2$, then by Theorem 2.1.7, $W_n(R) \notin \boldsymbol{SSR}$.

Next, Assume that $n = 2$ and suppose that there exists an operation $\oplus$ on $W_2^0(R)$ such that $(W_2^0(R), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $W_2^0(R)$. Since $I_2 \in W_2(R)$, $(W_2^0(R), \oplus, \cdot)$ is a ring by Proposition 1.1(vi). Then $I_2 \oplus A = 0$ for some $A \in W_2(R)$. It therefore follows that for every $B \in W_2(R)$,

$$B \oplus AB = (I_2 \oplus A)B = 0 = B(I_2 \oplus A) = B \oplus BA.$$

Hence $AB = BA$ for all $B \in W_2(R)$. By Lemma 2.1.3, $A = aI_2$ for some $a \in R$. Thus

$$I_2 \oplus aI_2 = 0. \tag{2.1.8.1}$$

Case 1: $\operatorname{char} R = 2$. Then $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in W_2(R)$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = I_2$. Since $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \neq aI_2$, by (2.1.8.1), $I_2 \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \neq 0$. But

$$\left(I_2 \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus I_2 = I_2 \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

and $W_2(R)$ is cancellative, so $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = I_2$, a contradiction.

Case 2: char$R \neq 2$. Then $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \in W_2(R)$ and $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \neq I_2$. We have that

$$\left(I_2 \oplus \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right) \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \oplus I_2 = I_2 \oplus \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Since $W_2(R)$ is cancellative and $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \neq I_2$, it follows that

$$I_2 \oplus \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = 0. \tag{2.1.8.2}$$

Consequently, $I_2 \oplus I_2 \neq 0$, so $I_2 \oplus I_2 \in W_2(R)$. It is clear that $I_2 \oplus I_2 \in C(W_2(R))$. By Lemma 2.1.3, $I_2 \oplus I_2 = bI_2$ for some $b \in R$. Hence $1 = \det(bI_2) = b^2$. It follows that

$$(I_2 \oplus bI_2)(bI_2) = bI_2 \oplus I_2 = I_2 \oplus bI_2.$$

If $I_2 \oplus bI_2 \neq 0$, then $bI_2 = I_2$, so $b = 1$. Thus $I_2 \oplus I_2 = I_2$ which implies by (2.1.8.2) that $I_2 = 0$, a contradiction. Thus $I_2 \oplus bI_2 = 0$, so $bI_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ by (2.1.8.2). It follows that $b = -1$. Hence by (2.1.8.2), $I_2 \oplus I_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, so $I_2 \oplus I_2 \oplus I_2 = 0$. We there have

$$A \oplus A \oplus A = 0 \text{ for all } A \in W_2(R). \tag{2.1.8.3}$$

It can be seen easily from (2.1.8.3) that

$$(I_2 \oplus A)^3 = I_2 \oplus A^3 \text{ for all } A \in W_2(R). \tag{2.1.8.4}$$

Since $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \in W_2(R)$ and

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

by (2.1.8.4) and (2.1.8.2), we have

$$\left(I_2 \oplus \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}\right)^3 = I_2 \oplus \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = 0.$$

This implies that $I_2 \oplus \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = 0$ which is contrary to (2.1.8.2).

The converse holds since $W_1^0(R) \cong (\{0,1\}, \cdot) \cong (\mathbb{Z}_2, \cdot)$.

Hence the theorem is proved. $\square$

2.2. Linear Transformation Semigroups

In this section, we investigate when some semigroups of linear transformations belong to the class $\boldsymbol{SSR}$. Let V be a vector space over a division ring R. The following semigroups of linear transformations on V given in Chapter I are recalled as follows:

$$\begin{aligned} L(V) &= \{\alpha : V \to V \mid \alpha \text{ is a linear transformation}\}, \\ G(V) &= \{\alpha : V \to V \mid \alpha \text{ is an isomorphism}\}, \end{aligned}$$

$$
\begin{aligned}
IF(V) &= \{\alpha \in L(V) \mid \dim(\mathrm{Im}\alpha) \text{ is finite}\}, \\
M(V) &= \{\alpha \in L(V) \mid \alpha \text{ is one-to-one}\}, \\
E(V) &= \{\alpha \in L(V) \mid \mathrm{Im}\alpha = V\}, \\
AM(V) &= \{\alpha \in L(V) \mid \dim(\mathrm{Ker}\alpha) \text{ is finite}\}, \\
AE(V) &= \{\alpha \in L(V) \mid \dim(V/\mathrm{Im}\alpha) \text{ is finite}\}, \\
OM(V) &= \{\alpha \in L(V) \mid \dim(\mathrm{Ker}\alpha) \text{ is infinite}\}, \\
OE(V) &= \{\alpha \in L(V) \mid \dim(V/\mathrm{Im}\alpha) \text{ is infinite}\}, \\
BL(V) &= \{\alpha \in L(V) \mid \alpha \text{ is one-to-one and } \dim(V/\mathrm{Im}\alpha) \text{ is infinite}\} \\
&\quad \text{where } \dim V \text{ is infinite}, \\
OBL(V) &= \{\alpha \in L(V) \mid \dim(\mathrm{Ker}\alpha) \text{ is infinite and } \mathrm{Im}\alpha = V\} \\
&\quad \text{where } \dim V \text{ is infinite}, \\
AI(V) &= \{\alpha \in L(V) \mid \alpha \text{ is almost identical}\} \\
(&= \{\alpha \in L(V) \mid \dim(V/F(\alpha)) \text{ is finite}\} \\
&\quad \text{where } F(\alpha) = \{v \in V \mid v\alpha = v\}\ ).
\end{aligned}
$$

Since $(L(V), +, \cdot)$ is a ring where $+$ and $\cdot$ are respectively the usual addition and composition of linear transformations, we have that $L(V) \in \boldsymbol{SSR}$. If $\dim V$ is finite, then for each $\alpha \in G(V)$, $(L(V)\backslash G(V)) \cup \{\alpha, \alpha^2, \alpha^3, ...\}$ is clearly a subsemigroup of $L(V)$ containing $L(V)\backslash G(V)$. Then we can deduce that in general, there are many proper subsemigroups of $L(V)$ containing $L(V)\backslash G(V)$. The following theorem shows that there is no proper subsemigroup S containing $L(V)\backslash G(V)$ such that $S \in \boldsymbol{SSR}$ if $\dim V > 1$.

Theorem 2.2.1. *Assume that* $\dim V > 1$ *and let* S *be a subsemigroup of* $L(V)$ *such that* $L(V)\backslash G(V) \subseteq S$. *If* $S \in \boldsymbol{SSR}$, *then* $S = L(V)$.

Proof. Let $\oplus$ be an operation on S such that $(S, \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on S. To show that $S = L(V)$, let $\alpha \in G(V)$. Let B be a basis of V. Then $\mid B \mid \geq 2$. Let $u \in B$ be fixed. Then $\{u\alpha\}$ and $(B \setminus \{u\})\alpha$ are not bases of V. Let $\beta, \gamma \in L(V)$ be defined by

$$v\beta = \begin{cases} v\alpha & \text{if } v \in B \setminus \{u\}, \\ 0 & \text{if } v = u \end{cases}$$

and

$$v\gamma = \begin{cases} u\alpha & \text{if } v = u, \\ 0 & \text{if } v \in B \setminus \{u\}. \end{cases}$$

Then we have $\beta, \gamma \notin G(V)$, so $\beta, \gamma \in S$ by assumption. Thus $\beta \oplus \gamma \in S$. We claim that $\beta \oplus \gamma = \alpha$. For each $w \in B$, let $\lambda_w \in L(V)$ be defined by

$$v\lambda_w = \begin{cases} w & \text{if } v = w, \\ 0 & \text{if } v \in B \setminus \{w\}. \end{cases}$$

Then $\lambda_w \in S$ for all $w \in B$, and so

$$\lambda_w(\beta \oplus \gamma) = \lambda_w\beta \oplus \lambda_w\gamma \ \ forall \ \ w \in B.$$

We clearly have

$$\lambda_u\beta = 0, \ \ u(\lambda_u\gamma) = u\alpha, \tag{2.2.1.1}$$

and also

$$v(\lambda_v\beta) = v\alpha \ \text{ for all } v \in B \setminus \{u\} \text{ and}$$

$$\lambda_v\gamma = 0 \ \text{ for all } v \in B \setminus \{u\}. \tag{2.2.1.2}$$

From (2.2.1.1) and (2.2.1.2), we have respectively that

$$u(\beta \oplus \gamma) = u\lambda_u(\beta \oplus \gamma) = u(\lambda_u\beta \oplus \lambda_u\gamma) = u\lambda_u\gamma = u\alpha$$

and for $v \in B \setminus \{u\}$,

$$v(\beta \oplus \gamma) = v\lambda_v(\beta \oplus \gamma) = v(\lambda_v\beta \oplus \lambda_v\gamma) = v\lambda_v\beta = v\alpha.$$

Hence $\alpha = \beta \oplus \gamma \in S$. This proves that $S = L(V)$, as required. $\square$

From [8], page 415 and 424, we have that $IF(V)$ is a unique minimal ideal of the ring $(L(V), +, \cdot)$ where $+$ and $\cdot$ are respectively the usual addition and composition of linear transformations. Then

Theorem 2.2.2. *$IF(V) \in \boldsymbol{SSR}$ for any dimension of V.*

We recall that if dim$V$ is finite, then $M(V) = G(V) = E(V)$ and $AM(V) = L(V) = AE(V)$. We also note that for every dimension of V, in $M^0(V)$ and $E^0(V)$, 0 is a zero adjoined. Moreover, if dim$V$ is infinite, then $AM(V)$ and $AE(V)$ have no zero. Next, the subsemigroups $M(V)$, $E(V)$, $AM(V)$, $AE(V)$ are characterized when they belong to the class $\boldsymbol{SSR}$ in terms of the dimensions of V. We give two proofs for each characterization for $M(V)$, $E(V)$, $AM(V)$ and $AE(V)$. However, every proof need suitable constructions of linear transformations. The first proof of each one refers Proposition 1.5. We use Proposition 1.6 for the second proofs of both $M(V)$ and $E(V)$.

Theorem 2.2.3. *$M(V) \in \boldsymbol{SSR}$ if and only if dim$V \leq 1$.*

Proof 1. Assume that $M(V) \in \boldsymbol{SSR}$. Since $1_V \in M(V)$, by Proposition 1.1(vi), $M(V) \in \boldsymbol{SR}$. Then there exists an operation $\oplus$ on $M^0(V)$ such that $(M^0(V), \oplus, \cdot)$ is a ring where $\cdot$ is the operation on $M^0(V)$. To show that dim$V \leq$

1, suppose on the contrary that $\dim V > 1$. Let B be a basis of V and let $u, w \in B$ be distinct. Then $(u,w)_B \in M(V)$, $(u,w)_B \neq 1_V$, $(u,w)_B \neq -1_V$ and $(u,w)_B^2 = 1_V$. By Proposition 1.5, $1_V \oplus (u,w)_B \neq 0$. Therefore $1_V \oplus (u,w)_B \in M(V)$. Thus

$$(u,w)_B(1_V \oplus (u,w)_B) = (u,w)_B \oplus 1_V = 1_V \oplus (u,w)_B \in M(V).$$

It follows that

$$u(u,w)_B(1_V \oplus (u,w)_B) = u(1_V \oplus (u,w)_B).$$

But $1_V \oplus (u,w)_B$ is a one-to-one map, so $u(u,w)_B = u$ and hence $w = u$, a contradiction. Therefore $\dim V \leq 1$.

The converse holds because

$$M^0(V) = G^0(V) \cong \begin{cases} (\mathbb{Z}_2, \cdot) & \text{if} \quad \dim V = 0, \\ (R, \cdot) & \text{if} \quad \dim V = 1. \end{cases}$$

Proof 2. Let $\oplus$ be a binary operation on $M^0(V)$ such that $(M^0(V), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $M^0(V)$. Suppose that $\dim V$ is infinite. Let B be a basis of V. Fix $u, w \in B$ with $u \neq w$. Then there is a bijection φ from B onto $B \backslash \{u, w\}$. Define $\alpha \in L(V)$ by

$$v\alpha \ = \ v\varphi \ \text{ for all } v \in B.$$

Then $\alpha \in M(V)$. Since $B\alpha = B \backslash \{u, w\}$, it follows that $v\alpha(u,w)_B = v\alpha$ for all $v \in B$, so we have $\alpha(u,w)_B = \alpha$. Consequently,

$$0 = \alpha \ominus \alpha = \alpha(u,w)_B \ominus \alpha = \alpha((u,w)_B \ominus 1_V),$$

But since $\alpha \neq 0$, we have $(u,w)_B \ominus 1_V = 0$ so $(u,w)_B = 1_V$, a contradiction. Hence dim$V$ is finite and thus $M(V) = G(V)$. We then have by Proposition 1.6 that dim$V \leq 1$.

The converse is obtained as in the first proof. $\square$

Theorem 2.2.4. $E(V) \in \boldsymbol{SSR}$ *if and only if dim*$V \leq 1$.

Proof 1. Assume that $E(V) \in \boldsymbol{SSR}$ and let $\oplus$ be an operation on $E^0(V)$ such that $(E^0(V), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $E^0(V)$. Since $1_V \in E(V)$, $(E^0(V), \oplus, \cdot)$ is a ring. Suppose that dim$V > 1$. Let B be a basis of V and $u, w \in B$ such that $u \neq w$. Then $(u,w)_B \in E(V)$, $(u,w)_B \neq 1_V$ and $(u,w)_B \neq -1_V$. By Proposition 1.5, $1_V \oplus (u,w)_B \neq 0$. Hence $1_V \oplus (u,w)_B \in E(V)$, so there exists $z \in V$ such that

$$z(1_V \oplus (u,w)_B) = u.$$

But

$$(1_V \oplus (u,w)_B)(u,w)_B = (u,w)_B \oplus 1_V = 1_V \oplus (u,w)_B,$$

so we have

$$z(1_V \oplus (u,w)_B)(u,w)_B = z(1_V \oplus (u,w)_B).$$

It follows that $u(u,w)_B = u$. Hence $w = u$, a contradiction. Therefore dim$V \leq 1$.

We obtain the converse similarly to the first proof of Theorem 2.2.3.

Proof 2. Let $\oplus$ be a binary operation on $E^0(V)$ such that $(E^0(V), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $E^0(V)$. Suppose that dim$V$ is infinite and let B be a basis of V. Fix $u, w \in B$ with $u \neq w$. Then there is a bijection φ from $B \backslash \{u, w\}$ onto B. Let $\alpha \in L(V)$ be defined by

$$v\alpha = \begin{cases} 0 & \text{if} \quad v \in \{u, w\}, \\ v\varphi & \text{if} \quad v \in B\backslash\{u, w\}. \end{cases}$$

Then Im$\alpha = <B\alpha> = <B> = V$. It follows that $\alpha \in E(V)$. By the definition of α, we have

$$u(u, w)_B\alpha = w\alpha = 0 = u\alpha, \qquad w(u, w)_B\alpha = u\alpha = 0 = w\alpha,$$
$$v(u, w)_B\alpha = v\alpha \qquad \text{for all } v \in B\backslash\{u, w\}.$$

Then $(u, w)_B\alpha = \alpha$, and hence

$$0 = \alpha \ominus \alpha = (u, w)_B\alpha \ominus \alpha = ((u, w)_B \ominus 1_V)\alpha.$$

But since $\alpha \neq 0$, $(u, w)_B \ominus 1_V = 0$. Thus $(u, w)_B = 1_V$, a contradiction. Therefore dim$V$ is finite, and so $E(V) = G(V)$, hence we have by Proposition 1.6 that dim $V \leq 1$.

The converse is obtained as in the first proof. $\square$

Theorem 2.2.5. *If $S(V)$ is $AM(V)$ or $AE(V)$, then $S(V) \in$ **SSR** if and only if dim$V$ is finite.*

Proof 1. Assume that there exists an operation $\oplus$ on $S^0(V)$ such that $(S^0(V), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $S^0(V)$. Then $(S^0(V), \oplus, \cdot)$ is a ring since $1_V \in S(V)$. Suppose that dim$V$ is infinite. It follows that $S(V)$ has no zero. Let B be a basis of V and let $u, w \in B$ with $u \neq w$. Define $\alpha \in L(V)$ by

$$v\alpha = \begin{cases} 0 & \text{if} \quad v = u \text{ or } v = w, \\ v & \text{if} \quad v \in B \backslash \{u, w\}. \end{cases}$$

Then $\alpha^2 = \alpha$, Ker$\alpha = <u, w>$ and Im$\alpha = <B \backslash \{u, w\}>$. It follows that

$$\dim(\text{Ker}\alpha) = 2 \text{ and } \dim(V/\text{Im}\alpha) = \dim(V/<B \backslash \{u, w\}>) = 2.$$

Hence α, $-\alpha \in S(V)$. Since $\alpha \neq 1_V$ and $\alpha \neq -1_V$, it follows from Proposition 1.5 that $1_V \oplus \alpha \neq 0$ and $1_V \oplus (-\alpha) \neq 0$. Thus $1_V \oplus \alpha$, $1_V \oplus (-\alpha) \in S(V)$. Consequently,

$$0 \neq (1_V \oplus \alpha)\alpha = \alpha \oplus \alpha^2 = \alpha \oplus \alpha \tag{2.2.5.1}$$

and

$$0 \neq (1_V \oplus (-\alpha))(-\alpha) = (-\alpha) \oplus (-\alpha)^2 = (-\alpha) \oplus \alpha = \alpha \oplus (-\alpha). \tag{2.2.5.2}$$

Hence Proposition 1.5, (2.2.5.1) and (2.2.5.2) yield a contradiction.

Conversely, assume that dim$V$ is finite. Then $S(V) = L(V)$, so $S(V) \in$ ***SSR***.

Proof 2. Define α as in the first proof. We have by the definition of α that

$$u(u, w)_B\alpha = w\alpha = 0 = u\alpha, \qquad w(u, w)_B\alpha = u\alpha = 0 = w\alpha,$$
$$v(u, w)_B\alpha = v\alpha \qquad \text{for all } v \in B \backslash \{u, w\}.$$

Then $(u,w)_B\alpha = \alpha$. Hence

$$0 = \alpha \ominus \alpha = \alpha \ominus (u,w)_B\alpha = (1_V \ominus (u,w)_B)\alpha.$$

But since $\alpha \neq 0$, we have $1_V \ominus (u,w)_B = 0$. Thus $(u,w)_B = 1_V$, a contradiction. Then dim V is finite.

The converse holds as in the first proof. □

The next two theorems show that for any infinite dimension of V, neither $OM(V)$ nor $OE(V)$ is in $\boldsymbol{SSR}$.

Theorem 2.2.6. *$OM(V) \notin \boldsymbol{SSR}$ where dim$V$ is infinite.*

Proof. Assume that $OM(V) \in \boldsymbol{SSR}$. Let $\oplus$ be a binary operation on $OM(V)$ such that $(OM(V), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $OM(V)$. Let B be a basis of V. Then there are subsets B_1 and B_2 such that $B_1 \cap B_2 = \emptyset$, $B = B_1 \cup B_2$ and $|B| = |B_1| = |B_2|$. Thus V is a direct sum of $<B_1>$ and $<B_2>$. Let $\alpha, \beta \in L(V)$ be defined by

$$v\alpha = \begin{cases} v & \text{if} \quad v \in B_1, \\ 0 & \text{if} \quad v \in B_2 \end{cases}$$

and

$$v\beta = \begin{cases} 0 & \text{if} \quad v \in B_1, \\ v & \text{if} \quad v \in B_2. \end{cases}$$

Then Ker$\alpha = <B_2>$ and Ker$\beta = <B_1>$, so dim(Kerα) $= |B_2|$ and dim(Kerβ) $= |B_1|$. Thus $\alpha, \beta \in OM(V)$. Clearly, $\alpha^2 = \alpha$, $\beta^2 = \beta$ and $\alpha\beta = 0 = \beta\alpha$. Thus

$$(\alpha \oplus \beta)\alpha = \alpha^2 \oplus \beta\alpha = \alpha^2 = \alpha \tag{2.2.6.1}$$

and

$$(\alpha \oplus \beta)\beta = \alpha\beta \oplus \beta^2 = \beta^2 = \beta. \tag{2.2.6.2}$$

By the definitions of α and β, we have

$$\begin{aligned} &v\alpha = v \text{ and } v\beta = 0 \text{ for all } v \in <B_1>, \\ &v\beta = v \text{ and } v\alpha = 0 \text{ for all } v \in <B_2>. \end{aligned} \tag{2.2.6.3}$$

Let $u \in \mathrm{Ker}(\alpha \oplus \beta)$. Then $u(\alpha\oplus\beta) = 0$. Since $V = <B_1> + <B_2>$, $u = u_1 + u_2$ for some $u_1 \in <B_1>$ and $u_2 \in <B_2>$. By (2.2.6.1), (2.2.6.2) and (2.2.6.3),

$$\begin{aligned} u(\alpha \oplus \beta)\alpha &= u\alpha = (u_1 + u_2)\alpha = u_1, \\ u(\alpha \oplus \beta)\beta &= u\beta = (u_1 + u_2)\beta = u_2. \end{aligned}$$

But $u(\alpha \oplus \beta) = 0$, so $u(\alpha \oplus \beta)\alpha = 0 = u(\alpha \oplus \beta)\beta$. It follows that $u_1 = 0 = u_2$. Hence $u = 0$. This proves that $\mathrm{Ker}(\alpha \oplus \beta) = \{0\}$, so $\alpha \oplus \beta \notin OM(V)$, a contradiction. Therefore we have $OM(V) \notin \boldsymbol{SSR}$, as required. □

Theorem 2.2.7. *$OE(V) \notin \boldsymbol{SSR}$ where $dim V$ is infinite.*

Proof. Assume that $OE(V) \in \boldsymbol{SSR}$. Let $\oplus$ be a binary operation on $OE(V)$ such that $(OE(V), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $OE(V)$. Let B be a basis of V. Then there are subsets B_1 and B_2 such that $B_1 \cap B_2 = \emptyset$, $B = B_1 \cup B_2$ and $|B| = |B_1| = |B_2|$. Let $\alpha, \beta \in L(V)$ be defined by

$$v\alpha = \begin{cases} v & \text{if} \quad v \in B_1, \\ 0 & \text{if} \quad v \in B_2 \end{cases}$$

and

$$v\beta = \begin{cases} 0 & \text{if} \quad v \in B_1, \\ v & \text{if} \quad v \in B_2. \end{cases}$$

Then $\mathrm{Im}\alpha = <B_1>$ and $\mathrm{Im}\beta = <B_2>$ which imply that

$$\begin{aligned} \dim(V/\mathrm{Im}\alpha) &= \dim(V/<B_1>) = |B \setminus B_1| = |B_2|, \\ \dim(V/\mathrm{Im}\beta) &= \dim(V/<B_2>) = |B \setminus B_2| = |B_1|\,. \end{aligned}$$

Thus $\alpha, \beta \in OE(V)$ and so $\alpha \oplus \beta \in OE(V)$. Since

$$\text{for } v \in B_1, v\alpha\beta = v\beta = 0 \text{ and } v\beta\alpha = 0\alpha = 0,$$
$$\text{for } v \in B_2, v\alpha\beta = 0\beta = 0 \text{ and } v\beta\alpha = v\alpha = 0,$$

we have $\alpha\beta = 0 = \beta\alpha$. Clearly, $\alpha^2 = \alpha$ and $\beta^2 = \beta$. Consequently,

$$\alpha(\alpha \oplus \beta) = \alpha \text{ and } \beta(\alpha \oplus \beta) = \beta.$$

Claim that $v \in \mathrm{Im}(\alpha \oplus \beta)$ for all $v \in B$. Let $v \in B$. Then $v \in B_1$ or $v \in B_2$.

Case 1: $v \in B_1$. Then $(v\alpha)(\alpha \oplus \beta) = v(\alpha(\alpha \oplus \beta)) = v\alpha = v$.

Case 2: $v \in B_2$. Then $(v\beta)(\alpha \oplus \beta) = v\beta = v$.

Hence $V = <B> = \mathrm{Im}(\alpha \oplus \beta)$, it follows that $\dim(V/\mathrm{Im}(\alpha \oplus \beta)) = 0$, a contradiction. Therefore $OE(V) \notin \boldsymbol{SSR}$. $\square$

We show next that neither $BL(V)$ nor $OBL(V)$ belongs to $\boldsymbol{SSR}$. Each proof needs one lemma.

Lemma 2.2.8. *If $\beta \in E(V)$ and $\alpha \in OE(V)$, then $\beta\alpha \in OE(V)$.*

Proof. It is clear since $\mathrm{Im}\beta\alpha = V\beta\alpha = V\alpha = \mathrm{Im}\alpha$. $\square$

Theorem 2.2.9. *$BL(V) \notin \boldsymbol{SSR}$ where dim$V$ is infinite.*

Proof. Assume that there exists a binary operation $\oplus$ on $BL^0(V)$ such that $(BL^0(V), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $BL^0(V)$. Let B be a basis of V. Then there are subsets B_1 and B_2 such that $B_1 \cap B_2 = \emptyset$, $B = B_1 \cup B_2$ and $|\,B\,| = |\,B_1\,| = |\,B_2\,|$. Let $\varphi : B \to B_1$ be a bijection and let $\alpha \in L(V)$ be defined by $v\alpha = v\varphi$ for all $v \in B$. Since φ is ono-to-one, α is one-to-one. Also, $\mathrm{Im}\alpha = \, <B_1>$ and hence

$$\dim(V/\mathrm{Im}\alpha) = \dim(V/<B_1>) \; = |\,B \backslash B_1\,| = |\,B_2\,|\,.$$

Then $\alpha \in BL(V)$. Let $u, w \in B_2$ with $u \neq w$. Then $u\alpha \neq w\alpha$. Since $B\alpha = B_1$, it follows that $v\alpha(u,w)_B = v\alpha$ for all $v \in B$. Hence $\alpha(u,w)_B = \alpha$ and thus $\alpha(u,w)_B\alpha = \alpha^2$. By Lemma 2.2.8, $(u,w)_B\alpha \in BL(V)$. Thus

$$0 = \alpha(u,w)_B\alpha \ominus \alpha^2 = \alpha((u,w)_B\alpha \ominus \alpha)$$

which implies that $(u,w)_B\alpha = \alpha$. Therefore $u\alpha = u(u,w)_B\alpha = w\alpha$, a contradiction. Hence $BL(V) \notin \boldsymbol{SSR}$. $\square$

Lemma 2.2.10. *If $\beta \in M(V)$ and $\alpha \in OM(V)$, then $\alpha\beta \in OM(V)$.*

Proof. It is directly obtained from the fact that for $v \in V$, $v\alpha\beta = 0$ if and only if $v\alpha = 0$ since β is one-to-one. $\square$

Theorem 2.2.11. *$OBL(V) \notin \boldsymbol{SSR}$ where $dimV$ is infinite.*

Proof. Assume that there exists a binary operation $\oplus$ on $OBL^0(V)$ such that $(OBL^0(V), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $OBL^0(V)$. Let B be a basis of V. Then there are subsets B_1 and B_2 such that $B_1 \cap B_2 = \emptyset$, $B = B_1 \cup B_2$ and $|\,B\,| = |\,B_1\,| = |\,B_2\,|$. Let φ be a bijection from B_1 onto B. Define $\alpha \in L(V)$ by

$$v\alpha = \begin{cases} v\varphi & \text{if} \quad v \in B_1, \\ 0 & \text{if} \quad v \in B_2. \end{cases}$$

Then $\dim(\text{Ker}\alpha) = \dim(< B_1 >) \;= |\,B_1\,|$ and $\text{Im}\alpha = < B > = V$.Thus $\alpha \in OBL(V)$. Choose $u, w \in B_1$ with $u \neq w$ such that $u\alpha, w\alpha \in B_2$. Since $\alpha\,|_{B_1}$ is one-to-one, $u\alpha \neq w\alpha$. We have $\alpha(u\alpha, w\alpha)_B\alpha = \alpha^2$ by the following equalities.

$$\begin{aligned} &u(\alpha(u\alpha, w\alpha)_B)\alpha = w\alpha^2 = 0 = u\alpha^2, \\ &w(\alpha(u\alpha, w\alpha)_B)\alpha = u\alpha^2 = 0 = w\alpha^2, \\ &\text{for } v \in B_1 \backslash \{u, w\}, v(\alpha(u\alpha, w\alpha)_B)\alpha = v\alpha^2, \\ &\text{for } v \in B_2, v(\alpha(u\alpha, w\alpha)_B)\alpha = 0 = v\alpha^2. \end{aligned}$$

By Lemma 2.2.10, we have that $\alpha(u\alpha, w\alpha)_B \in OBL(V)$. Thus

$$0 = \alpha(u\alpha, w\alpha)_B\alpha \ominus \alpha^2 = (\alpha(u\alpha, w\alpha)_B \ominus \alpha)\alpha.$$

It follows that $\alpha(u\alpha, w\alpha)_B = \alpha$. Therefore $u\alpha = u\alpha(u\alpha, w\alpha)_B = w\alpha$, a contradiction. Hence $OBL(V) \notin \boldsymbol{SSR}$. $\square$

Finally, we prove that the semigroup $AI(V)$ belongs to $\boldsymbol{SSR}$ if and only if dim$V$ is finite.

Theorem 2.2.12. *$AI(V) \in \boldsymbol{SSR}$ if and only if dim$V$ is finite.*

Proof. Assume that $AI(V) \in \boldsymbol{SSR}$. Then there exists an operation $\oplus$ on $AI^0(V)$ such that $(AI^0(V), \oplus, \cdot)$ is a skew-ring where $\cdot$ is the operation on $AI^0(V)$. Suppose that dim$V$ is infinite and B a basis of V. Fix $u \in B$. Define $\alpha \in L(V)$ by

$$v\alpha = \begin{cases} 0 & \text{if} \quad v = u, \\ v & \text{if} \quad v \in B \backslash \{u\}. \end{cases}$$

Then $F(\alpha) = \, < B\backslash\{u\} >$, so $\dim(V/F(\alpha)) = 1$. Thus $\alpha \in AI(V)$. We see that $\alpha^2 = \alpha$, so

$$0 = \alpha \ominus \alpha = \alpha^2 \ominus \alpha = \alpha(\alpha \ominus 1_V)$$

which implies that $\alpha = 1_V$, a contradiction.

Conversely, if dim$V$ is finite, then $AI(V) = L(V)$, so $AI(V)$ belongs to the class $\boldsymbol{SSR}$. □

CHAPTER III

GROUPS ADMITTING SKEW-SEMIFIELD STRUCTURE

In this chapter, we also divide into two sections. For the first section, we consider when some matrix groups over a commutative ring with identity $1 \neq 0$ belong to the class $\boldsymbol{GSSF}$. For the second section, some subgroups of linear transformations of a vector space over a division ring are investigated in the same way.

3.1. Matrix Groups

Throughout this section, let n be a positive integer and R a commutative ring with identity $1 \neq 0$. The following matrix groups are recalled.

$$\begin{aligned}
G_n(R) &= \{A \in M_n(R) \mid A \text{ is an invertible } n \times n \text{ matrix over } R\}, \\
U_n(R)[L_n(R)] &= \{A \in G_n(R) \mid A \text{ is upper[lower] triangular}\}, \\
P_n(R) &= \{A \in G_n(R) \mid \ A \text{ is a permutation matrix}\}, \\
O_n(R) &= \{A \in G_n(R) \mid A \text{ is orthogonal}\}, \\
V_n(R) &= \{A \in G_n(R) \mid \ \det A = \pm 1\} \text{ and} \\
W_n(R) &= \{A \in G_n(R) \mid \ \det A = 1\}.
\end{aligned}$$

The purpose of this section is to characterize in terms of n and R when the matrix groups mentioned above belong to the class $\boldsymbol{GSSF}$.

In [11], the matrix groups $G_n(F)$, $U_n(F)[L_n(F)]$, $P_n(F)$, $O_n(F)$, $V_n(F)$ and $W_n(F)$ have been completely characterized in terms of n and F when they are in $\boldsymbol{GSSF}$ where F is a field. In this section, we generalize these characterizations by replacing F by R. We obtain more general results and the mentioned results in [11] become our special cases.

Theorem 3.1.1. *$G_n(R) \in \boldsymbol{GSSF}$ if and only if $n = 1$ and $U_R \in \boldsymbol{GSSF}$ where U_R denotes the multiplicative group of all invertible elements of R.*

Proof. Assume that $n > 1$. Define $A, B \in G_n(R)$ by

$$A = \begin{bmatrix} 1 & 1 & 0 & \ldots & 0 \\ 0 & -1 & 0 & \ldots & 0 \\ 0 & 0 & -1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & -1 \end{bmatrix},$$

$$B = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix}.$$

Then $A, B \in G_n(R) \backslash \{I_n\}$, $A^2 = B^2 = I_n$ and $A \neq B$. By Proposition 1.3, $G_n(R)$ does not belong to the class $\boldsymbol{GSSF}$.

Next, assume that $n = 1$ and $U_R \notin \boldsymbol{GSSF}$. Then $U_R \cong G_1(R) \notin \boldsymbol{GSSF}$.

The converse holds because $G_1(R) \cong U_R$. □

Theorem 3.1.2. *$P_n(R) \in \boldsymbol{GSSF}$ if and only if $n \leq 2$.*

Proof. Assume that $n > 2$. Define $A, B \in G_n(R)$ by

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix},$$

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Then $A, B \in P_n(R)\backslash\{I_n\}$, $A^2 = B^2 = I_n$ and $A \neq B$. By Proposition 1.3, $P_n(R) \notin \boldsymbol{GSSF}$.

Since $P_1^0(R) \cong (\{0,1\}, \cdot) \cong (\mathbb{Z}_2, \cdot)$ and

$$P_2^0(R) = \left(\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}, \cdot \right) \cong (\mathbb{Z}_3, \cdot),$$

we have that $P_1(R)$ and $P_2(R)$ belong to the class $\boldsymbol{GSSF}$. Hence the converse holds. $\square$

Theorem 3.1.3. *$U_n(R)[L_n(R)] \in \boldsymbol{GSSF}$ if and only if (i) $n = 1$ and $U_R \in \boldsymbol{GSSF}$ or (ii) $n = 2$ and $|R| = 2$.*

Proof. We prove the theorem for $U_n(R)$. For $L_n(R)$, the proof can be given similarly. Assume that (i) and (ii) do not hold. Then one of the following conditions holds: (1) $n > 2$, (2) $n = 1$ and $U_R \notin \boldsymbol{GSSF}$ and (3) $n = 2$ and $|R| > 2$.

Case 1: $n > 2$. Then the matrices $A, B \in G_n(R)$ defined by

$$A = \begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & -1 \end{bmatrix},$$

$$B = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & -1 \end{bmatrix}$$

are in $U_n(R)\backslash\{I_n\}$, $A^2 = B^2 = I_n$ and $A \neq B$. Then by Proposition 1.3, $U_n(R) \notin \boldsymbol{GSSF}$ if $n > 2$.

Case 2: $n = 1$ and $U_R \notin \boldsymbol{GSSF}$. Then $U_R \cong U_1(R) \notin \boldsymbol{GSSF}$.

Case 3: $n = 2$ and $|R| > 2$.

Subcase 3.1: char$R = 2$. Let $a \in R\backslash\{0, 1\}$. Then $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in U_2(R)\backslash\{I_2\}$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$. Since char$R = 2$, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = I_2 = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^2$. Thus for this subcase, $U_2(R) \notin \boldsymbol{GSSF}$ by Proposition 1.3.

Subcase 3.2: char$R \neq 2$. Then $-2 \neq 0$ in R, $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \in U_2(R)\backslash\{I_2\}$, $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}^2 = I_2$ and

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \neq \begin{bmatrix} 1 & -2 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}.$$

From Proposition 1.4, $U_2(R) \notin \boldsymbol{GSSF}$ for this subcase.

Conversely, assume that (i) $n = 1$ and $U_n(R) \in \boldsymbol{GSSF}$ or (ii) $n = 2$ and $|R| = 2$. If $n = 1$ and $U_R \in \boldsymbol{GSSF}$, then $U_R \cong U_1(R) \in \boldsymbol{GSSF}$. Next, assume that $n = 2$ and $|R| = 2$. Then

$$U_2^0(R) \cong \left(\left\{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right\}, \cdot\right) \cong (\mathbb{Z}_3, \cdot),$$

so $U_2(R) \in \boldsymbol{GSSF}$. $\square$

Theorem 3.1.4 . *$O_n(R) \in \boldsymbol{GSSF}$ if and only if (i) $n = 1$ and $H \in \boldsymbol{GSSF}$ or (ii) $n = 2$ and $|R| = 2$ where H is the subgroups of U_R consisting of all elements of R of order ≤ 2.*

Proof. Assume that (i) and (ii) are not true. Then one of the following conditions holds: (1) $n > 2$, (2) $n = 1$ and $H \notin \boldsymbol{GSSF}$ and (3) $n = 2$ and $|R| > 2$.

Case 1: $n > 2$. Observe that since the matrices A, B defined in the proof of Theorem 3.1.2 are symmetric, they are also orthogonal, hence $O_n(R) \notin \boldsymbol{GSSF}$.

Case 2: $n = 1$ and $H \notin \boldsymbol{GSSF}$. Then $H \cong O_1(R) \notin \boldsymbol{GSSF}$.

Case 3: $n = 2$ and $|R| > 2$.

Subcase 3.1: char$R = 2$. Let $a \in R\backslash\{0, 1\}$ and define $C \in M_2(R)$ by

$$C = \begin{bmatrix} a & 1+a \\ 1+a & a \end{bmatrix}.$$

Then $C = C^t$ and

$$C^2 = \begin{bmatrix} a^2+1+2a+a^2 & a+a^2+a+a^2 \\ a+a^2+a+a^2 & 1+2a+a^2+a^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

since $\text{char}R = 2$. Thus $C \in O_2(R)\backslash\{I_2\}$. Also,

$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in O_2(R)\backslash\{I_2\}$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = I_2$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \neq C$. Thus $O_2(R) \notin$ $\boldsymbol{GSSF}$ by a Proposition 1.3.

Subcase 3.2: $\text{char}R \neq 2$. Then $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ are distinct elements of $O_2(R)\backslash\{I_2\}$ and $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}^2 = I_2$. It then follows from Proposition 1.3 that $O_2(R) \notin \boldsymbol{GSSF}$.

The converse holds because of the following facts.

$$O_1^0(R) \cong H.$$

If $|R| = 2$, it is clear that

$$O_2^0(R) = \left(\left\{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right\}, \cdot\right) \cong (\mathbb{Z}_3, \cdot).$$

□

The last theorem of this section, we investigate when the matrix group $W_n(R)$ belongs to the class $\boldsymbol{GSSF}$. The result is the following theorem.

Theorem 3.1.5. *$V_n(R) \in \boldsymbol{GSSF}$ if and only if $n = 1$.*

Proof. Assume that $n > 1$ and define the matrices A, B as in the proof of Theorem 3.1.1. Then $\det A = 1$ or -1 and $\det B = -1$, so $A, B \in V_n(R)$. Hence $V_n(R) \notin \boldsymbol{GSSF}$ by Proposition 1.3.

Since

$$V_1^0(R) \cong (\{0,1,-1\},\cdot) \cong \begin{cases} (\mathbb{Z}_3,\cdot) & \text{if} \quad \mathrm{char}R \neq 2, \\ (\mathbb{Z}_2,\cdot) & \text{if} \quad \mathrm{char}R = 2, \end{cases}$$

the converse holds. $\square$

Theorem 3.1.6. *$W_n(R) \in \boldsymbol{GSSF}$ if and only if $n = 1$.*

Proof. Assume that $n \geq 2$.

Case 1: $n \geq 3$. Let $A, B \in W_n(R)$ be defined by

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & -1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \end{bmatrix}$$

and

$$B = \begin{bmatrix} 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & -1 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \end{bmatrix}.$$

Then $A^2 = B^2 = I_n$, $A \neq I_n$ and $B \neq I_n$, so by Proposition 1.3, $W_n(R) \notin \boldsymbol{GSSF}$ for this case.

Case 2: $n = 2$.

Subcase 2.1: char$R = 2$. Then the matrices $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ are in $W_2(R)\backslash\{I_2\}$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = I_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \neq I_2$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \neq I_2$. Hence $W_2(R) \notin \boldsymbol{GSSF}$ for this subcase.

Subcase 2.2: char$R \neq 2$. To show that $W_2(R) \notin \boldsymbol{GSSF}$, suppose on the contrary that there exists an operation $\oplus$ on $W_2^0(R)$ such that $(W_2^0(R), \oplus, \cdot)$ is a skew-semifield where $\cdot$ is the operation on $W_2^0(R)$. Now we have

$$\left(I_2 \oplus \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right)\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \oplus I_2 = I_2 \oplus \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

If $I_2 \oplus \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \neq 0$, then $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = I_2$ so $1 = -1$, a contradiction. Therefore

$$I_2 \oplus \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = 0. \tag{3.1.5.1}$$

and $(W_2^0(R)), \oplus)$ is an abelian group. Since $I_2 \oplus I_2 \in C(W_2(R))$, by Lemma 2.1.3, $I_2 \oplus I_2 = aI_2$ for some $a \in R$. By (3.1.5.1), $a \neq 0$. Then $\det(aI_2) = a^2 = 1$, so

$$(I_2 \oplus aI_2)(aI_2) = aI_2 \oplus I_2 = I_2 \oplus aI_2.$$

If $I_2 \oplus aI_2 \neq 0$, then $aI_2 = I_2$ and so $a = 1$. Hence $I_2 \oplus I_2 = I_2$ which implies by (3.1.5.1) that $I_2 = 0$, a contradiction. Therefore $I_2 \oplus aI_2 = 0$, so $aI_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ by (3.1.5.1) which implies that $a = -1$. Now we have

$I_2 \oplus I_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$.

Thus $I_2 \oplus I_2 \oplus I_2 = 0$ by (3.1.5.1). Hence

$$A \oplus A \oplus A = 0 \quad \text{for all } A \in W_2(R). \tag{3.1.5.2}$$

We obviously obtain from (3.1.5.2) that

$$(I_2 \oplus A)^3 = I_2 \oplus A^3 \quad \text{for all } A \in W_2(R). \tag{3.1.5.3}$$

Since $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \in W_2(R)$ and

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

we have from (3.1.5.1) and (3.1.5.3) that

$$\left(I_2 \oplus \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}\right)^3 = I_2 \oplus \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = 0.$$

This implies that $I_2 \oplus \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = 0$. By (3.1.5.1), $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, a contradiction.

The converse holds because

$$W_1^0(R) \cong (\{0, 1\}, \cdot) \cong (\mathbb{Z}_2, \cdot).$$

□

Remark 3.1.7. It follows directly from the definitions of skew-rings and skew-semifields that if G is a group such that $G \in \boldsymbol{SSR}$, then $G \in \boldsymbol{GSSF}$. Thus any group which is not in $\boldsymbol{GSSF}$ must not be in $\boldsymbol{SSR}$. Hence Corollary 2.1.5, Corollary 2.1.6 and Corollary 2.1.7 can be considered respectively as corollaries of Theorem 3.1.1, Theorem 3.1.5 and Theorem 3.1.6.

3.2. Groups of Linear Transformations

First, we characterize the group $G(V)$ when it belongs to the class $\boldsymbol{GSSF}$.

Theorem 3.2.1. *$G(V) \in \boldsymbol{GSSF}$ if and only if dim$V \leq 1$.*

Proof. Assume that dim$V \geq 2$. Let B be a basis of V. Fix $u, w \in B$ with $u \neq w$. Then $(u, w)_B^2 = 1_V$ and $(u, w)_B \neq 1_V$. Since $u, u + w$ are linearly independent, there exists a basis B' of V containing u and $u + w$. We now have $(u, u + w)_{B'}^2 = 1_V$ and $(u, u + w)_{B'} \neq 1_V$. Since $u \neq w$, $(u, w)_B \neq (u, u + w)_{B'}$. By Proposition 1.3, $G(V) \notin \boldsymbol{GSSF}$.

Conversely, assume that dim$V \leq 1$. Then $G(V) = \{1_V\}$ or $G(V) \cong (R\backslash\{0\}, \cdot)$. Thus $G(V) \in \boldsymbol{GSSF}$. $\square$

Next, recall the two subgroups $GAI(V)$ and $G_B(V)$ where B is a basis of V as follows.

$$GAI(V) = \{\alpha \in G(V) \mid \alpha \text{ is almost identical}\},$$

that is,

$$\begin{aligned} GAI(V) &= \{\alpha \in G(V) \mid \dim(V/F(\alpha)) \text{ is finite}\} \\ &\quad \text{where } F(\alpha) = \{v \in V \mid v\alpha = v\}, \end{aligned}$$

and $G_B(V)$ is the subgroup of $G(V)$ generated by the subset

$$\{(v_1, v_2, ..., v_n)_B \mid n \in \mathbb{N}, v_1, v_2, ..., v_n \text{ are distinct in } B\}$$

of $G(V)$.

Theorem 3.2.2. *$GAI(V) \in \boldsymbol{GSSF}$ if and only if $\dim V \leq 1$.*

Proof. Assume that $\dim V \geq 2$. Let B be a basis of V. Fix $u, w \in B$ with $u \neq w$. Then $F((u,w)_B) = \; < B \backslash \{u,w\} >$, and so $\dim(V/F((u,w)_B))$ $= \dim(V/ < B\backslash\{u,w\} >) \; = 2$. Since $u, u+w$ are linearly independent, there is a basis B' of V such that $u, u+w \in B'$. Thus

$$F((u,u+w)_{B'}) = \; < B'\backslash\{u,u+w\} >,$$

and so $\dim(V/F((u,u+w)_{B'})) = 2$. Hence $(u,w)_B, (u,u+w)_{B'} \in GAI(V)$, and

$$\begin{aligned}
&(u,w)_B \neq (u,u+w)_{B'}, (u,w)_B^2 = 1_V, \\
&(u,u+w)_{B'}^2 = 1_V, (u,w)_B \neq 1_V \text{ and} \\
&(u,u+w)_{B'} \neq 1_V.
\end{aligned}$$

By Proposition 1.3, $GAI(V) \notin \boldsymbol{GSSF}$.

Conversely, if $\dim V \leq 1$, then $GAI(V) = G(V)$ which belongs to $\boldsymbol{GSSF}$ by Theorem 3.2.1. □

Finally, we show that for a fixed basis B of V, the group $G_B(V)$ belongs to the class $\boldsymbol{GSSF}$ if and only if $|B| \leq 2$.

Theorem 3.2.3. *For a fixed basis B of V, $G_B(V) \in \boldsymbol{GSSF}$ if and only if $|B| \leq 2$.*

Proof. Assume that $|B| > 2$. Let $u, v, w \in B$ be distinct. Then

$$
\begin{aligned}
&(u,v)_B \neq (u,w)_B, (u,v)_B^2 = 1_V,\\
&(u,v)_B \neq 1_V, (u,w)_B^2 = 1_V \text{ and}\\
&(u,w)_B \neq 1_V.
\end{aligned}
$$

By Proposition 1.3, $G_B(V) \notin GSSF$.

Conversely, assume that $|B| \leq 2$. Then

$$
G_B^0(V) \cong \begin{cases} (\mathbb{Z}_2, \cdot) & \text{if} \quad |B| \leq 1, \\ (\mathbb{Z}_3, \cdot) & \text{if} \quad |B| = 2 \end{cases}
$$

where $\cdot$ is the usual multiplication. Hence $G_B(V) \in \boldsymbol{GSSF}$. $\square$

REFERENCES

[1]. Adkins, W. A., and Weintraub, S. H. **Algebra**. New York: Springer-Verlag, 1992.

[2]. Chaopraknoi, S. **Generalizations of some theorems in group and ring theory to skew-rings**. Master 's Thesis, Department of Mathematics, Graduate School, Chulalongkorn University, 1998.

[3]. Chu, D. D., and Shyr, H. J. Monoids of languages admitting ring structure. **Semigroup Forum** 19 (1980): 127-132.

[4]. Clifford, A. H., and Preston, G. B. **The Algebraic Theory of Semigroups**. Vol. 1, Mathematical Surveys, American Mathematical Society, Providence, R. I., 1961.

[5]. Higgins, P. M. **Techniques of Semigroup Theory**. New York: Oxford University Press, 1992.

[6]. Hoffmann, K., and Kunze, R. **Linear Algebra**. $2^{\underline{nd}}$ ed., Prentice-Hall, New Jersey, 1971.

[7]. Howie, J. M. **An Introduction to Semigroup Theory**. London: Academic Press, 1976.

[8]. Hungerford, T. M. **Algebra**. New York: Springer-Verlag, 1974.

[9]. Isbell, J. R. On the multiplicative semigroup of a commutative ring. **Proceedings of the American Mathematical Society** 10(1959): 908-909.

[10]. Kemprasit, Y. Hyperring structures on some subsemigroups of linear transformations. **Italian Journal of Pure and Applied Mathematics** 12 (to appear).

[11]. Kemprasit, Y., and Triphop, N. Some matrix groups admitting skew-semifield structure. **East-west Journal of Mathematics** 3(2001): 11-22.

[12]. Lawson, L. J. M. **The multiplicative semigroup of a ring**, Doctoral dissertation, University of Tennessee, 1969.

[13]. Light, S. On the class of semigroups admitting ring structure. **Semigroup Forum** 13(1976): 37-46.

[14]. Mitchell, S. S., and Sinutok, P. The theory of semifields, **Kyungpook Mathematical Journal** 22(1981): 325-347.

[15]. Peinado, R. E. On semigroups admitting ring structure. **Semigroup Forum** 1(1970): 189-208.

[16]. Satyanarayana, M. On semigroups admitting ring structure. **Semigroup Forum** 3(1971): 43-50.

[17]. Satyanarayana, M. On semigroups admitting ring structure II. **Semigroup Forum** 6(1973): 189-197.

[18]. Satyanarayana, M. On 0-simple semigroups admitting ring structure. **Semigroup Forum** 19(1980): 307-312.

VITA

Mr. Manoj Siripitukdet was born on July 21, 1960 in Phitsanulok. He got a Bachelor of Science in 1982 from Srinakharinwirot University in Phitsanulok. In 1988, he got a Master of Science at Chulalongkorn University. He started working as an instructor at the Department of Mathematics, Faculty of Science, Naresuan University, Phitsanulok in 1994. For his Ph.D. program in mathematics, he got a UDC scholarship to study at Chulalongkorn University in 1997. He was sponsored by this scholarship for three years. He got married in 1991 and now he has two daughters.